

Lecture Notes on Data Engineering
and Communications Technologies 73

Kavita Khanna
Vania Vieira Estrela
Joel José Puga Coelho Rodrigues *Editors*



Cyber Security and Digital Forensics

Proceedings of ICCSDF 2021



Springer

Lecture Notes on Data Engineering and Communications Technologies

Volume 73

Series Editor

Fatos Xhafa, Technical University of Catalonia, Barcelona, Spain

The aim of the book series is to present cutting edge engineering approaches to data technologies and communications. It will publish latest advances on the engineering task of building and deploying distributed, scalable and reliable data infrastructures and communication systems.

The series will have a prominent applied focus on data technologies and communications with aim to promote the bridging from fundamental research on data science and networking to data engineering and communications that lead to industry products, business knowledge and standardisation.

Indexed by SCOPUS, INSPEC, EI Compendex.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at <http://www.springer.com/series/15362>

Kavita Khanna · Vania Vieira Estrela ·
Joel José Puga Coelho Rodrigues
Editors

Cyber Security and Digital Forensics

Proceedings of ICCSDF 2021

Editors

Kavita Khanna
The NorthCap University
Gurugram, India

Joel José Puga Coelho Rodrigues
Federal University of Piauí (UFPI)
Teresina-PI, Brazil

Instituto de Telecomunicações
Aveiro, Portugal

Vania Vieira Estrela 
Telecommunications Department
Federal Fluminense University (UFF)
Duque de Caxias, Rio de Janeiro, Brazil

ISSN 2367-4512

ISSN 2367-4520 (electronic)

Lecture Notes on Data Engineering and Communications Technologies

ISBN 978-981-16-3960-9

ISBN 978-981-16-3961-6 (eBook)

<https://doi.org/10.1007/978-981-16-3961-6>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.

The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

International Conference on Cyber Security and Digital Forensics (ICCSDF 2021) was held on April 3–4, 2021, at the NorthCap University, Gurugram, India. The conference was organized with the aim to bring together the leading academic scientists, researchers, industrialists to exchange and share their experiences and research results in all aspects of cybersecurity and digital forensics. This international conference was conceived after analyzing the increase in the prevalence of cybercrime attacks on business organizations, government infrastructures, and individuals. With this conference, we encouraged the community of multinational researchers to showcase the research work done in their field of cybersecurity. The conference provided an opportunity to researchers on an international forum to learn about the latest developments through scientific information interchange in the field of cybersecurity and digital forensics. The topics were categorized into four tracks, namely cryptology and its applications, cyber and digital forensics, network and mobile security, blockchain, and software technologies. We received a total of 205 submissions; each submission was anonymously reviewed by three reviewers. After extensive reviews and shepherding, 50 papers were accepted, and this proceeding contains revised versions of all accepted papers.

In addition to the presentations of the accepted papers, the occasion was graced by the presence of Honorable Chief Guest **Dr. Gulshan Rai**, *Former National Cyber Security Coordinator, at the Prime Minister Office, Government of India*, and four keynote speakers, namely **Prof. (Dr.) Gregory Conti**—*Co-founder and Principal at Kopidion, New York, USA*, **Ms. Vandana Verma**—*Security Solutions Architect at IBM India Software Labs and Member of the OWASP Global Board of Directors*, **Mr. Shree Parthasarathy**—*Leader South Asia Cyber and Strategy Services, APAC Cyber-Innovation, Deloitte*, and **Mr. Santosh Khadsare**—*Cyber Forensics Expert, Government of India*. The conference featured respective keynote talks, namely “The current and future state of Cybersecurity: Deflecting the Trajectory,” “Careers in AppSec: Lead with Grit,” “Digital Forensics,” and “Digital Era and its impacts”.

A number of people contributed to the success of ICCSDF 2021. The organizers are truly grateful to all the committee members for smoothly completing their assigned responsibilities and also thankful to the external reviewers for assisting in the reviewing process and their in-depth discussions. We must mention that the selection of the papers was an extremely challenging task. We would like to thank everyone who contributed directly or indirectly in making this conference a success and ensured its smooth running. The Conference was organized and facilitated by **Dr. Mehak Khurana** as Convener and **Dr. Pooja Sapra** as Co-Convener.

The support of technical partners, Open Web Application Software Project (OWASP), Spoken Tutorial, Infosecgirls, Women In Application (WIA), Computer Society of India (CSI), The Institution of Engineers (India) IEI is also appreciatively acknowledged. As per standard, editor's names and their locations (city and country) have been inserted in Preface. Please check and amend if necessary.

Gurugram, India
Duque de Caxias, Brazil
Teresina, Brazil

Kavita Khanna
Vania Vieira Estrela
Joel José Puga Coelho Rodrigues

Contents

Section–A

A Systematic Approach for Analyzing Log Files Based on String Matching Regular Expressions	3
Keshav Kaushik, Gargeya Sharma, Gaurav Goyal, Asmit Kumar Sharma, and Ashish Chaubey	
An Efficient Detection and Prevention Approach of Unknown Malicious Attack: A Novel Honeypot Approach	11
Aatif Sarfaraz, Atul Jha, Avijit Mondal, and Radha Tamal Goswami	
Analysis of Risk and Security Within Fog Computing-Enabled e-Healthcare System in Uttarakhand	21
Naveen Tewari and Sandeep Kumar Budhani	
Android Malware Detection Using Extreme Learning Machine Optimized with Swarm Intelligence	31
Rahul Gupta, Aviral Agarwal, Devansh Dua, and Ankit Yadav	
Asymmetric Image Cryptosystem Based on Chaotic Zone Plate Phase Mask and Arnold Transform	45
Mehak Khurana and Hukum Singh	
Authentication of Digital Media Using Reversible Watermarking	53
Geeta Sharma, Vinay Kumar, and Kavita Chaudhary	
Automatic Test Case Generation and Fault-Tolerant Framework Based on N-version and Recovery Block Mechanism	65
Seema Rani and Amandeep Kaur	
Chatbot to Map Medical Prognosis and Symptoms Using Machine Learning	75
Himani Aggarwal, Saniya Kapur, Varun Bahuguna, Preeti Nagrath, and Rachna Jain	

Cloud Security: The Future of Data Storage	87
Parv Bajaj, Ritika Arora, Mehak Khurana, and Shilpa Mahajan	
Curbing Criminal Acts on Mobile Phone Network	99
Olasina Jamiu Rotimi, Sanjay Misra, Akshat Agrawal, Ezenwoke Azubuike, Rytis Maskeliunas, and Robertas Damasevicius	
Designing of Fuzzy Logic-Based Intrusion Detection System (FIDS) for Detection of Blackhole Attack in AODV for MANETs	113
Ruchi Makani and B. V. R. Reddy	
Detection of Phishing Websites Using Classification Algorithms	129
Sumathi Ganesan	
IoT-Based Smart Security System for Agriculture Fields	143
Sukhwinder Sharma, Puneet Mittal, and Anuradha	
Efficient Clustering of Transactional Data for Privacy-Preserving Data Publishing	153
Vartika Puri, Parmeet Kaur, and Shelly Sachdeva	
Passive Video Forgery Detection Techniques to Detect Copy Move Tampering Through Feature Comparison and RANSAC	161
Jatin Patel and Dr. Ravi Sheth	
Evaluation and Performance Analysis of Apache Pulsar and NATS	179
Vanita Jain, Aarush Ahuja, and Dharmender Saini	
Problems of Providing Access to a Geographic Information System Processing Data of Different Degrees of Secrecy	191
Vitaly Gryzunov and Darina Gryzunova	
Security Augmented Symmetric Optical Image Cryptosystem Based on Hybrid Transform Employing Rear Mounted Technique Using Three Different Complex Masks	199
Priyanka Maan, Hukum Singh, and A. Charan Kumari	
Security Considerations in the Design of IEEE 802.15.4 Transceiver: A Review	213
K. Vivek Raj, P. Dinesha, and S. I. Arpitha Shankar	
An Enhanced Security Framework for Robotic Process Automation	231
K. Murugappan and T. Sree Kala	
Analysis of the Trust and Resilience of Consumer and Industrial Internet of Things (IoT) Systems in the Indian Context	239
Akaash R. Parthasarathy	
A Comprehensive Study on Vulnerabilities and Attacks in Multicast Routing Over Mobile Ad hoc Network	253
Bhawna Sharma and Rohit Vaid	

An Offensive Approach for Hiding Malicious Payloads in an Image	265
Keshav Kaushik and Sneha Surana	
A Review of Anti-phishing Techniques and its Shortcomings	273
Bhawna Sharma and Parvinder Singh	
Assessment of Open Source Tools and Techniques for Network Security	289
U. Guru Prasad, R. Girija, R. Vedhapriyavadhana, and S. L. Jayalakshmi	
A Detailed Comparative Study and Performance Analysis of Standard Cryptographic Algorithms	301
Chetan Rathod and Atul Gonsai	
Secured Communication Using Virtual Private Network (VPN)	309
Paul Joan Ezra, Sanjay Misra, Akshat Agrawal, Jonathan Oluranti, Rytis Maskeliunas, and Robertas Damasevicius	
Survey for Detection and Analysis of Android Malware(s) Through Artificial Intelligence Techniques	321
Sandeep Sharma, Kavita Khanna, and Prachi Ahlawat	
Section–B	
A Blockchain-Based Secure Car Hiring System	341
Sonakshi and Seema Verma	
A Correlation Blockchain Matrix Factorization to Enhance the Disease Prediction Accuracy and Security in IoT Medical Data	351
P. Renuka and B. Booba	
A Self-Sovereign Identity Management System Using Blockchain	371
Tripti Rathee and Parvinder Singh	
Blockchain and IoT for Auto Leak Unearthing	381
Pooja Sapra, Vaishali Kalra, and Simran Sejwal	
Coin Drop—A Decentralised Exchange Platform	391
Vanita Jain, Akanshu Raj, Abhishek Tanwar, Mridul Khurana, and Achin Jain	
Smart Contracts and NFTs: Non-Fungible Tokens as a Core Component of Blockchain to Be Used as Collectibles	401
Akash Arora, Kanisk, and Shailender Kumar	
Blockchain in Health Care: A Review	423
Sanya Bindlish, Sargam Chhabra, Kshitij Mehta, and Pooja Sapra	

Section–C

A Comparative Study of the Energy-Efficient Advanced LEACH (ADV-LEACH1) Clustering Protocols in Heterogeneous and Homogeneous Wireless Sensor Networks	433
Nitin Kumar, Vinod Kumar, and Pawan Kumar Verma	
Cognition of Driver Drowsiness to Inculcate Predictive Analysis	445
Abra Shafiq Siddiqi, Md. Afshar Alam, Sherin Zafar, Samia Khan, and Nida Iftekhhar	
Correlation Between K-means Clustering and Topic Modeling Methods on Twitter Datasets	459
Poonam Vijay Tijare and Jhansi Rani Prathuri	
Design and Analysis of 2 × 4 Microstrip Patch Antenna Array with Defected Ground Structure for 5G Mobile Communication	479
Sameena Zafar, Vineeta Saxena, and R. K. Baghel	
Efficiency Analyzing on Vehicle Tracking Systems	487
L. Rahunathan, D. Harish, A. Antony Samson, and D. Sivabalaselvamani	
Evaluation and Transformation Analysis of the Mithi River	501
Saumya Deshmukh, Shrishti Karkera, Prachi Rawale, and Chhaya Narvekar	
Human-Sensing Technologies for Business Solutions	513
Rajeev Tiwari, Kamal Kumar, Satyam Kumar, and Shelly	
Identification and Minimization of Churn Rate Through Analysing Financial Routines Using Machine Learning	523
Rahul Pahuja, Niket Dheeryan, Lovish Sethi, Preeti Nagrath, and Rachna Jain	
Machine Learning-Based Predictive Analysis to Abet Climatic Change Preparedness	541
Abra Shafiq Siddiqi, Md. Afshar Alam, Deepa Mehta, and Sherin Zafar	
Deep Learning Approaches for Anomaly and Intrusion Detection in Computer Network: A Review	551
Khushnaseeb Roshan and Aasim Zafar	
Forest Cover Change Detection Using Satellite Images	565
Achal Kalwar, Rohan Mathur, Shubham Chavan, and Chhaya Narvekar	
FPGA-Based Design Architecture for Fast LWE Fully Homomorphic Encryption	575
Sagarika Behera and Jhansi Rani Prathuri	

Hierarchical Communication Architecture for Multi-level Energy Harvesting Support in Underwater Sensor Network	585
Anuradha, Amit Kumar Bindal, Devendra Prasad, and Afshan Hassan	
Review of Evolutionary Algorithms for Energy Efficient and Secure Wireless Sensor Networks	597
Rajiv Yadav, S. Indu, and Daya Gupta	
Utilization and Energy Consumption Optimization for Cloud Computing Environment	609
Rajeev Tiwari, Roohi Sille, Nilima Salankar, and Pardeep Singh	
Author Index	621

About the Editors

Prof. Kavita Khanna has done M.Tech. Computer Engineering, MDU, Rohtak, and Ph.D. in Computer Graphics and Soft Computing Techniques, GGSIPU, Delhi. With 21 years of teaching, administration, and research experience, currently she is associated with The NorthCap University, Gurugram, as Professor and Head of the Department (CSE Department). Her interests include artificial neural networks, computer graphics, cryptographic techniques, artificial intelligence: metaheuristic techniques, neural networks, machine learning, and analysis and design of algorithms. She has more than 60 publications in reputed journals, conferences, and chapters. She has guided many M.Tech. and Ph.D. students. Prof. Khanna is receiving a research grant from the Department of Science and Technology (DST), India, and NTRO for research projects. She has also organized various conferences, workshops, FDPs and has been Reviewer, Session Chair, and Committee Member of conferences and journals.

Vania Vieira Estrela B.S. degree from Federal University of Rio de Janeiro (UFRJ) in Electrical and Computer Engineering (ECE); M.Sc. from the Technological Institute of Aeronautics (ITA), Brazil; M.Sc. degree in ECE at Northwestern University, USA; and Ph.D. in ECE from the Illinois Institute of Technology (IIT), Chicago, IL, USA. Taught at DePaul University, USA, and Universidade Estadual do Norte Fluminense (UENF), Brazil. She was visiting professor at the Polytechnic Institute of Rio de Janeiro (IPRJ)/State University of Rio de Janeiro (UERJ) in Brazil and currently working at UFF's Department of Telecommunications. Research interests include signal/image/video processing, inverse problems, computational & mathematical modeling, stochastic models, multimedia, communications, motion estimation, machine learning, and geoprocessing. She reviews several journal/magazine articles, and she is deputy editor of the Neuroscience Informatics journal (Elsevier). She is engaged in technology transfer, STEAM education, environmental issues, and digital inclusion. Editor of several books and special issues. Member of IEEE and ACM.

Joel José Puga Coelho Rodrigues [Fellow, AAIA and IEEE] is a professor at the Federal University of Piauí, Brazil; and senior researcher at the *Instituto de Telecomunicações*, Portugal. Prof. Rodrigues is the leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), an IEEE Distinguished Lecturer, Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis—Covilhã Science and Technology Park. He was Director for Conference Development—IEEE ComSoc Board of Governors, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee (TC) on eHealth and the TC on Communications Software, a Steering Committee member of the IEEE Life Sciences Technical Community and Publications co-Chair. He is the editor-in-chief of the International Journal of E-Health and Medical Communications and editorial board member of several high-reputed journals (mainly, from IEEE). He has been general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He has authored or coauthored about 1000 papers in refereed international journals and conferences, 3 books, 2 patents, and 1 ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. Prof. Rodrigues is a member of the Internet Society, a senior member ACM, and Fellow of AAIA and IEEE.

Section–A

A Systematic Approach for Analyzing Log Files Based on String Matching Regular Expressions



Keshav Kaushik, Gargeya Sharma, Gaurav Goyal,
Asmit Kumar Sharma, and Ashish Chaubey

Abstract In the past few years, there has been a tremendous increase in cyberattacks and cybercrimes. Technology is changing at a very fast pace, thus inviting more advanced cyberattacks. Any event that is triggered on the system is recorded in the form of logs in log files. It may be any warning, any alert, and information, and all the things get stored in the logs. Therefore, from the security point of view, analyzing the logs plays a crucial role in the forensic investigation or for analytics purposes also. This paper highlights a systematic approach for analyzing the log files using a string-matching algorithm and regular expressions. Thus, it helps in log analysis, management, and analytics for future reference. Analyzing logs in a systematic way is always crucial in digital forensics, and it will help in the smooth conduction of forensic investigations.

Keywords Log analysis · String matching · Regular expressions · Cyberattacks

1 Introduction

We live in a world where data surrounds us in every direction. Where there is technology, some amount of data is always involved. One of the many data sources that accumulate around us is in the form of log files. These log files are automatically produced files that contain the record of events from various software and operating systems. According to statistics, an average enterprise accumulates up to 4 GB of log data a day from all their servers and other network devices. Over 95% of that data within those log files are the entries that record every successful/unsuccessful event or transaction taking place in those systems. For example, it can be a server crash, user logins, logouts, applications start-up and shutdown, file access, etc. These log files are unnoticed by many people working under that enterprise because their production is a regular process and relatively holds less priority and attention than other tasks. However, it is the active and complete

K. Kaushik (✉) · G. Sharma · G. Goyal · A. K. Sharma · A. Chaubey
University of Petroleum and Energy Studies, Dehradun, India

analysis of these log data that creates the differences among organizations, how they handle failures, changes to adapt by looking at the behavior of daily analysis periodically, etc. So, underestimating these data files is not advised for the smarter functioning of any organization and its client interactions.

This paper focuses on the same fundamental of not ignoring these log files and analyzing them in a much faster and easier way by the owners of these log files. Data analysis is getting more popular in the current few years than it has ever been. Since, we are achieving some invaluable information using analysis on the unstructured data present around us with the help of big data analytics, machine learning, and other scientific techniques. Analyzing logs is also a part of them. They contain some very intuitive information about the users, services, machines, their patterns, and various relationships between them, which can help us formulate techniques to take advantage of such information and provide more personal and better services. In addition to better services, this also mitigates a large amount of risk involved in the process. With predictive and descriptive analysis, organizations can build a more secure and effective network, which in turn prevents losses and increases their overall profits. Due to its increased popularity and attention, log analysis has spread its role in various directions. For example, correlational analysis: This is where you find the correlation between data that is not visible in a single log, especially since multiple logs are relevant over a single incident. For instance, if an attack is experienced, then you can perform correlation analysis using logs generated by servers, firewall, network devices, and other possible sources involved and find those logs that are relevant to that particular attack. During such conditions, log files play an important role as a piece of evidence as their analysis helps to find the cause and suspect of the attack.

There are other useful use cases as well with log analysis, one of which is anomaly detection. Through this, we can overlook the usual less important logs and only focus on unusual and unique log entries for further investigation. This paper focused on achieving anomaly detection on IPs through their number of occurrences either overall or in a particular period. Other than just detection of any existing anomalies, the feature to block such IP addresses if the user wishes to be also included, while adding all the blocked IPs in a separate file to maintain for reporting or future references. All the functionalities are further discussed in detail in the working methodology section. This paper fulfills the intention of providing enterprises and organizations with a tool that will help reduce the extensive searching and crawling through the entire log files related to the required situation and makes the process easier for further investigation and analysis. The implementation for this paper worked on a command-line interface and built using C language on top of the Linux operating system. With this, many users can be covered in the industry, as most of the servers out there are Linux kernel-based, contributing toward speeding the process of analyzing logs for various use cases.

2 Related Work

The extensive quantity of research proposing different technologies that can be used for analysis is increasing every year. Among them, many are focusing on the automated systems for the analysis of log files. Pinjia He in [1] reveals his dataset “log hub” that contains 17 datasets including stand-alone software, web server, mobile, and operating systems logs. These can be used for AI-powered log analytics which focuses on anomaly detection. It is an approach for log analysis in combination with machine learning. In this, regularly generated usual logs are ignored, and the unique or different ones in the log files are recognized as anomalies and treated as potential threats, respective to how the model was trained earlier. Zengchao NI and Honqui Liu in [2] discussed the idea of dealing with massive web system logs by extracting log templates based on the label recognition method effectively solving the problem of insufficient log format. Effective log monitoring allows us to do behavioral analysis. Xiaojian Liu and Yi Zhu in [3] talk about generating valued genealogy information that helps in generating attributes for specialized profiles. Specialized profiles lead to personalized recommendations, and thus biased monitoring and blocking of users are attained. Analyzing the data stored in logs of web search services provides a great view of the information searching tactics of the user. This can help in developing information systems, design, interface development, and information architecture construction for content collection. Robust learning of web search logs is quite important. Laura M. Koesten in [4] describes the drawback of web search engines in finding the most relevant datasets that meet the user’s query. They suggested the first query analysis for dataset search containing logs of four open data portals. Logs from that reveal that queries stated on the data portal are quite different from those issued to web search engines in their length and structure, which finally draws the result that portals are used explorative rather than answer focused questions. Nevertheless, the exploration does not stop here as researchers are using log datasets to find anomalies in the system. Traditionally, anomalies are detected by using keyword search and regular expression match that is the root idea of our project. In modern times, many machine learning-based detection mechanisms have been proposed as discussed in [1]. Qimin Cao and Yinrong Qiao in [5] carry the above-stated idea by implementing a two-level machine learning algorithm and using a decision tree model to classify between normal and anomalous datasets, thus adding future inspiration for our work.

3 Working Methodology

The log file of any server consists of multiple records, and each record takes up one row in the log file. These log files could be in terabytes or more, thus it becomes very difficult to filter out required data. Each row of a log file could contain multiple

columns, for example, the log file of a web server contains, source IP address, date, time, time zone, status code, response code, etc. These columns depend on a server that generates them. Thus, we often require a tool that can filter out required data whenever needed. Our project aims to create a tool that can filter the log files based on the requirement. As soon as the tool is executed, it displays a menu to the user that lists all the features provided by the tool. While writing the code, we kept the basic requirements in mind.

This tool provides five features to deal with logs as of now. These features are as follows:

- I Convert the log file into CSV format.
- II Search for a particular keyword in the log file.
- III Block and unblock any IP address from the server.
- IV Visualize the log files.
- V Filter the logs in a particular time frame (Fig. 1).

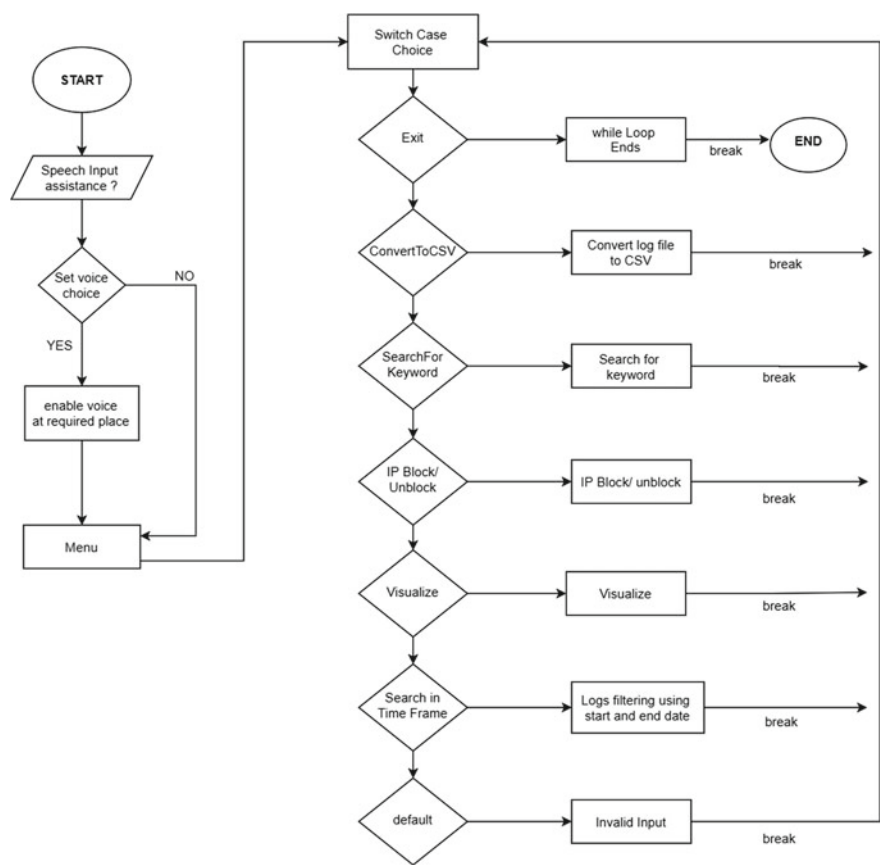


Fig. 1 Flow diagram explaining the working methodology

3.1 Converting the Log File into CSV Format

Log files could be very difficult to read most of the time, and this is why we need to convert them into such a format so that further processing can be done with ease. We wrote the code to convert the log file into comma-separated values (CSV) format. Nevertheless, why did we choose the CSV format specifically? Performing data cleaning, data processing, and data analysis can be done easily on a CSV file. We used Linux utilities like “sed”, “awk”, and regular expressions to convert the log [6] file into CSV format. We used “awk” to separate fields of a log file and write the output into a separate file. Then we used “sed” to remove unwanted special characters and separate different columns with a comma (“,”).

3.2 Search for a Particular Keyword in the Log File

Sometimes or the other, we might run into a situation where we want to search a pattern or keyword in a log file [7]. We implemented this feature using a basic pattern-matching algorithm. We used the “strstr()” method from the “string.h” header file of the C programming language. This algorithm has the quadratic worst case time complexity with respect to the searched time. Through the median of this tool, we are providing five options to search for a keyword. The user can search for either an IP address, date, HTTP method, status code, response code, or other. These options are specifically provided to deal with the web server logs, though this can be tweaked accordingly.

3.3 Block and Unblock an IP Address

This is a vital feature of any log analysis tool. While dealing with logs, we might need to blacklist certain IP addresses belonging to various users trying to access the server. To block and unblock the IP address, we use the “firewall-cmd” command-line tool to do the same. The program initially creates a new file “block.txt” which will store all the blocked user’s IP addresses. We take the IP addresses to be blocked or unblocked from the user.

- **Command to block the IP**

```
“firewall-cmd --permanent --add-rich-rule=rule family='ipv4' source address={input IP here} reject”
```

- **Command to unblock the IP**

```
“firewall-cmd --permanent --remove-rich-rule=rule family='ipv4' source address={input IP here} reject”
```


The input IP address is concatenated within the command. The command is then executed to block/unblock the file. However, this is not it; we will be maintaining the list of blocked IP addresses (block.txt) so that our tool is unambiguous. Before blocking the IP address, the “block.txt” is traversed and if the IP address, is already blocked, then it will prompt an alert to the user. Similarly, while unblocking the IP address, it should be present in the “block.txt”, only then it will be unblocked.

3.4 Visualizing Log Files

The detailed working of this feature will be explained in the next section. In short, we will take a list of IP addresses from the user as input and then plot a graph that will represent the number of occurrences of an IP address in the log file. This representation is not limited to occurrences of IP addresses only; it can also be used to visualize the number of requests in a day that were made to the server.

3.5 Search for Logs in a Time Frame

This feature provides an option to search for logs [8] in a particular period (e.g., we can filter out logs that were recorded between January 1, 2021, to January 5, 2021). Both beginning and end dates were taken from the user. To print the output, we traverse the log file line by line. If the beginning date is found in any line, then the “flag” variable is set to “true”. Then if the “flag” variable is set to “false”, the end date is found in any line. Within each iteration, we print out the corresponding line if the “flag” is set to “true”. This will print out logs from the beginning date to the end date (exclusive). Now we have to print only those records of the end date. This can be easily done by traversing the log file and print only those records that contain the end date. Pattern matching is again the core algorithm for this feature.

4 Results and Discussion

After the experimentation for further convenience and better understanding, we visualized the final output in the form of a bar graph. As mentioned above, we provided functionality in our tool for visualizing IP addresses (refer to Sect. 3.4). We know that visualizing statistics [9] in a proper way provides additional intuition for a better understanding of the data, which often leads to a better examination of that same data. The below-represented bar graph depicts the visualization of the number of occurrences of different IP addresses required by the user in the required time frame in order to examine if any one of them shows abnormal behavior or in simple words shows a huge increase in its occurrences which could be directing

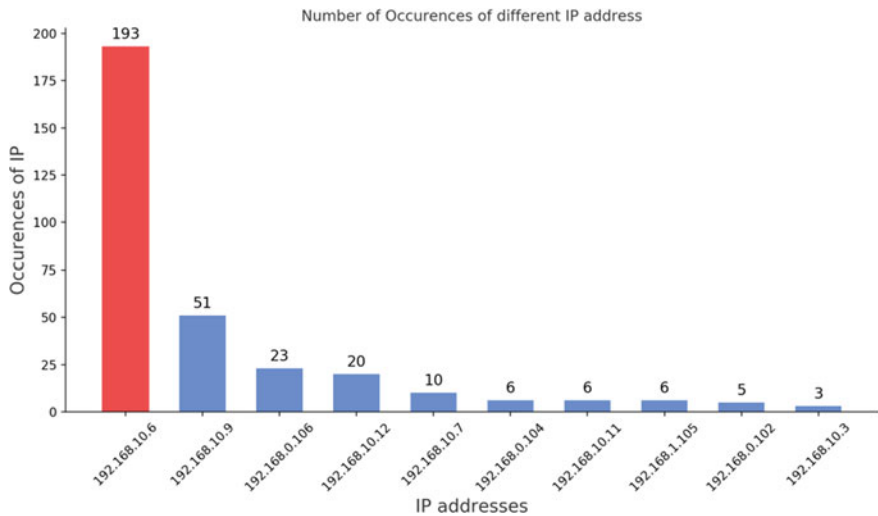


Fig. 2 Occurrences of IP addresses in the log file

toward some kind of malicious behavior or signs of malicious activity taking place. In Fig. 2, we can see that the first IP address (192.168.10.6) that is selected by the user within the selected time frame occurred the most (193 times to be precise) which is undoubtedly a high number for any IP address. This is also the case, due to the current threshold being set at a limit of 100 occurrences within a period, which implies that there is some issue or unethical activity is being performed. (Note: The threshold can be changed/set according to the requirements of the user). In Fig. 3, two pie plots are presented, one of the left represents the visualization over the comparison of occurrences of the different types of requests that were in the dataset,



Fig. 3 Distribution of various parameters (request type and status codes) in the log file

i.e., if the request was a GET or a POST request. The other plot on the right represents occurrences [10] of the number of requests that were associated with different status codes as the result of that request.

5 Conclusion

As we all know the importance of logs in event correlation and event reconstructions in cybercrime investigation, this article focuses on analyzing the logs in a systematic way with the help of a string-matching algorithm and regular expressions. The authors observed the visualization of log files, searching of logs, and finding the occurrences of IP addresses. The approach discussed in this paper can be further extended in various aspects like analyzing the logs in real time, deploying them using Docker containers, etc. The authors will extend the work in the near future and would like to explore the various possible dimensions of analyzing the logs.

References

1. He, S., Zhu, J., He, P., Lyu, M.R.: Experience report: system log analysis for anomaly detection. In: 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE), Ottawa, ON, pp. 207–218 (2016). <https://doi.org/10.1109/ISSRE.2016.21>
2. Ni, Z., Liu, H., Chen, Y., Wu, D.: Research and implementation of a method for web log analysis template extraction. *Procedia Comput. Sci.* **162**, 673–681 (2019). ISSN: 1877-0509
3. Liu, X., Zhu, Y., Ji, S.: Web log analysis in genealogy system. In: 2020 IEEE International Conference on Knowledge Graph (ICKG), Nanjing, China, pp. 536–543 (2020). <https://doi.org/10.1109/ICKG50248.2020.00081>
4. Kacprzak, E., Koesten, L., Ibáñez, L., Simperl, E., Tennison, J.: A query log analysis of dataset search. In: *Lecture Notes in Computer Science*, pp. 429–436 (2017). https://doi.org/10.1007/978-3-319-60131-1_29
5. Cao, Q., Qiao, Y., Lyu, Z.: Machine learning to detect anomalies in web log analysis. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, pp. 519–523 (2017). <https://doi.org/10.1109/CompComm.2017.8322600>
6. Best Practices: Event Log Management for Security and Compliance (2021). <https://www.whatsupgold.com/resources/best-practices/event-log-management>
7. Jansen, B.: The methodology of search log analysis. In: *Handbook of Research on Web Log Analysis*, pp. 100–123 (2009). <https://doi.org/10.4018/978-1-59904-974-8.ch006>
8. Sultana, N., Paira, S., Chandra, S., Alam, S.: A brief study and analysis of different searching algorithms. In: 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT) (2017). <https://doi.org/10.1109/icecct.2017.8117821>
9. IBM Knowledge Center.: *Ibm.com* (2021). https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzasp/rzasp_regularexpression.html
10. Lu, X.: The analysis of KMP algorithm and its optimization. *J. Phys. Conf. Ser.* **1345**, 042005 (2019). <https://doi.org/10.1088/1742-6596/1345/4/042005>

An Efficient Detection and Prevention Approach of Unknown Malicious Attack: A Novel Honeypot Approach



Aatif Sarfaraz, Atul Jha, Avijit Mondal, and Radha Tamal Goswami

Abstract In this modern era, security has gotten to be the foremost broadly concerned in each domain as recently approaching malware postures a danger to the systems. So our fundamental concern is to identify and anticipate a malware assault on the system. As the polymorphic worm postures, an enormous challenge to identify as they have more than one occurrence and exceptionally expansive endeavors is required to detain every occurrence and to generate signatures. This work proposes malicious attack detection and prevention using honeypot technology. We have proposed a double-honeynet framework, which can distinguish and avoid modern worms. We apply system call analysis to detect malware which mostly focuses on the polymorphic and metamorphic virus rather than utilizing a signature-based approach.

Keywords Polymorphic worm · Honeypot · Double honeypot · Sticky honeypot · System call analysis

1 Introduction

Nowadays, malicious attacks became the biggest threat to network security. Malicious attacks include viruses, worms and trojans. In each of these attacks, some codes are written called malicious code or malware. Malware could be a sort of computer program outlined to require over or harm a computer's working framework without the client's information or endorsement. Worms are being the major

A. Sarfaraz (✉) · A. Jha

Department of Computer Science, Techno International Batanagar, Kolkata, India

A. Mondal

Makaut, Kolkata, India

e-mail: avijit.mondal@tib.edu.in

R. T. Goswami

Techno International New Town, Kolkata, West Bengal, India

e-mail: rtgoswami@tict.edu.in

threat among all malicious attacks, because of their self-replicating nature [1]. It is capable of copying itself and sending it over the network to the computers on the network without any human interaction. Unlike viruses, worms did not need to attach themselves to any program in order to propagate. As there is a particular behavior, blocking software program is there which coordinates with the working framework and monitors the program behavior in genuine time for malicious activities. With the evolution of network security tools and techniques, malware is getting to be more intelligent each day, and polymorphic malware is the most recent participants in this calamitous amusement of overcoming the adversary. Polymorphic worm being one of the latest and effective among all [2]. A polymorphic worm changes its appearance with every occurrence [3] such that each occurrence of which receives a totally distinctive personality from its parent, which makes it difficult to get detected.

Network intrusion detection system (NIDS) must be established in order to protect the network from malware, and it acts as an alarm that notifies the network admin every time malware is detected. IDSs basically are of two types: host-based and network-based. Host-based IDSs inspect data held on discrete computers in the network which serves as a host, whereas network-based IDSs inspect data interchanged between computers.

Security specialists physically create the IDS signature by studying the network traces after the modern worm has been discharged. Tragically, this work takes a parcel of time. Analysts have, as of late, given consideration to computerizing the era of marks for IDS to coordinate worm activity.

Our research is based on the honeypot technique which provides a solution for the above-mentioned problem. A honeypot may be a trap that mimics an authentic network resources, a self-contained secure and monitored area [4, 5]. Its essential objective is to bait and detect malicious attacks and intrusions. It can be used for surveillance and early warning; it can also benefit security researchers to understand emerging threats. Honeypots can be categorized as high and low interaction honeypot [6]. A high interaction honeypot like honeynet works as a real operating system, whereas a low interaction honeypot like honeyd imitates one or more than one real system.

Our research proposes a double-honeynet architecture which gathers all possible instances of the polymorphic worm and sends them for signature generation. In our research, we have used system call analysis approach instead of signature-based approach for the detection of the polymorphic worm inside the signature generator. Our system makes it possible to gather all the instances of the polymorphic worm and then forward those instances to the signature generator which then generates the signature.

This paper is divided into the following segments. Segments 1.1 and 1.2 give a brief idea about worms and polymorphic worms. Segment 2 reviews the associated work for the automatic signature generation framework. Segment 3 presents our proposed framework to describe the problem encountered by the current automatic signature generator. The signature generator algorithm for polymorphic and metamorphic virus using system call analysis will be discussed in Segment 4. The

algorithm for our proposed architecture is discussed in Segment 5. Segment 6 concludes the paper, and in Segment 7 we will discuss some future work that we intend to perform in the future.

1.1 Worms

“A worm is a self-reproducing program that can be created with the capabilities to perform any kind of task,” for example, deletion of files or sends documents via e-mail. There can be an adverse effect on network traffic due to the worm self-replicating property:

A worm:

- (a) may install a pathway also called a backdoor for unprotected access by the attacker in the infected system.
- (b) vulnerability introduces the worm into the system.
- (c) may infect one system and by the property of self-replication, it can spread all over the system network.

1.2 Polymorphic Viruses

Polymorphic infections assume numerous forms by scrambling code in an unexpected way with every infection. This term caught in within the mid-1990s with devices that risen to produce thousands of modern slight variations of code based on transformed routines to subvert-signature innovation utilized by an anti-virus computer program.

A polymorphic infection incorporates an encrypted infection body and a decryption routine, to begin with controlling the computer and later decodes the infection body [7].

However, a polymorphic infection moreover includes a mutation engine that produces randomized decryption routines that alter each time an infection infects an unused program. The mutation engine and virus body were both encrypted in a polymorphic infection.

As soon as the users run an infected program, following activities will take place:

- The framework is beneath the control of the decryption routine that can decode both the infection body and the mutation engine [8].
- Next, the control has been shifted from the system to the virus through the decryption routine which finds a new program to infect.
- Next the infection replicates itself along with the mutation engine in RAM.

- At this point, mutation engine gets invoked by the virus which then arbitrarily produces a new decryption routine that can decrypt the virus. However, it marks a very little or no likeness to any earlier decryption routine
- At this point, the current copy of the virus body and the mutation engine gets encrypted by the virus [9, 10].
- Ultimately, the virus adds the current encryption routine, together with the recently encrypted virus body and mutation engine, onto the latest program.

As a consequence of the above-mentioned process, the virus body is encrypted as well as virus decryption routine differs from malware to malware. With no predetermined signature to scan for and no predetermined decryption routine to malware, it cannot look the same.

2 Literature Review

Levin et al. [9] in his paper outlined the technique of how the honeypot pulls out the characteristics of worm exploits, which can be examined for signature generation. The drawback of his paper is that the signature for the worm exploit is detected manually, and this process of manual signature generation for the worm takes a lot of time which gives worms more time to propagate and infect other hosts in the network. Our paper uses double-honeynet architecture which overcomes the above-mentioned problem by consequently producing signatures for worms. Our framework reduces the time and effort required for signature generation.

Honeycomb was one of the first proposed frameworks for signature generation designed by Kreibich and Crowcroft [11]. Honeycomb can be implemented as a honeyd plugin, and it produces signatures from the detected activities at honeypot. The honeycomb system is based on the LCS algorithm, mainly focuses on the “longest-shared-byte” sequence between different sets of packets. To match almost all kinds of worm instances, a honeycomb generates a signature that comprises a single or contiguous substring of worm payload. In this paper, the major drawback is the signature which is generated by the honeycomb fails to capture all the instances of the polymorphic worm with low false negative and low false positive. Our paper uses double-honeynet architecture which is based on system call analysis that overcomes the above-mentioned drawback by capturing almost all instances of polymorphic worms. The system call analysis is used in our framework over the signature-based approach as it focuses mostly on polymorphic and metamorphic worms which help in capturing almost all kinds of polymorphic worm instances.

Goswami et al. [12] in their paper described how to automatically generate the signature for a polymorphic worm using double-honeynet framework which is built on the PCA, which uses the most noteworthy information shared between each and every polymorphic worm instances as the signature. The drawback of this framework is that it may not distinguish all the occasions of the polymorphic worm.

Singh et al. [13] in their paper outlined a system called the Earlybird system for the signature generation to identify worm. This architecture calculates packet content prevalence at a single observation point like a network demilitarized zone. The Earlybird system differentiates benign repetitions from outbound content, by counting the number of definite starting and endpoints related to the string that repeats frequently in the payload. Similar to honeycomb, Earlybird also generates a signature which comprises a single-contiguous substring of a payload to coordinate most of the worm occasions. In this paper, the major drawback is the signature which is generated by the Earlybird system fails to catch all the occurrences of the worm with low false negative and low false positive. This paper uses a system call analysis-based double honeynet framework which focuses more on polymorphic and metamorphic worms that overcomes the above-mentioned paper's drawbacks.

3 System Architecture

A polymorphic worm could be a sort of worm which can alter its appearance each time it propagates, so a polymorphic worm has numerous instances. After infecting every host, a new occurrence of polymorphic worm is produced for propagation. A single honeynet is capable of detecting only one instance of it. Therefore, we need a double-honeynet framework which will catch all the conceivable polymorphic worm instances. The proposed double-honeynet model establishes a loop that accumulates all polymorphic worm occurrences as shown in Fig. 1. For all of the above-mentioned reasons, we propose a double honeynet architecture for the detection of zero-day polymorphic worm automatically.

The process begins when the incoming traffic approaches the gate translator and passes through it. The gate translator then separates the suspicious incoming traffic and swerve them to honeynet 1. "The gate translator consists of publically attainable addresses, which represent wanted amenities." Traffics linked to any additional addresses, other than the publicly attainable addresses, were considered suspicious and are swerve to the honeynet 1 by gate translator.

In the next step, the unwanted suspicious traffic which arrived at honeynet 1 will strive to make an outbound connection. An internal translator that is implemented in the router and associated with each honeypot separates the honeypot from the entire network. All the outbound connections that are made from honeynet 1 will be obstructed by the internal translator and are swerve to honeynet 2. Honeynet 2 does the same forming a loop.

When adequate occurrences of worm payloads are accumulated by honeynet 1 and honeynet 2, then they are passed through a sticky honeypot which moderates down the worm proliferation rate so that it will be easy for the signature generator to generate signatures. Afterward, the signature generator generates signatures automatically by system call static analysis that will be discussed in the next section. All the malicious traffic will go through the system call analysis, and a corresponding signature will be generated. The generated signatures are forwarded

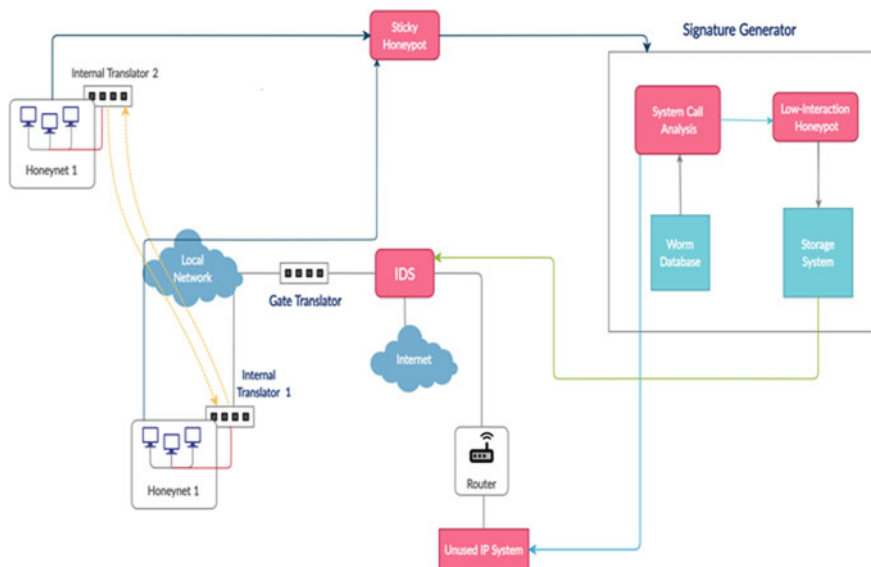


Fig. 1 System architecture

to the centralized storage system via a low interaction honeypot. Then the IDS can get all the information so that by analyzing it can protect against any attack. If the system call analysis is incapable of detecting any signature, then the payload will be automatically transferred to the unused IP system.

4 System Call Analysis

It is utilized to distinguish malware, generally focuses on the polymorphic and metamorphic infections. This strategy works based on the presumption that all malware variations share a common core signature—a combination of many highlights of the programming code [14]. In this technique, two fundamental steps were included: To start with, the portable executable (PE) decompressed and passed through a parser, this parser makes a list of Windows APIs calling grouping. Minute, this API grouping will be compared against the worm database, and a similarity measure was utilized to conclude the analyzed file [15]. In the event, if the similarity is more noteworthy than a certain limit, then at that point detection is triggered.

5 Proposed Algorithm

Step 1: The gate translator swerves the traffic coming from the Internet toward honeynet 1.

Step 2: Internal translator that is implemented in the router disconnects honeynet 1 from the entire network.

Step 3: All the outbound connection from honeynet 1 was obstructed by the internal translator and swerves them to honeynet 2. Honeynet 2 does the same forming a loop.

Step 4: When an adequate amount of worm instances are acquired by looping through honeynet 1 and honeynet 2, then they are swerved to the sticky honeypot to slow down the worm propagation rate.

Step 5: Sticky honeypot transfers the worm instances to the signature generator to generate their signatures.

Step 6: Signature generator consists of system call analysis, worm database, low interaction honeypot, and centralized storage system.

Step 7: In system call analysis, portable executable file is decompressed and passed through a parser which creates a list of windows API calling sequences.

Step 8: These API sequences will be compared against the worm database, if the similarity is greater than a certain threshold, then detection is triggered.

Step 9: All these worm signatures which are detected by system call analysis will be transferred to a centralized storage system through low interaction honeypot by which IDS can get all the payload information.

Step 10: In case, the system call analysis is incapable of detecting any signature, then that payload will be automatically redirected to the Internet through an unused IP system.

6 Conclusion

We have proposed an algorithm to generate the signature of newly emerged polymorphic worms automatically. In this paper, we have proposed a new detection technique “double honeynet” for the detection of newly emerged polymorphic or metamorphic worms. The Framework also includes a sticky honeypot which slows down the worm propagation rate. The system is based on the system call analysis that compares windows API sequences with the worm database; if the similarities are greater than a certain threshold, the detection is triggered.

7 Future Work

As honeypots are moderately a modern innovation and have a great scope for future applications, we plan to execute this proposed framework on an experimental test bed.

In the future, we intend to propose a new architecture which will be based on sandboxing. Using a sandboxing for modern malware discovery gives another layer of assurance against modern security threats—zero-day polymorphic worm. And whatever happens within the sandbox remains within the sandbox—avoiding system failures and keeping computer program vulnerabilities from spreading.

“A sandbox in a cybersecurity domain is a secluded environment on a network that imitates an end user working environment. Sandboxes are used to execute malicious code to analyze the results without having any adverse effect on the rest of the network. Sandbox environment gives a proactive layer for network security defense against threats.”

The key objective of our research is to lower the false alarm rates and to produce high-quality signatures for the polymorphic worm.

References

1. Spitzner, L.: *Honeypots: Tracking Hackers*. Addison Wesley Pearson Education, Boston (2002)
2. Tang, Y., Chen, S.: An automated signature-based approach against polymorphic internet worms. *IEEE Trans Parallel Distrib Syst* **18**(7), 879–892 (2007)
3. Cavallaro, L., Lanzi, A., Mayer, L., Monga, M.: LISABETH: automated content-based signature generator for zero-day polymorphic worms. In: *Proceedings of the Fourth International Workshop on Software Engineering for Secure Systems*, Leipzig, Germany, May 2008, Lissa (2008)
4. Mohammed, M.M.Z.E., Anthony Chan, H., Ventura, N.: HoneyCyber: automated signature generation for zero-day polymorphic worms. In: *Proceedings of the IEEE Military Communications Conference, MILCOM* (2008)
5. Fogla, P., Sharif, M., Perdisci, R., Kolesnikov, O., Lee, W.: Pol polymorphic blending attacks. In: *Proceedings of the 15th Conference on USENIX Security Symposium*, Vancouver, B.C., Canada (2006)
6. Li, Z., Sanghi, M., Chen, Y., Kao, M.Y., Chavez, B.: Hamsa: fast signature generation for zero-day polymorphic worms with provable attack resilience. In: *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May (2006)
7. Kim, H.-A., Karp, B.: Autograph: toward automated, distributed worm signature detection. In: *Proceedings of 13 USENIX Security Symposium*, San Diego, CA, Aug. (2004)
8. Kreibich, C., Crowcroft, J.: Honeycomb—creating intrusion detection signatures using honeypots. In: *Workshop on Hot Topics in Networks (Hotnets-II)*, Cambridge, Massachusetts, Nov. 2003 (2003)
9. Levine, J., La Bella, R., Owen, H., Contis, D., Culver, B.: The use of honeynets to detect exploited systems across large enterprise networks. In: *Proceedings of IEEE Workshops on Information Assurance*, New York, June 2003, pp. 92–99 (2003)
10. Gusfield, D.: *Algorithms on Strings, Trees and Sequences*. Cambridge University Press, Cambridge (1997)

11. Krebitch, C., Crowcroft, J.: Honeycomb: creating intrusion detection signatures using Honeypots. *ACM SIGCOMM Comput Commun Rev* **34**(1), 51–56 (2004)
12. Goswami, R. T., Mondal, A., Mishra, B. K., Mahanti, N. C.: *Handbook of Information Security*. John Wiley & Sons, Inc., Hoboken, New Jersey
13. Singh, S., Estan, C., Varghese, G., Savage, S.: <https://www.lastwatchdog.com/internets-40th-anniversary-timeline-milestones/>
14. <https://epdf.pub/official-isc2-guide-to-the-sscp-cbk-second-edition.html>
15. Salah, E.D., Aslan, H.K., El-Hadidi, M.T.: A detection scheme for the SK Virus. In: *Proceedings International Federation for Information Processing* (2002)

Analysis of Risk and Security Within Fog Computing-Enabled e-Healthcare System in Uttarakhand



Naveen Tewari and Sandeep Kumar Budhani

Abstract With the advent of fog computing, various e-governance services get influenced as fog provides new service delivery models and new ways to interact with the citizens. Uttarakhand, as a state of 86% hilly region and 65% of forest area, got geographical conditions that are not so favored for cloud-enabled technologies, because cloud needs regular and high bandwidth Internet connectivity. Fog computing can be a key player, in terms of providing e-Governance service. E-Health is the major service provided under the e-governance platform. With the application of Internet-enabled and IoT-based e-Healthcare systems in the state like Uttarakhand, there can be a drastic improvement in health services. E-Health services require real-time processing, low latency, high consistency, and high data rate, and these all parameters are fulfilled by fog computing. There are many kinds of research that describe how fog can be used in e-Healthcare systems. In this research paper, we discuss fog computing in the context of Uttarakhand. Our main concerns are security issues and challenges faced by fog computing while using the E-Healthcare system in hilly areas of Uttarakhand. In studying those challenges and security issues, the technologies related to fog computing are also discussed.

Keywords Fog computing • Internet of Things • Cloud computing • e-Health care • e-Governance

1 Introduction

Uttarakhand is a state of the Himalayan region that has very different geographical conditions than other states in India. Many services and applications use Internet of Things (IoT) today, due to a variety of sensor availability, low-cost Internet, and cloud services [1]. Technology like IoT and fog can be installed within the people's

N. Tewari (✉)

School of Computing, Graphic Era Hill University, Bhimtal, India

S. K. Budhani

Computer Sciences and Engineering, Graphic Era Hill University, Bhimtal, India

range and serve them with different offerings. One such important e-Governance service provided by fog computing is in e-Health care. It also raises the patient's life quality by providing real-time health data analysis [2].

IoT extends the services drastically that are traditionally given by Internet-based technology. With the advancement in sensors used in IoT, the data collection techniques raised their standards significantly. CISCO forecasts that the size of data accumulated by IoT devices may reach 600 zeta bytes per year by the year 2020 [3]. When this large amount of health data gets transferred between devices and the cloud, it creates the problem of low latency and system idleness. As we are concern about e-Health implementation, the above-stated issue represents some difficulties in how to deal with a large number of accumulated health datasets to keep low latency in real-time applications [2].

Fog computing solves some of the difficulties raised by the cloud of things (CoT). Fog computing has the potential to give reasonable answers to all issues related to the use of IoT and cloud in e-Healthcare applications. In the E-Health solution, all the data gathered from IoT sensors must not be transferred to the cloud, some can be interpreted at the data generation point, and the processed information is then transferred to cloud or any other device for further usage. This can only be done with the help of fog computing [1].

E-Healthcare platform consists of applications and services used to gather and provide clinical data [4]. Our main focus in this research is to figure out the risk factors involved in fog-enabled e-Health system in Uttarakhand. The cost will also cut down because the patient does not have to come to the hospital for monitoring purposes, they can be monitored remotely with the help of fog architecture [5].

The present research gives the details of fog-enabled e-Healthcare systems. This research also gives the main characteristics of an e-Health system combined with fog computing. Some of the main objectives of this paper include

- i. An overview of e-Healthcare systems in Uttarakhand.
- ii. An investigation of how e-Health applications profit by the fog computing.
- iii. Present the various terms in a presentable way, so that it can be understood why these technologies are collaborating.
- iv. Finding the risk of involving fog in the e-Healthcare system in a state like Uttarakhand and analyzing them.

2 Methodology

This is a descriptive study in which several published reports, research studies, articles, e-books, vulnerabilities notes, and government notifications are used as the secondary data source to assess and analyze the security vulnerabilities in popular web browsers. To gather the secondary data, Google Scholar (<https://scholar.google.com/>), Directory of Open Access Journals (<https://doaj.org/>) and Connecting Repositories (<https://core.ac.uk/>) are used. Appropriate search keywords are used to

find the requisite data on the above-used databases, such as e-Health, fog computing, cloud-based e-Health system, fog-based e-Health system, e-Health in Uttarakhand, etc. Further, the data is reviewed and analyzed accordingly to the objectives of the study.

3 Overview of Key Technologies

E-Health care is the utilization of data and correspondence innovative technology in health care and is viewed as basic for an advanced, financially savvy health administration system that is prepared to address difficulties and challenges. Various technologies are combined to provide the foundation for an e-Healthcare system. In this section, these technologies are discussed as follows:

Internet of Things—In recent years, devices are developed with the inbuilt feature of Internet communication. These smart devices or things can communicate with each other via the wireless network. Devices can be hardware, software, or even physical objects that can talk to each other [6]. With its rapid advancement and low cost, IoT will be very beneficial if included in the healthcare environment. Using data gathered with IoT sensors, one can advance his decision-making abilities, and when used in health care, doctors or health managers can take quick and decisive measurements for the betterment of patients. The patients also take part in the system actively and contribute by checking and maintaining their health records and IoT devices [5].

Cloud Computing—Cloud computing as defined by NIST is a pool of shared computing resources accessed on-demand on a network [7]. Computing resources can be shared with the help of three service models (SaaS, PaaS, and IaaS) and four deployment models (public, private, hybrid, and community) [7]. Scalability, rapid deployment, and low cost are the key characteristics of cloud computing. Consumers can use, switch, or end any computing service automatically according to its need [2]. One of its main advantages is the availability of enormous data storage capacity.

Fog Computing—Fog computing was characterized by Cisco as an amplification of cloud computing where data is stored at the edge to raise the standard of services with low latency and high data analysis [1, 8]. It has the same features as implemented by the cloud, i.e., computation, storage, and services, etc. Fog processes data and can segregate and transmit it after analyzing, resulting in time and resource saving [9].

The Network Technology Used in IoT, Cloud, and Fog Computing—The network is also a vital player in using IoT, cloud, or fog. Some of the important network technologies used are discussed here:

- (i) *RFID*—The short-range communication can be done by using radio frequency identification (RFID) for each device used in the network [10]. RFID can be very well suited for healthcare fog devices, as these are cheap, reliable, and trackable.

- (ii) *Bluetooth*—Short-wavelength UHF radio waves are used in this standard to exchange data between mobile and fixed devices from 2.402 to 2.480 GHz [11]. It can provide speed up to 3 Mbps over a range of 100 m.
- (iii) *WiFi*—WiFi is one of the main network technology used in IoT. This is the method through which millions of devices are connected to offer Internet-based services [12]. Some WiFi exceeds the speed of 1 Gbit/s over a range of 100–150 m. Most of the healthcare environments in hospitals have a WiFi network available. WiFi can be accessed with mobile devices as well as wearable sensor devices, which makes it a highly commendable option for fog computing.
- (iv) *WiMax*—WiMax provides a range of up to 50 km. It is best suited for communication between fog nodes that are in different parts of a city. Different standards of WiMax starting from IEEE 802.16a to IEEE 802.16c provide flexibility in choosing bandwidth range from 2 to 66 GHz [13].
- (v) *Mobile Network (2G, 3G, 4G, LTE, 5G, etc.)*—The use of mobile in IoT and fog is a necessity without which the concept does not work. 2G, 3G, 4G, LTE, and 5G are the cellular technology known to use for long-range connectivity wirelessly [14]. E-Healthcare facility uses a mobile device and network to authenticate and share information and services. Long-range connectivity is also needed for healthcare facilities in Uttarakhand state. Cost-effective development in smart devices in recent years allows common people to use its services and connect to the world with the latest technology [14].
- (vi) *WSN*—Wireless sensor network or WSN is a network of geographically detached sensors that are used to take care of physical environments [15]. Information assortment and transmission are the essential activities of WSNs [16]. And, like IoT, fog is dependent on their sensors for data collection; therefore, WSN has the advantage to be used in these technologies. The advancement of detecting IoT devices makes WSNs continuously develop into a classic detecting stage, which can give information mindful administrations to a variety of uses [17].

4 Background Study

This section is to study the work done by other researchers to get an understanding of implementing fog computing-based e-Healthcare systems in rural areas of Uttarakhand. Fog computing is becoming an important delivery model of Internet-based services. Implementing fog gives benefits as well as some disadvantages to be discussed. This section will be focused on getting and reviewing the work in the last few years implemented in this area. The aim of getting the gray area (security challenges) will also be done through this literature review.

Kuo [18] described and focused on the use of cloud computing in the e-Healthcare environment. In the research paper, Kuo elaborated on the challenges of cloud computing some are lack of trust by the user, cultural resistance, not defining proper service level agreement by the service provider, data lock-in, low

latency, and virus in distributed cloud systems, etc. Many other security issues are discussed in the paper with a detailed explanation.

Alharbi et al. [19] study the role of cloud base e-Healthcare applications in the context of Saudi Arabia. The study provides a business perspective on the healthcare model and shows its cost effectiveness. Habiba et al. [20] give the security issues involved in the cloud computing identity management paradigm. They analyze various cloud identity management systems and discussed their security issues and also provide ways to solve these vulnerabilities.

Ouedraogo et al. [21] address the lack of transparency in security models of cloud, whereas Hashizume et al. [22] discussed the differences between vulnerabilities and threats and created a relationship between them. Then they also proposed new security techniques to mitigate these threats. Wang et al. [23] dissect the productivity, avg. frame rate, delivering execution bottleneck of the cloud delivering framework, and set forward an extraordinary boundary change technique to improve framework execution, by advancing related server and delivering machine setup. They conclude that an increase in the number of users directly increases the average response time, i.e., low latency.

Mitton et al. [24] include sensors in cloud computing in their research. They coined the name sensing and actuation as a service (SAaaS) for this architecture. This architecture is used to provide sensors and actuators as a service to the user. And the cloud is involved to give the computation and data storage benefits. We can also say this as CoT, i.e., cloud of things.

Ibrahim et al. [25] defined the term fog health as the inclusion of fog computing into the healthcare paradigm. They also recapitulate the issues in the domain of fog computing and health care. From their literature review, they found that low latency and slow data analysis are the main issues in distant healthcare monitoring systems. Silva and de Aquino Junior [26] also consider low latency in cloud computing as one of the main issues that can cause a failure of the healthcare system. Fog-enabled healthcare systems are liable to solve the problem of low latency. Therefore, the authors suggested the use of fog computing in this area for solving much of its issues. They also figure the lack of well-demonstrated architecture of fog-enabled e-Healthcare systems. Vilela et al. [2] present a review of the application and challenges of the fog-enabled e-Healthcare system. They summarize the already available solution to the problems raised within the system like latency, security, privacy, etc. They also study communication protocols used between edge and cloud computing.

By introducing fog computing for various e-Health services that are previously delivered by cloud computing, most of the vulnerability (issues) can be solved. But whether these services are beneficial and practical if implemented in rural and hilly regions of Uttarakhand, we will study the challenges that have to come in those distant areas.

5 Healthcare Scenario in the Himalayan Region (Uttarakhand)

Admittance to medical services in the rural parts of Uttarakhand keeps on being poor. Given the limitations of territory and geology and the small and dissipated nature of the provincial settlements, expanding access represents a significant challenge. As most of the people living in hilly areas are poor, they cannot bear the cost of the significant expense of private clinical consideration. There is an intense lack of different healthcare human resources in the state-run Primary Health Centers (PHC). Almost 90–94% of physician’s posts are vacant in the state. In hilly areas, there are only two PHC which are operational per 100,000 peoples [27]. This shows that the ratio between health facilities and patients is very low. This scarcity leads to the unsuccessful implementation of health services provided by the government [27, 28]. For raising the standard of healthcare facilities and improving the service availability to common and poor people, there should be a mechanism that will address the problem in hilly and rural areas of Uttarakhand.

In the Himalayan state, Uttarakhand, initiatives are been taken by the state government to fulfill the need of people for e-Healthcare services. Many projects are going on successfully like [29].

The e-Health services (Table 1) that are started by the Uttarakhand Government are unproductive due to lack of Internet infrastructure and awareness. Expanding and reinforcing the quantity of health facilities focus that could work nonstop, particularly in rural zones, would go far in diminishing the health problems in the state. This can be done if health facilities are incorporated with fog computing. Using fog computing for providing e-Health services can help in the timely recognition and avoidance of diseases.

Several healthcare services can be provided by incorporating fog computing in e-Health systems like smart health monitoring systems/smartphone-based e-Health solutions [30], home healthcare systems [5], collecting health data in real time [9], automatics dialing of emergency numbers, hospital e-Management [5], etc.

Table 1 Various e-Healthcare services running in Uttarakhand

e-Healthcare service	Benefit/Use of service
e-Parchi	Outpatient department (OPD) registration system
e-Attendance	Attendance tracking of medical staff
e-Aushadhi	Record of medication data from providers to the stockroom to healthcare offices to patients
e-RaktKosh	Online facility to collect blood, plasma, and platelets
108 Services	24 × 7, toll-free emergency telephone number for calling Healthcare ambulance from any location within the state

6 Security and Challenges

This section gives a clear idea of security and challenges that must be covered to build a reliable, user-friendly, manageable, and secure fog-implemented e-Healthcare system. Fog provides many advantages to authorities and patients, also enhances the quality and effectiveness of the various services provided by healthcare systems. In a region where demographic conditions are not-so-good, fog-based e-Healthcare systems can provide an expert solution to the health problems of the citizen. As there are several merits, fog also has some issues that must be addressed before applying it to healthcare systems. Fog-based healthcare system manages very sensitive health datasets, so security is the main concern while using it.

Important security concerns/challenges in fog-based e-Healthcare system are as follows:

Safety of Healthcare Data—Safety of data is the main concern in the healthcare system. Patient-related data that is generated through IoT sensors is very much sensitive and should be handled carefully [9]. Data security concern contains issues like illegitimate data access, data changing and removing issues, ownership changing issues, and data sharing with other users. With the said issues, there is a very high risk of illegal file/database access in the fog system. Data should be encrypted with secured keys and transferred via secured socket layer (SSL) for maintaining data security. Ownership access should be managed securely so that the user cannot view the health dataset of other people.

Wireless Security Issues—Generally, a wireless network is used between fog devices for data communication [31]. This network is also vulnerable to various attacks like data infringe, losing data in-between communication, IDimitation, communication response attacks, etc. This can result in low privacy, inadequate accuracy, and also lower the trustworthiness of the system. Encrypted communication is a way to overcome this type of attack. Proper authentication and secure data routing will enhance wireless security features.

Computer Virus—These issues are related to computer viruses like Trojans, malware, worms, spyware, etc., which can degrade the performance of the system and can also spoil the health data permanently. Various antivirus programs are available that can be included in the system, for getting rid of these computer viruses. Data backups should be taken periodically to overcome any such vulnerability.

Although monitoring the health of old age people become very easy if we include fog computing into the system, this system is tracked with the help of a mobile phone. There is also a problem with aged people as they are almost unaware of modern gadgets like smartphones, etc., and they are not able to use them efficiently and accurately. This is a major challenge in applying smartphone-based technology in health care.

7 Conclusion

Despite various improvements in the health infrastructure in Uttarakhand, there is a shortage of health personals and primary health care centers. The geographical condition is also not very favorable for infrastructural development. An insufficient number of trained health personals give rise to the system that enables to monitor the health of people without much human intervention. Fog computing-based e-Healthcare system provides a way to enhance the capability of health monitorial without including trained health personals, as almost all the monitoring is done by the IoT and fog-based sensors. So this technology enhances the option of giving better e-Health solutions to the distant people of Uttarakhand. There are a good number of benefits seeing we can suggest fog computing as a technology that can change the scenario of health facilities in Himalayan regions. But there are some security issues and challenges also that must be entertained before proceeding further. For future work, we are working on an architectural model of a fog computing-based e-Health system that includes RFID, NFC, LWPAN, and other WiFi technologies so that the healthcare department gets benefitted from these advancements.

References

1. Caiza, G., Saeteros, M., Oñate, W., Garcia, M.V.: Fog computing at industrial level, architecture, latency, energy, and security: a review. *Heliyon* **6**(4) (2020). <https://doi.org/10.1016/j.heliyon.2020.e03706>
2. Vilela, P.H., Rodrigues, J.J., Righi, R.D., Kozlov, S., Rodrigues, V.F.: Looking at fog computing for e-Health through the lens of deployment challenges and applications. *Sensors* **20**(9), 2553 (2020). <https://doi.org/10.3390/s20092553>
3. Networking, C.V.: Cisco Global Cloud Index: Forecast and Methodology, 2015–2020. White Paper; Cisco Public, San Jose, CA, USA (2016)
4. Bisio, I., Estatico, C., Fedeli, A., Lavagetto, F., Pastorino, M., Randazzo, A., Sciarrone, A.: Brain stroke microwave imaging by means of a newton-conjugate-gradient method in L_p Banach spaces. *IEEE Trans. Microw. Theory Tech.* **66**, 3668–3682 (2018). <https://doi.org/10.1109/TMTT.2018.2849060>
5. Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., Alizadeh, M.: The application of Internet of things in healthcare: a systematic literature review and classification. *Univ. Access Inf. Soc.* **18**(4), 837–869 (2018). <https://doi.org/10.1007/s10209-018-0618-4>
6. Jung, S., Myllyla, R., Chung, W.: Wireless machine-to-machine healthcare solution using Android mobile devices in global networks. *IEEE Sens. J.* **13**(5), 1419–1424 (2013). <https://doi.org/10.1109/jsen.2012>
7. Mell, P., Grance, T.: The NIST Definition of Cloud Computing; Computer Security Division. Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, Gaithersburg, MD, USA (2011)
8. Tewari, N., Datt, G.: Towards FoT (fog-of-Things) enabled architecture in governance: transforming E-Governance to smart governance. In: 2020 International Conference on Intelligent Engineering and Management (ICIEM) (2020). <https://doi.org/10.1109/iciem48762.2020.9160037>

9. Khan, S., Parkinson, S., Qin, Y.: Fog computing security: A review of current applications and security solutions. *J. Cloud Comput.* **6**(1) (2017). <https://doi.org/10.1186/s13677-017-0090-3>
10. Yue, Z., Sun, W., Li, P., Rehman, M.U., Yang, X. (eds.): Internet of things: architecture, technology and key problems in implementation. In: 2015 IEEE 8th International Congress on Image and Signal Processing (CISP) (2015)
11. Gentili, M., Sannino, R., Petracca, M.: BlueVoice: voice communications over Bluetooth low energy in the Internet of things scenario. *Comput. Commun.* **89–90**, 51–59 (2016). <https://doi.org/10.1016/j.comcom.2016.03.004>
12. Lee, I., Kim, M.: Interference-aware self-optimizing Wi-Fi for high efficiency Internet of things in dense networks. *Comput. Commun.* **89–90**, 60–74 (2016). <https://doi.org/10.1016/j.comcom.2016.03.008>
13. Zemrane, H., Abbou, A.N., Baddi, Y., Hasbi, A.: Wireless sensor networks as part of IOT: performance study of WiMax—Mobil protocol. In: 2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech) (2018). <https://doi.org/10.1109/cloudtech.2018.8713351>
14. Basir, R., Qaisar, S., Ali, M., Aldwairi, M., Ashraf, M.I., Mahmood, A., Gidlund, M.: Fog computing enabling industrial Internet of things: state-of-the-art and research challenges. *Sensors* **19**(21), 4807 (2019). <https://doi.org/10.3390/s19214807>
15. Alhalafi, A., Sboui, L., Naous, R., Shihada, B.: GTBS: A green task-based sensing for energy efficient wireless sensor networks. In: 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2016). <https://doi.org/10.1109/infcomw.2016.7562060>
16. Akber, S.M.A., Khan, I.A., Muhammad, S.S., Mohsin, S.M., Khan, I.A., Shamshirband, S., Chronopoulos, A.T.: Data volume based data gathering in WSNs using mobile data collector. In: Proceedings of the 22nd International Database Engineering and Applications Symposium on—IDEAS 2018, pp 199–207. ACM Press, New York (2018). <https://doi.org/10.1145/3216122.3216166>
17. Chen, Y., Liu, W., Wang, T., Deng, Q., Liu, A., Song, H.: An adaptive retransmit mechanism for delay differentiated services in industrial WSNs. *EURASIP J Wireless Commun. Netw.* **2019**(1) (2019). <https://doi.org/10.1186/s13638-019-1566-2>
18. Kuo, A.M.: Opportunities and challenges of cloud computing to improve health care services. *J. Med. Internet Res.* **13**(3), e67 (2011). <https://doi.org/10.2196/jmir.1867>
19. Alharbi, F., Atkins, A., Stanier, C.: Understanding the determinants of cloud computing adoption in Saudi healthcare organizations. *Complex Intell. Syst.* **2**(3), 155–171 (2016). <https://doi.org/10.1007/s40747-016-0021-9>
20. Habiba, U., Masood, R., Shibli, M.A., Niazi, M.A.: Cloud identity management security issues and solutions: a taxonomy. *Complex Adapt. Syst. Model.* **2**(1) (2014). <https://doi.org/10.1186/s40294-014-0005-9>
21. Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S., Dubois, E.: Security transparency: The next frontier for security research in the cloud. *J. Cloud Comput.* **4**(1) (2015). <https://doi.org/10.1186/s13677-015-0037-5>
22. Hashizume, K., Rosado, D.G., Fernández-Medina, E., et al.: An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **4**, 5 (2013). <https://doi.org/10.1186/1869-0238-4-5>
23. Wang, R., Zhang, B., Wu, M., Zhang, J., Guo, X., Zhang, X., Li, H., Jiao, D., Ma, S.: Performance bottleneck analysis and resource optimized distribution method for IoT cloud rendering computing system in cyber-enabled applications. *EURASIP J Wireless Commun Netw* **2019**(1) (2019). <https://doi.org/10.1186/s13638-019-1401-9>
24. Mitton, N., Papavassiliou, S., Puliafito, A., Trivedi, K.S.: Combining cloud and sensors in a smart city environment. *EURASIP J Wireless Commun Netw* **2012**(1) (2012). <https://doi.org/10.1186/1687-1499-2012-247>
25. Ibrahim, W.N.H., Selamat, A., Krejcar, O., Chaudhry, J.A.: Recent advances on fog health—a systematic literature review. In: Fujita, H., Herrera-Viedma, E. (eds.) *New Trends in Intelligent Software Methodologies, Tools and Techniques—Proceedings of the 17th International Conference SoMeT_18*, Granada, Spain, 26–28 Sept 2018; *Frontiers in*

- Artificial Intelligence and Applications, vol. 303, pp 157–170. IOS Press, Amsterdam, The Netherlands (2018). <https://doi.org/10.3233/978-1-61499-900-3-157>
26. Silva, C.A., de Aquino Junior, G.S.: Fog computing in healthcare: a review. In: 2018 IEEE Symposium on Computers and Communications (ISCC) (2018). <https://doi.org/10.1109/iscc.2018.8538671>
 27. Directorate of Economics and Statistics, Planning Department, Government of Uttarakhand (2018). https://des.uk.gov.in/files/uttarakhand_human_development_report_.pdf
 28. Joshi, M., Tewari, N., Budhani, S.K.: Security challenges in implementing a secured hybrid cloud model for e-health services. In: 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, pp. 3–7 (2020). <https://doi.org/10.1109/SMART50582.2020.9337096>
 29. Uttarakhand Health Services Dashboard. Retrieved 27 Oct. 2020, from <https://healthdashboard.uk.gov.in/>
 30. Kharel, J., Reda, H. T., Shin, S.Y.: An architecture for smart health monitoring system based on fog computing. J. Commun. (2017). <https://doi.org/10.12720/jcm.12.4.228-233>
 31. Sen, S. (ed.): Invited-context-aware energy-efficient communication for IoT sensor nodes. In: Proceedings of the 53rd Annual Design Automation Conference. ACM (2016)

Android Malware Detection Using Extreme Learning Machine Optimized with Swarm Intelligence



Rahul Gupta, Aviral Agarwal, Devansh Dua, and Ankit Yadav

Abstract Android devices remain vulnerable to an increasing number of unidentified Android malware that has greatly compromised the efficacy of traditional security measures. Most classifiers are programmed to use a training process to learn from the data itself, since full expert insight to evaluate classifier parameters is difficult or impossible. This paper proposes a methodology which is a hybrid of machine learning and swarm intelligence. This methodology combines the successful exploration algorithm called the particle swarm optimization (PSO) with the extreme learning machine (ELM) classifier. ELM is a single-hidden layer feed-forward neural network (FFNN) consisting of large number of hidden layer neurons, which has proved to be an excellent classifier. In this research, the optimum values of input weights and biases for the ELM classifier are determined using PSO, and it further improves the classifier's accuracy. The dataset consists of 1700 benign and 418 malicious Android applications from which over 15,000 features of different types were extracted, and feature selection techniques were applied. The aforementioned dataset was used to experiment our proposed model, and significant results were achieved.

Keywords Android security · Malware analysis · Machine learning · Swarm intelligence · Static analysis

1 Introduction

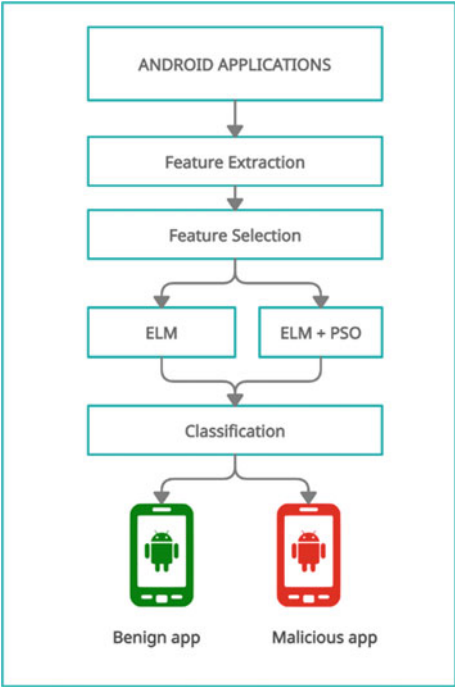
Smartphones are ubiquitous today, serving as a portable way to enter personal data, accounts, contacts, and communication services. The Android platform has become the most dominant mobile OS since 2012. Android privacy is seriously jeopardized because of Android's open nature due to which innumerable adware, ransomware, etc., are disguised in a large number of non-malicious apps. Given this, smartphones have been tempting victims of cyber-attacks over the years. During

R. Gupta · A. Agarwal (✉) · D. Dua · A. Yadav
Delhi Technological University, New Delhi, India

installation, Android device users who do not regularly check or understand app permissions allow malwares to be installed and gain access to sensitive resources, even without understanding the risk. Users’ private data, such as IMEI, SMS data, call logs, contact list, and application usage statistics, is the main target for intruders, posing a significant threat to mobile users’ confidentiality and security. Therefore, immediate measures are needed to identify and deal with malware for Android devices.

In this research article, we present a machine learning (ML)-based solution for classifying applications into benign and malware classes using an extreme learning machine (ELM) classifier whose parameters are optimized by particle swarm optimization (PSO) algorithm. We had a collection of 2118 Android applications (1700 benign + 418 malicious) as APK files [1]. We generated a dataset by unpacking these APK files into source code and extracted static information including permissions, actions, intents, services, and receivers from AndroidManifest.xml files. Using this, we created a feature set consisting of over 15,000 features. Then, we preprocessed our dataset using feature selection techniques before feeding it into the aforementioned model for classification of Android applications into benign and malicious. The explained architecture is depicted in Fig. 1.

Fig. 1 Architecture of the proposed model



2 Related Work

Substantial research has been devoted in applying different machine learning and deep learning algorithms to classify malicious Android apps based on features which are extracted from static as well as dynamic analysis. In [2], authors have implemented a bio-inspired hybrid intelligent method for detecting Android malware (HIMDAM). This research classifies Android apps by applying extreme learning machine (ELM) as a classifier. Further, the model's accuracy was increased by using evolving spiking neural networks (eSNNs). In this paper [3], an engine for Android malware detection (DroidDetector) based on deep learning is proposed which uses deep belief network (DBN) architecture giving 96.76% testing accuracy. A feature set consisting of 192 features was extracted using static and dynamic analysis of Android applications. This work [4] proposes DroidDeep which merges the concept of static analysis and deep learning. Firstly, more than 30,000 static features were extracted and then fed into a deep learning model based on DBN to reduce the number of features. Finally, the new feature set was put into a support vector machine (SVM) model to detect Android malware. In this paper [5], detection of probable anomalies in two malware datasets was done using a high-performance extreme learning machine (HP-ELM). The results show that this approach achieved a maximum accuracy of 95.92% for top three features. In this study [6], an efficient model is introduced which is based on feature extraction and ELM classifier to detect Android malware. This model utilizes three different feature extraction methods including independent component analysis (ICA), Karhunen–Loeve transform (KLT), and principal component analysis (PCA) and then finally compiles the results using various stacking methods. In [7], authors have proposed a fully connected deep neural network approach for malware detection resulting with maximum accuracy of 94.65%. The dataset used here consists of 331 features including information about permissions in API. This paper [8] presents an effective machine learning approach based on Bayesian classification model. The features were extracted through static analysis, and total of 58 features were selected. DroidMat [9] is a model that collects static information including API calls, required permissions, etc., from AndroidManifest.xml file and then enhances the malware detection efficiency using K-means algorithm. Singular value decomposition (SVD) was used to determine the cluster's number, and finally, KNN algorithm was used to classify apps as benign or malicious.

3 Methodology

Static analysis for the identification of mobile malware is a fast and inexpensive approach. This method tests an application without any code execution and detects malware before the inspected application is executed. Dynamic analysis detects malware after the program under review is run or during it. Hybrid analysis consists

of static as well as dynamic analysis. We are concentrating on the static analysis of mobile applications in this research.

The proposed system consists of three phases—feature extraction, feature selection and detection using machine learning models. All the phases are discussed in detail in this section.

3.1 Creating the Dataset (Feature Extraction)

We received a total of 2118 Android applications consisting of 1700 benign and 418 malicious applications [1]. The corresponding APK files were unpacked to their source code using APK tool. For static analysis, AndroidManifest.xml files were fetched. For each application, this XML file was parsed using Python 3 modules, and information related to permissions, actions, features, and receivers was gathered. These parameters would become the features of the dataset which would be used to train and test the classifier to detect malware in Android applications. Figure 2 diagrammatically represents the feature extraction process.

In this way, after parsing all the applications, we obtained a total of 15,939 features consisting of the aforementioned parameters. Note that any feature is Boolean or binary, meaning that its feature value is 1 whenever a feature appears in an application; otherwise, it is 0.

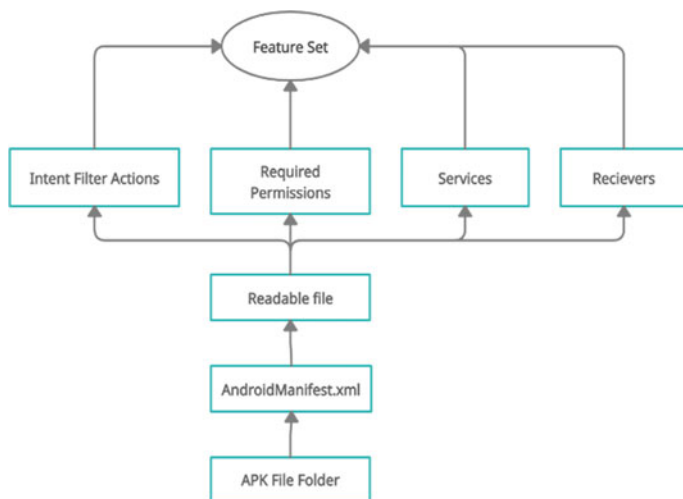


Fig. 2 Feature extraction process for an Android application

3.2 Feature Selection

One possible solution to reduce the amount of features is to use small datasets, resulting in a smaller feature set. A second approach for reducing the number of the features is to consider a limited set of possible features, e.g. permissions for Android only. A third approach is to use methods of feature ranking and feature selection, e.g. univariate statistical tests (chi-square), evaluation of correlation-based features, information gain, gain ratio, and community-based identification and elimination of recursive features. The strength of the relationship between an individual feature and the response variable is determined by these methods. Thus, a single score indicating this relationship is obtained by each feature. Then, according to these scores, all the features in the feature vector are ranked, and the top k features are considered.

For this research, we have applied the chi-square (χ^2) [10] test to find out the correlation among the features and to select the necessary features from these 15,939 features.

For a relationship with a given number of variables and sample size, the chi-square method compares the differences between the actual and the predicted results. Degrees of freedom (DOF) is considered for these experiments to determine whether, based on the cumulative number of variables and samples, a specific null hypothesis can be rejected. χ^2 provides a way to assess how well a data sample fits the characteristics of the wider population the sample is supposed to represent. If the sample data does not match the population's predicted properties that we are interested in, then we may not want to use this sample to draw conclusions about the larger population.

We apply the sklearn's select KBest function for feature selection and use the chi-square test to evaluate the best features. We receive the scores and alpha values (p_values) for each feature. The rejection region lies when the value to alpha drops below 0.05. This indicates that the features with $p\_values < 0.05$ are not useful for the classification of our results, and we can discard them.

After selecting the features using chi-square, we finally get a dataset with 2654 features which will be fed to the machine learning classifiers in the next phase.

3.3 Model Design

Computational models are built which are capable of generalizing a concept when a machine learning algorithm is trained with a sample of input data. In our situation, trained models generalize whether or not an application is malicious or not. Therefore, when a new unidentified dataset is used by this model, it should be able to synthesize it, understand it, and provide us a reliable result.

Firstly, we are going to split the dataset into two groups: 80% for training and 20% for testing. Next, to understand its efficiency, we will run the primitive ELM.

To compare the proposed ELM with particle swarm optimization outcomes, the outcomes of the native ELM will be regarded as the gold standard [11–13].

3.4 Extreme Learning Machine (ELM)

Machine learning methods have gained interest in artificial intelligence in recent years, primarily because of their contributions to various disciplines. A specific case of machine learning techniques is the extreme learning machine. ELM can be labelled as supervised learning algorithm competent of figuring out linear and nonlinear problems of classification. ELM is described by conventional artificial neural network architectures as the single layer feedforward neural network (SLFN), where it is not necessary to compute input weights and hidden layer biases iteratively [11]. An example of an ELM model is shown in Fig. 3.

For each hidden neuron, let IW be $(L \times n)$ input weights and B be $(L \times 1)$ bias values and O be $(C \times L)$ output weights. In a problem with N observations for a multi-category classification (K -distinct classes) $\{X_i, T_i, i = 1, 2, \dots, N - 2, N - 1, N\}$, the ELM network outputs with L hidden layer neurons are identified as:-

$$y_k = \sum_{j=1}^L O_{kj} F_j(IW, B, X_i), \quad k = 1, 2, \dots, K - 1, K \quad (1)$$

For the j th hidden neuron, the output is $F_j(\cdot)$, and the corresponding activation function is $F(\cdot)$.

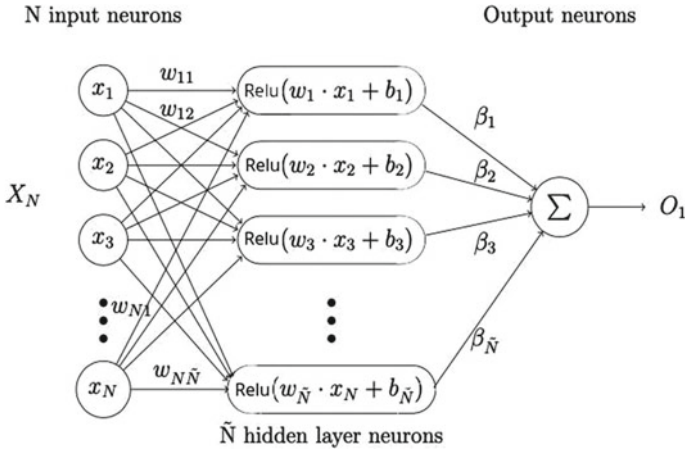


Fig. 3 ELM architecture

The target t is defined as

$$t_i^p = \begin{cases} 1 & \text{if } k_i = p \\ 0 & \text{Otherwise} \end{cases} \quad k = 1, 2, \dots, K-1, K \quad (2)$$

In the matrix representation, it can be written as— $Y = OY_l$, where Y_l is an $L \times n$ matrix, which is represented as

$$Y_l = \begin{bmatrix} F_1(IW, B, X_1) & \cdots & F_1(IW, B, X_N) \\ \vdots & \ddots & \vdots \\ F_L(IW, B, X_1) & \cdots & F_L(IW, B, X_N) \end{bmatrix} \quad (3)$$

In our case, $K = 2$ for binary classification. For a given number of hidden layer neurons in the ELM algorithm, the input weights (IW) and bias (B) are initialized with random values. The output weights (O) are determined analytically by considering the classifier output (Y) equal to the Boolean class label (t):

$$O = YY_l^+ \quad (4)$$

where Y_l^+ is defined as the Moore–Penrose pseudo-inverse of matrix Y_l .

3.5 Optimization Technique—Particle Swarm Optimization (PSO)

PSO belongs to the group of techniques of swarm intelligence, influenced by the behavioural interactions of animals that huddle together such as ants, fireflies, and bees. It is an algorithm based on the interaction of individuals which consist of a population, in a search space to evaluate for promising regions. The action of an individual is influenced by either the best personal value achieved or the best global value achieved. Using fitness parameters just like that of evolutionary algorithms, the performance of each individual is determined. The population is called as a swarm, and particles are referred as individuals. The particles remember their best position in the past in the PSO and the optimal global position the particles have ever reached. This property lets particles search more rapidly in multidimensional space [12].

Let us consider a swarm with S number of individuals. Every P_i ($i = 1, 2, \dots, S-2, S-1, S$) particle in the population is defined by

- (i) Its current $p_i(k)$ position, referring to a probable solution to the optimization problem at iteration k ;
- (ii) Its $v_i(k)$ velocity;
- (iii) The optimal $Pbest_i(k)$ position attained in its previous path.

Let $Gbest(k)$ be the optimal global position that the particles of the swarm have found across all trajectories. Optimality of position is determined by using one or more fitness parameters specified in accordance with the optimization problem considered. The particles travel according to the following equations during the search process:

$$v_i(k+1) = Wv_i + c_1r_1(Pbest_i(k) - p_i(k)) + c_2r_2(Gbest_i(k) - p_i(k)) \quad (5)$$

$$p_i(k+1) = p_i(k) + v_i(k+1) \quad (6)$$

These steps are shown as a flow chart in Fig. 4. The values of constants in the above equations such as W , c_1 and c_2 should be calculated before the experiment for the velocity updating process. The parameters c_1 and c_2 denote the weighting of the

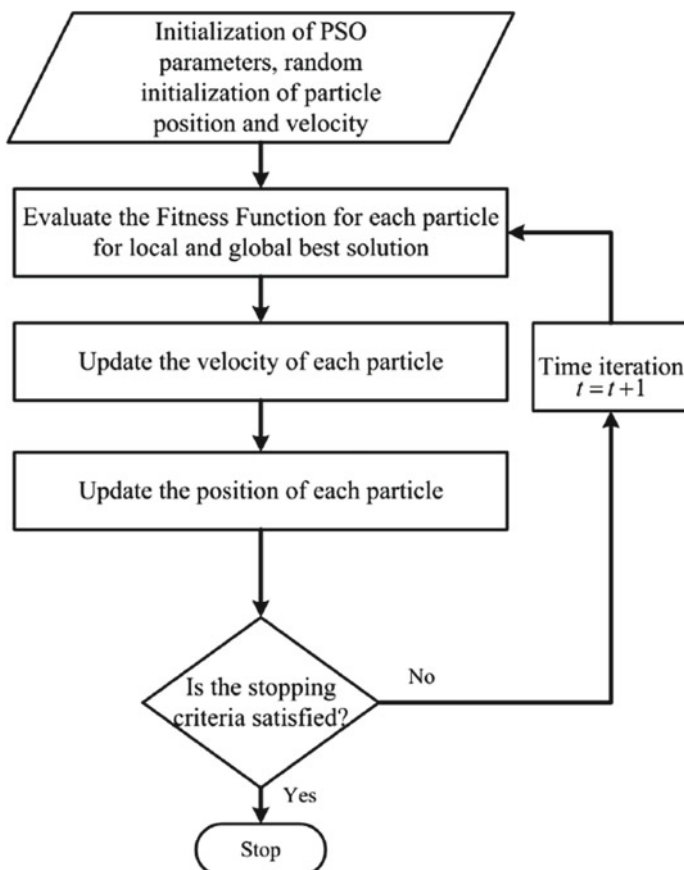


Fig. 4 Native PSO flow chart

terms of stochastic acceleration pulling each particle towards the positions of $Pbest_i$ and $Gbest$. The parameters r_1 and r_2 are random variables in the range of $[0, 1]$.

3.6 PSO Algorithm for ELM Optimization

The following major steps need to be taken to create an ELM classifier which uses PSO to optimize its parameters. These steps are as follows:

1. Randomly generate a swarm with population of S particles.
2. Initialize the vectors of velocity parameter v_i ($i = 1, 2, 3, \dots, S$) for each particle with random values.
3. Train an ELM classifier for each particle position of the particle p_i ($i = 1, 2, 3, \dots, S$), and calculate the respective accuracy/fitness function.
4. Initialize the $Pbest_i$ of the particle with its starting position configuration.
5. Detect $Gbest$ representing the maximum value of the fitness function observed over all paths pursued.
6. Update the velocities and the positions of the particles using the equations mentioned in the previous section.
7. For every candidate particle p_i , create an ELM model, train the classifier, and calculate the accuracy.
8. Update the particle's best position ($Pbest_i$) if the current accuracy is greater than the previous attained maximum value for $Pbest_i$.
9. If maximum number of iterations have been completed, then proceed to step 10, else go to step 5.
10. Select the best global value from the swarm of these particles, and use its values for input weights and biases to train the final ELM classifier which will have the best accuracy from all the models that PSO will have trained.
11. Use this ELM classifier to classify applications into benign and malware classes (Fig. 5).

4 Results

After finalizing our dataset by reducing the feature set to 2654 features using chi-square feature selection method, the proposed experimental model was divided into two major experiments.

The first experiment consisted of training a native ELM classifier using the dataset for different values of various parameters. The second experiment was the main focus of this research work. The previously developed ELM classifier was optimized using particle swarm optimization (PSO) and was trained using the same dataset for same parameter settings as the previous experiment and the results were compared.

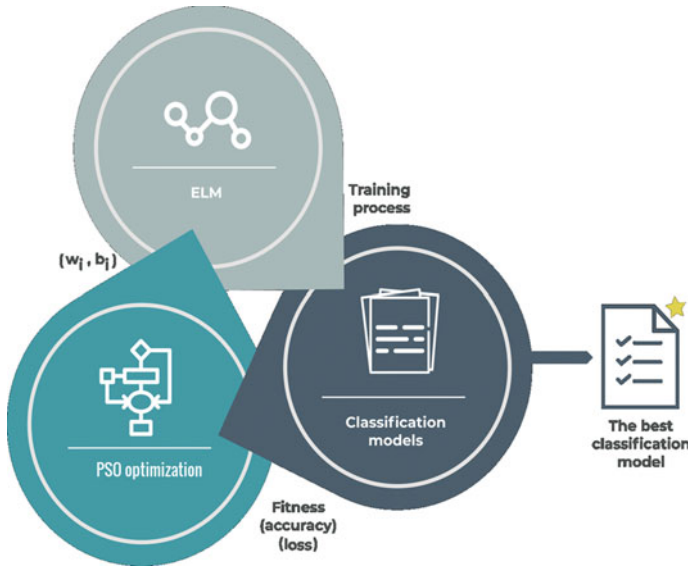


Fig. 5 Method representation used in the proposed PSO-ELM. ELM is trained and produces a learning model. This model offers accuracy and loss, all of which are used as the fitness by the PSO algorithm to be evaluated. Finally, for the ELM, the PSO algorithm measures new weights and biases. This approach works when a stop condition is met.

These experiments were performed using the Python environment on a system with the specifications—Core i5-9300H @2.40 GHz with 8 GB memory.

4.1 Experiment 1

An extreme learning machine (ELM) classifier was implemented in Python using various modules like NumPy, SciPy, etc. The whole experiment was conducted twice using two activation functions—Relu and Sigmoid [13]. In each experiment, we trained a number of ELM classifiers with different number of hidden neurons starting from 100 till 1000 neurons with a step increase of 100 neurons. For a specific number of hidden neurons, ELM classifier was tested 31 times, and the mean of these accuracies was considered.

The maximum average accuracy achieved using Relu as an activation function was **93.28%** at 600 neurons in hidden layer, whereas Sigmoid achieved a maximum average accuracy of **94.12%** at 500 neurons in hidden layer.

Table 1 Values for PSO constants

Constant Parameters	Values
Swarm population	100
No. of iterations	100
C_1 —Self confidence	2
C_2 —Swarm confidence	2
W —Velocity scaling factor	0.5

Table 2 Comparison of accuracies

No. of hidden neurons	ELM—Accuracy (%)		ELM + PSO—Accuracy (%)	
	Relu	Sigmoid	Relu	Sigmoid
100	90.07	90.93	96.93	97.17
200	91.96	92.86	97.88	98.35
300	92.85	93.53	97.88	98.35
400	92.94	93.93	97.88	98.82
500	93.27	94.12	98.35	98.11
600	93.28	93.71	98.58	98.35
700	92.66	93.21	97.40	98.35
800	92.09	92.86	97.64	97.87
900	91.39	91.49	96.46	97.65
1000	90.12	89.59	95.51	96.69

4.2 Experiment 2

Particle swarm optimization (PSO) was used to improve the performance by optimizing the values of input weights and biases of ELM classifiers. This experiment was also conducted twice with the same activation functions and same iterations for the number of hidden neurons. But at each step, ELM classifier was optimized using PSO algorithm explained in Sects. 3.5 and 3.6. The parameter settings used in the PSO algorithm for this experiment are mentioned in Table 1.

The maximum accuracy achieved using Relu as an activation function was **98.58%** at 600 neurons in hidden layer, whereas Sigmoid achieved a maximum accuracy of **98.82%** at 400 neurons in hidden layer.

The complete results of both the experiments are described in Table 2, and their comparison is visualized in Fig. 6.

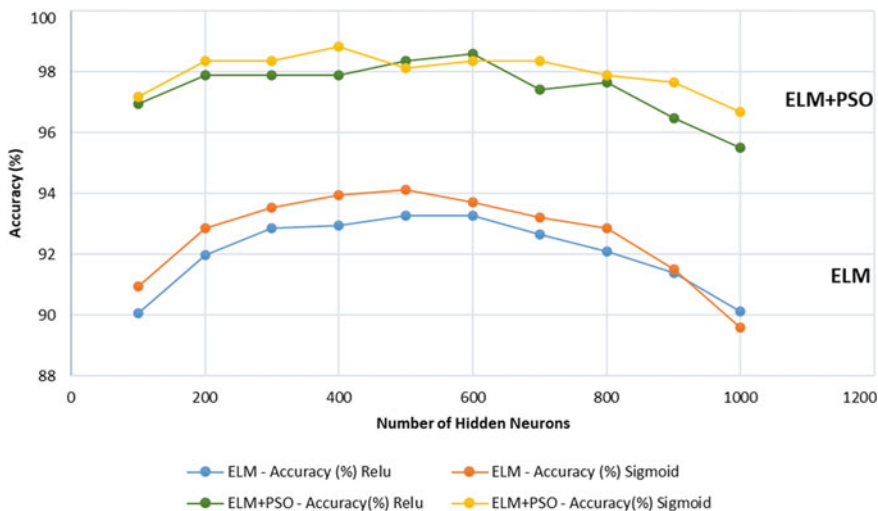


Fig. 6 Comparison of accuracies for various classifiers with different parameters

5 Conclusion and Future Work

Malware poses a serious threat to Android applications in today's world because data security and data privacy are of important concern to users. To tackle this problem, in this research, we came up with a modified approach to classify malicious applications from benign ones using machine learning techniques and optimized it with swarm intelligence. We extracted a total of 15,949 features which were used to create the dataset. After applying feature selection techniques, we reduced the dataset to achieve better results using our proposed model. Extreme learning machine (ELM) was used to classify the applications, which is a native method that provided us average results. Particle swarm optimization (PSO) was used to improve the performance of the classifier which gave us a maximum accuracy of **98.82%** which is far superior than the traditional algorithms. The proposed idea gives us a fine-tuned model which can tackle the problem efficiently and can be of great help to expert users.

For further enhancements, we plan to upgrade this model using other machine learning and deep learning techniques and aim to optimize it further using different swarm intelligence algorithms. Work done in this research is of static analysis, and we plan to update our dataset by adding new features extracted through dynamic analysis.

References

1. Lashkari, A.H., Kadir, A.F.A., Taheri, L., Ghorbani, A.A.: Toward developing a systematic approach to generate benchmark android malware datasets and classification. In: Proceedings—International Carnahan Conference on Security Technology 2018-Oct 50 (2018). <https://doi.org/10.1109/CCST.2018.8585560>
2. Demertzis, K., Iliadis, L.: Bio-inspired hybrid intelligent method for detecting android malware. *Adv. Intell. Syst. Comput.* **416**, 289–304 (2016). https://doi.org/10.1007/978-3-319-27478-2_20
3. Yuan, Z., Lu, Y., Xue, Y.: Droiddetector: Android malware characterization and detection using deep learning. *Tsinghua Sci. Technol.* **21**, 114–123 (2016). <https://doi.org/10.1109/TST.2016.7399288>
4. Su, X., Zhang, D., Li, W., Zhao, K.: A deep learning approach to android malware feature learning and detection. In: Proceedings—15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Processing, pp. 244–251 (2016). <https://doi.org/10.1109/TrustCom.2016.0070>
5. Shamshirband, S., Chronopoulos, A.T.: A new malware detection system using a high performance-ELM method. *arXiv* (2019)
6. Hutchison, D., Mitchell, J.C.: Advances in neural networks—ISNN 2015. In: Theoretical Computer Science, pp. 166–173 (2015). <https://doi.org/10.1007/978-3-319-25393-0>
7. Sandeep, H.R.: Static analysis of android malware detection using deep learning. In: 2019 International Conference on Intelligent Computing and Control Systems, ICCS, pp. 841–845 (2019). <https://doi.org/10.1109/ICCS45141.2019.9065765>
8. Suleiman, Y., Sezer, S., McWilliams, G., Muttik, I.: New android malware detection approach using Bayesian classification. In: Proceedings—International Conference on Advanced Information Networking and Applications, AINA, pp. 121–128. <https://doi.org/10.1109/AINA.2013.88>
9. Wu, D.J., Mao, C.H., Wei, T.E., et al.: DroidMat: android malware detection through manifest and API calls tracing. In: Proceedings of the 2012 7th Asia Joint Conference on Information Security, Asia JCIS, pp. 62–69 (2012)
10. Tallarida, R.J., Murray, R.B.: Chi-square test. In: *Manual of Pharmacologic Calculations*, pp. 140–142. Springer, New York, New York, NY (1987)
11. Huang, G., Zhu, Q.Y., Siew, C.K.: Extreme learning machine: theory and applications. *Neurocomputing* **70**, 489–501 (2006). <https://doi.org/10.1016/j.neucom.2005.12.126>
12. Marini, F., Walczak, B.: Particle swarm optimization (PSO): a tutorial. *Chemom. Intell. Lab. Syst.* **149**, 153–165 (2015). <https://doi.org/10.1016/j.chemolab.2015.08.020>
13. Ratnawati, D.E., Marjono, Widodo, Anam, S.: Comparison of activation function on extreme learning machine (ELM) performance for classifying the active compound. In: AIP Conference Proceedings, p 140001. American Institute of Physics Inc. (2020)

Asymmetric Image Cryptosystem Based on Chaotic Zone Plate Phase Mask and Arnold Transform



Mehak Khurana and Hukum Singh

Abstract An optical asymmetric cryptosystem built on chaotic zone plate phase mask (CZPPM) has been proposed. Here the pixels of an image are shuffled by employing Arnold transform (AT^{ω}) and is then modulated with the CZPPM featuring in the gyrator Transform domain (GT). This increases randomness and adds chaotic parameters that make the system highly secure. The proposed system strengthens the security of the cryptosystem and does not permit the attacker to retrieve the initial image without the expertise of keys. The robustness of the projected cryptosystem has been investigated and validated based on an extra degree of freedom by simulating on MATLAB 9.9.0 (R2020b), and investigational outcomes have been shown to emphasize the efficacy of the algorithm.

Keywords Fresnel zone plate • Chaotic phase mask • Arnold transform • Gyrator transform

1 Introduction

With substantial innovations in transmission and information processing technologies, it has become a challenge to convey the information with security. An optical $4f$ system of DRPE in Fourier domain proposed by Refregier and Javidi was a great accomplishment in this arena in 1995 [1]. This set off the path for many researchers for constructing other cryptosystem centered on DRPE with superior security and elevated noise diminution. These systems were still exposed to many attacks known as known plaintext attack (KPA) [2, 3], chosen plaintext or ciphertext attack (CPA, CCA), etc. [4] An idea has been taken in the direction to

M. Khurana (✉)

Department of Computer Science, The NorthCap University, Gurugram, India

e-mail: mehakkhurana@ncuindia.edu

H. Singh

Department of Applied Sciences, The NorthCap University, Gurugram, India

e-mail: hukumsingh@ncuindia.edu

model an asymmetric system [5] that deliver solution to insecure transmission concern and make it resilient from numerous attacks by boosting the randomness and improving chaotic mask key parameters.

2 Key Generation: Chaotic Zone Plate Phase Mask

Chaotic random phase masks (CRPM) [6] are used to increase randomness and to add chaotic parameters which makes the system highly secure in terms of private keys. Logistic map is one dimension (1D) non-linear chaotic maps and is used to generate the randomness in the CRPM. It can be expressed [7, 8].

$$x_{n+1} = px_n(1 - x_n) \quad (1)$$

It is iterated n times. Where p is bifurcation parameter and lies between $0 < p < 4$, x_0 is an initial value and $x_n \in [0, 1]$ is an iterative value where n varies from 0 to $M \times N$. M and N are size of a chaotic random mask in pixels. The 1D sequence $X = x_1, x_2, x_3, x_4, \dots, x_{M \times N}$ that is produced by Eq. (1) is rearranged into 2D matrix as $Y = y_{ij}$, where i varies from $\{1, 2, \dots, M\}$ and j varies from $\{1, 2, \dots, N\}$ and $y_{ij} \in (0, 1)$. CRPM a 2D matrix is expressed as

$$\text{CRPM}(x, y) = \exp(i2\pi y_{ij}(x, y)) \quad (2)$$

The Fresnel lens is built on quadratic phase change and the efficacy of zone plates. It is given [3] by

$$L_{\lambda, f}(r) = \exp(-i\pi r^2 / \lambda f) \quad (3)$$

where r is the lens radius, f is the focal length, and λ is the wavelength of incident light. Now, CZPPM(x, y) is obtained by multiplying above two functions $L_{\lambda, f}(r)$ and CRPM(x, y), i.e., Equation (1) and (2) and can be stated as

$$C(x, y) = \exp\left\{i\pi \left[2y_{ij}(x, y) + \frac{r^2}{\lambda f}\right]\right\} \quad (4)$$

3 Proposed Cryptosystem

Asymmetric encryption technique built on CZPPM and AT^o [9, 10] is proposed in this paper. The AT^o scrambles the image $I(x, y)$ of size $M \times M$ by shuffling the pixels arbitrarily as in Eq. (5). Then the obtained result is transformed in gyrator domain [10], and phase is truncated to produce $G(u, v)$ as in Eq. (6). The encrypted

image is generated by multiplying $G(u, v)$ with arbitrary phase mask in gyrator domain and further truncating its phase as in Eq. (7). The CZPPM and AT^ω applied through encryption operates as supplementary key because it comprises number of parameters as well as expands the randomness which further enhances the security.

$$I(x', y') = AT^\omega(I(x, y)) \times C_1(x, y) \quad (5)$$

$$G(u, v) = PT[GT^\alpha(I(x', y'))] \quad (6)$$

$$E(x, y) = PT[GT^{-\beta}[G(u, v) \times C_2(x, y)]] \quad (7)$$

Two decryption keys DK_1 and DK_2 were generated in the process where amplitude truncation is performed as shown in Eqs. (8) and (9)

$$DK_1 = AT[GT^\alpha(I(x', y'))] \quad (8)$$

$$DK_2 = AT[GT^{-\beta}[G(u, v) \times C_2(x, y)]] \quad (9)$$

The current graph of the planned encryption stated is displayed in Fig. 1.

The decipherment procedure is the reversal process of the encryption which retrieves the original image $I(x, y)$. Following are the equations to decipher the encoded image $E(x, y)$.

$$G(u, v) = [IGT^{-\beta}[E(x, y) \times DK_2] \times C_2^*(x, y)] \quad (10)$$

$$I(x', y') = IGT^\alpha[G(u, v) \times DK_1] \times C_1^*(x, y) \quad (11)$$

$$I(x, y) = AT^\omega(I(x', y')) \quad (12)$$

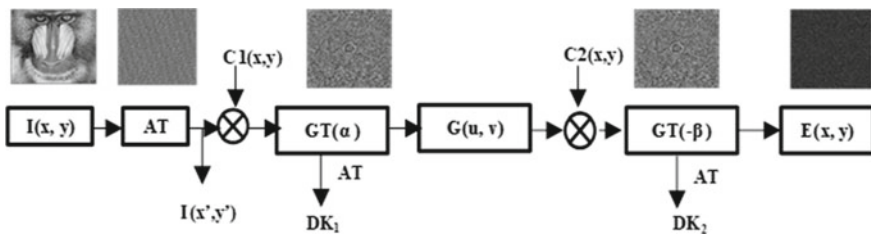


Fig. 1 Flow graph for proposed encryption scheme

4 Simulations Results

This paper demonstrates the statistical analysis and simulation results verifies the sensitivity of the indicated procedure and reveals that it accomplishes superior performance of recuperating a good superiority image. Findings also confirms the protection assessment based on correlation coefficient, noise attack, and key sensitivity. Contemplate initial image of baboon with size 256×256 .

For simulation values use are $p = 3.96$, $x_0 = 0.35$, $\lambda = 6328 \text{ \AA}$, $f = 200 \text{ mm}$, $\omega = 5$ and orders of GT are $\alpha = 0.4\pi$ and $\beta = 0.7\pi$. Figure 2 shows the CZPPM key generated from CRPM and Fresnel zone plate (FZP).

4.1 Statistical Analysis

For statistical analysis, entropy [11] of the image has been analyzed, and the obtained value for baboon image is 6.319 which is close to standard value that guarantees failure of information is nearby zero. The information is homogenously scattered, and it does not deliver any valuable information to the attacker. It can be confirmed from the value obtained above that the projected system is extremely efficient.

Peak signal to noise ratio (PSNR) [12] achieved 23 dB after first level of phase retrieval and 28 dB attained after the second level of phase retrieval.

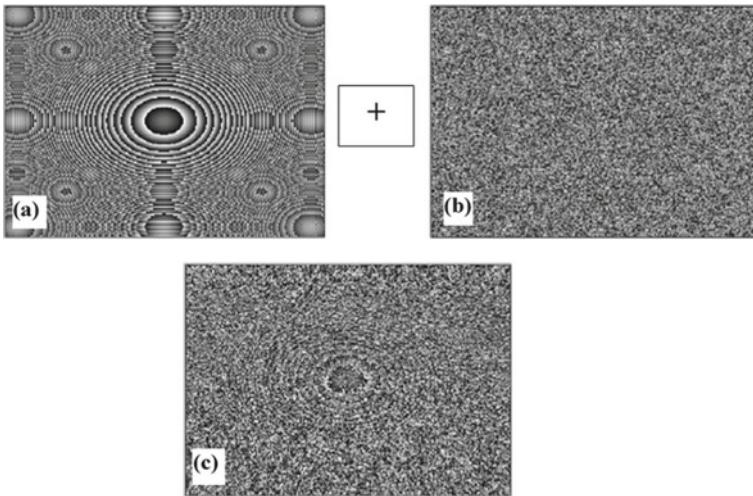


Fig. 2 **a** Fresnel zone plate, **b** chaotic random phase masks, **c** chaotic zone plate phase mask

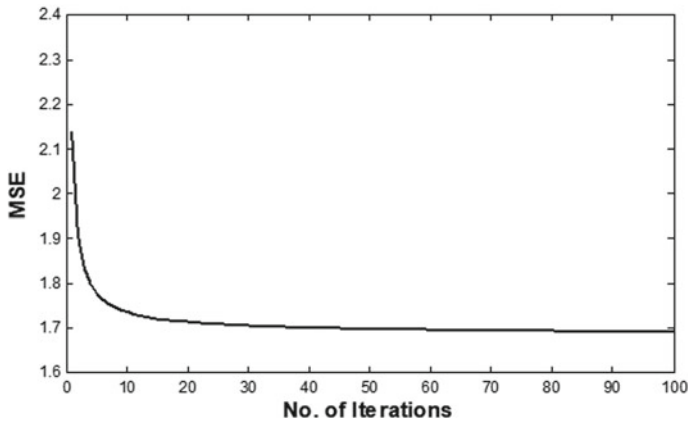


Fig. 3 MSE versus number of iteration graph

4.2 Performance Analysis

The mean square error (MSE) [13] determined for baboon image is 5.6346×10^{-22} . Figure 3 presents the number of iterations versus MSE. Here, MSE drops with the increase in number of iterations and after 50 iterations, MSE becomes constant therefore image randomization stabilizes.

4.3 Robustness Analysis

The proposed algorithm is verified against occlusion attack [14, 15] where the encrypted image has been occluded for different sizes, but the images are still visible from human eye till 75% which proves the system is robust. 45% and 70% occluded encrypted images and its retrieved images are presented in Fig. 4.

4.4 Robustness Analysis

This system has been investigated against KPA, CPA, and special attack to verify its strength. Sets of initial and cipher images have been picked to uncover the authentic key, the erroneous value of parameter headed to incorrect generation of key. To verify the conjunction of the iteration procedure, MSE versus iterations are employed to recover the decryption keys. It can be viewed from MSE plot that decipherment key cannot be recovered even with large iteration number as shown in Fig. 5.

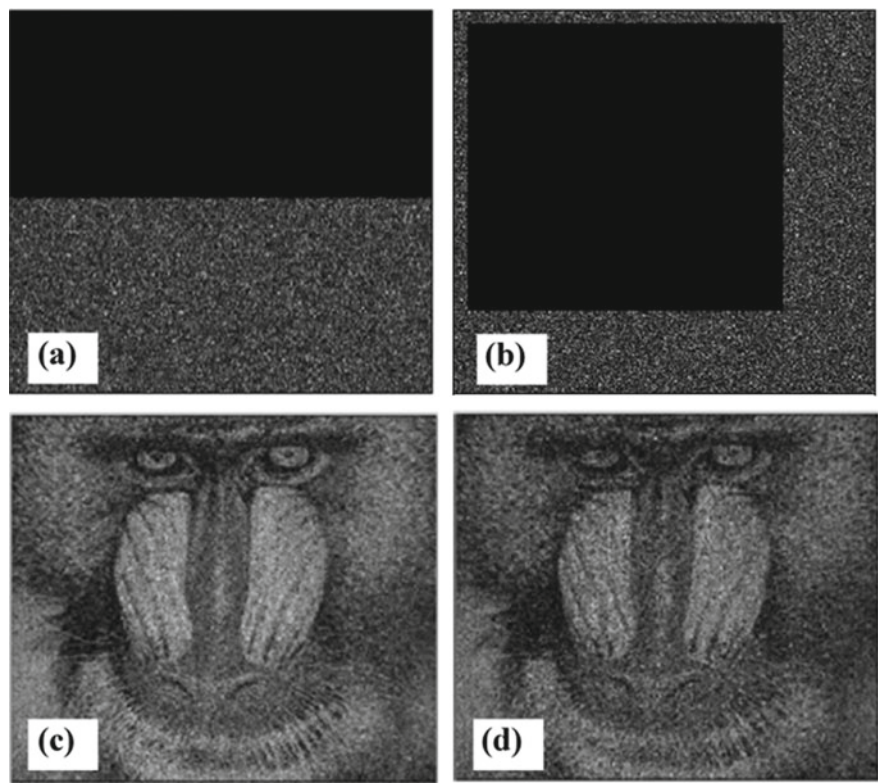


Fig. 4 **a** 45% occluded encoded image, **b** 70% occluded encoded image, **c** recovered image after 45% of occlusion, **d** recovered image after 70% of occlusion

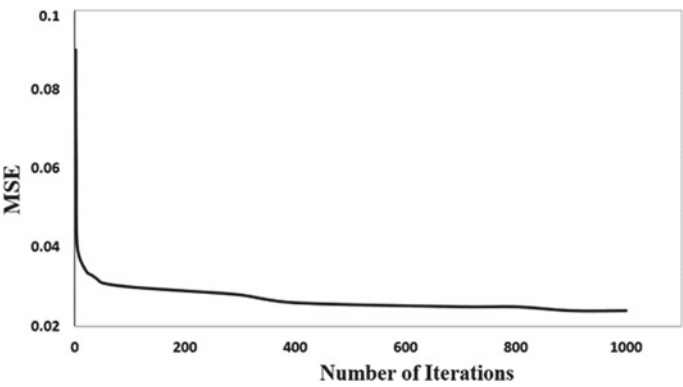


Fig. 5 MSE plot versus number of iterations for decipherment key generation with proposed scheme for 1000 iterations

5 Conclusion

The proposed asymmetric cryptosystem improves the security of the scheme as chaotic mask shifts the phase of the retrieved output and scrambling creates dispersion in the system. The introduced masking accomplishes superior execution of PSNR, MSE, occlusion, and noise as equated to existing systems. The CZPPM is further protected and cannot recapture initial image without the knowledge of all the parameters utilized for producing key. Experimental result reveals the viability and robustness of asymmetric cryptosystem.

References

1. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**(7), 767–769 (1995)
2. Peng, X., Zhang, P., Wei, H., Yu, B.: Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **31**(8), 1044–1046 (2006)
3. Gopinathan, U., Monaghan, D.S., Naughton, T.J., Sheridan, J.T.: A known-plaintext heuristic attack on the Fourier plane encryption algorithm. *Opt. Express* **14**(8), 3181–3186 (2006)
4. Zhang, C., Liao, M., He, W., Peng, X.: Ciphertext-only attack on a joint transform correlator encryption system. *Opt. Express* **21**(23), 28523–28530 (2013)
5. Qin, W., Peng, X.: Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **35**(2), 118–120 (2010)
6. Abuturab, M.R.: Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition. *Opt. Laser Tech.* **98**, 298–308 (2018)
7. Barrera, J.F., Henao, R., Torroba, R.: Optics encryption method using toroidal zone plates. *Opt. Commun.* **248**, 35–40 (2005)
8. Liansheng, S., Bei, Z., Xiaojuan, N., Ailing, T.: Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. *Opt. Express* **24**(1), 499–515 (2016)
9. Chen, L., Zhao, D., Ge, F.: Image encryption based on singular value decomposition and Arnold transform in fractional domain. *Opt. Commun.* **291**, 98–103 (2013)
10. Liu, Z., Chen, H., Liu, T., Li, P., Xu, L., Dai, J., Liu, S.: Image encryption by using gyrator transform and Arnold transform. *J. Electron. Imaging. Proc. SPIE.* **20**(1), 013020 (2011)
11. Khurana, M., Singh, H.: A spiral-phase rear mounted triple masking for securing optical image encryption based on gyrator transform. *Recent Patents Comput. Sci.* **12**(2), 80–94 (2019)
12. Khurana, M., Singh, H.: Two-level phase retrieval in fractional Hartley domain for secure image encryption and authentication using digital signatures. *Multimedia Tools Appl.* **79**, 13967–13986 (2020)
13. Wang, S., Meng, X., Yin, Y., Wang, Y., Yang, X., Zhang, X., Peng, X., He, W., Dong, G., Chen, H.: Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform. *Opt. Lasers Eng.* **114**, 76–82 (2019)
14. Liansheng, S., Xiao, Z., Chongtian, H., Ailing, T., Krishna Asundi, A.: Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. *Opt. Lasers Eng.* **113**, 29–37 (2019)
15. Singh, H., Khurana, M.: An asymmetric optical cryptosystem of double image encryption based on optical vortex phase mask using Gyrator transform domain. *Recent Patents Comput. Sci.* **13**(3), 672–685 (2020)

Authentication of Digital Media Using Reversible Watermarking



Geeta Sharma, Vinay Kumar, and Kavita Chaudhary

Abstract Digital watermarking is a technique to hide and transmit the data in such a manner that attackers cannot perceive it. The watermarks can be used for authentication, and the creator/owner of the digital data can claim the rights, in case of any dispute. The reversible digital watermarking ensures the reusability of the cover media. In this research paper, we are suggesting a more robust method of watermarking using the combination of LWT-SVD. The digest of the message is generated using MD5 algorithm, and a quantum representation is used as the trap door. The results are measured for the existing quantum technique, LSB quantum watermarking, and the proposed algorithm. We have compared the results for MSE, SSIM, and PSNR in the analysis section. The improvements can be seen in the results persistently.

Keywords Digital watermarking • DWT • Singular value decomposition • Quantum representation

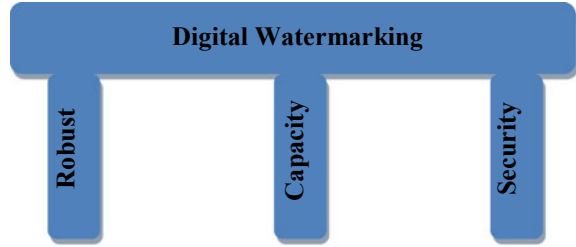
1 Introduction

Multimedia, Internet of things and the Web of digital devices around us are rapidly generating digital data. This data need to be protected in such a manner that no unintentional receivers can even perceive the very presence of the data. Digital watermarking provides a strong method for information hiding as data is stored in the cover in non-perceivable manner and the process can be reversed by the intended users with security information provided by the sender. A digital water-

G. Sharma (✉)
IP University, Delhi, India
e-mail: geeta.sharma@jimsindia.org

V. Kumar
NIC, Delhi, India

K. Chaudhary
Jagannath University, Jaipur, India

Fig. 1 Three pillars

marking technique has three major parameters that are robustness, capacity, and security as in Fig. 1. Robustness indicates that any kind of attacks will not affect the watermark much. Capacity is the maximum information that the cover can hold. Security, as name suggests, refrains the unauthorized access. Another important parameter is reversibility of the watermarking process that allows the use of cover image at the receiver's end.

The lifting system is an efficient way of implementing wavelet filtering, which also increases the wavelet transformation process speed. The prediction stage of the lifting scheme for the Haar transform predicts that the each odd element will be equal to its even element. The dissimilarity between the even value (the predicted element) and the original value of the odd value restores an odd element. The basics of the work is already discussed in [1].

2 Literature Review

Digital watermarking technique/algorithms can be characterized on the basis of many factors. The cover that is used for the information hiding can be text, image, sound, video, etc. A watermark can be visible or invisible, according to capacity of human eye to perceive. An invisible watermark can be fragile and robust both. Since fragile means imperceptible, it can be further divided into fragile and semi-fragile categories. The process of data hiding can be reversible and irreversible. In reversible data hiding, the cover can be used by the receiver after extracting the watermark. Watermarking is divided into two main groups: spatial domain and transform domain. Now, we will discuss few papers that helped in understanding and formed a base of the research.

For image steganography, the suggested technique is a mixed method that combines discrete wavelet transform (DWT) along with singular value decomposition (SVD) and lifting wavelet transform (LWT) techniques.

2.1 Discrete Wavelet Transform

In digital images, the discrete wavelet transform is used. There are several DWTs accessible. The most acceptable one should be used, depending on the application. Integer wavelet transformation can be used to cover text details. When DWT is applied to an image, it divides it into four sub-bands: LL, HL, LH, and HH. The first section (LL) consists of the most critical features. So if the data is hidden in the LL section, the compression or other changes do not affect the stego image to great extent. In the stego picture, distortion can sometimes be created and now other sub-bands can be used. The expanded function is discrete (i.e., a number sequence), and the resultant coefficients are named discrete wavelet transformation (DWT).

“Thakkar and Srivastava” [2]: “A blind image watermarking technique based on DWT and SVD was developed in this paper. The DWT technique was used in the medical image's Region of Interest. On the low-frequency sub-band LL-ROI, the program Block-SVD was used to obtain separate singular matrices. A pair of elements with identical values was discovered using either the left singular value matrix of all of the selected blocks. Using some criterion to embed a bit with watermark information, their properties of these pairs are changed. In order to achieve that imperceptibility of the medical image with watermark material, acceptable thresholds were selected.”

“Zear et al.” [3]: “Throughout this study, an algorithm with multiple watermarking based on discrete wavelet transformations (DWT), discrete cosine transformation (DCT), and singular value decomposition (SVD) was proposed for healthcare applications. The suggested application uses a total of three watermarks: a medical ‘Lump picture watermark,’ a code for the doctor’s signature, and the patient’s diagnosis details as text watermarks for identity authentication. Back Propagation Neural Network (BPNN) was used on both the derived watermark i.e. image format and the image watermark to reduce the potential impact on the watermarked image and to increase the image watermark’s robustness.”

2.2 Quantization-Based Watermarking

In 1984, Bennett and Brassard presented the first quantum key distribution protocol. Since then it was used in many theories-based and/or practical research. In the traditional method, a computer stores the pixel representation of the image with the necessary color information and the corresponding coordinates of each point. The same method was used by Shahrokh and Mosayeb [4], and the picture information is converted into the quantum state. The basic unit of quantum information is known as quantum bits (qubits).

Nezhadarya et al. [5]: “This paper proposed a robust picture watermarking framework based on quantization, referred to as quantization-based authentication path watermarking (GDWM), with a focus on uniform gradient vector direction

quantization. The watermark bits become embedded in GDWM through quantifying vector angles and critical gradient vectors on many wavelet scales. The current technique had the following key features: (1) increased invisibility of both embedded watermarks, owing to the fact that watermarks were embedded in major gradient vectors, (2) strength against amplitude scaling attacks, owing to the fact that watermarks were embedded across the entire gradient vector angles, and (3) increased watermarking capability, owing to the method's ability to allow multiple-scale embedding. Throughout recognition of both the discrete wavelet transform (DWT) coefficients, that gradient vector at one pixel was expressed. The DWT coefficients were updated to quantize that gradient direction mostly on resultant relationship here amongst changes during the coefficients or the modification in the gradient direction."

Sachdeva and Kumar [6]: "Digital images are most prevalent cover files used only for steganography would those be. In this article, a current format of steganography called JMQT were introduced based on an updated table of quantization. Its method of steganography has been contrasted with the JPEG-JSteg method of steganography. Two output parameters are being contrasted, namely capability and stego scale. Existing customers and stego scale represents the amount. Therefore, JMQT offers better power and JPEG-JSteg offers better stego-size."

2.3 Singular Value Decomposition

Through the discernment of image processing, a picture can be interpreted as a matrix of non-negative scalar entries. The SVD method for decomposing a rectangular matrix "A" into an orthogonal matrix U, a diagonal matrix S, and transposing an orthogonal matrix V is an efficient linear algebra numerical analysis method. Through image processing, SVD decomposes a given image A of size MN as decomposition (SVD) of A, which is interpreted as a matrix of non-negative scalar entries. The SVD method for decomposing a rectangular matrix "A" into an orthogonal matrix U, a diagonal matrix S, and transposing an orthogonal matrix V is an efficient linear algebra numerical analysis method. A given image A of size MN is decomposed as decomposition (SVD) of A using SVD.

"Ali et al." [7]: "By analyzing multiple scaling variables in image watermarking, a Differential Evolution (DE) algorithm has been used to balance the trade-off between robustness and imperceptibility in this article. To begin, the original image was divided into blocks, which were then transformed into discrete cosine transformation domains (DCT). The DC coefficients from each block were used to create a low-resolution approximation image, which was then subjected to the Singular Value Decomposition (SVD) algorithm. After that, the watermark was merged by replacing the singular values of both watermarks with the singular values of both watermarks."

“Du et al.” [8]: “In order to ensure the copyright of a color image, a robust image watermarking approach based on ‘Tensor-Singular Value Decomposition (T-SVD)’ was proposed. The color image was created by transforming the third-order tensor with T-SVD to produce three orthogonal tensors and a diagonal tensor in order to establish clear associations between the three RGB color image channels. Because the main energies of that color picture are contained in the diagonal tensor, robustness can be used and the watermark can be embedded. Second, three color image channels were decomposed into four sub bands using discrete wavelet transformation (DWT), but only the LL sub band of each channel was used to create an approximate image. In addition, the approximation picture was divided into non-blocks of 4×4 dimensions, and the first, second, and third diagonal matrices were calculated using TSVD from each block. Finally, singular value decomposition was used to decompose the grayscale watermark (SVD).”

3 Method Proposed

Based on the standard existing algorithm, this proposed algorithm is similar to performing. The embedding is performed on the images, generally a loss less file format is used. The DWT method is combined with the benefits of SVD for embedding the image. The quantum representation is used as the trap door to fetch the watermark without changing the picture information of the cover. So the embedding ability and image quality are enhanced effectively by this algorithm. The ability for embedding is doubled over and the graphical output is greatly enhanced. The recommended reversible image watermarking algorithm largely helps increase the embedding rate of the watermark while retaining better visual quality than other algorithms.

3.1 Embedding Algorithm

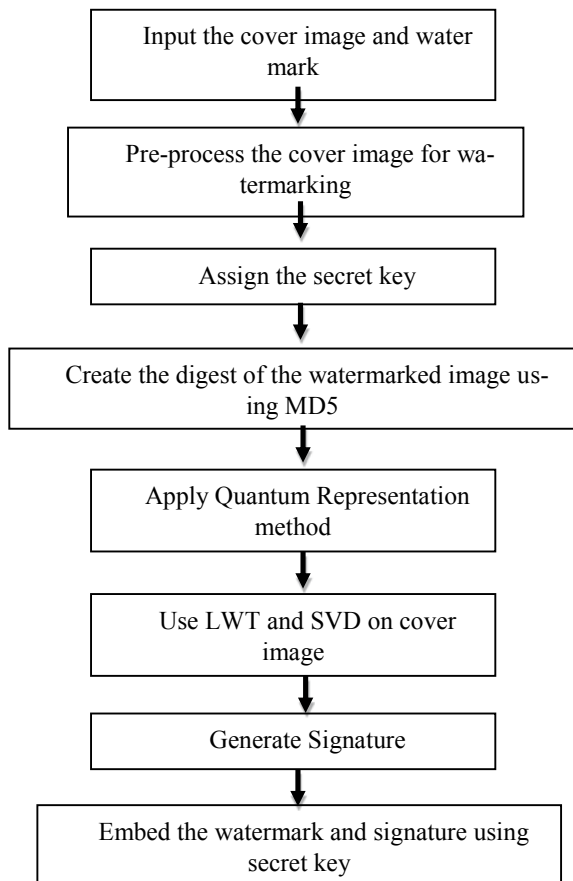
This function extracted the watermark without damaging the cover image, using the cover image, watermark/hidden message, key, signature as an input. The flow of the function is explained in Fig. 2.

Step 1: Import cover image and watermark (image).

Step 2: For each channel apply following to the cover image:

- (a) Resize image to 512×512 using bilinear algorithm.
- (b) Assign a random key (secret key).
- (c) Get the non-negative integer seed key.
- (d) Assign 10 to QR block size.

Fig. 2 Flowchart of the embedding algorithm



Step 3: Apply quantum representation on secret image using MD5.

Step 4: Convert watermark to B&W and apply following operations on watermark:

- (a) Decompose the watermarked image or signal into four sub-bands, using Haar wavelet.
- (b) Apply DWT on LL band up to fourth level.
- (c) Also perform single value decomposition (SVD) to the high-frequency band (HH) of the watermark.

Step 5: Also decompose the watermarked image using SVD and replace values of HH band with SV of the watermark.

Step 6: Generate signature using values from watermark and key, and then embed the signature in LL band of the cover.

Step 7: After getting the updated HH band of cover image, finally acquire the watermarked image by applying inverse LWT.

3.2 Extraction Algorithm

Step 1: Import watermarked image (cover image + watermark embedded as single unit).

Step 2: Apply following operations on the watermarked image:

- (a) Convert the watermarked image into four sub-bands, using Haar wavelet.
- (b) Apply LWT on LL band up to fourth level.
- (c) Also perform single value decomposition (SVD) to the high-frequency (HH) band.

Step 3: Generate signature using matrices of the watermarked image.

Step 4: Reconstruct the signature from the fourth level LL and HH band.

Step 5: Compare these signatures and follow these steps if the user is authenticated, else the extraction process should be stopped:

- (a) Apply SVD to the HH band.
- (b) Get the singular values from the HH band.
- (c) Now, get the watermark image using orthogonal matrices and singular values.

Step 6: The watermark and the cover image both are in useable forms.

4 Analysis

Authentication and copyright management are two of the most common uses for reversible digital watermarking. In the field of image steganography, many studies have been conducted using the discrete wavelet, lifting scheme, and singular value decomposition. During our research, we examined the outcomes of various variations before settling on the most promising technique. We have taken into account the results of quantum steganography, LSB quantum watermarking, and LWT-QR-MD5 for this analysis.

The image Fig. 4 is clearly showing the high correlation between the input image and the resultant image. This high correlation indicates that embedding of the watermark to the cover image is not making much difference in the actual image that further ensures the better imperceptibility. As we discussed earlier, if a watermark is not able to perceive easily than it automatically reduce the number of attacks. It is also visible in the histogram of the image in Fig. 3. Now, we will use the algorithm on the basic three images Lena, Barbara, and Peppers and see the results.

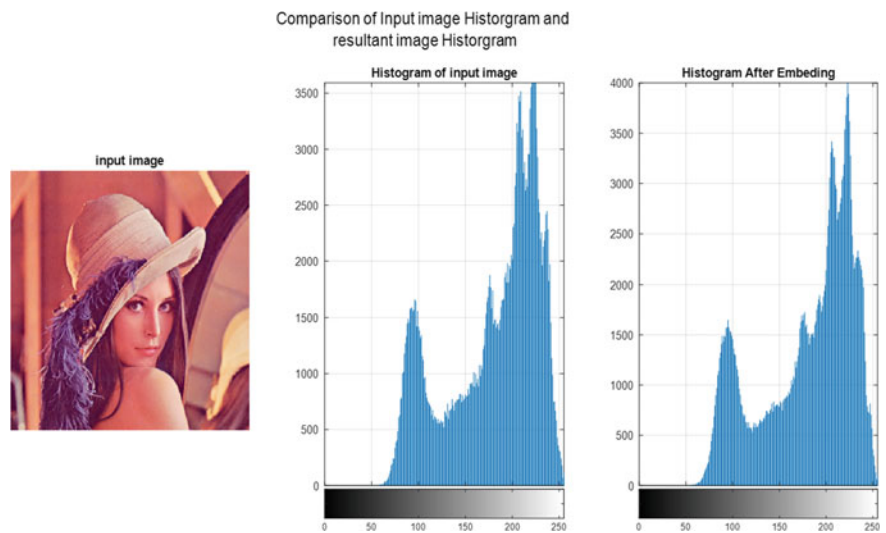


Fig. 3 Comparison of original and resultant image “Lena”

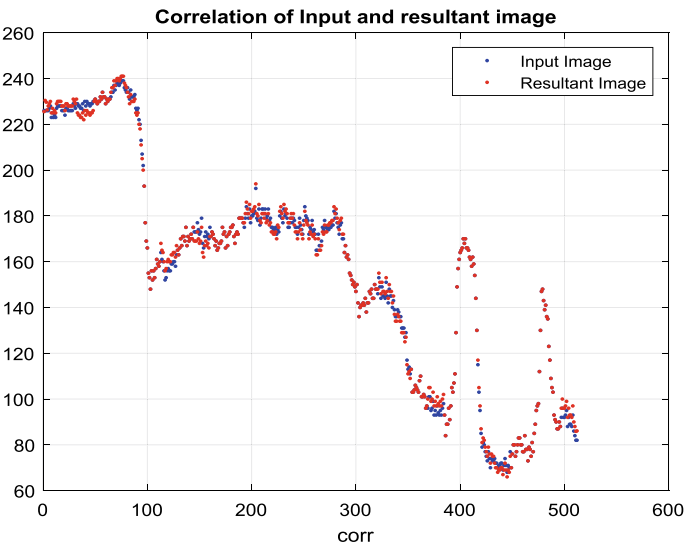


Fig. 4 Depiction of correlation

4.1 PSNR

It is used to check and compute the strength of the signal [9]. Figure 5 is showing the PSNR results after improvement in absolute term and percentage have been

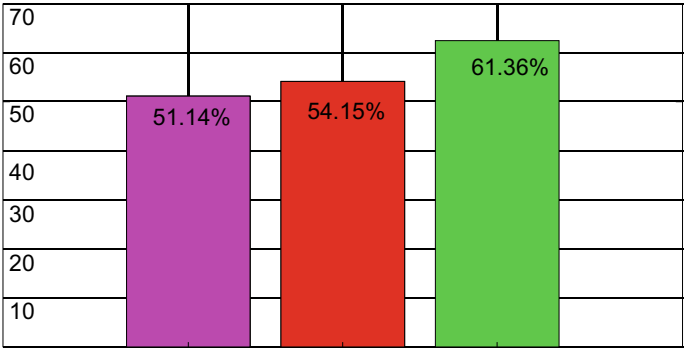


Fig. 5 Mean value of PSNR

Table 1 PSNR results

Image	Quantum steganography	LSB quantum watermarking	LWT-QR-MD5	PSNR improvement	% Improvement
Lena	51.1789	54.24	62.69	8.44	15.6
Barbara	51.0889	54.10	59.94	5.85	10.8
Peppers	51.1549	54.13	61.44	7.31	13.5
Average	51.1409	54.156	61.356	7.2	13.3

found that mean value of the PSNR applied on the various images like Lena, Barbara, and Peppers. The comparison was made for the three algorithms, i.e., quantum steganography, LSB watermarking, and the proposed algorithm. If we look at the average improvement of the resultant images, there is a clear increase of more than 13% that is a significant improvement (Table 1).

4.2 MSE

It is used to see how closely the original image and the watermarked image resemble each other [10]. This discrepancy is then squared, according to Wikipedia. Y_i denotes the pixel position in the original image and Y_i denotes the pixel value in the watermarked image at the same location. The MSE value is then computed by multiplying the difference by two [11]. Table 2 presented the mean square error results after applied proposed algorithm with LSB quantum watermarking, LWT-QR-MD5, MSE improvement, % improvement with three images. It was found that image Lena was showed that LSB quantum watermarking was 24.69, LWT-QR-MD5 8.14, MSE improvement 16.55, and it increased up to 67.02%, respectively (Fig. 6).

Table 2 MSE results

Image	LSB quantum watermarking	LWT-QR-MD5	MSE improvement	% Improvement
Lena	24.69	8.14	16.55	67.02
Barbara	25.50	11.75	13.74	53.91
Peppers	25.32	17.09	8.24	32.52
Average	25.17	12.32	12.84	51.15

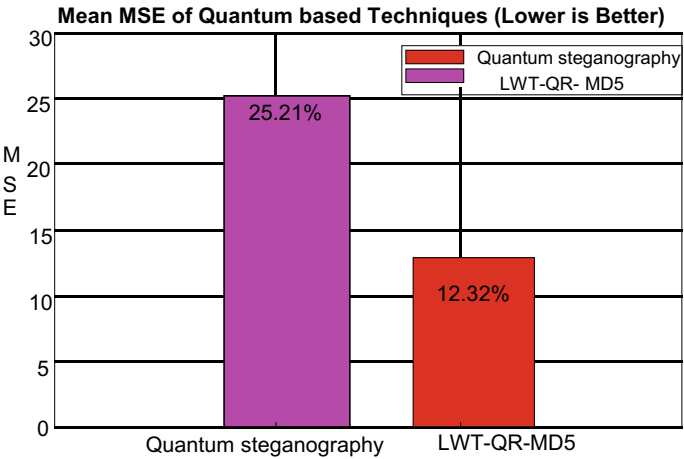


Fig. 6 Mean of MSE

It was found that image Barbara was showed that LSB quantum watermarking was 25.50, LWT-QR-MD5 11.75, MSE improvement 13.74, and it increased up to 53.91%, respectively. It was found that image Peppers was showed that LSB quantum watermarking was 25.32, LWT-QR-MD5 17.09, MSE improvement 8.24, and it increased up to 32.52%.

4.3 SSIM

Structural similarity (SSIM) was used to calculate the similarity between the filtered residual images and original images [12]. From Table 3 presented, we can observe the improvements in SSIM improvements. The three images were observed under LSB quantum watermarking, LWT-QR-MD5, SSIM improvement, and % improvement. It was found that Lena was showed that LSB quantum watermarking was 81.53, LWT-QR-MD5 93.71, SSIM improvement 12.18, and it increased up to 14.94%, respectively. It was found that Barbara was showed that LSB quantum watermarking was 84.33, LWT-QR-MD5 95.83, SSIM improvement 11.50, and it

Table 3 SSIM results

Image	LSB quantum watermarking	LWT-QR-MD5	SSIM improvement	% Improvement
Lena	81.53	93.71	12.18	14.94
Barbara	84.33	95.83	11.50	13.64
Peppers	82.69	89.88	7.19	8.70
Average	82.85	93.14	10.29	12.29

increased up to 13.64%, respectively. It was found that Peppers was showed that LSB quantum watermarking was 82.69, LWT-QR-MD5 89.88, SSIM improvement 7.19, and it increased up to 8.70%, respectively.

5 Conclusion and Future Scope

Watermarking is typically used to include evidence of digital data control. Generally, that is done by integrating certain copyright knowledge into digital details. Since it can be found on the World Wide Web for automated tracking of copywrite products. The algorithm suggested is capable of retrieving the secret message without making significant changes to the cover image. For authentication and copyright management, reversible automated watermarking is largely utilized. Through the usage of quantum watermarking, LWT-QR-MD5 techniques, this loss less approach ensures the improvement in the existing algorithms.

LWT promises faster computation while consuming less memory. Furthermore, the MD5 algorithm ensures better security and improves the algorithm's robustness against various attacks. In the steg analysis, this reversible watermarking technique produces better results. In future, we are planning to apply the same algorithm on more images and will also execute some attacks on the watermarked image.

References

1. Sharma, G., Kumar, V.: Review of different parameters for digital reversible watermarking. *Int. J. Res. Anal. Rev.* (2018). E-ISSN 2348–1269, P- ISSN 2349–5138
2. Thakkar, F.N., Srivastava, V.K.: A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools Appl.* **76**(3), 3669–3697 (2017)
3. Zear, A., Singh, A.K., Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia Tools Appl.* **77**(4), 4863–4882 (2018)
4. Shahrokh, H., Mosayeb, N.: A Novel LSB based quantum watermarking. *Int. J. Theor. Phys.* Springer Science + Business Media New York (2016)

5. Nezhadarya, E., Wang, Z.J., Ward, R.K.: Robust image watermarking based on multiscale gradient direction quantization. *IEEE Trans. Inf. Forensics Secur.* **6**(4), 1200–1213 (2011)
6. Sachdeva, S., Kumar, A.: Colour image steganography based on modified quantization table. In: 2012 Second International Conference on Advanced Computing and Communication Technologies, pp. 309–313. IEEE (2012)
7. Ali, M., Ahn, C.W., Pant, M.: A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik* **125**(1), 428–434 (2014)
8. Du, M., Luo, T., Li, L., Xu, H., Song, Y.: T-SVD-based robust color image watermarking. *IEEE Access* **7**, 168655–168668 (2019)
9. Jadhav, A., Kolhekar, M.: Digital watermarking in video for copyright protection. In: 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), pp. 140–144. IEEE (2014)
10. Lou, D.C., Chou, C.L., Tso, H.K., Chiu, C.C.: Active steg analysis for histogram-shifting based reversible data hiding. *Optics Commun.* **285**(10–11), 2510–2518 (2012)
11. Botta, M., Cavagnino, D., Pomponiu, V.: A modular framework for color image watermarking. *Sig. Process.* **119**, 102–114 (2016)
12. Song, C., Sudirman, S., Merabti, M., Llewellyn-Jones, D.: Analysis of digital image watermark attacks. In: *IEEE CCNC 2010 Proceedings* (2010)
13. Le, P.Q., Ilyyasu, A.M., Dong, F., Hirota, K.: A flexible representation and invertible transformations for images on quantum computers. In: Ruano, A.E., Várkonyi-Kóczy, A.R. (eds) *New advances in intelligent signal processing. Studies in Computational Intelligence*, vol. 372. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-11739-8_9

Automatic Test Case Generation and Fault-Tolerant Framework Based on N-version and Recovery Block Mechanism



Seema Rani and Amandeep Kaur

Abstract A fault is any type of bug or error or failure that occurs in the system when any hardware is failed and requires replacement or strained to reboot or software fails to give the result. System failure occurs when the fault in system is not revealed and corrected in time. Software fault tolerance is the major research area in software development industry. Software fault tolerance enables a system to operate efficiently if any fault exists in the system and makes 011.0210 s a system capable to protect against any type of accidental or malicious destruction of the information in system. Many techniques of fault tolerance and recovery have been proposed in work of literatures in order to ensure efficient working of software. The main objective of this paper is to propose fault-tolerant framework based on N-version and recovery block mechanism for automatic test case generation. Simulation results show that proposed framework improves the reliability in terms of elapsed time, classification accuracy, and mean square error.

Keywords Software testing • Software fault prediction • Software fault tolerance • Software fault tolerance techniques • Real-time systems

1 Introduction

In the specific area of testing software, the main goal is to find the maximum number of faults or failures with the different test cases. The systematic and step-wise recognition of faults or errors with less time and less effort is the main aim of software testing [1]. With the growth and popularity of computer technology, the recent development is inclined to be more intelligent, complex, and automated. Software fault prediction is the process to recognize software modules containing the faults prior to the actual software testing process starts. It is essential to detect early fault prediction. One-third of the faults in software development is to be

S. Rani (✉) · A. Kaur

Computer Science and Engineering Department, Maharishi Markandeshwar University, Ambala, Haryana, India

identified early to minimize the rework. A fault prediction is helpful in developing high-quality software with optimized efforts, time, and cost. It also helps in the maintainability of the software [2]. So there is a requirement of fault tolerance techniques that can handle different types of faults. Fault tolerance is a process where the system tries to work even if numbers of faults exist in the system. To handle these kinds of problems, our research focuses on software fault tolerance. In modern industrial practice, real-time data-based fault detection methods like a prediction of faults have been used [3]. For these types of problems, software fault tolerance is a proficient and competent method. Due to incapability to produce fault-free complex systems, software fault tolerance is the major issue. Software fault tolerance is mainly required in designing of a highly reliable system that can work under undesirable and difficult situations.

The main objective of software fault prediction is to predict where the fault might exist in the future and to quantify the importance of various factors [4]. Software fault tolerance makes a system proficient to work properly under any faulty conditions. It protects the system from any malevolent demolition of information. Software fault techniques can be categorized in two ways: single version and multiversion. Single-version techniques deal with single software, whereas multiversion deals with multiple numbers of versions of the same software to make sure that faults in one version do not cause a system failure. In this research, we compared the N-version and recovery block techniques from multiversion fault-tolerant techniques here. In earlier research, an efficient framework is designed for the automatic generation of test cases and prioritization. The research paper is well-thought-out as Sect. 1 is related to the introduction of the research work. Section 2 deals with the literature review. Section 3 describes software fault tolerance and deals with software fault tolerance techniques. Section 4 describes the proposed software fault-tolerant framework for automatic test case generation. Section 5 shows the simulation results. Section 6 gives the conclusion of the research.

2 Literature Review

D'Ambros et al. [5] compared bug prediction approaches. They compared the explanative and extrapolative power of bug prediction approaches in the form of a public dataset. Chinnaiah and Niranjana [6] projected an approach with an algorithm that provides the best candidate (fault-tolerant) for software having a critical configuration and developed techniques for the frequency of configuration interactions (IFrFT), and characteristics and frequency of interactions (ChIFrFT) to achieve fault tolerance and reliability with minimum cost. Choudhary and Khan [7], with industry data proposed a structure for fault tolerance and validation for the system.

Gao et al. [8] proposed a component analysis method based on enhanced kernel principal by using the theory of indiscernibility and compared conventional techniques for fault prediction. Sumra et al. [9] describe a comparative study of

techniques of software fault-tolerant and surveyed to find out the issues of implementing SFT techniques in a project are: quality items missing, quality of code, project duration, team problem, lack of SFT techniques, skills and training, high cost, duplication, more space, code complexity, critical application, selection algorithm, difficult maintenance, need of SFT, work load, and ambiguous specification of requirements. A solution of some of the issues has also been suggested in this research work, i.e., quality items missing, quality of code, project duration, team problem, lack of SFT techniques, skills and training, high cost, selection algorithm, difficult maintenance, work load, and ambiguous specification of requirements.

Perälä [10] analyzed the probable drawbacks of automatic test implementation and provided an approach to handle and recover bugs that occurred in the system under test (SUT). Rathore and Kumar [11] described the review for software fault tolerance into three classes: fault prediction techniques, software metrics, and data quality which helps to deal with various elements and issues related to the fault prediction process. Alam [12] discussed the development of software fault tolerance techniques and their characteristics. Sharma and Yadav [13] projected a structure for fault prediction in a real-time system which is reliable and validated by using the simulation process.

3 Software Fault Tolerance

Software fault tolerance is a rising and emergent concern for long-run applications. Software fault tolerance makes a system able to function perfectly in any flawed situation and protects the system from any erroneous outputs and the destruction of information [14]. Software fault tolerance is very important in real-time and critical applications like flight control systems, medical systems, etc. So in software testing, researchers try to develop the software fault tolerance system continuously. Despite its popularity, it is extremely difficult to develop fault-free software. Varieties of approaches are proposed for software fault prediction and tolerance [15]. High software reliability and high quality are the main target in the software testing. Software reliability and software quality are the possibility of fault-free software for a specific period and environment. The reliability of any element can be calculated as Eq. (1):

$$\text{Reliability} = \frac{n(t)}{N} = \frac{\text{Failure free elements}}{\text{Numbers of elements at time} = 0} \quad (1)$$

The main purpose of software fault tolerance is to provide an alternate solution to fault problems where fault can be detected and the recovery to normal operation is carried out as internal functions of the system itself. A system cannot be truly fault-tolerant until software fault-tolerant techniques are applied to the system. Almost 60–90% of system failures are recognized as software failures. These

failures can be controlled by applying software fault tolerance techniques that resolve the problems related to cost and time [16]. Software fault tolerance techniques are of two types, i.e., single-version and multiversion techniques. In this work, multiversion techniques, i.e., N-version programming (NVP) and recovery block (RcB) are used. The basic difference between NVP and RcB is the type of decision algorithm used. In NVP decision algorithm, delivering agreement/disagreement decision is implemented whereas in RcB acceptance test specific to the application program is implemented. From the same initial requirements, NVP has defined as an independent generation of $N \geq 2$ software modules, known as versions.

4 Proposed Software Fault-Tolerant Framework for Automatic Test Case Generation

The software fault tolerance concept is very popular these days. The significant growth and application of fault tolerance is an essential and unique architectural attribute of software testing. Nowadays, automated software fault-tolerant techniques are used [17]. The primary function of automation is to reduce the necessity of human intervention.

Automated software fault-tolerant techniques detect the faults in the system without any interaction of the human users. It also provides solutions to these faults and repairs them without human interaction. In the proposed framework, N-version and recovery block software fault-tolerant techniques applied to automated test case generation and prioritization framework using IGA proposed by Rani et al. [18]. With the addition of this software fault tolerance, the proposed framework minimizes the expenditure, to lessen time and minimize the effort for the development of better-quality software.

The existing software fault tolerance technique recovers the software or system from an error and prevents system failure. The key idea is to replace the erroneous state with a stable state. For this N-version and recovery block fault-tolerant techniques are used in the proposed framework. To enhance the reliability, the proposed framework declares an error condition and provides correct output with a very high probability. The proposed framework is compared based on elapsed time, classification accuracy, and mean square error (MSE) here. For all these parameters, the genetic algorithm evaluates the test cases by the program execution with the inputs.

The detailed process of fault tolerance and comparison of both techniques for the proposed framework of automated test case generation and test case prioritization is described in two phases, i.e., training phase, recovery, and classification phases below (Figs. 1 and 2).

```

/*Training Phase- Algorithm*/
Step A: Generating Training Models
1. For each FI in Uploaded File: (i=1:1000 test cases)
a. Measure
i. Cosine Similarity
ii. Soft Cosine Similarity
iii. Cosine + Soft Cosine Similarity (Hybrid)
b. Vary the Similarity Index to create N-versions (N=200)
c. Find the average of N-version's
i. Cosine Similarity
ii. Soft Cosine Similarity
iv. Cosine + Soft Cosine Similarity (Hybrid)
Step B: Training
1. Train The system Model
2. Classify each sample in its accurate class
Step C: Measuring Statistics in Training
1. Calculate elapsed time for the completion of each case
2. Calculate Classification Accuracy
-----* End of Training Phase*-----

```

Fig. 1 Algorithm for training phase

```

/* Recovery and Classification Phase */
Step A: Getting Similarity Metrics
1. For each FI in Uploaded File:
Measure:
i. Cosine Similarity
ii. Soft Cosine Similarity
iii. Cosine + Soft Cosine Similarity (Hybrid)
2. Getting the BASIS bias for applying Clustering and classification:
- The SIMILARITY INDEXES and the SIMILARITY MATRIX be evaluated
Step B: Classification
1. Apply k-means clustering to divide the data in two segments.
2. The basis or the measure in k-means clustering is SIMILARITY INDEX.
3. Calculate MSE(Mean Squared Error) for each group in k-means clustering.
4.  $MSE = 1/n ((\text{Sum}(\text{Ele}) * \text{Group1} - \text{Sum}(\text{Ele}) * \text{Group2})^2)$ 
Where n: is the total number of calculated similarity
5. if(MSE_group1 > MSE_group2)
{Classify it as Faulty Class- Group 1}
Else{Classify it as Faulty Class- Group 2}
Step C: Training and Calculating Metrics
1. For each Group in each cluster
i. Train
ii. Classify and Evaluate Class Accuracy
iii. Calculate Elapsed Time

```

Fig. 2 Algorithm for recovery and classification phase

5 Simulation Results

To appraise the performance, the proposed framework is implemented on MATLAB-R2015 software with Java code-based files. The main focus of this work is to analyze the efficiency of the proposed framework using a genetic algorithm in terms of fault prediction and fault tolerance. Parameters used to compare the performance of both fault-tolerant techniques, N-version (NVP) and recovery blocks (RcB), are elapsed time, classification accuracy, and mean square error. For analysis, 1000 test cases are generated by a designed framework with the use of the genetic algorithm. The test units and the tables are listed with a difference of 10 cases. So for 1000 cases, 100 sample values have been evaluated for software fault tolerance purpose on the proposed framework. Simulation results of the proposed framework are described below.

Elapsed Time (EL): Elapsed time in simple terms is the amount of time that passes from the start of an event to its end. In the proposed work, elapsed time is done for the fault tolerance. Evaluation results of the proposed implementation are as given in Table 1 and Fig. 3.

In proposed framework, elapsed time for recovery block is better than the N-version. The proposed framework has achieved 78% improvement as compared to existed framework.

Classification Accuracy (CA): Classification accuracy can be defined as the number of total correct classifications or predictions divided by the total number of classified elements or predictions made and to find the percentage multiplied by 100. So it is the rate of correct classifications for an independent test dataset. We had calculated the classification accuracy for both N-version (NVP) and recovery blocks (RcB). Evaluation results of the proposed implementation are as given below in Table 2 and Fig. 4. The formula used for calculating classification accuracy is:

$$\text{Classification Accuracy(CA)} = \frac{\text{Total Correct Classified}}{\text{Total Classified Elements}} * 100 \quad (2)$$

Table 1 Calculated results of NVP and RCB with parameter elapsed time

S. no.	N-version	Recovery block
1	0.32684	0.440169
2	0.471102	0.201985
3	0.179231	0.484462
4	0.407456	0.422244
5	0.615325	0.188306
:	:	:
99	0.744868	0.446134
100	0.75522	0.490227

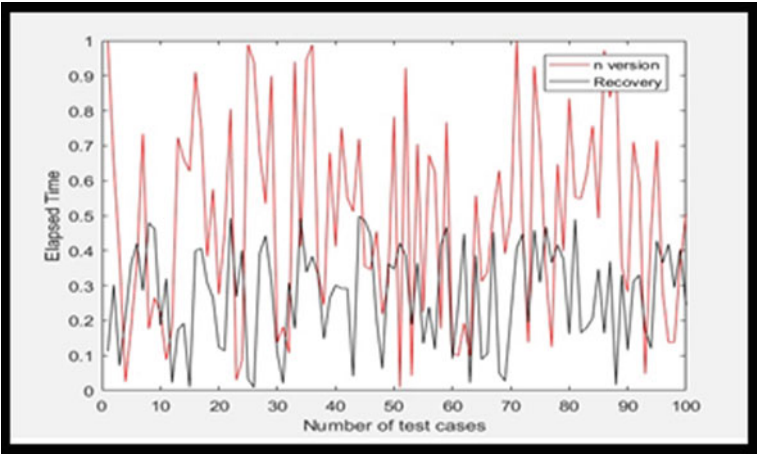


Fig. 3 Comparison result of NVP and RCB with parameter elapsed time

Table 2 Calculated results of NVP and RCB with parameter classification accuracy

S. no.	N-version	Recovery block
1	76.01701	82.59435
2	78.80281	81.04229
3	77.82223	83.65898
4	75.68417	82.32762
5	78.95729	81.88432
:	:	:
:	:	:
99	80.57971	81.84588
100	76.01328	83.2355

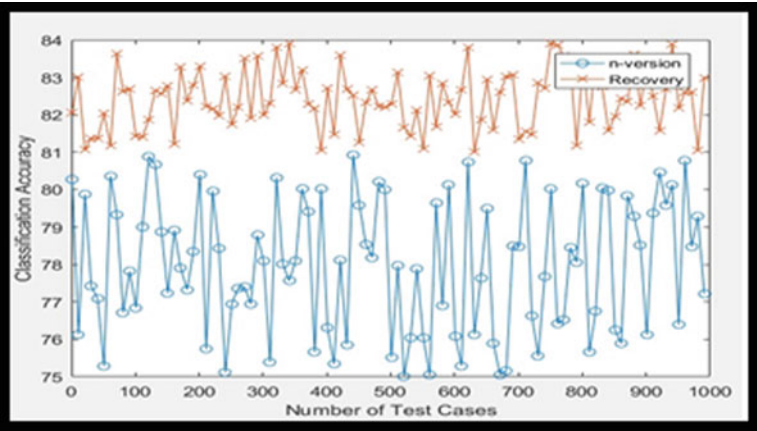


Fig. 4 Comparison result of of NVP and RCB with parameter classification accuracy

In the proposed work, the proposed elapsed time gives better results for recovery block than the N-version. The proposed framework has achieved 78% improvement as compared to the existing framework. The proposed framework offered better performance than existing.

Mean Square Error: Mean square error (MSE) is an estimator which measures the average of the square of errors. MSE can be calculated as the difference between estimated and actual values. We had calculated the mean square error (MSE) for both N-version programming (NVP) and recovery blocks (ReB). Evaluation results of the proposed implementations are as given below in Table 3 and Fig. 5. Mean square error (MSE) is calculated as:

Table 3 Calculated results of NVP and RCB with parameter classification accuracy

S. no.	MSE non-faulty N-version	MSE faulty N-version	MSE non-faulty recovery	MSE faulty recovery
1	2.075012	3.248718	1.538479	1.806141
2	2.007644	3.279142	1.536538	1.85851
3	2.015366	3.282688	1.530096	1.838388
4	2.076627	3.237418	1.518986	1.86465
5	2.06386	3.259207	1.532529	1.898895
:	:	:	:	:
:	:	:	:	:
99	2.019203	3.277696	1.58645	1.833358
100	2.031861	3.225238	1.520007	1.806901

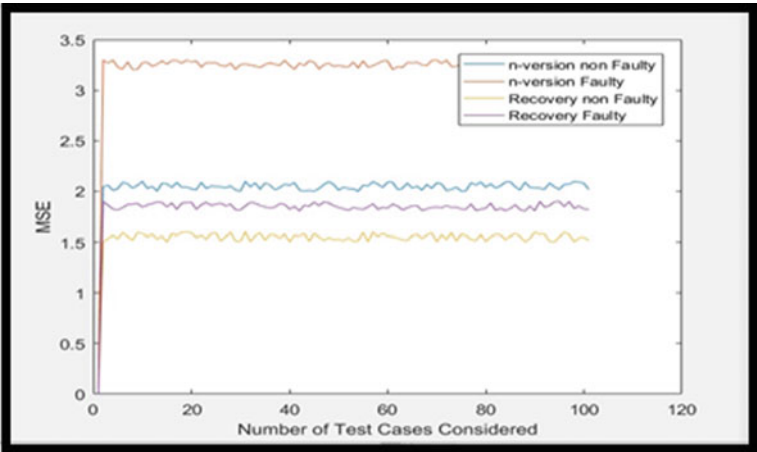


Fig. 5 Result of NVP and RCB with parameter mean square error

$$\text{MSE} = \frac{1}{n} \sum_{i=1}^n (Y_i - \tilde{Y}_i)^2 \quad (3)$$

In proposed work, the proposed elapsed time gives better results for recovery block than the N-version. The proposed framework has achieved 78% improvement as compared to existed framework. The proposed framework offered better performance than existed.

6 Conclusion

The purpose of software testing is the systematic detection of different types of faults with minimum effort and time. In this work, software fault tolerance techniques, N-version (NVP), and recovery blocks (RcB) are implemented for the proposed framework. To analyze the performance of the proposed framework, implementation is done in the .Net platform and various parameters are calculated with different experimentation. To analyze the performance of the proposed framework, in terms of fault prediction and fault tolerance, a set of different numbers of files is uploaded and results are calculated with three parameters elapsed time, classification accuracy, and mean square error (MSE). It concludes that the proposed efficient automated test case generation and test case prioritization framework is a good fault-tolerant framework. From the results, it is tested and proved that the proposed framework is an effective and reliable fault-tolerant framework within the budget of software. It also proved that from both used fault tolerance techniques the recovery block (RcB) gives better result as compared to N-version (NVP). Recovery blocks (RcB) on the proposed framework show better performance as compared to N-version programming (NVP). The experimental result shows the performance with parameters elapsed time, classification accuracy, and mean square error and concludes the effectiveness and reliability of the proposed framework for fault tolerance.

References

1. Rani, S., Gupta, D.: A comparative study of different software testing techniques: a review. *J. Adv. Shell Program.* **5**(1), 1–8 (2018). ISSN: 2395-6690 (Online)
2. Rani, S., Kaur, A.: Software fault prediction using boundary value analysis testing and loop testing techniques. In: 8th International Conference on Advancements in Engineering and Technology (ICAET-2020), Bhai Gurdas Institute of Engineering and Technology, Sangrur (Punjab), India, pp.192–196 (2020). ISBN: 978-81-924893-5-3
3. Baraldi, P., Cadini, F., Mangili, F.: Model-based and data-driven prognostics under different available information. *J. Prob. Eng. Mech.* **32**(4), 66–79 (2013)

4. Kamei, Y., Shihab, E.: Defect prediction: accomplishments and future challenges. In: 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER), IEEE, Publons, United States (2016). <https://doi.org/10.1109/SANER.2016.56>
5. D'Ambros, M., Lanza, M., Robbes, R.: An extensive comparison of bug prediction approaches. In: 7th IEEE Working Conference on Mining Software Repositories (MSR 2010): Co-located with ICSE, Cape Town, South Africa, pp. 31–41 (2010). <https://doi.org/10.1109/MSR.2010.5463279>. ISBN: 978-1-4244-6803
6. Chinnaiyah, M.R., Niranjan, N.: Fault tolerant software systems using software configurations for cloud computing. Springer J. Cloud Comput. Adv. Syst. Appl, 1–17 (2018). <https://doi.org/10.1186/s13677-018-0104-9>
7. Choudhary, R.K., Khan, R.A.: Testing software fault tolerance techniques—future direction. ACM SIGSOFT Softw. Eng. Notes **36**(3), 1–5 (2011). <https://doi.org/10.1145/1968587.1968604>
8. Gao, Q., Liu, W., Zhao, X., Li, J., Yu, X.: Research and application of the distillation column process fault prediction based on the improved KPCA. In: International Conference on Mechatronics and Automation (IEEE ICMA 2017), Takamatsu, Japan (2017)
9. Sumra, M., Qadri, S., Fahad, M.: Issues and challenges of automated software fault tolerance techniques. Int. J. Nat. Eng. Sci. **9**(3), 39–44 (2015). ISSN: 1307-1149. E-ISSN: 2146-0086
10. Perälä, J.: Improving TTCN-3 test system robustness using software fault tolerance. In: First International Conference on Advances in System Testing and Validation Lifecycle, Porto, Portugal. IEEE (2009). ISBN: 978-1-4244-4862-3
11. Rathore, S.S., Kumar, S.: A study on software fault prediction techniques. Artif. Intell. Rev. **51**(2), 255–327 (2019). <https://doi.org/10.1007/s10462-017-9563-5>
12. Alam, M.J.: Analysis of different software fault tolerance techniques. J. Eng. Sci. (JES). **1**(1) (2009). ISSN: 2078-6174
13. Sharma, G., Yadav, A: Fault tolerance in real time distributed system. Rev. Comput. Eng. Res. **5**(2), 20–24 (2018). <https://doi.org/10.18488/journal.76.2018.52.20.24>
14. Bhat, A., Samii, S., Rajkumar, R.: Practical task allocation for software fault-tolerance and its implementation in embedded automotive systems. In: IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Pittsburgh, PA, pp. 87–98 (2017). <https://doi.org/10.1109/RTAS.2017.33>
15. Sheng, J., Dong, S., Liu, Z.: Fault feature extraction method based on local mean decomposition Shannon entropy and improved kernel principal component analysis model. J. Clim. Change **8**(8), 625–635 (2016)
16. Ekwutuoha, I.P., Levy, D., Selic, B., Chen, S.: A survey of fault tolerance mechanisms and checkpoint/restart implementations for high performance computing systems. Springer J. Soft Comput. **35**, 1302–1326 (2013)
17. Rani, S., Kaur, A.: A literature survey on automatic generation of test cases using genetic algorithm. Wesleyan J. Res. (UGC Care Listed) **13**(2), 65–76 (2020). ISSN: 0975-1386
18. Rani, S., Kaur, A.: Efficient framework for fully automatic test case generation and prioritization using genetic algorithm in software testing. J. Comput. Theor. Nanosci. **17**(11), 5198–5204 (2020)

Chatbot to Map Medical Prognosis and Symptoms Using Machine Learning



Himani Aggarwal[✉], Saniya Kapur, Varun Bahuguna,
Preeti Nagrath, and Rachna Jain

Abstract Computer-aided system is a subject of great importance and extensive requirement. Nowadays, deep learning and machine learning have gained quite a knack in people's eye and widely used among them. Gone are the occasions when the products were utilized for complex count issues or graphical portrayal alone. And Chatbots are proven revolutionary in our day-to-day lives where they are present in health, career, insurance and customer care support. In this paper, we have built up a Health-Bot using RNN network and Keras classifier. During such a pandemic period when there is an enormous crowd present in hospitals, people can get themselves checked at their homes with this interactive language system. Neural network adds more exactness to our work and reactions. And we further implemented our model on StreamLit which is an open-source framework for machine learning and deep learning.

Keywords Health-Bot · Machine learning · Deep learning · Keras model · Recurrent neural networks · Sequential model

1 Introduction

There are poverty-stricken regions in our country where the necessities are neglected or are not provided. These issues cannot be resolved by a bot. There comes a time back in 1966 when the first-ever Chatbot was created 'ELIZA' [1].

H. Aggarwal · S. Kapur · V. Bahuguna (✉)

Electronics and Communication Engineering, Bharati Vidyapeeth's College of Engineering,
New Delhi, India

P. Nagrath · R. Jain

Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering,
New Delhi, India

e-mail: preeti.nagrath@bharatividyaapeeth.edu

R. Jain

e-mail: rachna.jain@bharatividyaapeeth.edu

It was capable of mimicking human conversation using pattern matching. Be that as it may, a bot can assist by improving a circumstance. The genuine intensity of a Chatbot is to give data just on your order, which could help one lead a better life, a healthier life and install people with basic knowledge of proper health care. A sufficient number of populations need information about safe sex and have no mindfulness about an infection that is explicitly transmitted, because it is as yet considered as a No–No in the family to discuss sex. According to a WHO report, very nearly 11 million individuals infuse drugs, out of which 1.3 million people are surviving with HIV. It is additionally realized that a great region of the total populace does not have a clue about the right use of essential medications and anti-infection agents, also according to WHO [2] approximately 31 million people across the globe each year suffer from drug use disorder, which at later stage prompts clinical maltreatment and by implication cause to be in certain conditions the infused therapy more or less ineffective. In a recent report, it is proved that artificial intelligence is playing a crucial role in battling against these chronic diseases which start at a small level and grow up to be life threatening [3]. Internet work and the entrance to enormous chunks of medical resource are proved revolutionary to medical science and artificial intelligence helping to curb and cure people to live a substantial and better life. Bots are intelligent agent formed by deep learning and machine learning as a parent domain by this train and test our dataset to derive our accurate results and predict the accuracy of different models imposed on it. In this study, we have built a Health-Bot using Keras classifier and RN network to help others in the health sector [4]. The primary domain of our bot is in healthcare domain to provide people with their necessities.

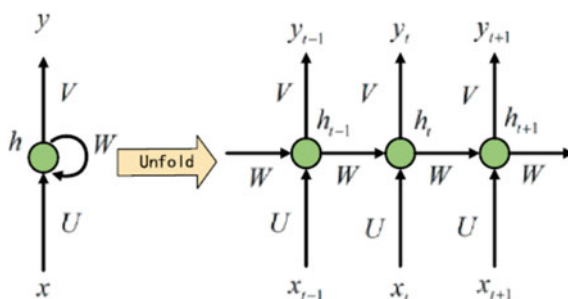
Organization of the paper is as follows: Sect. 1 includes previous work in this field aka related work; in Sect. 2, we discuss various methodologies, designs, activation functions and neural networks applied; Sect. 3 walks us through features offered by our model; in Sect. 4, we talk about result generated methodology. Next, this work is concluded and future prospects of the presented project.

2 Related Work

Chatbots, or Health-Bots, interact with humans in a humane way. The presence of Chatbot has been increased significantly and has a great potential to be used in education [5], entertainment [6] and the public sector like this one. The development of Chatbot has increased by many folds. Chatbot respond to the doubt or query related to health which a person is afraid to discuss; recently due to the progress in development, there are many methods to implement Health-Bot visually by using web frameworks such as Django. Bots designed using deep learning [7] have a vast amount of data to train. In this, we have used recurrent neural networks (RNN) for the understanding of both encoding and [8] decoding. Eliza was the first Chatbot created by the Massachusetts Institute of Technology. On the off chance that a patient said ‘my head hurts,’ Eliza would react with, ‘Why do you say your

head hurts?’ Eliza, with just 200 lines of code, works like a [1] therapist. It is a typical inclination to have a human association in practically the entirety of our day-by-day exercises; be that as it may, innovation enhances our capacities. Today, on account of AI and NLP, we can utilize Chatbot innovation to give practically human-like discussions. The discussions are fueled by AI (man-made reasoning). A decent human services foundation is the basic for any country’s metro life, and the must wipe out be conceded an indigenous arrangement to get to better social insurance, without the need to hang tight for quite a long time or months only for a little while. These calculated issues can easily be solved with the help of the Internet work and access to large chunks of medical resources—which are primarily free. These intelligent personal assistants (IPA) on our phones suddenly become definite responses for certain needs which are supported by machine learning and neural networks. It is close to unfeasible to determine these troubles with a bot, be that as it may, a bot can assist by improving the circumstance. The genuine favorable position of these Chatbots is the capacity to give appropriate direction and data to have a sound existence, as there are numerous individuals who despite everything do not have the essential information on legitimate social insurance [9]. AI is the parent space from which profound learning is inferred, which when joined with calculations of structure and working of the human mind clears approach to fake neural systems. Profound learning design comprises neural systems comprised of neurons, initiation capacities and loads that learn on their utilizing learning calculations [10]. Bots are only savvy operators dwelling on a worker to speak with people or different bots to make the human assignment a lot simpler, without the need of a particular convention or APIs nor with any ‘ace bots,’ for example, Google Assistant [11]. They convey in plain English, and profound learning makes them more precise in tossing the proper reaction to the given inquiry. In this examination, we have manufactured a relevant Chatbot utilizing TensorFlow [10] and Python to contribute to the well-being area. Our bot is equipped for diagnosing the medical problem, recommending a suitable doctor, giving updates about medicine and making an online meeting with the doctor. The most significant and essential advantage of Chatbots in the medicinal services area is the preeminent capacity to give exhortation and data to a solid life to help those individuals who need fundamental information on social insurance (Fig. 1).

Fig. 1 Recurrent Neural Networks



3 Methodology and Design

3.1 *Neural Networks*

Neural networks have a main working concept which is to allow distribution of activity throughout the link with the help of a learning algorithm that is similar to the working of the human brain. Neural networks are trained and tested by a simulator [1]. It works along with the definition of neural network topologies. Neural units are of three types: input, hidden or output units. The relation that is connecting them is unidirectional, even though it supports recurrent links. There are many algorithms used for training a dataset that are available. Standard back-propagation and momentum back-propagation are only used. A pattern file directly receives the values of the input. Result file gets passed the output unit values, or values from pattern files can be received by it. Many input values and linked output values are contained in a pattern file. The simulator can also support a dynamic mode [13]. N-gram model can be implemented using these features. Values from the previous units can be received by units and hidden units. Further changes to that value are specified by the output function.

3.2 *Recurrent Neural Network*

A sequence or a collection of most frequently occurring consecutive words are fed into an RNN. It analyzes the data with the technique of finding the words occurring more frequently and creates a model that predicts the next or upcoming word in the sentence, i.e., it auto-fills the most probable data [14].

Recurrent neural networks are preferred because in feed forward neural network, it only considers the current input and cannot memorize previous outputs. So, in RNN [15] it memorizes what is going on the hidden layers and that produces a data to feed into the next one. Therefore, it allows to handle sequential data.

Types of RNN

1. **ONE TO ONE NEURAL NETWORK:** one to one type of RNN is also known as the most basic (Vanilla) form of artificial neural network. It is required for regular machine learning problems.
2. **MANY TO ONE NEURAL NETWORK:** Many to one neural network takes in a sequence of inputs. For example, in sentiment analysis where a given sentence can be classified as expressing positive or negative sentiments.
3. **MANY TO MANY NEURAL NETWORKS:** Many to many networks takes in a sequence of outputs, for example, in machine translation.

3.3 Label Encoding

Sometimes, our label is not a number but a string. We want to convert these strings to numbers that start from zero and one. If the classification is three classes, then the label is zero, one and two. Label encoder can help encode labels with a value between zero and $n\_classes - 1$.

3.4 ReLU Activation Function

The ReLU function also can be expanded as rectified linear unit function. It is signified as follows:

$$R(x) = \max(0, x) \quad (1)$$

ReLU function basically avoids and solves vanishing gradient and removes the negative part [12].

$$\Rightarrow y = \max(0, o_i) \quad (2)$$

$$\Rightarrow \arg \max f(x) \quad (3)$$

$$\Rightarrow i \in 1, 2, \dots, N \quad (4)$$

3.5 Softmax Activation Function

Softmax activation function is similar to the sigma function. A sigmoid clamps the value in between zero and one, but it does not represent the probability of something happening. In this function, we take the sum of the wakes times the previous output and plug that into the sigmoid function. This sum that we just quoted is like before we put it in an activation function. So, there is a need to find an activation function that can deal with real probability. That is where Softmax activation function comes handy. It does not really have a proper graph [16].

Softmax work is equivalent to the exponential of the component at position 'k' partitioned by the whole of the exponentials of all components of the vector. It is unique in relation to other actuation capacities which is on the grounds that while the other enactment capacities get an info esteem and change it paying little mind to different components, and the Softmax considers the data about the entire set of numbers one has. In this sense, Softmax is special because the output depends on the entire set of elements of input. A key part of Softmax transformation is that the estimations of yield are in the range from 0 to 1 and their aggregate is one [17]. The point of the Softmax transformation is to transform a lot of discretionarily big or

small values that come out of previous layers and fit them into a valid probability distribution. This makes everything so intuitive and useful that the Softmax activation function is often used as the activation of the final output layer in classification problems [12].

$$p_k = \frac{\exp(o_k)}{\sum_{k=0}^{n-1} \exp(o_k)} \quad (5)$$

3.6 Keras

Keras is a Python-based deep learning framework which is widely used. It basically runs on top of TensorFlow and is very simple to work in as building models in Keras are as simple as stacking layers and later connecting these graphs. It is an open source project which is actively developed by developers and contributors across globe, also the documentation offered is vast and new features are added almost daily. It reduces the cognitive load which ensures that that the APIs are simple and consistent [12]. Keras provides clear feedback upon occurrence of any error, and this minimizes the number of user actions required for the majority of the common use cases. Keras also provides high flexibility to all of its developers by integrating with the lower-level deep learning framework languages like TensorFlow or Theano. This ensures that you can implement anything that you actually built in your base language. Keras supports multi-platform and lets its users work with multiple back ends. It feels like a tailor-made API for framework. The code can be run on the CPU or the GPU as well. Producing models on Keras is very effective and beneficial as it has total support to run with TensorFlow serving, GPU acceleration, example CUDA, native support to develop Android and iOS apps using TensorFlow and core ML and a full-blown support to work with Raspberry Pi as well.

Working Principle

Features: Computational graphs are used for expressing complex expression as a combination of simple operations for Keras to work with. It is mainly useful for calculating the derivatives during the phase of back-propagation and hence it makes it easier to implement distributed computing on a whole [18]. So, all it takes is to specify the inputs and outputs and to make sure that the graph is connected throughout (Fig. 2).

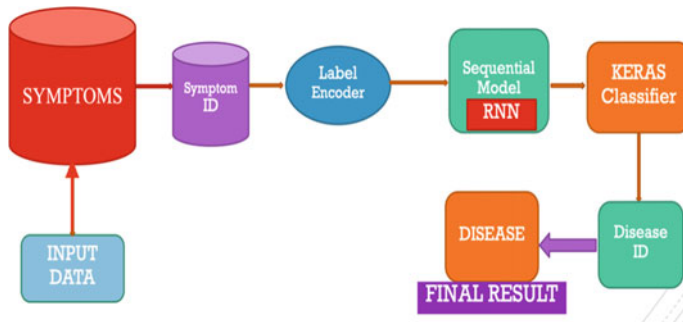


Fig. 2 Data Pipelining Model

3.7 Sequential Model

The working of the sequential model is like a linear stack of layers. This model is majorly useful for building simple classification network and encoder/decoder model. So, here we treat every layer as an object that feeds into the next layer and so on [19]. Features: `model.fit()` is used to train network. Bunch size is the quantity of training models in one forward and in reverse pass, so higher the batch size, the more memory you require.

Functional Model: It is a widely used model and holds good for about 95% of use cases. This model supports multi-input, multi-output and arbitrary graph topology. It has branches so wherever there is a complex model, it is folded onto two or more branches based on the requirement.

4 Features

1. Build an interactive real-time chat system [20]

Chatbots give customers a more amicable encounter. It has been very much wanted that individuals lean toward the feeling of discussion and association in which Chatbot furnishes overlooking with a mouse and snap. Regardless of whether it is something profound established in our mankind that we anthropomorphize, the truth of the matter is that individuals feel more joyful with a correspondence experience by means of a bot than something else. Clients have to search a ton and bother around which is disappointing and tedious; however with Chatbots, they get a human language-type communication. This is significantly more agreeable for patients as the cooperation is refined, giving them a customized proactive encounter. Through Chatbots, answers are gotten rapidly and productively. Who has the opportunity to be required to be postponed on the telephone or hustled starting with one office then onto the next? None of us. We need the data as fast as

could be expected under the circumstances. A Chatbot spares time, letting loose patients for other activities [20]. There are two types of Chatbot's unintelligent ones that act using predefined conversation flows written by people and intelligent AI Chatbot's [21] that use machine learning.

2. Made for all types of OS devices

The services [22] must be available at all times on any type of operating system. Hence, this app will be made on Flask/Django web framework which will intend that it can be used on computers and on mobile platforms such as macOS, iOS, Android and Windows such that more and more can be connected to this application and can be benefitted from it.

3. Effective symptom-based disease prediction

As we all know that each disease at some later point shows its unique kind of problem which might convert into a life-threatening disease if not treated or judged early, the most common diseases can be easily identified by analyzing the symptoms. The symptoms can be anything like headache, itching, etc. So, by reading the symptoms and analyzing them, any possible health problem can be predicted [23], if any. If a person's body is analyzed periodically, it is possible to predict [24] any possible problem even before they start to cause any damage to the body.

4. Easily integrable and updatable

The system should be integrated [24], which signifies it has many individual modules since we use different types of modules which is used in performing a task, so they can be upgradeable individually. This will be helpful in increasing the efficiency of the system which will help to predict the data better.

5 Result-Generated Methodology

Initially, we created a custom dataset by consulting various healthcare practitioners where we asked them about commonly occurring illnesses and diseases and created a dataset out of it. We feature engineered our data as in machine learning one of the challenges is selecting the best features which are most appropriate and suitable for.

Figure 3 gives us the graphical representation of the dataset how it is mapped to identify the symptom with the help of its ID. This shows the plots of various symptoms ID (i.e., 1, 2 and 3) on the Y-axis and Disease ID on X-axis. This gives us the graphical representation of the dataset how it is mapped to identify the symptom with the help of its ID.

The type of algorithm you are trying to model, also many times the existing features, is not enough which results in re-engineering new features to be used to train the machine learning model which can be called feature engineering (FE). Then we label encoded our mapping of the symptoms to diseases [Sect. 3.3]. Once we got our data label encoded, then we implemented the recurrent neural network

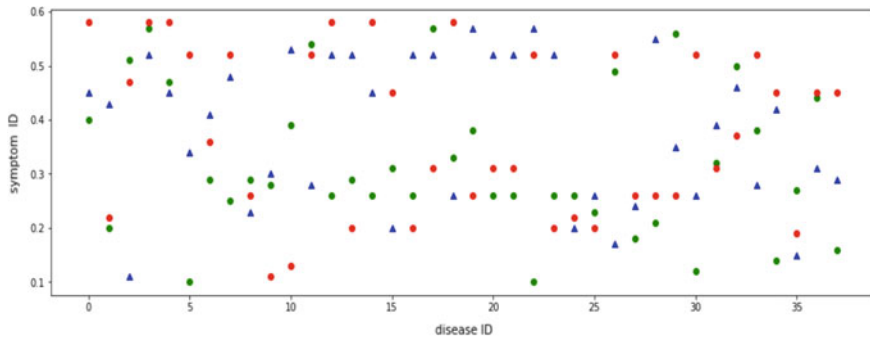


Fig. 3 Scatter plot representation of symptom ID w.r.t Disease ID

model. Recurrent neural network model [Sect. 3.2] is a type of neural network, and they require data to learn. The more the data is provided, more accuracy will be given back. On RNN, we used Keras framework [Sect. 3.6] which runs on top of TensorFlow. In this RNN model, we used activation functions like ReLu and Softmax. This function is attached to each neuron in the network and determines whether it should be activated ('fired') or not, based on whether each neuron's input is relevant for the model's prediction. Also in recurrent neural network (RNN), we used sequential model as it is used in problems related to classification. Here we treat every layer as an object that feeds into the next layer and so on. Once the symptoms were mapped with the disease, corresponding precautions and descriptions were displayed. Then using JSON file, we implemented a chat function to engage with the user. By doing this, the Chatbot will calculate the similarity between the trained text sequence and the user's input. We integrated our chat application with StreamLit which is an open-source framework for machine learning and deep learning models to make it effective for real-world users.

6 Conclusion

In this paper, we have effectively actualized a powerful Health-Bot which is where we also were successfully able to implement a train test model from sklearn model selection, where 20% of the model was given for testing and the rest 80% for training our model. Then we were able to implement cross-validation where we resample the procedure to assess the AI model on a constrained information test. Hence, we also used the K-fold method where k represents the number of folds. Further, we were successfully able to implement the Keras framework on the sequential model. In the coming years, prospects of Chatbot or Health-Bot specifically are very high by looking at the present needs of the people. The way this industry is prospering it is more prominent to be seeing it in other people's life. In addition, there are further prospects that Chatbots should be offering setup with

different regional languages to people who are not having knowledge of the English language and more into the regional tongue. As on looking the need of peoples knowledge of replying to what their mother tongue is, but there is much room to improve quality in terms of generalization of the chat templates by clustering similar topics and grouping similar replies and improving coherence among the consecutive chat replies by understanding the styles of replies. Also, on looking at the fact that how vast can we pull off our datasets meeting the need of people, we plan to improve the qualities of the extraction of data, the method of selecting varied diseases and extracting suited precautions.

References

1. Szymczak, A.: Introduction to chatbots in healthcare. <https://blog.infermedica.com/introduction-to-chatbots-in-healthcare/>. Accessed July 2017
2. World Health Organization: Management of substance abuse advice for the public. Available https://www.who.int/substance_abuse/facts/en/. Accessed 23 June 2020
3. Alqudah, A.M., Qazan, S., Alqudah, A.: Automated systems for detection of COVID-19 using chest X-ray images and lightweight convolutional neural networks (2020). <https://doi.org/10.21203/rs.3.rs-24305/v1>
4. Kumar, A., Shanmugavadivu, P.: Space of RGB-H-CMYK. **1**(Feb). Spring Singapore (2019). <https://doi.org/10.1007/978-981-13-1708-8>
5. Mckie, I.A.S., Narayan, B.: Enhancing the academic library experience with Chatbots: an exploration of research and implications for practice. *J. Aust. Lib. Inf. Asso.* (2019). <https://doi.org/10.1080/24750158.2019.1611694>
6. Melián-González, S., Gutiérrez-Taño, D., Bulchand-Gidumal, J.: Predicting the intentions to use chatbots for travel and tourism. *Curr. Issue Tour.* (2019). <https://doi.org/10.1080/13683500.2019.1706457>
7. Emima, Y., Rajesh, M., Rao, K.S.: Experimental investigation on performance and exhaust emission characteristics of diesel engine using eesame blends with diesel and additive. *Int. J. Rec. Technol. Eng.* **8**(1), 6–11 (2019)
8. Pati, B., et al. (eds.): Progress in advanced computing and intelligent engineering. In: *Advances in Intelligent Systems and Computing*, vol. 713. https://doi.org/10.1007/978-981-13-1708-8_10
9. Kucherbaev, P., Bozzon, A., Houben, G.: Human-aided bots. *IEEE Internet Comput.* **22**(6), 36–43. <https://doi.org/10.1109/MIC.2018.252095348>
10. Singh, R., Paste, M., Shinde, N., Patel, H., Mishra, N.: Chatbot using TensorFlow for small Businesses. In: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, pp. 1614–1619. <https://doi.org/10.1109/ICICCT.2018.8472998>
11. López, G., Quesada, L., Guerrero, L.A.: Alexa vs. Siri vs. Cortana vs. Google assistant: a comparison of speech-based natural user interfaces. In: Nunes, I. (eds.) *Advances in Human Factors and Systems Interaction. AHFE 2017. Advances in Intelligent Systems and Computing*, vol. 592. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60366-7_23
12. Agarap, A.F.: Deep learning using rectified linear units (relu). *arXiv preprint arXiv:1803.08375* (2018)
13. Marques, N.C., Lopes, G.P.: A neural network approach to part-of-speech tagging. In: *Proceedings of the 2nd Meeting for Computational Processing of Spoken and Written Portuguese*, pp. 21–22 (1996)

14. Yousif, J.: Neural computing based part of speech tagger for Arabic language: a review study. *Int. J. Comput. Appl. Sci. IJOCAAS* **5**(1) (2018)
15. Ramadevi, R., Sheela Rani, B., Prakash, V.: Role of hidden neurons in an Elman recurrent neural network in classification of cavitation signals. *Int. J. Comput. Appl.* **37**(7), 9–13 (2012)
16. Chen, J., Jing, H., Chang, Y., Liu, Q.: Gated recurrent unit based recurrent neural network for remaining useful life prediction of nonlinear deterioration process. *Reliab. Eng. Syst. Saf.* **185**, 372–382 (2019)
17. Shim, K., Lee, M., Choi, I., Boo, Y., Sung, W.: Svd-Softmax: Fast Softmax approximation on large vocabulary neural networks. In: *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pp. 5469–5479 (2017)
18. Abdul-Kader, S.a., Woods, J.: Survey on Chatbot design techniques in speech conversation systems. School of Computer Science and Electronic Engineering/University of Essex Colchester/UK
19. Vidnerova, P., Neruda, R.: Evolving Keras architectures for sensor data analysis. In: *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 109–112. IEEE (2017)
20. Choi, K., Joo, D., Kim, J.: Kapre: On-gpu audio preprocessing layers for a quick implementation of deep neural network models with Keras (2017). arXiv preprint [arXiv:1706.05781](https://arxiv.org/abs/1706.05781)
21. Atanasov, A.: Dynamic Working Memory in Recurrent Neural Networks
22. Awwalu, J., Garba, A., Ghazvini, A., Atuah, R.: Artificial intelligence in personalized medicine application of AI algorithms in solving personalized medicine problems
23. Chantarotwong, B.: The learning Chatbot. Fall (2006)
24. Kelly, J.E.: Computing, cognition and the future of knowing how humans and machines are forging a new age of understanding. IBM Research and Solutions Portfolio

Cloud Security: The Future of Data Storage



Parv Bajaj, Ritika Arora, Mehak Khurana, and Shilpa Mahajan

Abstract In this modern era, all the organizations seem to be shifting their data and services to cloud because of the increase in information leaks and data thefts. It has become easier for intruders to break into the organization's data stored locally. As cloud provides a significant hike in security levels, it is slowly turning into the future of data storage. It has become crucial to acknowledge the issues regarding cloud security. Cloud security is the security of all the services provided by the cloud—storage, servers, networking, and databases. In this paper, the issues related to the same are covered along with the mitigation proposed to deal with those problems. The key to the overall security of the cloud is identity access management (IAM). IAM is inherently more secure than a simple username and password combinations because of the profile of information IAM collects. It can make access to data and networks a much more convenient process.

Keywords Identity and access management • Cloud service models • Authorization • Cloud security

1 Introduction

Cloud security refers to the security dedicated towards protecting cloud computing systems from intruders. This involves keeping data safe and private across online applications, and platforms. Ample amount of security is provided by the cloud providers as end-users trust them with their personal data. Client's trust is a key component in their business. Cloud security methods are used to keep client's data safe and private. It will be wrong to say cloud security entirely depends on the cloud provider because some part of it is certainly in the end user's hand.

P. Bajaj (✉) · R. Arora · M. Khurana · S. Mahajan
The NorthCap University, Gurugram, India
e-mail: mehakkhurana@ncuindia.edu

S. Mahajan
e-mail: shilpa@ncuindia.edu

Cloud security consists of:

- IAM
- Data security
- Policies
- Data retention
- Legal compliance.

The security guidelines focus on these three phases:

Phase 1: Understanding cloud usage and risk assessment.

Phase 2: Protecting the cloud.

Phase 3: Responding to cloud security issues.

These guidelines are related to protecting the hosts running the computer instances and the network these instances are connected to. This is where IAM plays the most important role because in order to secure the network, managing users and their access privilege are necessary. The protection of cloud data assets is done through encryption of all the data present in cloud storage.

The currently used cloud environments are:

- Public cloud services are offered by third-party datacenter provider to end-user. Public cloud offers resource pooling, self-service, service accounting, multi-tenancy to manage the solutions, deployment, and securing the resources and applications.
- Private clouds are deployments set up within the organization's firewall (on-premises datacenters) and traditionally run by on-site servers. Some of the benefits of a public cloud computing environment, such as elastic on-demand capacity, service-based access, and self-service provisioning are offered [1]. Private cloud is suitable when the traditional requirements, such as control, security, and resiliency, are more emphasized by an organization with the restricted and designated user access and authorization.
- A hybrid cloud is a combination of an interoperating public and private cloud. This is the model where consumer takes the noncritical application or information and compute requirements to the public cloud while keeping all the critical information and application data in control. It is an intermediate step in the evolution process, providing businesses an onstage from their present IT conditions into the cloud environment. A hybrid cloud provides you with resources of public cloud for small projects at a cheaper rate than if you use data center's IT infrastructure. With this, you do not invest much in the resources you need on a temporary basis.
- A community cloud is the cloud managed by groups of people, communities, and agencies especially government to have common interests—such as maintaining the compliance, regulation, and security parameters—working on the same mission.
- Shared private cloud is a shared compute capacity with variable usage-based pricing to business units that are based on service offerings, accounts

datacenters. It requires an internal profit center to buy infrastructure made available through account consolidations.

2 Cloud Service Models

Before we dive into cloud security, it is necessary to study about cloud service models. Clouds will transform the IT industry and profoundly affect how we live and how businesses operate. Cloud computing:

1. Offers the scalable compute model to be accessed from anywhere.
2. Offers you with simplified service delivery.
3. Disaster recovery.
4. Provides dynamic infrastructure for upcoming technologies data center.

Some say it is grid or utility computing or software-as-a-service, but it is all three of those combined—software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

2.1 SAAS

In software as a service model, it is not required to install an application instead you can reliably access it via the Internet. It saves you from complex software and hardware management. A third-party provider hosts it on the internet, and it can be used by various customers. These applications are not actually managed by your company but by the software provider itself. It is more convenient as it relieves you from a pestering of software maintenance, network security, data availability, infrastructure management, and all other operational issues involved with keeping applications up and running. SAAS model onboard has the largest market share in cloud security.

2.2 PAAS

Platform as a service (PaaS) is more of a complete development and deployment environment in cloud security. In this platform-as-a-service (PaaS) model, the developers hire almost everything they need to design an application, depending on a cloud provider for development tools, infrastructure, and operating systems. The PaaS provider makes available everything like servers, networks, storage, operating system software, databases at their centralized data center. The user can purchase

the resources as per need from a cloud service provider on a pay-as-you-go basis and access them over a secure Internet connection.

2.3 IAAS

Infrastructure as a service model hosts applications on the public cloud and private cloud rather than in a traditional on-premises data center. The application is made available to users on-demand while it is being fully controlled by the cloud service provider (CSP) itself. The enterprises hire servers for computation and storage in the cloud environment. Infrastructure as a service is highly flexible as you need to purchase only the components you need according to your needs and demand and scale them up or down based on your business needs. Infrastructure as a service model is identical to utility computing, the user gets the resources on the rental basis and pays only for the resources he uses like power, data storage space, etc., on your business needs (Fig. 1).

3 Threats in Cloud Security

3.1 Data Breaches

The risk of a data breach is not new to cloud security, but it consistently ranks as a top threat to cloud customers. Common data breach exposures incorporate personal information, such as social security numbers, credit card numbers, and healthcare histories of customers, as well as corporate information, such as customer lists and software’s source code [2].

Mitigation:

You can encrypt the data using data-at-rest and data-in-transit security. Traffic monitoring technique (log management to identify unreliable IP addresses) is also

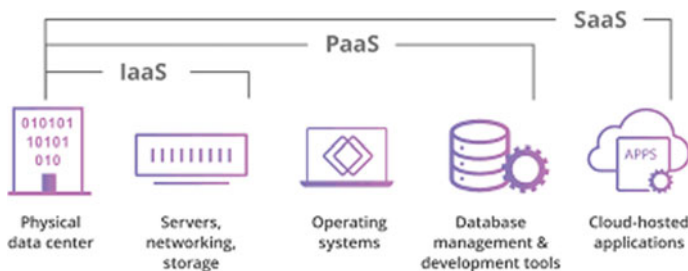


Fig.1 Cloud services models

advisable to prevent data breaches. Implementation of data access governance and establishing data remediation workflows to secure data.

3.2 Insecure APIs

The APIs are delivered by the cloud service providers to software developers to build the interfaces and with these interfaces; they can interconnect to the cloud services. Unique characteristics of API leave the door wide open for threats. The difficulties like anonymous access, reusing passwords, or tokenization could hamper the cloud services and could restrict logging, monitoring capabilities, and API dependencies which could result in DDoS attack or repudiation attack.

Mitigation:

Testing techniques that mimic an outsider attack which targets specified API endpoints and aim to break the security and get access to company's sensitive data. API keys must be protected and not reused.

3.3 Denial-Of-Service Attacks (DoS/DDoS)

A denial of service (DOS/DDoS) attack is an attempt to tie up a website's resources so that users who need to access the site cannot do so. It generally makes a website service unavailable by overwhelming it with traffic from multiple sources. These are usually launched by bots or malware from hundreds of infected hosts. Application-level DoS/DDoS attacks can easily manifest themselves as high-volume Web page reloads, XML* web services requests [3]. This attack consumes all available resources in the Web server such as memory, CPU, space in disk and indirectly abuses the functioning of the website.

Mitigation:

Implement firewalls and allowing only legitimate IP addresses or blocking ones from known attacker is one of best ways to mitigate DDoS attacks. These attacks can be nullified by rate-limiting the amount of traffic available to a specific network interface controller. The impact of DDoS attack can be reduced by filtering requests upstream, long before it reaches the target network.

3.4 Misconfigured Cloud Storage

Misconfigured cloud storage is when there are critical gaps in your cloud security that leave your organizational data at risk. It happens when you make errors while

configuring the security controls, or you forget to implement them at all. One of the repeated misconfigurations grants public access to storage buckets. These buckets are often vulnerable because of authentication methods such as passwords, making them available to everyone and prone to attacks. Although, access to these storage buckets is one of the examples of the type of misconfiguration. Organizations face innumerable types of misconfigurations as they drift to public IaaS cloud environments [4].

Mitigation:

Cloud security configurations must be double-checked upon setting up a particular cloud server. This should be understood that configurations are part of security. A third-party security tool should be used that can look at configurations constantly. It provides a constant check and alerts you when things are misconfigured. Outside security testers should be hired to ensure that everything is configured correctly. Sometimes audits can find things that a client may overlook. The stuff being uploaded on the storage should be checked for hidden malwares.

4 Identity and Access Management

Identity and access management refers to the ability to manage user identities and their privileges to access the resources. IAM is the first step to make an organization effective in communication, reliability and securing sensitive data. Identity is the necessity for the foundation of identity and access management. It lubricates the path of providing user's privacy and secure guarding their sensitive information from data theft using identity. Identity plays a crucial role in this heterogeneous cloud environment. IAM strategies have been an important facet of IT platform as it helps to make work possible. IAM as a framework consists of policies which authenticate and authorize user to access a specific resource.

IAM ensures that you as an identity are accessing the appropriate resource at the right point of time securely and you are right person to access it with the help of these two components:

- Authentication.
- Authorization.

Within **authentication**, applications recognize you as a person by looking at your identity cards, digital certificates, etc.

Within **authorization**, applications check what permissions you have to perform actions in that specific environment considering roles, attributes of your identity, or other affiliations to decide if you are authorized to have access to a particular resource. Both these calls help to reduce the load of help desks and maintain the user's privacy. Main functionalities required from an IAM system are:

- An individual may have multiple accounts requiring PINs or passwords.
- Authentication of the user is done by a unique ID provided by IAM system.
- For authentication purpose, complexity of passwords are determined; SSO techniques and OTPs are used to prevent stealing of passwords.
- IAM manages log activity so no suspicious activity passes unnoticed resulting in preventing identity thefts.
- IAM lets individuals manage their personal and confidential data and lets organizations modify data of their employees.

IAM stops threatening activities with the help of techniques like log management, machine learning, and other algorithms. It maintains policies to make users comply with security agreement of the companies.

5 Authentication

The methods to determine that someone is who they claim to be. The most commonly used authentication method is the log-on credentials. But using passwords alone for authentication is increasingly regarded as insecure since passwords are easy for hackers to crack using various attacks (Fig. 2).

5.1 Single Sign-On (SSO)

SSO is an Internet access management tool that allows a user to log in to one of an organization's portal and automatically be logged in to a designated set of other properties. For example, when you log in to Google, you are automatically logged in to your Gmail and YouTube accounts. For users, since they do not have to keep track of different credentials for every application, SSO reduces friction. For organizations, SSO helps in collecting valuable insights about client's behavior and

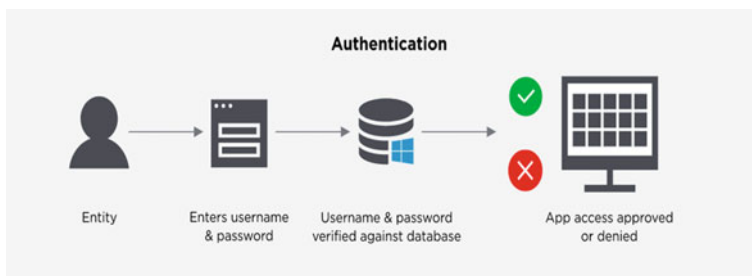


Fig. 2 Authentication basic concept

preferences since it tracks them as they move from one application to another, connected by a single login.

5.2 Multi-Factor Authentication (MFA)

Implementing multi-factor authentication is crucial to protect your organization's data and crucial information from malicious intrusions. Every IAM platform offers some form of MFA. However, it is equally crucial to customize MFA with the appropriate level of security. IN B2C contexts, you need to consider UX (user experience) and try not to create unnecessary friction for users who do not want to be subjected to heightened scrutiny every time they log in. For IAM in workplace, you may want more stringent multi-factor authentication, since the consequences of an unauthorized party gaining access to your private network can be so devastating. A modern IAM solution will allow you to implement MFA only when it is needed. This can be accomplished through step-up authentication or adaptive authentication in which users only trigger MFA if they are trying to access sensitive data or their behavior is flagged as risky.

5.3 Anomaly Detection

In the past few years, identity has become a preference for hackers to break into systems. Credential stuffing attacks, brute-force attacks and even highly targeted phishing campaigns are all attempts by hackers to break in through an organization's front door: the login box. These attacks can be devastating, leading to legal fallout, huge spikes in traffic that crash applications and most of all, stolen data. IAM solutions are designed to get in front of those issues through anomaly detection. There are multiple ways identity access management systems can help to detect and mitigate malicious attacks. For example, by detecting attacks by monitoring signals such as the velocity of traffic, detection of login patterns that differ from a user's routine (such as location and browser), use of devices and IP addresses with a poor reputation, or use of a breached password.

5.4 OpenID

OpenID is a protocol which allows users to be authenticated by cooperating sites—RP (relying parties) using a third-party identity vendor. It is an open standard authentication protocol. A relying party (RP) is a service that depends on a third-party identity provider to identify and authenticate a user who is requesting

access to a digital resource [4]. OpenID supports single sign-on services by allowing users to sign in to multiple websites and web services using just one identity.

5.5 *Federated Identity*

While in single sign-on, the tool lets users log in to different properties or brands owned by a single organization; federated identity does the same thing across multiple organizations. The example of federated identity we see in real life is through social login, in which you can use your Google, Facebook, or Apple ID to log in to a wide range of apps. Federation is built on trust, so when you order from a food delivery app with your Samsung pay ID, you are not ordering from Samsung but indicating that the app trusts Samsung enough to take their word that you are who you claim to be.

5.6 *SAML*

SAML works by transferring the client's identity from the identity provider to the service provider. This is done via an exchange of digitally signed XML documents [5].

5.7 *OAuth*

OAuth offers one-way authentication. It is an open-standard authorization framework that allows a user to grant a third-party website access to the user's protected resources, without necessarily revealing their long-term credentials or even their identity [6]. Commonly used by consumer applications and services, so users do not have to sign up for a new username and password. Some examples of OAuth in real world are when you go to log on to a website and it offers one or more ways to log on using another website's logon—"Sign in with Google" or "Log in with Facebook".

6 Authorization

Authorization is the module that is used to determine users' privileges for a particular resource which usually includes system data, files, network services, etc. To explain it better, we can look at some examples: privilege to access any service at all, to access any service with a well-stated write access, to access only a part of the network service or permission to get into whole cloud console. Authorization in



Fig. 3 Authorization basic concept

organizations is usually achieved by access control policies or access right delegations. Access control policies can be defined as—only the authorized clients will be able to access both the resources and services. Authorization is based on complex access control mechanisms which keep record of user attributes like session id, personal information, etc. It helps in safeguarding sensitive information and reducing security risks (Fig. 3).

6.1 Access Control Mechanisms

6.1.1 MAC (Mandatory Access Control)

Mandatory access control sets up access policies and states security attributes for the clients where the system provides users with access rights. The access policies are handled by the director, and the users are not given the rights to set, alter, or repeal permissions. When a user tries to access any program, the operating system examines the user's security attributes and decides whether the access can be granted or not. The system verifies the credentials of every individual when any resource is accessed by them. All the security measures are forced by the kernel itself. The system provides access to users based on their clearance level. This type of access control is implemented on systems with high security such as army systems or bank systems. In mandatory access control model, security labels are assigned to every file system object (determines whether it is confidential, secret, etc.). The classification label is maintained by the operating system. If a client wants to access a confidential or a secret file, he must have a secret clearance or high clearance level [5].

6.1.2 DAC (Discretionary Access Control)

In the discretionary access control model, power lies in the hands of owner of the resource; he decides who can have access to a specific object. In DAC, controls are

discretionary as the users can access a file on identity basis. The file owner has the authority to change the permissions of the file. The owner can grant access to other clients as per the requirements. Discretionary access control offers a high level of security to data networks of company [7]. DAC minimizes threats and attacks by setting up a firewall with a well-organized IP-tables rules. Unauthorized users are blind to resource characteristics, such as file size, file name, and directory path. All operating systems like Windows, UNIX, and Linux use discretionary access control. DAC provides more flexibility as compared to MAC and is labor-intensive.

6.1.3 RBAC (Role-Based Access Control)

Role-based access control is a way for organizations to manage and assign access privileges across the network in a structured way. RBAC grants permissions based on the employee groups and their subsequent roles. The duties for those groups of employees can be segregated and only the amount of access the groups needs to perform their jobs can be granted. Users may be assigned multiple roles as required. In RBAC, an employee's position determines the permissions they are granted and ensures that lower-level employees are not able to access sensitive information or perform high-level tasks. Organizations that utilize RBAC are better able to secure their sensitive data and critical application [8]. RBAC provide the organizations with some benefits like:

- The process of adding or changing roles of the employees is automated resulting in less paperwork, therefore, increasing in efficiency.
- In RBAC, the data access is appropriately managed resulting in overall better control of compliance efforts.
- RBAC reduces the possibility of data theft, breaches, and information leaks by ensuring that only authorized users have permission to access certain areas of the system.

6.1.4 ABAC (Attribute-Based Access Control)

Attribute-based access control provides access rights based on any type of attributes—environmental attributes, resource attributes, and user attributes.

- Environmental attributes are those that relate to environmental conditions. It includes the location of the data, time of access, and current organizational threat levels [9].
- Resource attributes can be used to enable access control that relates to a particular resource, such as an operating system or application. It includes things like resource owner, creation date, file name, and data sensitivity [10, 11].
- User attributes include things like the user's role, name, ID, and security clearance [12].

7 Conclusion

We can conclude that for digital success in the future, IAM with strong privilege access management is necessary. This paper summarized every security issue that might occur in cloud environment, proposed mitigation for those issues, and potential threats are discussed with an emphasis on IAM. If all these threats are acknowledged and provided mitigation methods are performed, the transfer from local storage to cloud storage can be carried out very smoothly. As with proper implementation of IAM, cloud is going to become the most secure place to keep confidential data, and all the organizations will be shifting to cloud for storage resulting in cloud becoming the future of storage.

References

1. Singh, A., Chatterjee, K.: Identity management in cloud computing through claim-based solution. In: 2015 Fifth International Conference on Advanced Computing and Communication Technologies (2015). <https://doi.org/10.1109/acct.2015.89>
2. Rowe, N.S.: The future of identity management (2018). Retrieved from <https://techvisionresearch.com/>
3. Mogull, R., Arlen, J., Gilbert, F.: Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1 (2009). <http://www.cloudsecurityalliance.org/>
4. Sharmaa, H.D., Dr. Dhoteb, C.A., Poteyc, M.: Identity and access management as security-as-a-service from clouds. In: 7th International Conference on Communication, Computing and Virtualization (2016)
5. Bresz, F., Renshaw, T., Jeffrey R., Torpey, W.: Identity and access management (2007). Retrieved from <https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%209%20%20Identity%20and%20Access%20Management.pdf>
6. Dragoş, M.M.: Cloud identity and access management—a model proposal. Account. Manag. Inf. Syst. **11**(3), 484–500 (2012)
7. Indu, I., Anand, P.M.R.: Identity and access management in cloud environment: mechanisms and challenges (2015). Retrieved from <https://www.researchgate.net/publication/325336543>
8. Zhu, Y., Huang, D., Hu, C.-J., Wang, X.: From RBAC to ABAC: constructing flexible data access control for cloud storage services. IEEE Trans. Serv. Comput. (2015). <https://doi.org/10.1109/tsc.2014.2363474>
9. Mohammed, H.K., Hassan, A., Yusuf, D.M.: Identity and access management system: a web-based approach for an enterprise. Path Sci. **4**(11), 1–11 (2018)
10. Khurana, M., Singh, H.: Two level phase retrieval in fractional Hartleydomain for secure image encryption and authentication using digitalsignatures. Multimed. Tools. Appl. **79**(19), 13967–13986 (2020)
11. Khurana, M., Singh, H.: An asymmetric image encryption based onphase truncated hybrid transform. 3D Res. **8**, 1–17 (2017)
12. Rohilla, A., Khurana, M., & Singh, L.: Location privacy usinghomomorphic encryption over cloud. Proquest. Int. J.Comput. Netw. Inf. Secur. **09**(08), 32–40 (2017)

Curbing Criminal Acts on Mobile Phone Network



Olasina Jamiu Rotimi, Sanjay Misra, Akshat Agrawal,
Ezenwoke Azubuike, Rytis Maskeliunas, and Robertas Damasevicius

Abstract It is no longer a story that the criminal act is now the order of the day in Nigeria with the way mobile phones and network applications are being used. A lot of Nigerian citizens have in one way or the other fallen prey to this crime through online fraud, hacking into the person's account, retrieving vital information, and the likes. It is, therefore, necessary to detect some of these crimes, reveal them, and proffer possible solutions on how to avoid them, and possibly, how to solve such problems. To do this, the most recent papers were reviewed to create awareness of such criminal act detection and how to curb such activities to create a friendly environment for the usage of mobile phones and network applications without any panic. It is also evident that with the stated methods in this paper, such criminal acts would have been greatly mitigated.

Keywords Mobile phones • Criminal act • Crime • And network

O. J. Rotimi · S. Misra (✉) · E. Azubuike
Covenant University, Ota, Nigeria
e-mail: sanjay.misra@covenantuniversity.edu.ng

E. Azubuike
e-mail: azu.ezenwoke@covenantuniversity.edu.ng

A. Agrawal
Amity University, Gurgaon, Hairiyan, India

R. Maskeliunas · R. Damasevicius
Vytautas Magnus University, Kaunas, Lithuania
e-mail: rytis.maskeliunas@vdu.lt

R. Damasevicius
e-mail: robertas.damasevicius@vdu.lt

1 Introduction

Criminal offenses on mobile phones vary from one level of occurrence to another. This act is ranging from virus attacks, malware activities, hacking, and the likes to mobile phones. It is a criminal offense to illicitly have access to data such as contacts, files, private information (such as Bank Verification Number (BVN), passwords, account details, e-mails, and others) and also to induce destructive mobile software such as malware in the system. It is evident that mobile phone is a necessity, and as such, it makes life easier for people in the way we do businesses, carries out researches, fast-tracking of online processes and activities and for these; it has therefore become what we cannot do without. A paper iterated the outrageous development the Internet use and widespread acceptance [1]. The paper proved the increase in security threats and Nigeria of today, cybercrimes are committed in many ways, and these include frauds on e-mails, wrong identity, hacking, criminal harassment, spamming, spoofing on the use of ATM, piracy acts, phishing, and many more. Cybercrime is no doubt a threat to our immediate environment, and people who used their mobile phones to connect to the Internet are the major points of reference [2]. Information and communication (ICT) trends aided these activities by its enormous tools to perpetrate cybercrimes [3].

Viruses are illicitly introduced software into the system to disrupt the system activities, but malware includes SMS fraud—where users unknowingly subscribed to the service, and at the later end, a cruel way was used to charge users without their knowledge, Spyware—it steals data from users without prior permission of the owner, and so on. [4]. Also, the echo reflection of mobile phones has made them very important means of exchanging information, in the field of communication. Furthermore, there also exists a limitation to how to convey criminal activities to law agencies for quick and needed actions [5, 5]. According to [7], the growth of the telephone network and its availability to the Voice over Internet Protocol (VoIP) has made it a major contribution to its flexibility and also the very easy-to-use artifact for end users. This also contributed significantly to the increase in cyber-criminal activities, and these criminals use emergent technologies to conduct illegal and suspicious activities. Crime analysis is a law enforcement function, and it involves systematic analysis for patterns and trends identification and analysis in crime and disorder. Information acquired from this pattern can then be used in aiding the activities of detectives in identifying and apprehending criminals [8].

The likelihood that a crime is detected and its offender is appropriately charged is a central component of the standard economic model of crime. It is also critical to the incapacitation channel, by which societies can prevent hardened criminals from reoffending. Yet, the economics literature has barely devoted any attention to studying the determinants of crime detection in detail. Typical approaches include examining whether police numbers, police composition, or high visibility patrolling are associated with lower crime rates. The implicit assumption is that a change in these variables can lead to higher chances of catching offenders, which has an immediate deterrence effect as well as an incapacitation effect over longer horizons

[9]. As part of the study, it is necessary to incorporate the action of the police force and other law enforcers to the needed technologies to apprehend the offenders who are cybercriminals. At times, the police may visit the perpetrators at home for questioning as the data of the ownership of the phone in question would be automatically captured for necessary actions. Due to the rapid need for telephone by the service it renders, criminals are now abusing its use to perpetrate various cyber-crime attacks, and it is therefore necessary to logically detect and study some of the already existing solutions to these problems and also propose a new solution as there have never been any of the existing solutions without its setback.

In recent years, the number of online crimes, such as the various emerging scams and criminal schemes, has tremendously increased, and also, the online crime suspects utilize the anonymous nature of the Web to disguise their identity through various methods to evade detection and surveillance from law enforcement agencies. The prime suspect's communication methods and identifying numbers have become so hard to be verified under the electronic surveillance warrant for the Law Enforcement Monitoring Facilities (LEMF). When this is compared with traditional telephone and mobile phone communication records, online communication is more uncertain to be tracked, and its techniques require a sophisticated system [10]. Also, nowadays, providing information and security for mobile phones and also processing it in mobile network data is a great issue of importance and interest. As mobile phones and computers are provided with broader functions, the geometrical growth of vulnerabilities is also increasing in that regard. Today, an unauthorized person who is a criminal can make a call and eavesdrop on them, text message, drop malicious programs like malware, spyware, also steal money, and put the system out of order to his advantage without prior knowledge of the owner [11].

Mobile devices have become an integral part of our daily life, and there is no doubt about that. These have therefore proven to be an advantageous and almost the most successful scientific resolution of our time that fills personal and business needs in a very efficient manner [12]. In this era, the availability of mobile services has significantly increased because of the rich variety of mobile devices and essential applications provided by mobile device manufacturers as has been rightly emphasized in the previous chapter. At the same time, numerous mobile security issues and data privacy threats are challenging the use of this device in various aspects of human endeavor. Therefore, mobile devices are an ideal target for various security issues and data privacy threats in a mobile ecosystem [13]. Also, the impact of cybercrime poses a negative signal over the state of any system, and this can be felt on every individual, economy of a nation, international prospect, and integrity of a nation [1]. This paper, therefore, looks into threat detection and prevention, and also, necessary steps and algorithm to alert the security agencies are put up as a proposed framework and architectural modeling for the future most prominent solution to the problem at hand.

2 Background Information and Literature Review

Researchers have gone far as to carry out a lot of studies and investigations on the issues of threats posed by the use of mobile phones. Particularly, vulnerabilities of this amazing device to illegal act by cybercriminals have necessitated the prompt need of all researchers in the chosen area of the framework to be on their toes as the terror of criminal act has become the order of the day. Any attack on the use of the mobile phone that makes life uneasy for the user is indeed an action that has put such a user in a state of great concern. Therefore, any such challenges should be dealt with. Cybercrime issues encompass stakeholders such as the offender; its target/victim; technological; society and the law, and the architectural model was proposed. This does for the future reservoir of resources for mitigation of cybercrime [14]. The threat on the mobile phone includes (1) viruses, (2) malware, (3) spyware, and (4) limited way to convey information to the needed security agency. Authors [13] fully explained that the threat to the mobile device is multiple and it requires multiple means of protection and restrictions. These researchers proposed a defensive mechanism architecture that can simultaneously handle various threats on the use of mobile phones, but the security measure to alert the police was not put in place. Authors [15] explained that advanced persistent threat (APT) attack is a carefully planned attack that involved both social engineering and malware, where spear phishing is the most popular method that has been used by the attacker. The attacker will send an email to the targeted victim by including link (s) to the targeted Web or malicious attachment to carry out their illegal activities, but this was taken care of by the adoption of smartphones and implementation of security on bringing your device (BYOD). In [16, 17], authors launched preventive measures such as passwords, firewalls, encryption, and detection mechanisms such as tripwires, configuration-checking tools, and anomaly detection systems [18]. In their paper established a helping mechanism in investigating agencies in the detection and identification of criminal acts by the use of methods that involved six approaches—data extraction (DE), data preprocessing (DP), GSM technology, Google map representation, advanced embedded system (ES), and preprocessing of the dataset to safeguard its originality before its cluster analysis. Authors in [19] their paper posed that mostly threat is always from the Internet and therefore tackled by setting up Apache Hadoop cluster with Apache Ambari. Where master and slave nodes represent a Mesintempur as a cluster. Apache Hive was used to aggregate data from raw data for the attack type incorporated with related mechanism, deeper analysis was made, and the resultant attack data was converted to the dataset. The mining was done by the use of the SPMF tool. Besides, authors in [20] studied the Web site, using six different metrics, such as speed, SEO, security, broken links, updates, and availability to come to 54% of good Web sites of Web clustering.

Authors [21] in their paperwork validated the factual establishment of the generated results of their analytically solved problem that was based on leveraging phone numbers analysis in improving the world understanding of the underground markets, illegal activities with computers and software, and cybercrime in general

and by these emphatically stated that scam activities with phone numbers were often and more stable over the period than email addresses. This was backed up by the combination of graph analysis and geographical home location register (HLR) lookup. Authors in [22] went further in their work to gather dataset related to the criminal activities from the cloud, by making the criminal-related information available to the law enforcer to speed up their investigation of criminal identification by developing the police Android application and the general user mobile application.

In [23], authors stated algorithms and mechanisms such as statistics-based algorithm, decision tree-based algorithm, rule-based algorithm, Bayesian classification model to detect fraud in automobile insurance, Naïve Bayesian visualization for data analysis and interpretation, the classifier predictions, and the use of ROC curves data assessment. All these are used for data mining. As a proper check and unbiased technique, authors in [24] proposed discrimination prevention degree (DPD), discrimination protection preservation (DPP), misses cost (MC), and ghost cost (GC). The DPD and DPP measured the success of the proposed method in discrimination prevention which ideally should be 100%. The MC and GC, therefore, measured the degree of information loss that forms the impact on data quality, and it should ideally be 0%. Authors in [25] studied that the best-recommended cryptography application that can be used on IM is encrypt, followed by AES-Crypto, EnDe-Crypto, and Kryptokaz as it is a good way for securing data.

Nevertheless, authors [11] in his work studied three asymmetric encryption techniques: RSA, ElGamal, and elliptic curves to select the most efficient and appropriate algorithm for data transmission. Elliptic curves became the best, and RSA and ElGamal algorithms are not good for the text message at all. These comparisons were done on a carefully designed platform Java 2 Micro Edition (J2ME) using wireless messaging PI (API). The application runs on a mobile phone with an ARM9 processor with a frequency of 219 MHz and 10 Mb of internal memory and the Java virtual machine (JVM) with enabled just-in-time (JIT).

The key parameter of interest is to establish a framework to address spyware, malware, viruses, unauthorized access, and bad Web sites, as there is no single system or model which can take care of all the already existing cybercrimes at the present. Besides, there is no mobile-based app for this function, and in this work, HTML5, CSS, PHP, API-VIRUS TOTAL, and MYSQL would be greatly employed for the system design. One can find other security issues in mobile in various researches [26–29].

Motivation: The existing techniques are not on a mobile app, and besides, no existing solution used multiple solutions to solve the criminal acts. This system was proposed to use multiple techniques of different algorithms to mine data, detect unwanted data, and curb Internet crimes, and reporting to the necessary law enforcement agent using mobile phones at the discretion of the user is the required task. Also, the driven force centered on the gap created by the past researchers. This then enables us to come up with this tremendous model as a mobile app.

Aim and Objectives: The aim is to establish and build a mobile app to compliment the already existing algorithms, using different techniques of the framework

to prefer solutions to the cybercrimes. The objective is for the proposed framework to deliver real data to the receiving-end phone; send details of the sending-end phone handler to the law enforcement agent; and block any unwanted data from disrupting or intercepting the system.

3 Proposed Model

In this study, we propose an upgrade of existing technologies to curb cybercrimes on the use of mobile phones. In the upgrade, a Web-based application that will interrupt the activities going-on on a mobile phone will automatically be linked to the phone number of the police or law enforcer agencies for proper action. Besides, any bad Web would be kicked out of action, and only the good one will go through. We, therefore, propose the architectural framework that will detect, identify, and solve multiple problems of cybercrimes using a mobile app. The proposed model is shown in Fig. 1 below.

The model is divided into four categories, and these categories include the sending-end section, intruder section, mobile app section, and receiving-end

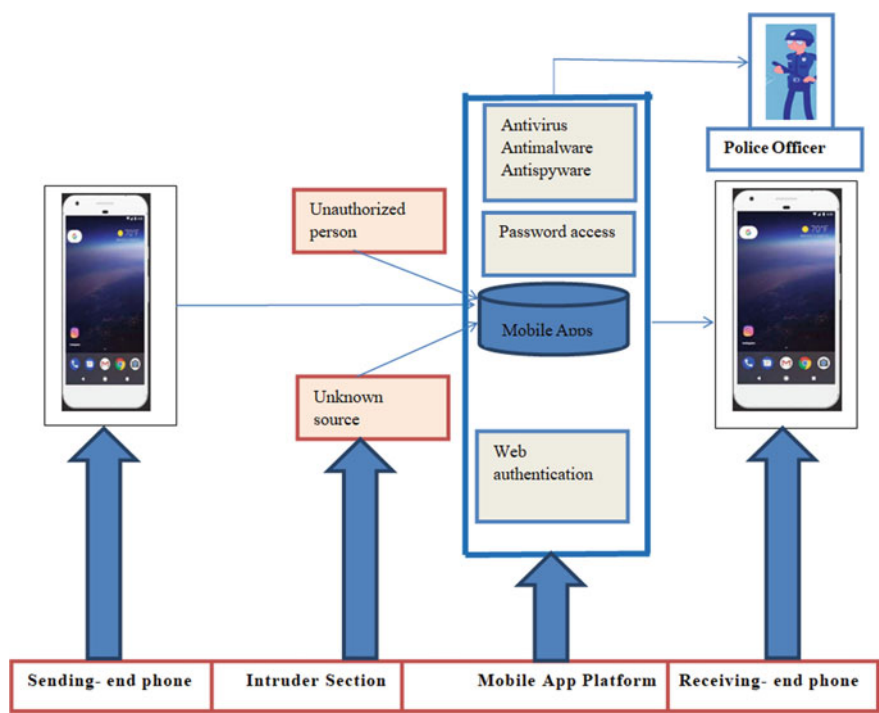


Fig. 1 Proposed architectural framework for the model

section. At the sending-end section, data which would either be a text message or multimedia message and so on is to be sent to the receiving-end phone section. But before then, such data would have to go through the mobile app section for necessary actions before it is finally received at the receiving-end phone. For the scope of this work, data from the sending-end phone is called real data, while data from unauthorized access and unknown sources, virus, malware, spyware, and the like is called unwanted data. The main function of the mobile app section is to detect unwanted data and block it, and a platform is provided to dial security code for necessary action or sanction of the culprit. The app will send personal information of the culprit to the law enforcer agent that is with such a phone identity number. The algorithm that explains the operational flow of the proposed framework and flowchart is shown in Fig. 2.

0 Start.

1 Log in your detail to open the APP (APP Launching).

2 If no details, create one (Create One).

3 Check if there is any data from an unauthorized person (Duk).

4 Check whether a good Web site (GWS) or bad Web site.

5 Check for any software threat (THREAT).

6 Allow the real data on the device (REAL DATA).

7 Block any unwanted data (UD) from having access to the recipient phone.

8 Forward the address of the sending-end phone to the closest law enforcer.

9 Stop.

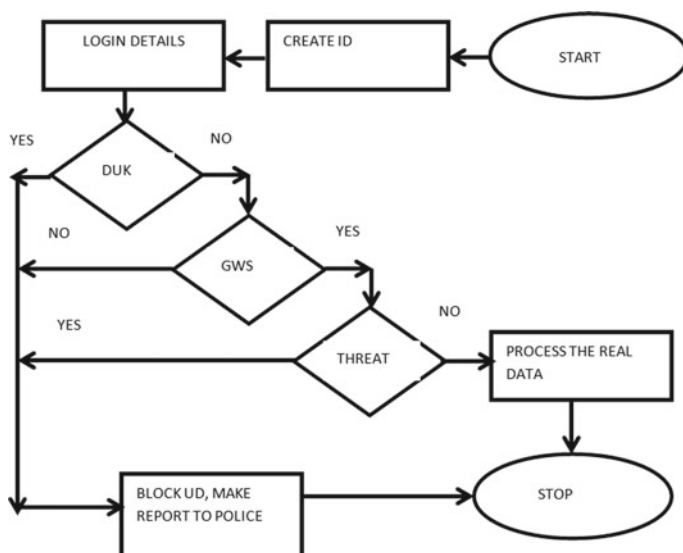


Fig. 2 Flowchart

3.1 Implementation of the Proposed Model

The process is divided based on the aim of the proposed work, and this goes down the line from specification to the evaluation across tasks to be handled by the mobile app section. The app should synchronize between the incoming data and the receiving-end phone. See Fig. 3, being a model for interoperability of the entire development process. The process is discussed below:

Specifications: The app will remove viruses, malware, spyware, and block bad Web sites and unwanted data. It will relay the good data to the intended receiver and channel details of any detected criminal act to the police agency if necessary by the user.

Design: The design was done by the use of HTML5, CSS, JQUERY, and PHP. These software tools were used to design both the front end and back end. The database that was used is MYSQL, and the Android-based application that was used for virus detection function is API-VIRUS TOTAL.

Implementation: The design as it has been listed is implemented following all algorithms incorporated in the mobile app model, and the necessary results were generated.

Evaluation: The mobile app was evaluated through deployment to check if any aspect will require visitation for the betterment of the system.

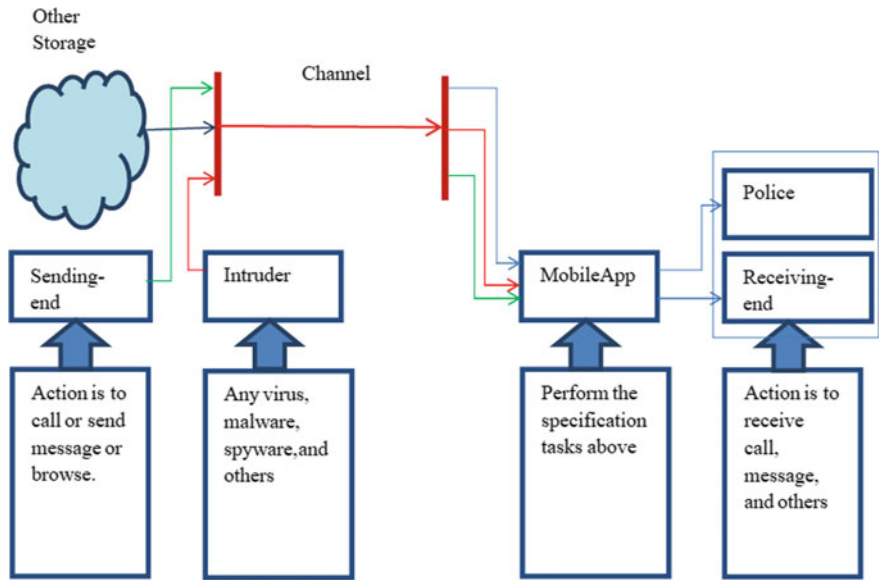


Fig. 3 Model for interoperability of the entire development process

4 Experimental Results

The results obtained are demonstrated in cropped screenshot pictures. The interface for each stage is shown under appropriate sections. See Figs. 6, 7, and 8, for the front-end view of options for test link, test files, file report, and help. The help option will guide any new user on how to use the app, for there are links that such users will follow to help with how it works.

When the mobile app is launched, it will display the front end as shown in Fig. 4 below. As soon as the requirement for logins is satisfied, it will launch the front end in Fig. 5, and from there, the option will be chosen for the link test, file test, file report, and help. The test link option will help to check if the link is a good one or not. The file option will check if the file is free from viruses and the data does not contain any malicious program. The file report option helps to show the environment where the user may decide to let law enforcer such as the police be aware.

Figure 6 is the front end that provides a space for testing any link whether such link is free of any software problem.

Figures 7 and 8 show the interfaces for the help menu and test file, respectively. At the help menu interface, the new user or any first-timer will be able to learn about the app and get familiar with how it works. On the other end, the test file platform provides a space to test a particular file and establish its state whether it is a problem-free file or not.

Fig. 4 Link for login

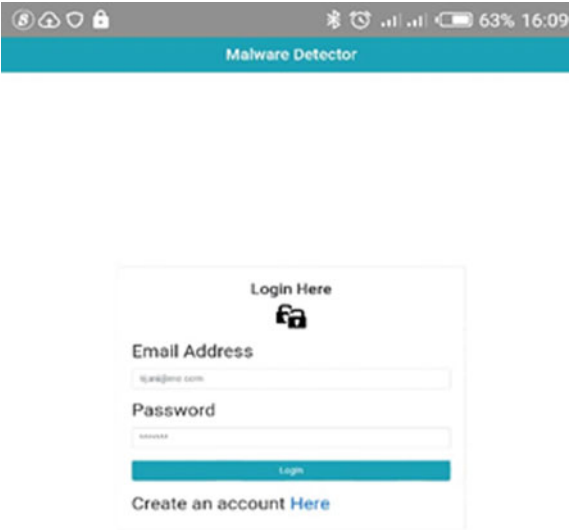


Fig. 5 Links for necessary actions

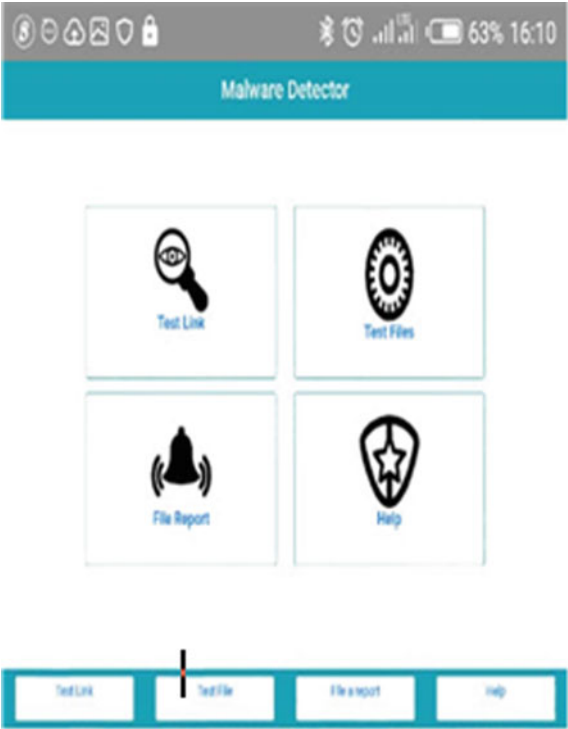


Fig. 6 Test link

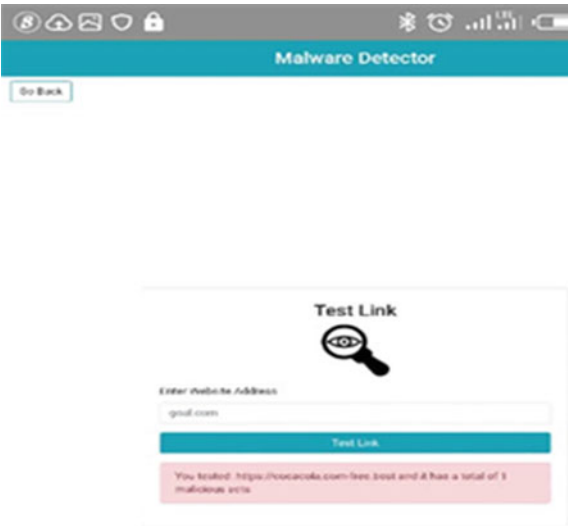


Fig. 7 Help



Fig. 8 Test file



5 Conclusion and Future Work

The proposed model was deployed using HTML5, CSS, JQUERY, and PHP to design the front end and back end of the Android-based mobile app, MYSQL was used for the database, and API- VIRUS TOTAL was used for virus detection application. This app has been implemented, and it works on Android mobile phones perfectly. This app can check for viruses, spyware, and malware, and also, it can link the phone caller for the option to send messages or details of any criminal activities to any law enforcer such as a police officer for necessary action. Also, it will disallow any infected data from affecting the receiver system, and it equally blocks such data. This work can further be extended by capturing detailed information of the criminals, block all his channels by which he was carrying out his usual criminal activities. Also, future work should address the identification of the criminal and his locations using the techniques of deep learning and artificial neural network.

Acknowledgements The authors appreciate the sponsorship from Covenant University through its Centre for Research, Innovation and Discovery, Covenant University, Ota Nigeria.

References

1. Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M., Esan, A.O.: Cybercrimes in Nigeria: analysis, detection and prevention. *FUOYE J. Eng. Technol.* **1**(1), 37–42 (2016)
2. Ishwarya, T.A.S.K.: Cyber crime : prevention and detection **4**(3), 45–48 (2015) <https://doi.org/10.17148/IJARCCCE.2015.4311>
3. Tanui, D.K.: Use of ICT in the detection and prevention of crime in Kenya **6**(9), 62–71 (2016)
4. Rashid, A.M., Al-oqaily, A.T.: Detect and prevent the mobile malware. *Int. J. Sci. Res. Publ. IJSRP* **5**(5), 9–11 (2015)
5. Agangiba, W.A., Agangiba, M.A.: Journal of Computing: mobile solution for metropolitan crime detection and reporting. *J. Emerg. Trends Comput. Inf. Syst. Univ. Cape Town, South Africa* **4**(12), 916–921 (2013)
6. Agangiba, W.A., Agangiba, M.A.: Journal of computing: mobile solution for metropolitan crime detection and reporting. *J. Emerg. Trends Comput. Inf. Sci.* (2019)
7. Bordjiba, H.E., Karbab, E.B., Debbabi, M.: Data-driven approach for automatic telephony threat analysis and campaign detection. *Digit. Investig.* **24**, S131–S141 (2018). <https://doi.org/10.1016/j.diin.2018.01.016>
8. Umamaheswari, B., Nithya, P., Chandran, N.S.: Survey on web crime detection using data mining technique **5**(1), 177–184 (2016)
9. Blanes, J., Kirchmaier, T.: The effect of police response time on crime detection * 1–47 (2015)
10. Chen, C., Chen, W., Wang, Y., Lo, C.: Procedia engineering a real-time crime detection system based on lawful interception—a case study of msn messenger (2011). <https://doi.org/10.1016/j.proeng.2011.08.304>.
11. Starikovskiy, A.: Text messages protection system text messages protection system. *Procedia Comput. Sci.* **123**, 457–466 (2018). <https://doi.org/10.1016/j.procs.2018.01.070>

12. Dong, Y., Pinelli, F., Gkoufas, Y., Nabi, Z., Calabrese, F., Chawla, N.V.: Inferring unusual crowd events from mobile phone call detail records **2**, 474–492 (2015) <https://doi.org/10.1007/978-3-319-23525-7>
13. Khan, J., Abbas, H., Al-Muhtadi, J.: Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Comput. Sci.* **56**(1), 376–383 (2015). <https://doi.org/10.1016/j.procs.2015.07.223>
14. Singh, M.M., Bakar, A.A.: A systemic cybercrime stakeholders architectural model a systemic cybercrime stakeholders architectural model. *Procedia Comput. Sci.* **161**, 1147–1155 (2019). <https://doi.org/10.1016/j.procs.2019.11.227>
15. Zulkefli, Z., Singh, M.M., Mohd Shariff, A.R., Samsudin, A.: Typosquat cyber crime attack detection via smartphone. *Procedia Comput. Sci.* **124**, 664–671 (2017). <https://doi.org/10.1016/j.procs.2017.12.203>
16. Smith, J.L., Smith, M., Smith, J.L.: The perpetration and prevention of cybercrimes. Available at SSRN 1123743
17. Prasanthi, M.M.L.: Cyber crime: prevention and detection. *Ijarccce* **4**(3), 45–48 (2015). <https://doi.org/10.17148/ijarccce.2015.4311>
18. Sathish, A., Prathyusha, M., Priyanka, M.: Crime detection and criminbal identification using IOT **4**(1), 2–4 (2018)
19. Hidayanto, B.C., Muhammad, R.F., Kusumawardani, R.P., Syafaat, A.: Network intrusion detection systems analysis using frequent item set mining algorithm FP-max and Apriori. *Procedia Comput. Sci.* **124**, 751–758 (2017). <https://doi.org/10.1016/j.procs.2017.12.214>
20. Rakhmawati, N.A., Ferlyando, V., Samopa, F., Astuti, H.M.: A performance evaluation for assessing registered websites. *Procedia Comput. Sci.* **124**, 714–720 (2017). <https://doi.org/10.1016/j.procs.2017.12.209>
21. Costin, A., Isacenkova, J., Balduzzi, M., Antipolis, S.: The role of phone numbers in understanding cyber-crime schemes
22. Dabhere, A., Kulkarni, A., Kumbharkar, K., Chhajed, V., Tirth, S.: Crime area detection and criminal data record **6**(1), 510–513 (2015)
23. Bhowmik, R.: Journal of digital forensics, security and law data mining techniques in fraud detection data mining techniques in fraud detection **3**(2) (2008)
24. Hajian, S., Domingo-Ferrer, J., Martinez-Balleste, A.: Discrimination prevention in data mining for intrusion and crime detection. *IEEE SSCI 2011 Symp. Ser. Comput. Intell. CICS 2011 IEEE Symp. Comput. Intell. Cyber Secur.* 47–54 (2011). <https://doi.org/10.1109/CICYBS.2011.5949405>
25. Liwandouw, V.B., Wowor, A.D.: The existence of cryptography: a study on instant messaging. *Procedia Comput. Sci.* **124**, 721–727 (2018). <https://doi.org/10.1016/j.procs.2017.12.210>
26. Jambhekar, N.D., Misra, S., Dhawale, C.A.: Mobile computing security threats and solution. *Int. J. Pharm. Technol.* **8**(4), 23075–23086 (2016)
27. Osho, O., Mohammed, U.L., Nimzing, N.N., Uduimoh, A.A., Misra, S.: Forensic analysis of mobile banking apps. *Lecture Notes Comput. Sci.* **11623**, 613–626 (2019)
28. Alhassan, J.K., Oguntoye, R.T., Misra, S., Adewumi, A., Maskeliūnas, R., Damaševičius, R.: Comparative evaluation of mobile forensic tools. *Adv. Intell. Syst. Comput.* **721**, 105–114 (2018)
29. Osho, O., Musa, F.A., Misra, S., Uduimoh, A.A., Adewunmi, A., Ahuja, R.: AbsoluteSecure: a tri-layered data security system. *Commun. Comput. Inf. Sci.* **1078**, 243–255 (2019)

Designing of Fuzzy Logic-Based Intrusion Detection System (FIDS) for Detection of Blackhole Attack in AODV for MANETs



Ruchi Makani and B. V. R. Reddy

Abstract Mobile Ad hoc networks (MANETs) are wireless/infrastructure-less and resource-constraint, having collection of nodes with high mobility feature (Ramanathan and Redi in IEEE Commun Magaz 40(5) 2002). It is a challenge to have efficient intrusion detection system (IDS) for such wireless and mobile architecture of systems. Researchers have presented in their research that the fuzzy logic-based intrusion detection systems are more adoptable to MANET's application because behavior of any mobile node may be visualized in fuzziness characteristics. It is required to design robust IDS system which can sustain and can work efficiently in MANET environments. The work presents the selection of suitable protocol features and fuzzy rules generation which exhibits substantial role for precision of the fuzzy logic-based intrusion detection system (FIDS). Here, set of fuzzy rules have been proposed to protect network against blackhole attack. These set of rules are created using three AODV critical attribute which are rate of *RREQ*, *RREP* and *Sequence number* value. The proposed FIDS, thereafter, evaluated using ns2 simulator and are found efficient to detect and isolate the attacker node from the network. The deployment of FIDS has resulted in increase of throughput of the network.

Keywords AODV · MANET · Fuzzy-logic · Intrusion detection · Blackhole

1 Introduction

Aim of an intrusion detection system (IDS) is to ascertain attack or malicious activities in a standalone system or in networked systems, by continuously monitoring the audit trail of traffic. IDS largely use soft-computing techniques to monitor the 'arriving at' and 'passing by' of traffic packets to detect intrusion. Fuzzy

R. Makani (✉) · B. V. R. Reddy
University School of Information, Communication & Technology,
Guru Gobind Singh Indraprastha University, Delhi, India
e-mail: ruchichaudhary@nic.in

logic-based intrusion detection model uses fuzzy rules or fuzzy classifiers to detect various intrusive behaviors by creating more abstract and flexible patterns for intrusion detection and provides significant advantages over other techniques [2, 3]. The use of fuzziness helps to understand the abrupt separation in normal and abnormal behavior of the node distinctly and also provides a measure of the degree of normality or abnormality of an event. Section 2 of this paper has presented general overview of fuzzy logic-based intrusion detection systems. Section 3 covers the critical filed of AdHoc on-demand distance vector (AODV) protocol used in MANETs. Section 4 is presenting proposed fuzzy rules for IDS designing in detail. Sect. 5 covering the simulation of FIDS for MANETs, and the performance of AODV has been recorded with and without blackhole attack. Section 6 concludes the finding of the work.

2 Overview of Fuzzy Logic-Based Intrusion Detection

Only fuzzy logic is a computational paradigm that builds a set of user-defined rules which are converted into mathematical equivalents [4–6]. Moreover, it has the advantage to offer valuable flexibility for reasoning that considers inaccuracies and uncertainties [7–10]. It can also manage approximate reasoning instead of fixed reasoning and able to handle imprecise and incomplete data. In standard set theory, each element is either completely a member of a category or not a member at all. In contrast, fuzzy set theory allows partial membership in sets or categories. In fuzzy logic, the truth value of any event can be termed between ‘0’ and ‘1’. Fuzzy logic-based intrusion detection (FLID) classifies the nodes into ‘trusted nodes’ and ‘malicious nodes’ after evaluating the nodes’ behavior (i.e., degree of reliability) by utilizing user-defined fuzzy inference rules [11–13]. Primarily, an FLID consists of three processing steps: fuzzification, inference system and defuzzification.

Fuzzification: In fuzzification, input data values are obtained and converted into fuzzy set by using fuzzy linguistic variables and membership functions. In inference processing system, a set of fuzzy rules are created (*in form of ‘IF–THEN’ decision statements to encode an expert’s knowledge of known patterns of attack and system vulnerabilities*) by the user, depending on the application environment/requirement.

Inferences System: Inferences are established after the processing of inputs based on fuzzy rules. The inferences are then combined to compute the fuzzy output distribution.

Defuzzification: In defuzzification, the resulting fuzzy output distribution is mapped back to a crisp output value using the membership functions. The detailed processing involved in each step of fuzzy-based intrusion system is available in [14, 15]. However, a broad flow chart of the FLID is shown in Fig. 1.

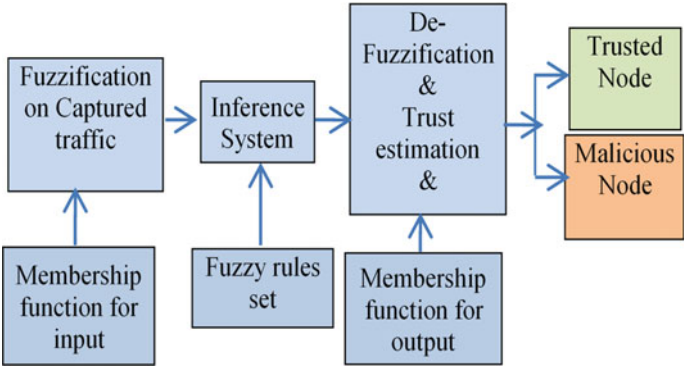


Fig. 1 Flow chart of fuzzy-logic-based IDS

3 Critical Fields of AODV Routing Protocol

AODV [16] is one of the most popular and widely used reactive routing protocols in MANETs. AODV ensures loop-free, single path and hop-by-hop distance vector routing [17]. AODV operates in two sub phases: *Route discovery* and *Route maintenance*. It uses four types of message packets to communicate among each other—route request (RREQ) and route reply (RREP) messages are needed in route discovery subphase, and route error (RERR) messages and HELLO messages are needed in route maintenance subphase. In each AODV routing packet, some critical fields such as control packet ID, type, hop count, sequence numbers of source and destination, IP addresses of source and destination, flags, lifetime are essential for correct protocol execution and routing [18, 19]. However, attackers may launch attack by advertising altered routing information to mislead correct routes (*known as route logic compromising attacks*) or by intently dropping the packets (*known as packet distortion attacks*). Any misuse or alteration of these critical fields by the attacker can cause AODV routing protocol to malfunction resulting in network performance degradation. Various publications relating to attacks of AODV and its effect on the network are available in [18, 19].

4 Proposed Fuzzy Rules for IDS Designing

In the above Sect. 3, the critical field of AODV protocols have been discussed which may be modified by attackers to deteriorate network performance. Here, efforts have been made to design a robust fuzzy logic-based intrusion detection (FIDS) system which is capable of detecting a blackhole attacker node in a network. For this, three attributes have been used to build up the fuzzy rules for fuzzification: (i) rate of forwarding RREQ control packet, (ii) rate of forwarding the RREP

packets and (iii) value of sequence number. For the development of robust and effective FIDS, three following steps have been taken for designing.

4.1 Fuzzification

For the designing of FDIS, the fuzzy logic designer MATLAB (version 9.7) toolbox has been used. The three inputs, i.e., RREQ, RREP and sequence number, have been taken. The RREQ input have been divided into three categories, viz., very high (*reqVH*), high (*reqH*) and low (*reqL*). RREP is divided into two datasets, viz., high (*repH*), low (*repL*), and the sequence number is divided into three datasets, viz., high (*nauH*), medium (*nauM*), low (*nauL*). The designed FIDS’s block diagram is shown in Fig. 2. The output value (*named as ‘trust’*) has been estimated from the FIDS.

The membership function for output ‘trust’ has been divided in five sets ranging from 0 to 1 as very high (*VH*), high (*H*), medium (*M*), low (*L*) and very low (*VL*), as depicted in Fig. 3. Data is converted into fuzzy set by using fuzzy linguistic

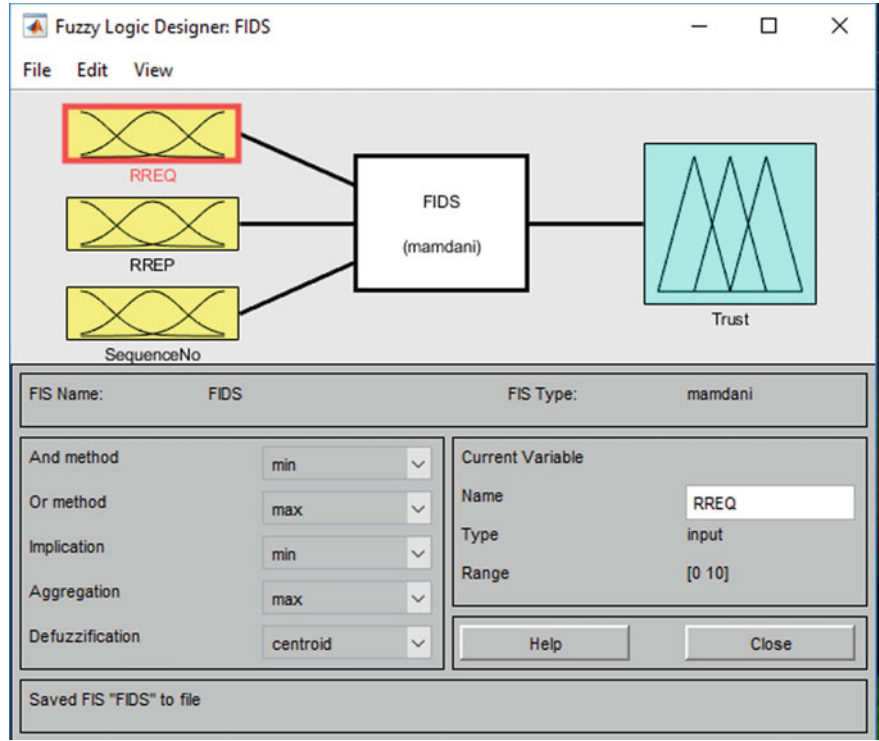


Fig. 2 FIDS designer

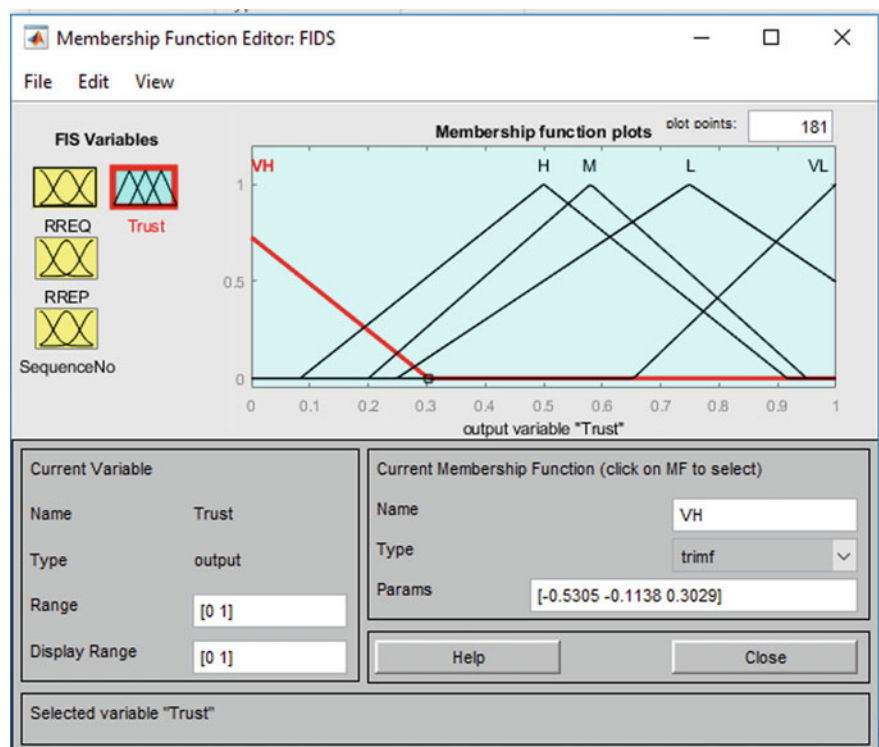


Fig. 3 Output fuzzy membership function plot

variables and membership functions. Here, triangular function (*trimf*) have been used for fuzzification. For the evaluation of the proposed FIDS, an input data value is obtained using simulations of MANET network in network simulator software (version ns 2.35) and has been discussed in the next section.

4.2 Inferences System

A set of 16 fuzzy rules have been created (in the form of 'IF-THEN' decision statements) to discern the behavior of node for the detection of a blackhole attacker (malicious node) in a given network. The blackhole attacker node broadcasts the route reply packet against the response of route request packet send by node with high sequence number to present the freshness of the loop. Based on this theory, following 16 rules have been included in FIDS. The details of the rules are listed in Table 1, and their inclusion in the fuzzy toolbox is shown in the Fig. 4. Inferences are derived after the processing of inputs based on fuzzy rules. The inferences are

Table 1 Proposed fuzzy rules

1. (REQ == reqL) (RREP == repL) (SequenceNo == nauL) => (Trust~ = VH) (1)
2. (RREQ == reqH) (RREP == repL) (SequenceNo == nauM) => (Trust=H) (0.1)
3. (RREQ == reqL) (RREP == repH) (SequenceNo == nauL) => (Trust=M) (0.1)
4. (RREQ == reqH) (RREP == repL) (SequenceNo == nauL) => (Trust=M) (0.1)
5. (RREQ == reqH) (RREP == repH) (SequenceNo == nauL) => (Trust=M) (0.1)
6. (RREQ == reqVH) (RREP == repL) (SequenceNo == nauL) => (Trust=M) (0.1)
7. (RREQ == reqVH) (RREP == repH) (SequenceNo == nauM) => (Trust=M) (0.1)
8. (RREQ == reqL) (RREP == repL) (SequenceNo == nauM) => (Trust=M) (0.1)
9. (RREQ == reqL) (RREP == repH) (SequenceNo == nauM) => (Trust=L) (0.1)
10. (RREQ == reqH) (RREP == repH) (SequenceNo == nauM) => (Trust=L) (0.1)
11. (RREQ == reqVH) (RREP == repL) (SequenceNo == nauM) => (Trust=L) (0.1)
12. (RREQ == reqVH) (RREP == repL) (SequenceNo == nauH) => (Trust=L) (0.1)
13. (RREQ == reqL) (RREP == repL) (SequenceNo == nauH) => (Trust~ = VL) (0.1)
14. (RREQ == reqL) (RREP == repH) (SequenceNo == nauH) => (Trust~ = VL) (0.5)
15. (RREQ == reqH) (RREP == repH) (SequenceNo == nauH) => (Trust~ = VL) (0.5)
16. (RREQ == reqVH) (RREP == repH) (SequenceNo == nauH) => (Trust~ = VL) (0.5)

then combined to compute the fuzzy output distribution. The graphical representation of the inference obtained after the computation is depicted in Fig. 5.

4.3 Defuzzification

The resulting fuzzy output distribution is mapped back to output value using the same membership functions which was used during fuzzification. Here, triangular function (*trimf*) has been used. In the following Table 2 are a few test data which were used in simulation to compute the defuzzification.

5 Simulations and Result Discussion

To establish the importance of intrusion detection systems in a mobile network in Sect. 5.1, performance of AODV has been recorded with and without blackhole attack. In Sect. 5.2, performance of FIDS has been evaluated in presence of blackhole attack.

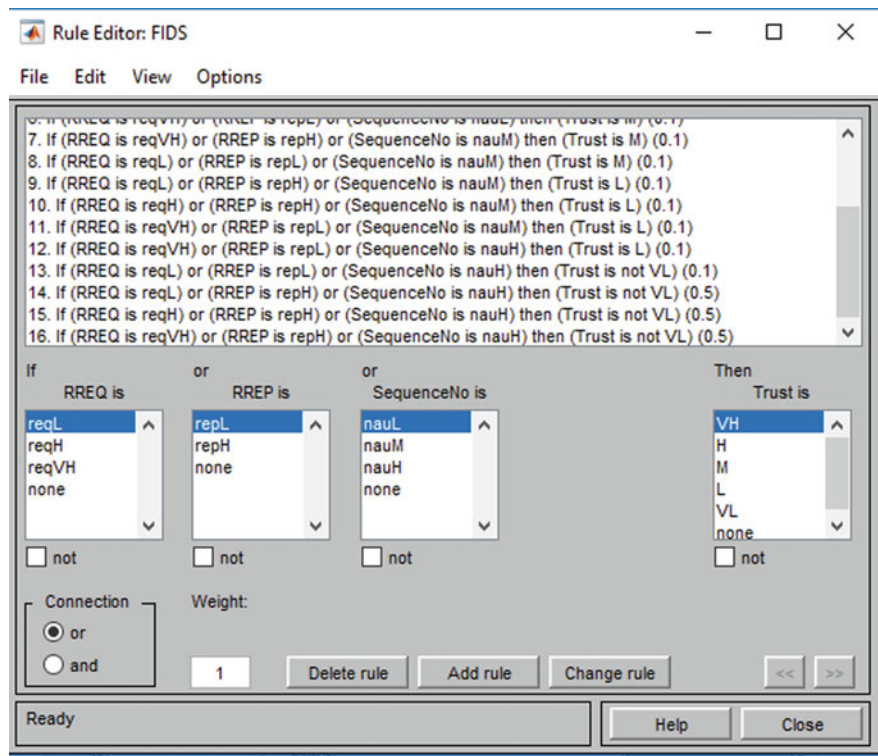


Fig. 4 Fuzzy rules (if-then-else form)

5.1 Performance Evaluation of AODV Protocol Under Attack

Firstly, within AODV protocol source codes, blackhole attacks have been simulated using network simulator software (ns2.35). The general simulation parameters are given in Table 3. The AODV performance is recorded in terms of packet delivery ratio, throughput, energy consumption and routing overhead in the presence of blackhole attack and without attack.

It is observed that packet delivery ratio decreases when there is a one blackhole node attack in a network. Further, this reduces by 60% when there is two blackhole node present in a network, and simulation results are shown in Fig. 6. It is observed that throughput is reduced in the presence of one blackhole node attack in a network. This reduces more significantly approximately 60% in the presence of two blackhole nodes in a network, and simulation results are shown in Fig. 7. Further, it is recorded that network energy consumption increases by 50% in the presence of two blackhole nodes in a network, and simulation results are shown in Fig. 8. Similarly, it is found that routing overhead in a given network also increases in the presence of two blackhole nodes in a network, and simulation results are shown in Fig. 9.



Fig. 5 Graphical representation of fuzzy rules

Table 2 Inference computation

Rate of RREQ	Rate of RREP	Sequence No	Computed trust	Inferences
5	5	5	0.5	Normal
0.301	5	5	0.544	Normal
0.301	9.46	5	0.544	Normal
0.958	9.46	9.22	0.458	Malicious
0.958	0.542	9.22	0.544	Normal
0.958	0.542	0.663	0.546	Normal
7.41	0.904	0.663	0.549	Normal
9.1	0.904	0.663	0.551	Normal
9.34	0.542	9.22	0.544	Normal
9.34	4.4	9.22	0.458	Malicious

Table 3 Simulation parameters for MANETS

Parameters	Value
Simulation tool	NS-2.35
Network nodes	20
Grid area	500 × 500
Routing protocol	AODV
Antenna	Omni directional
MAC type	802.11
Traffic type	CBR
Number of blackholes	2 nodes
Simulation time	500 s

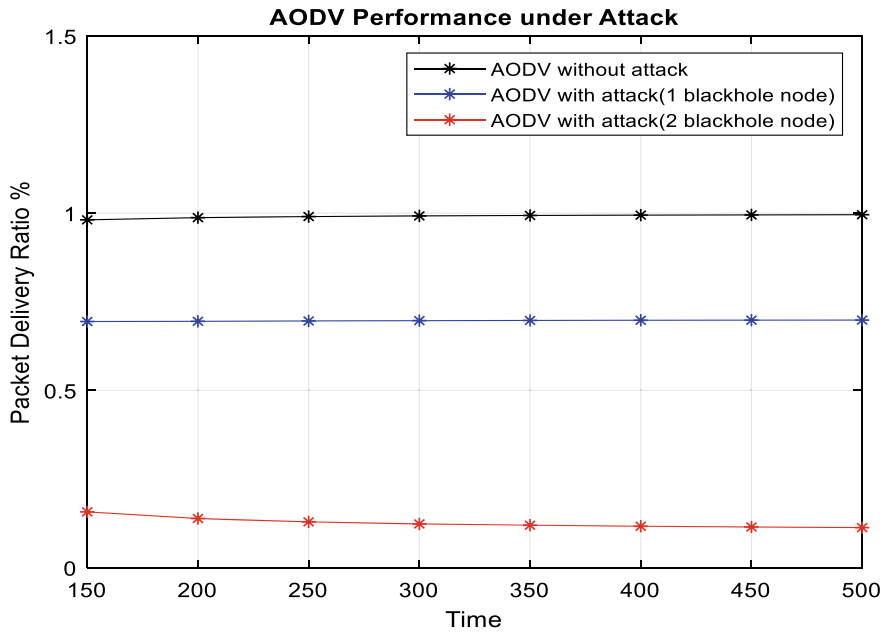


Fig. 6 AODV under attack—PDR versus simulation time

5.2 Performance Evaluation of Proposed FIDS in AODV Protocol

For the evaluation of the proposed FIDS, AODV source codes in ns 2.35 software have been modified and fuzzy-based intrusion detection module has been added. Further, the multiple blackhole attacks have been simulated in a given network.

It is observed that the performance of the network increases on the incorporation of proposed FIDS, as shown in the Figs. 10 and 11. Both PDR and throughput of the network are found to increase when FIDS has been included in AODV protocol.

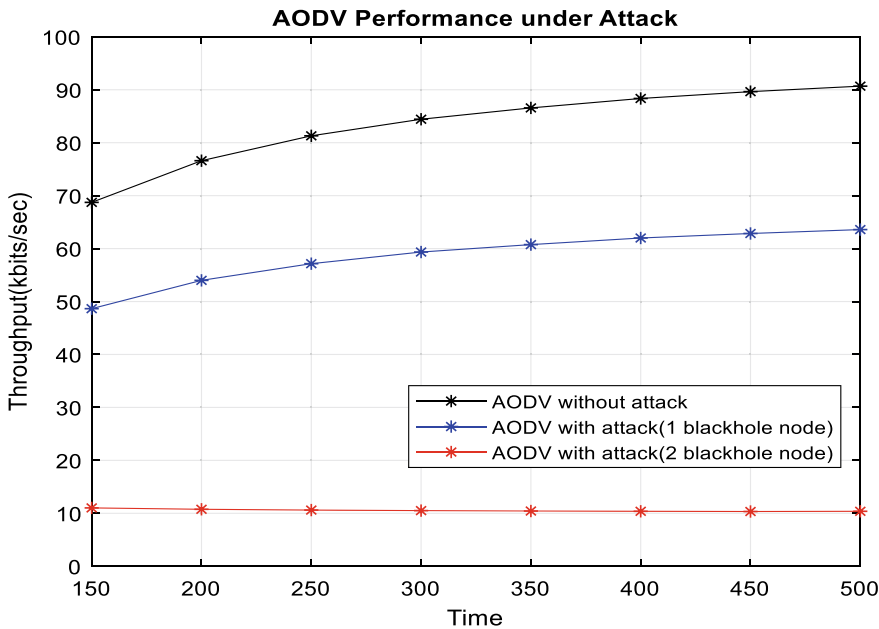


Fig. 7 AODV under attack—throughput versus simulation time

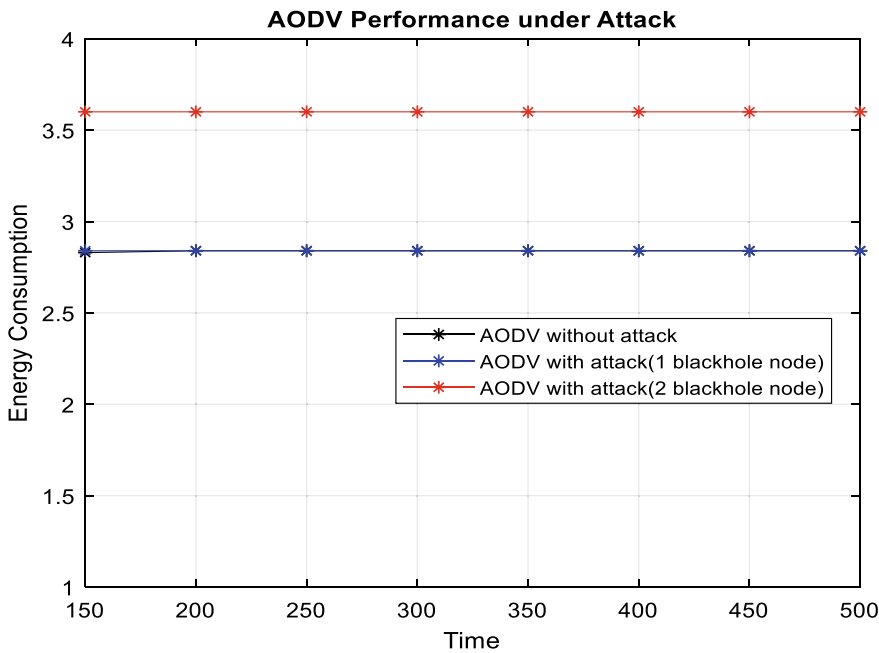


Fig. 8 AODV under attack—energy consumption versus simulation time

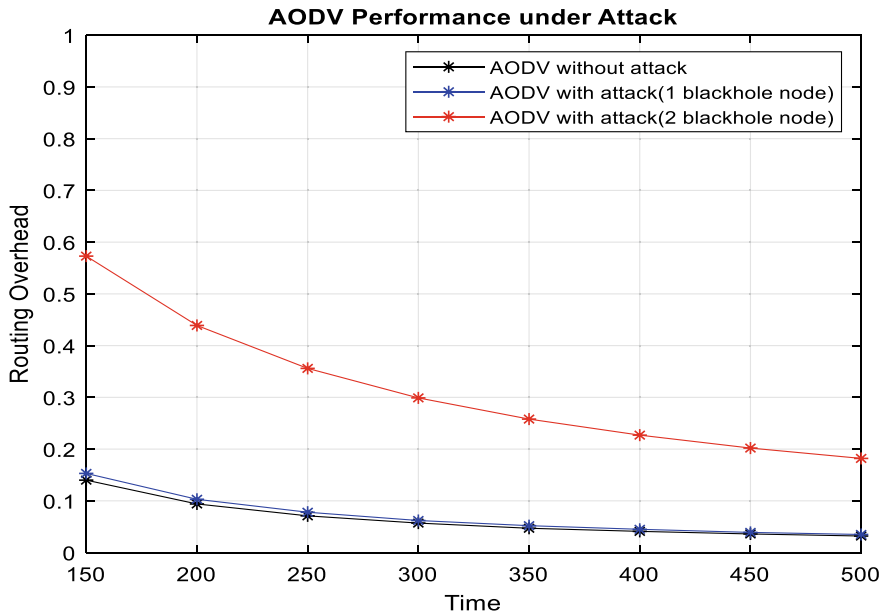


Fig. 9 AODV under attack—routing overhead versus simulation time

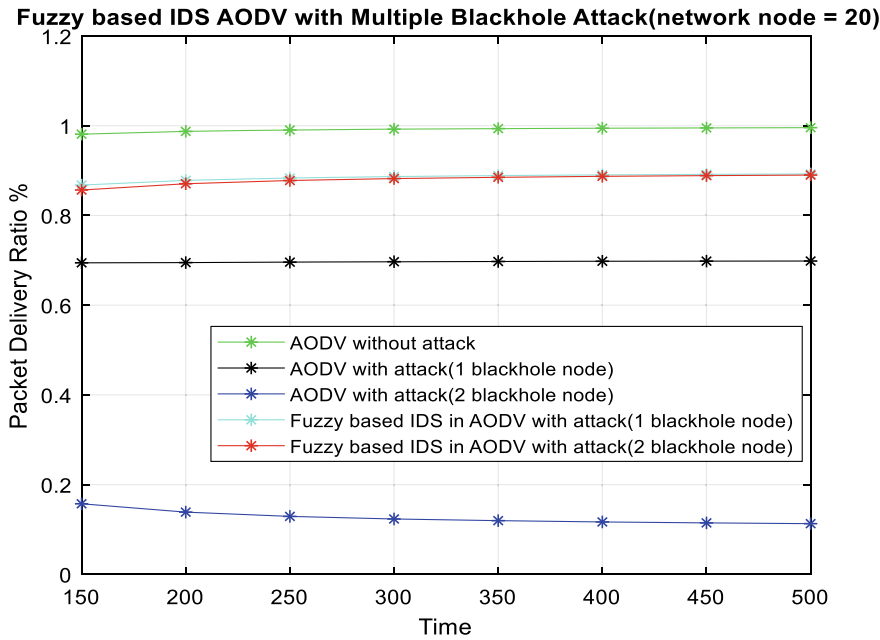


Fig. 10 FIDS performance under attack—PDR versus simulation time

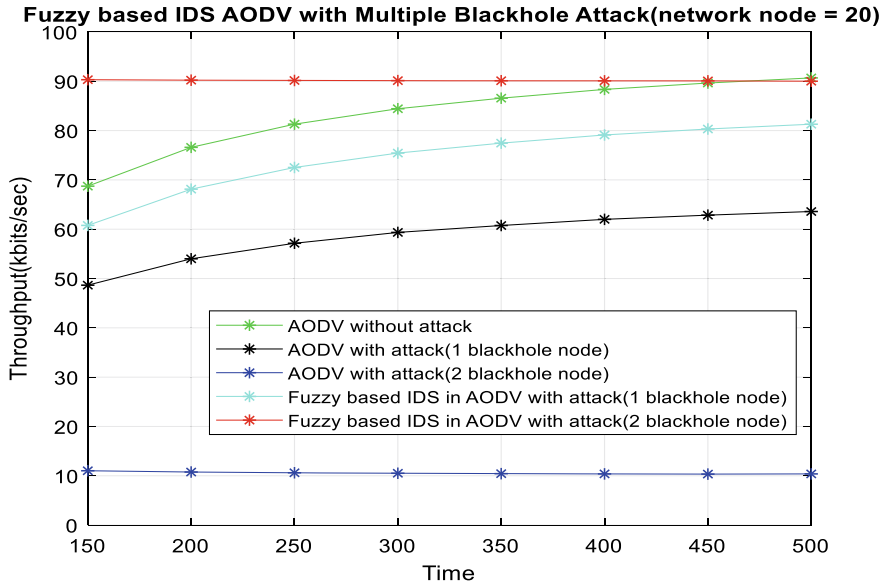


Fig. 11 FIDS performance under attack—throughput versus simulation time

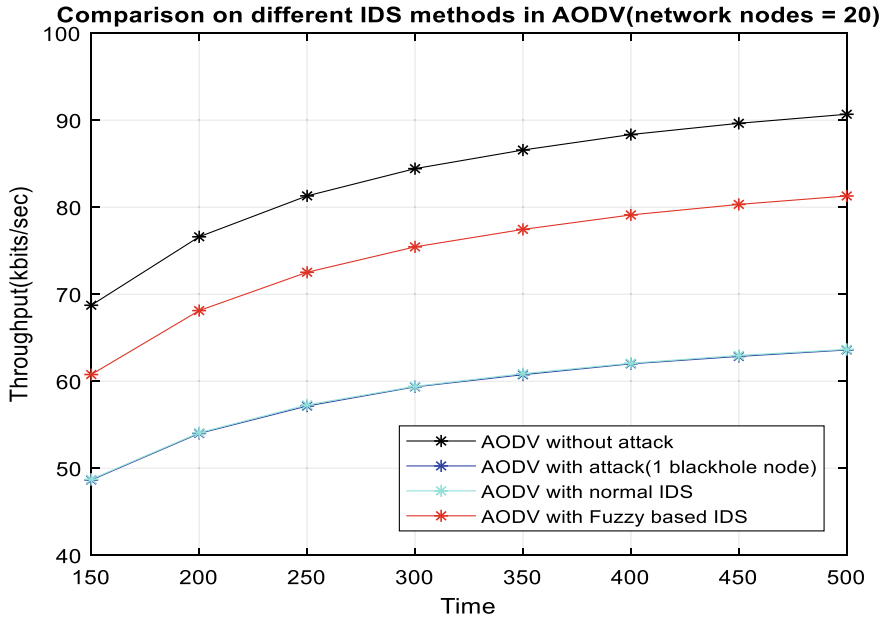


Fig. 12 Comparison on different IDS—throughput versus simulation time

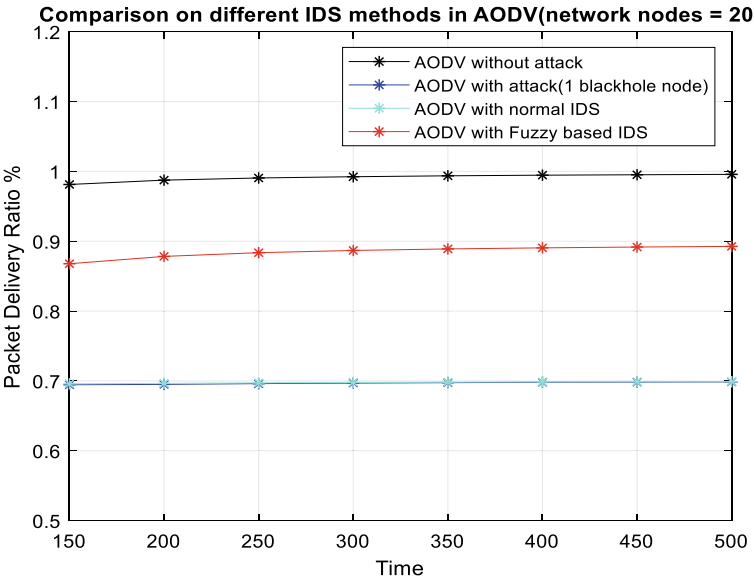


Fig. 13 Comparison on different IDS—PDR versus simulation time

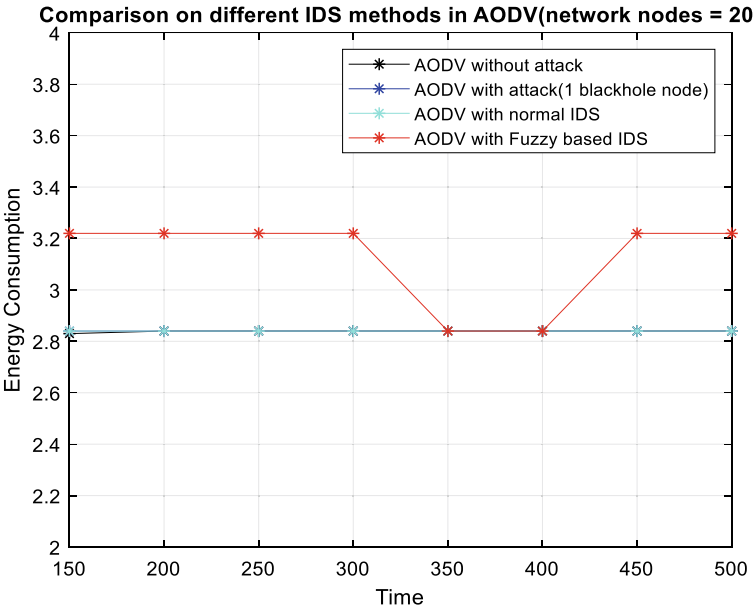


Fig. 14 Comparison on different IDS—energy consumption versus simulation time

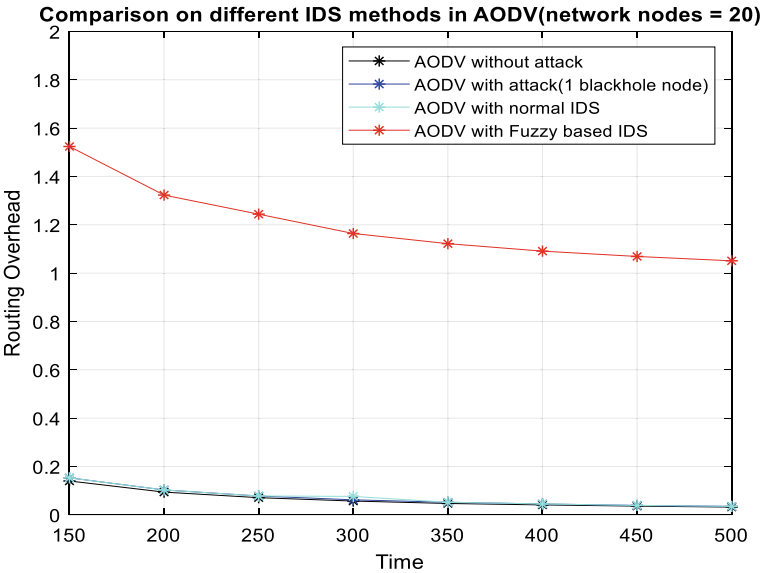


Fig. 15 Comparison on different IDS—routing overhead versus simulation time

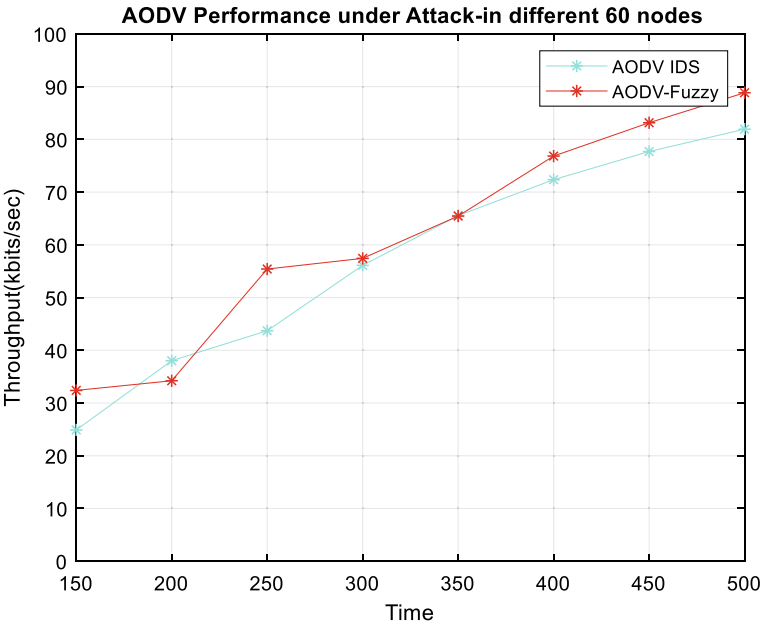


Fig. 16 Comparison on IDS with different node numbers—throughput versus simulation time

Moreover, in the presence of multiple blackhole attacks, similar results have been observed. In addition to this, the performance of FIDS is compared with the another IDS which was proposed by author Dokurer [20]; here, it is named as normal IDS which works on the principle of ignoring the first established route to reduce the effects of the blackhole attack because blackhole node always responds with a fake reply without making delay.

The evaluation of the proposed FIDS has been carried out by calculating the performance metrics, i.e., throughput, packet delivery ratio, energy consumption and routing overhead in the Figs. 12, 13, 14 and 15, respectively. At each time, it is being compared with the normal IDS. It is observed that in the proposed FIDS has increased throughput and PDR which results in better network performance. However, slight increase in energy consumption and routing overload is found because computation processing is involved in FIDS working. Further, results are also validated with different number of nodes present in a network, i.e., 60 nodes. Similar results like better throughput as compared to normal IDS are recorded and presented in the following Fig. 16.

6 Conclusion

Although MANETs are more vulnerable to inside and outside attacks than conventional wired networks, they are increasingly being used in many applications because they provide low-cost mobile connectivity solutions. Researchers are constantly focusing on developing or evolving methods for preventing, detecting and response mechanism for MANETs. Fuzzy-based intrusion detection has been identified as a suitable technique for dynamic environment (i.e., MANETs) by various researchers. It emerges that, to secure a network against the unknown attacks, the fuzzy-based intrusion detection may be the appropriate technique to tackle attacks in MANETs. Here, in this work, its applicability in MANETs has been presented. An effective set of fuzzy rules for inferences is necessary to be identified by making use of the fuzzy rule learning strategies, which would contribute more effectively for detecting intrusion in MANETs. Here, under the scope of this paper, the fuzzy rules (*set of 16 rules*) have been proposed for the detection of blackhole attack in a network. These fuzzy rules are developed on three critical attributes of AODV which are rate of RREQ, RREP and sequence number. Subsequently, the proposed FIDS has been evaluated for the detection of blackhole attack using different simulation parameters of MANETs. And it is observed that fuzzy logic-based intrusion detection systems performs better than the other method-based intrusion detection methods. However, here in the proposed solution, only limited features have been taken into account for the detection of blackhole attack ONLY, to use this model for different attacks, more features are required to be added for accuracy in detection of attack that may results in more computation processing on node which limits the operational philosophy of MANETs. As a result, IDS in MANETs remain a demanding, complex and challenging subject for researchers.

References

1. Ramanathan, R., Redi, J.: A brief overview of ad hoc networks: challenges and directions. *IEEE Commun. Magaz.* **40**(5) (2002)
2. Vydeki, D., Bhuvaneswaran, R.S.: Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks. *J. Comput. Sci.* **9**(4), 521–525, ISSN: 1549-3636 (2013)
3. Poongothai, T., Duraiswamy, K.: Cross layer intrusion detection system of mobile ad hoc networks using feature selection approach. *Wseas Trans. Commun.* **13** (2014)
4. Introduction to fuzzy logic. <http://www.francky.me/doc/course/fuzzy-logic.pdf>
5. Lectures on Fuzzy. <http://ce.sharif.edu/courses/92-93/1/ce9571/resources/root/Lectures/Lecture6&7.pdf>
6. Zadeh, L.A.: Fuzzy logic—computing with words. *IEEE Trans. Fuzzy Syst.* **4**, 103–111 (1996)
7. Ruchi, M., Reddy, B.V.R.: Taxonomy of machine leaning based anomaly detection and its suitability. In: *International Conference on Computation Intelligence and Data Science (ICCIDS 2018)*, *Procedia Computer Science*, vol. 132, pp. 1842–1849, Elsevier (2018)
8. Garcia Teodora, P., Diaz Verdejo, J., MaciaFarnandez, G., Vazquez, E.: Anomaly based network intrusion detection: techniques, systems and challenges. *J. Comput. Secur.* **28**(1), 18–28 (2009)
9. Shelly, X.W., Wolfgang, B.: The use of computational intelligence in intrusion detection systems: a review. *Appl. Soft Comput. Appl. Soft Comput.* **10**, 1–35 (2010)
10. Izakian, H., Pedrycz, W.: Agreement-based fuzzy c-means for clustering data with blocks of features. *Neurocomputing* **127**, 266–280 (2014)
11. Animato, M.E., Kim, H., Kim, K.: Another fuzzy anomaly detection system based on ant clustering algorithm. Kumamoto, Japan (2016)
12. Mkuzangwe, N.N.P., Nelwamondo, F.V.: A fuzzy logic based network intrusion detection system for predicting the TCP SYN flooding attack. Springer International Publishing, Part II, LNAI 10192, pp. 14–22 (2017)
13. Kulbhushan, Singh, J.: Fuzzy-logic-based intrusion detection system against blackhole attack AODV in Manet. *IJCA Special issue on “Network Security and Cryptography”*, vol. NSC, no. 2, pp. 28–35 (2011)
14. Mandal, S.N., Pal Choudhury, J., Bhadra Chaudhuri, S.R.: In search of suitable fuzzy membership function in prediction of time series data. *Int. J. Comput. Sci. Issues* **9**(3), 3 (2012)
15. Chaudhary, A., Kumar, A., Tiwari, V.N.: A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs. *IEEE Int. Conf. Optimiz. Reliab. Inf. Technol.* 178–181 (2014)
16. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: *Proceedings 2nd IEEE Workshop Mobile Computer System and Applications*, pp. 90100 (1999)
17. Ning, P., Sun, K.: How to misuse AODV: a case study of inside attacks against mobile ad-hoc routing protocols. In: *Proceedings of the 2003 IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY (2003)
18. Rajya Lakshmi, G.V., Anusha, K.: Detection of anomaly network traffic for mobile ad-hoc network using fuzzy logic. *Int. J. Emerg. Res. Manag. Technol.* (2013)
19. Chaudhary, A., Tiwari, V.N., Kumar, A.: Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks. *BIJIT—BVICAM s Int. J. Inf. Technol.* **6**(1) (2014)
20. Dokurer, S., Ert, Y.M., Acar, C.E.: Performance analysis of adhoc networks under blackhole attacks. In: *Southeast Con, 2007, Proceedings IEEE*, pp. 148–153 (2007)

Detection of Phishing Websites Using Classification Algorithms



Sumathi Ganesan

Abstract Phishing is a form of online fraudsters try to mimic genuine websites and get the user's sensitive and personal information. Such malicious users post phishing links and advertisements which may transmit malwares and viruses. Not only individual users are affected by such fraudsters but also several organizations and corporate those depend on internet for services and sales. Such malicious users adopt social engineering skills such as sending emails or by online pop-up advertisements. A number of solutions for detecting phishing websites are mentioned such as non-technical methods, method of black listing and white listing and machine learning techniques. In this paper, data mining techniques in machine learning have been applied to detect phishing websites. One of the data mining techniques is a classification which seems to have a high potential in detecting phishing websites. Here, bagging, C4.5 (J48) and random forest classifiers are tested on the phishing dataset. The dataset is taken from UCI repository which has 1353 instances. The C4.5 classification model has the highest accuracy rate of 90.8%.

Keywords Phishing websites • Data mining • Classification algorithms • Hackers

1 Introduction

Today's world has become impossible without Internet; right from booking a ticket to bank transactions and scientific research the information gained from the internet has played a very crucial role in human life. It is important for the users to know about certain illegal websites which were built with a motive to steal user's sensitive information for their benefit. Website phishing [1, 2] can be defined as imitating a trusted website to obtain sensitive information from the user. The fraudsters aim in gaining information from the user or sometimes try to destroy certain information from the users account. There are types of phishing based on the

S. Ganesan (✉)

Department of Mathematics, CEG Campus, Anna University, Chennai-25, TamilNadu, India
e-mail: sumisundhar@auist.net

types of users they aim at. Deceptive phishing websites are online threats which appear to be a copy of an honest organization's but aims at acquiring personal and sensitive details of the users such as username, password, transaction details, images, etc. These websites are lookalikes of the original legitimate websites and are hard to be detected by common man. Spear phishing aims at a specific user by customizing their attacks through mails making the receiver believe that they received it from a genuine sender. The mail may contain URL which redirects them into malicious sites which will obtain all their personals. CEO Phishing is similar to spear phishing but with a difference that these phishers send mails to targeted users. Pharma phishing tries to hijack a website's domain name and use to redirect it to a malicious website. Using DNS cache poisoning, the fraudster targets a DNS server and changes the IP address associated with the alphabetical website name. In drop box phishing, the fraudster sends emails that claim to come from drop box and asks the user to click to secure their account. In Google Docs phishing, the attackers mimic the Google account login screen to obtain user's information.

Website phishing [3, 4] has become a very serious problem because the number of such websites is increasing enormously, and hence, difficult for even experts to detect them. One of the most common methods used by the fraudsters is hiding the phishing URL. While visiting some websites, the Web browsers may assure us that the website is secure, but the user may end up landing into a malicious website. Such URLs may contain Unicode standard characters which resemble normal alphabets. So when a request to such a website is given, it directs us to a different domain and the user end up believing it is a genuine website. Such phishing URLs or links are sent through email. The hackers try to counterfeit the legitimate website, and the users are misled.

The phishing dataset forms the training dataset which has the class defined with it. Mining algorithms are applied to form association rules from the training data set. The features are selected in such a way that the learning process is done in a faster way. The efficiency of the rules formed depends upon the algorithm used and the input dataset. When a URL is requested within a Web browser, certain features are extracted from the URL and are applied to rules discovered by association classification to find out whether the requested website is genuine or not.

In this paper, the WEKA tool is used to conduct the experiments. The dataset was taken from UCI repository, and several classification algorithms are applied to the training dataset to form rules that could be used for a test data and the most efficient algorithm is determined to detect the phishing websites.

2 Related Works

Priya and Meenakshi [5] made a detailed study on phishing websites using C4.5 algorithm. They used a training dataset that contains 750 instances and a tree was generated. The trained model was used in the testing process and an accuracy was found to be 82.6%.

Babagoli et al. [6] proposed the technique for the detection of phishing website that uses a meta-heuristic-based non-linear regression algorithm. The dataset contained 30 attributes which was reduced using feature selection methods. Comparative study between two meta-heuristic algorithms was performed. The non-linear regression-based on harmonic search showed an accuracy of 94.13% for training data and 92.8% for test data.

Şentürk et al. [7] used J48 algorithm in WEKA tool to detect phishing in emails. They have used decision tree to build the classification model which has produced a success rate of 89%.

Ibrahim and Hadi [8] used several classification techniques in WEKA tool to detect phishing websites. A number of mining algorithms such as Prism, artificial neural networks, naïve Bayes and K star have been applied to compare their effectiveness in terms of accuracy. They concluded that artificial neural networks showed the highest accuracy of 94.8%.

Zaman and Sharmin [9] did an analysis on spam detection in social media. They used a number of machine learning algorithms such as naïve Bayes, K nearest neighbour, bagging and support vector machine. The performance measures have been analysed as well as performance of ensemble classifier over single classifier algorithm has been analysed. The analysis was done using the WEKA tool. In the study, it was observed that ensemble classifier and naïve Bayes gave better result in most of the cases.

Ramanathan and Wechsler [10] employed latent dirichlet allocation for semantic analysis and AdaBoost for classification. The dataset used for the analysis consisted of 47,500 phishing websites and 52,500 legitimate websites. The phishing website classifier is built using distribution probabilities for attributes latent dirichlet allocation and AdaBoost voting. The true positive rate and F-measure obtained was 99%.

Hu et al. [11] experimented on the legitimate website server of a financial company. Phishing websites may ask for resources from the user which is used to find whether the website is phishing or not from the logs. It was efficient and had high accuracy.

Abdelhamid et al. [12] proposed a method to detect phishing websites using multilayer classifier-based associative classification (MCAC). In associative classification, rules are formed in the training phase, and later, a classification model is constructed after removing useless and redundant rules. They have compared the performance MCAC with CBA, PART, C4.5 and JRip. They found that the MCAC algorithm had the highest accuracy of more than 90%.

3 Dataset Description

The dataset is taken from UCI repository. It contains 1353 instances, ten attributes and contains no missing values. There are three classes namely legitimate, phishing and suspicious. Out of the 1353 instances 702 are phishing, 103 are suspicious and

548 are legitimate. The ten attributes of phishing dataset are server form handler (SFH), popUpWindow, SSL_Final_State, Request_URL, URL_of_anchor, web_traffic, URL_Length, age_of_domain, having_IP_Address and Result [13].

4 Methodologies

The dataset must be pre-processed to remove noisy and inconsistent data before applying classification algorithm. The knowledge discovery process will become difficult if the dataset contains redundant values. A pre-processed dataset will give more accurate results than a data which is not pre-processed. Redundant attributes are found using correlation and covariance analysis, and such attributes are removed. Correlation and covariance are two similar measures used to identify how to attributes are related. Once all outliers are rectified, the data could be reduced in such a way that no information is lost. Finally, the dataset could be normalized or discretized if it contains numerical values.

Classification is a step-by-step procedure, used to classify the instances in a data set into their respective classes depending on the attribute values they take. In data mining, classification can be done either by building a model or by generation classification rules since the number of instances are too large to be classified individually. In both the methods, a training set, i.e. instances for which the class label is known, is taken and algorithms are applied to build the model/rules. These model/rules are used to classify the rest of the unclassified instances.

There are four types of test options, namely using training set, supplied test set, cross-validation and percentage split. Here, cross-validation and supplied test set are used for experiment.

4.1 Classification Algorithms

Input training data is utilized by the classification algorithms in machine learning to predict the likelihood that ensuing data can be classified as one of the predetermined categories. Perhaps the most well-known uses of classification is filtering emails into spam or non-spam. The following classification algorithms are applied to the pre-processed dataset.

C4.5 Algorithm Decision tree produce human interpretable models. J48 algorithm is used to generate decision tree to make predictions. It is the extended version of ID3 algorithm. It aims at generalizing until it is flexible and accurate.

This algorithm involves the following steps. The potential info or entropy of each attribute is found and info gain for each attribute is calculated. The attribute with the highest gain is selected and chosen to be the node and leaf node returns the class. C4.5 can deal with both discrete and continuous values. Missing values are

also handled. Pruning which generalizes the tree is also done. It constructs the tree based on the attribute value [14, 15].

$$\text{Entropy}(\vec{y}) = - \sum_{j=1}^n \frac{|y_j|}{|\vec{y}|} \log \left(\frac{|y_j|}{|\vec{y}|} \right) \quad (1)$$

$$\text{Entropy}(j|\vec{y}) = - \frac{|y_j|}{|\vec{y}|} \log \left(\frac{|y_j|}{|\vec{y}|} \right) \quad (2)$$

$$\text{Gain}(\vec{y}, j) = |\text{Entropy}(\vec{y}) - \text{Entropy}(j|\vec{y})| \quad (3)$$

Bagging Algorithm Bagging or bootstrap aggregation is an ensemble algorithm used in classification and to reduce variance. An ensemble method is a technique that combines the predictions from multiple machine learning algorithms together to make more accurate predictions than that of any individual model. Bootstrapping is a method in which a sample is taken from a large dataset and determines various model and statistic accuracy. The model is made efficient after the evaluation of each sample. In bagging, each sample model is overviewed, and the final model is the aggregated version of the individual sample models. By doing this, the efficiency is highly increased and reduces the variance that is over fitting the data [14, 15].

Random Forest Algorithm Random forest is a tree classifier which uses ensemble method to classify. Hence, it has a better predictive accuracy. It is a combination of many tree predictors, and each tree relies upon the value of a random vector tested independently. These random vectors govern the growth of each tree in the ensemble. The advantages of random forest are that it is non-parametric and has a high classification accuracy rate. It is also used to calculate missing values and can be used for several data analysis like classification, regression, survival analysis and unsupervised analysis. A random tree constructs several decision trees and applies it to the training data and output the class which is the mode or mean of each tree [14, 15].

5 Experimental Results

WEKA provides a number of classification techniques that includes fuzzy logic, Bayesian, decision tree and support vector machine. This paper analyses chosen three algorithms and infers the best-suited algorithm for the phishing dataset. WEKA provides different test options to provide classification results.

The experiment is conducted in WEKA tool. Here, three algorithms namely C4.5, random forest and bagging are used. The efficiency of these algorithms is calculated in terms of accuracy. The experiment was conducted using cross-validation with ten-folds and using supplied test set. Both the methods are compared and evaluated.

5.1 Pre-processing

The dataset has numerical attributes like request URL, URL anchor, web traffic, URL length and age of domain. These values were classified into different range groups; for example, the attribute URL length is divided into three groups: less than 54 characters, between 54 and 75 characters and greater than 75 characters. The dataset took for the study consists of ten attributes and 1353 instances. Figure 1 shows the sample of pre-processed results.

5.2 Evaluation Metrics

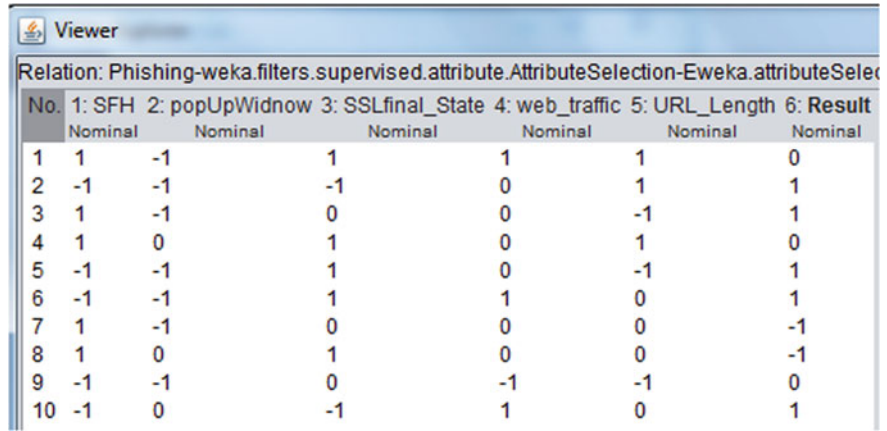
The results of various classification algorithms were evaluated by using the following metrics [11].

Accuracy is the percentage of the test tuples that are correctly classified by the classifier.

Accuracy = (TP + TN) / (P + N) (4)

Precision is defined as the percentage of positive tuples that are correctly classified.

Precision = TP / (TP + FP) (5)



No.	1: SFH	2: popUpWidnow	3: SSLfinal_State	4: web_traffic	5: URL_Length	6: Result
	Nominal	Nominal	Nominal	Nominal	Nominal	Nominal
1	1	-1	1	1	1	0
2	-1	-1	-1	0	1	1
3	1	-1	0	0	-1	1
4	1	0	1	0	1	0
5	-1	-1	1	0	-1	1
6	-1	-1	1	1	0	1
7	1	-1	0	0	0	-1
8	1	0	1	0	0	-1
9	-1	-1	0	-1	-1	0
10	-1	0	-1	1	0	1

Fig. 1 Sample of pre-processed result

Recall is nothing but the sensitivity of the classifier or TP rate.

$$\text{Recall} = \frac{TP}{(TP + FN)} \quad (6)$$

Specificity or FP rate is the percentage of negative tuples that are correctly classified.

$$\text{Specificity} = \frac{TN}{(TN + FP)} \quad (7)$$

F-measure is the method of combining both precision and recall. It is found with the harmonic mean of the values of both precision and recall.

$$F\text{-Measure} = 2 * \frac{(\text{Recall} * \text{Precision})}{(\text{Recall} + \text{Precision})} \quad (8)$$

The entire dataset containing 1353 instances is used to build a model using cross validation with ten-folds. Classification is done with C4.5, bagging and random forest. The results of the various classification algorithms are shown in the Table 1.

The confusion matrix of C4.5 algorithm is shown in the Table 2. The diagonal elements of the above confusion matrix are the correctly classified instances.

Hence, from Table 2, it is visible that the instances of 96, 489 and 643 are correctly classified into the classes suspicious, legitimate and phishing, respectively. Therefore, it has correctly classified 1228 instances.

Similarly, Tables 3 and 4 show the correctly classified instances of bagging and random forest, respectively. It shows that the bagging classifier has correctly classified 1215 instances and random forest has correctly classified 1217 instances.

Now, the experiment was done using supplied test set. For this, dataset is split into two: one with 1253 instances and one with 100 instances. The test dataset which contains 100 instances has 55 phishing, 36 legitimate and 9 suspicious instances. Table 5 summarizes the results of the supplied test set test.

From Tables 6, 7 and 8, the inferred instances of 92, 91 and 89 are correctly classified by C4.5, bagging and random forest, respectively, with the supplied test set containing 100 instances. The C4.5 algorithm which has the highest number of correctly classified instances has correctly classified all the suspicious websites. Among the 36 legitimate websites, 33 were correctly classified, and 55 phishing websites out of which 50 were predicted correctly by the model.

Table 1 Result with cross validation test

	Weighted average of C4.5	Weighted average of bagging	Weighted average of random forest
TPR	0.908	0.898	0.899
FPR	0.070	0.077	0.078
PRECISION	0.908	0.898	0.900

Table 2 Confusion matrix of C4.5

Class	0	1	-1
0	96	2	5
1	10	489	49
-1	9	50	643

Table 3 Confusion matrix of bagging

Class	0	1	-1
0	85	9	9
1	9	491	48
-1	12	51	639

Table 4 Confusion matrix of random forest

Class	0	1	-1
0	88	7	8
1	9	489	50
-1	9	53	640

Table 5 Result with supplied test set

	Weighted average of C4.5	Weighted average of bagging	Weighted average of random forest
TPR	0.920	0.910	0.890
FPR	0.060	0.048	0.084
PRECISION	0.921	0.918	0.892
RECALL	0.920	0.910	0.890
F-MEASURE	0.920	0.911	0.890

Table 6 Confusion matrix of C4.5

Class	0	1	-1
0	9	0	0
1	0	33	3
-1	1	4	50

5.3 Performance Comparison

The main objective of this study is to categorize websites into three classes namely suspicious, legitimate and phishing. This is a supervised classification problem in which the classifier C4.5 and two ensemble methods of bagging and random forest are used. Tables 9 and 10 show the accuracy with cross validation and supplied test set.

From Fig. 2, it is concluded that C4.5 algorithm has the highest accuracy and is quite efficient in both the cases: cross validation and supplied test set.

Table 7 Confusion matrix of bagging

Class	0	1	-1
0	8	1	0
1	0	35	1
-1	2	5	48

Table 8 Confusion matrix of random forest

Class	0	1	-1
0	7	1	1
1	0	33	3
-1	1	5	49

The other three metrics of precision, recall and F-measure are also used to evaluate the results of C4.5, bagging and random forest classification algorithms. Tables 11 and 12 shows the precision, recall and F-measure values with cross validation test and supplied test set.

Figures 3 and 4 show the performance comparison of C4.5, bagging and random forest classification algorithms with cross validation test and supplied test set. This comparison is analysed with the evaluation metrics of precision, recall and F-measure.

From the above figures, it is concluded that C4.5 algorithm has the highest values for precision, recall and F-measure with the cross validation test and supplied test set. It has been found that C4.5 model has the highest accuracy. And in most of the cases, the accuracy rate is above 80%. The C4.5 model correctly classified 93.20% while using the full training set, 90.76% while using cross validation with ten-folds, 92% while using supplied test set of 100 instances. Since the attribute values are discrete which are 1, 0 and 1, decision tree model has proven to be efficient.

Figure 5 shows the pruned tree of J48 algorithm. The size of the tree is 84 and total number of leaves is 55.

Table 9 Classifier accuracy results of cross validation

Testing mode	Ten-fold cross validation	
Classifier	Correctly classified	Incorrectly classified
C4.5	90.76	9.24
Bagging	89.8	10.20
Random forest	89.95	10.05

Table 10 Classifier accuracy results of supplied test set

Classifier	Correctly classified	Incorrectly classified
C4.5	92	8
Bagging	91	9
Random forest	89	11

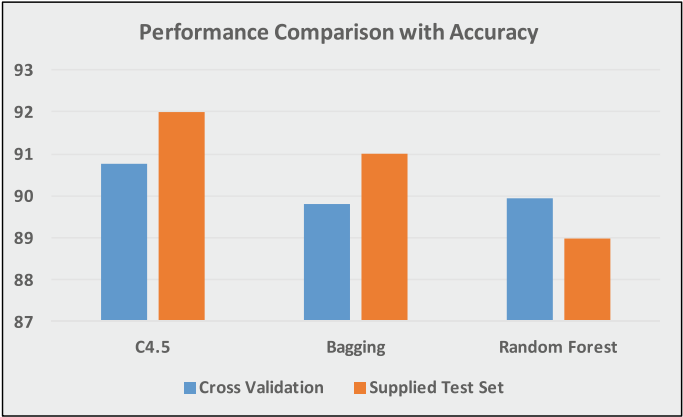


Fig. 2 Performance comparison with accuracy

Table 11 Result with cross validation test

Classifier	PRECISION	RECALL	F-MEASURE
C4.5	0.908	0.908	0.908
Bagging	0.898	0.898	0.898
Random forest	0.900	0.899	0.900

Table 12 Result with supplied test set

Classifier	PRECISION	RECALL	F-MEASURE
C4.5	0.921	0.920	0.920
Bagging	0.918	0.910	0.911
Random forest	0.892	0.890	0.890

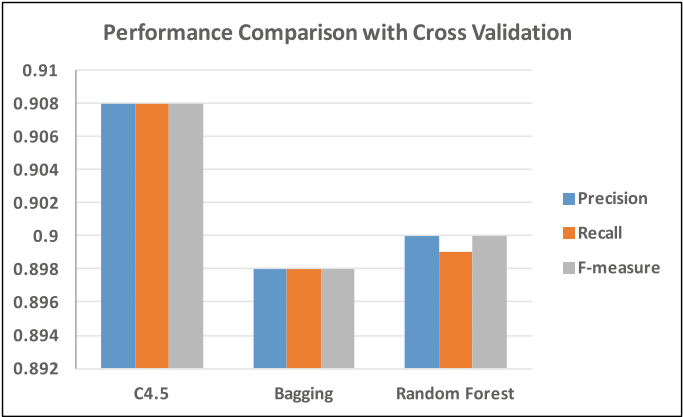


Fig. 3 Performance comparison with cross validation test

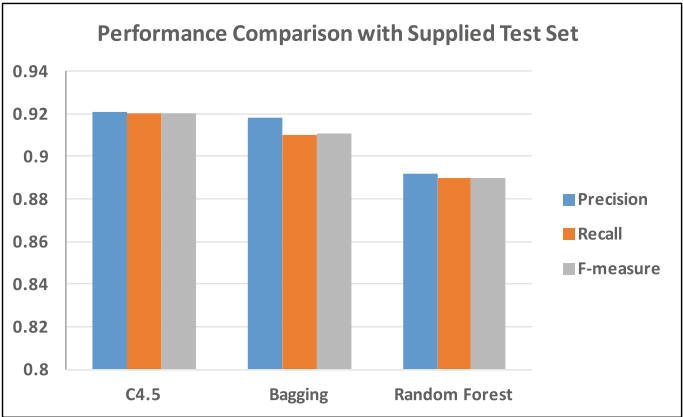


Fig. 4 Performance comparison with supplied test set

4. Zhang, Y., Hong, J.I., Cranor, L.F.: Cantina: a content-based approach to detecting phishing web sites. In: 16th International Conference on World Wide Web Proceedings, pp. 639–648 (2007)
5. Priya, A., Meenakshi, E.: Detection of phishing websites using C4. 5 data mining algorithm. In: 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology Proceedings, pp. 1468–1472 (2017)
6. Babagoli, M., Aghababa, M.P., Solouk, V.: Heuristic nonlinear regression strategy for detecting phishing websites. *Soft. Comput.* **23**(12), 4315–4327 (2019)
7. Şentürk, Ş., Yerli, E., Soğukpınar, İ.: Email phishing detection and prevention by using data mining techniques. In: International Conference on Computer Science and Engineering Proceedings, pp. 707–712 (2017)
8. Ibrahim, D.R., Hadi, A.H.: Phishing websites prediction using classification techniques. In: International Conference on New Trends in Computing Sciences Proceedings, pp.133–137 (2017)
9. Sharmin, S., Zaman, Z.: Spam detection in social media employing machine learning tool for text mining. In: 13th International Conference on Signal-Image Technology and Internet-Based Systems Proceedings, pp. 137–142 (2017)
10. Ramanathan, V., Wechsler, H.: Phishing website detection using latent Dirichlet allocation and Adaboost. In: IEEE International Conference on Intelligence and Security Informatics Proceedings, pp. 102–107 (2012)
11. Hu, J., Zhang, X., Ji, Y., Yan, H., Ding, L., Li, J., Meng, H.: Detecting phishing websites based on the study of the financial industry webserver logs. In: 3rd International Conference on Information Science and Control Engineering Proceedings, pp. 325–328 (2016)
12. Abdelhamid, N., Ayesh, A., Thabtah, F.: Phishing detection based associative classification data mining. *Expert Syst. Appl.* **41**(13), 5948–5959 (2014)
13. Website Phishing Dataset. <https://archive.ics.uci.edu/ml/datasets/Website+Phishing>. Accessed 23 Dec 2021
14. Abernethy, M.: Data mining with WEKA, Part 2: classification and clustering. IBM Developer (2010)
15. Han, J., Jian, P., Micheline, K.: Data mining: concepts and techniques. Elsevier, Third Edition (2011)

IoT-Based Smart Security System for Agriculture Fields



Sukhwinder Sharma^{ID}, Puneet Mittal^{ID}, and Anuradha^{ID}

Abstract Farmers face well-known challenges of crop protection from insect pests, diseases, and weeds along with protection from contrary weather conditions like hail or frost. However, they face another important challenge of protecting crops from wild animals that may cause severe damage to their grown crops by feeding on plant parts or trampling over the crops. As most of farmers stay away from their fields, continuous monitoring of fields is not possible due to distance as well as costs involved to appoint manpower for this purpose. Present technologies have made it possible to provide low cost, easy to install, and user friendly solution to such problems. This paper aims to develop and install IoT-based security system for agriculture fields capable to detect and communicate presence of wild animals using PIR sensor and GSM module. It generates SMS alerts on the farmer's mobile phone whenever some animal crosses specific area. It helps farmers to take timely action for crop protection. The security system is deployed in real environment to validate its applicability and possible future extensions.

Keywords Agriculture · GSM · IoT · PIR · Security system · Sensor

1 Introduction

Farmers plan their potential yields before the beginning of farm seasons. They prefer crops which grow well in their present environment and weather conditions as well as give financial benefits at the end. Even with their best possible efforts and planning, farmers face various challenges and obstacles that hamper their crop productivity and resulting financial outcomes. Protecting crops from insect pests,

S. Sharma (✉) · P. Mittal
Mangalore Institute of Technology and Engineering, Mangalore, India
Anuradha
The NorthCap University, Gurugram, India

diseases, and weeds are usually considered most important challenges, and a prior planning and timely usage of pesticides help to avoid any damages to crops [1]. Also, protection from contrary weather events such as hail or frost is done through immediate possible solutions. However, they face another important challenge of protecting crops from wild animals that may cause severe damage to their well grown crops by feeding on plant parts or trampling over the crops. As most of farmers stay away from their fields, continuous monitoring of fields is not possible due to distance as well as costs involved to appoint permanent manpower for this purpose. Therefore, the wild animals may cause serious yield losses and induce additional financial problems. This challenge necessitates deployment of some security system to protect crops from wild animals. Present technologies like Internet of Things (IoT) [2–6] have made it possible to provide low cost, easy to install, and user friendly solutions to such problems. Hence, this paper aims to develop and install IoT-based security system for agriculture fields capable to detect and communicate presence of wild animals using passive infrared (PIR) sensor and global system for mobile communications (GSM) module. It generates short message service (SMS) alerts on the farmer's mobile phone whenever some animal crosses specific area. It helps farmers to take timely action for crop protection. The security system is deployed in real environment to validate its applicability and possible future extensions.

The rest of paper is organized as follows. The existing security systems are discussed in Sect. 2. Section 3 presents proposed IoT-based smart security systems including its hardware and software requirements. Results are discussed in Sect. 4, while Sect. 5 gives conclusions and future research directions.

2 Existing Methods of Security for Agriculture Fields

Traditionally, farmers make frequent visits to their agriculture fields to check intrusions of wild animals and rush them out of fields if present. It fails to ensure complete protection as the animals may come back in absence of farmer. Some farmers even install wire fences, plastic fences, or electric fences to keep wild animals away from their fields. This method needs to fulfill guidelines set by local bodies, governments and regulatory bodies, and quite costly for larger field sizes. Another method is to use burglar alarm (see Fig. 1) having PIR sensor, to detect the presence of wild animals while they cross a particular area, and a buzzer to alert when an intrusion takes place. These kinds of burglar alarms are available in market and are useful only when the farmer is around the system within few meters to hear the alarm and respond. Such security systems are widely used for intrusion detection in smart homes and offices to protect against theft or damages [7–9]. Also, some solutions are proposed having Wi-Fi module to communicate within limited ranges [10].

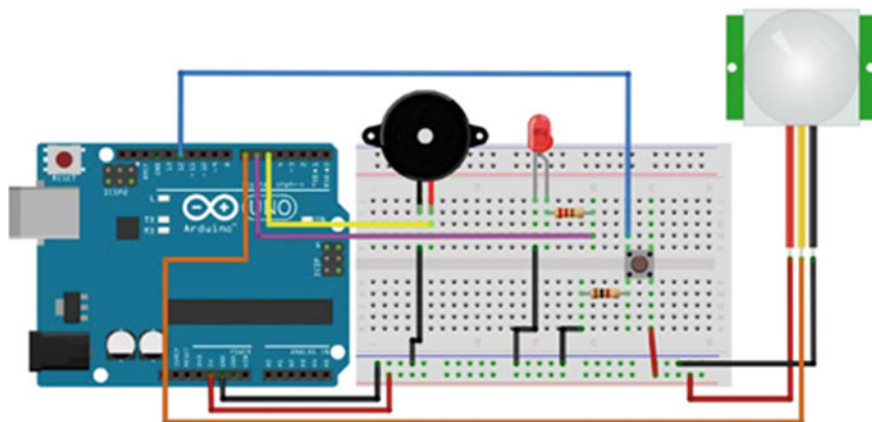


Fig. 1 Burglar alarm with buzzer [11]

These existing systems to protect crops in agriculture fields are not fruitful due to their cost and limited range resulting need of a better protection system having real-time communication and response to intrusion of wild animals. The proposed system is a low cost, portable, and easy to use solution to existing systems.

3 Proposed System and Its Implementation

The proposed system consists of device(s) having Arduino Uno microcontroller [12, 13], GSM module, and PIR sensor to detect and communicate presence of wild animals in agriculture fields. The microcontroller provides required control mechanism to set parameters for sensing, processing, and communication of information from this device to the farmer's mobile phone. The PIR sensor detects the presence of an object possibly an animal crossing the sensing area covered by the sensor. The microcontroller processes this object detection and turns on the GSM module. The GSM module makes the device capable to send an announcement in the form of preset short message service (SMS) message to the farmer's mobile phone. A buzzer is also provided to alert the farmer within audible range as well as rush the animals out of field through human like voices. Such devices can be easily installed on poles or trees depending upon the initial budget and can be further extended as per requirement. The block diagram of proposed smart security system for agriculture fields is shown in Fig. 2.

The proposed system development requires following hardware components:

- (1) Arduino Uno
- (2) Bread Board

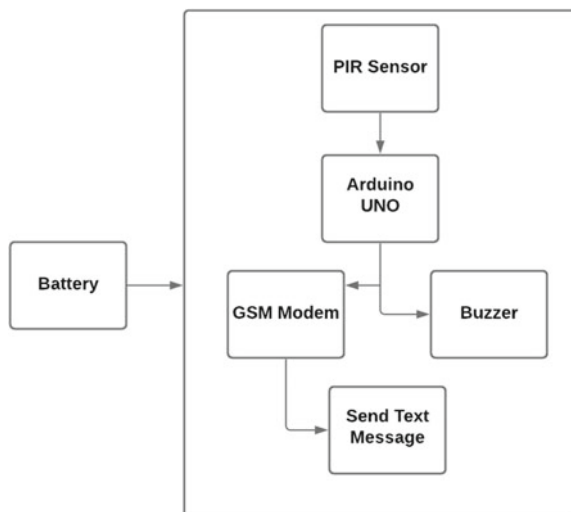


Fig. 2 Block diagram of security system

- (3) PIR Sensor
- (4) GSM module
- (5) Piezo Buzzer
- (6) Jumper Wires (as required)
- (7) Batteries

The device, having all components connected together, is shown in Fig. 3.

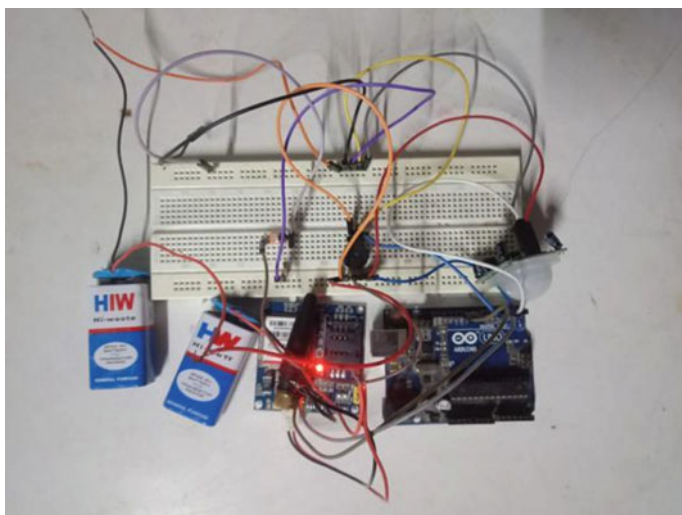


Fig. 3 Hardware implementation of security system

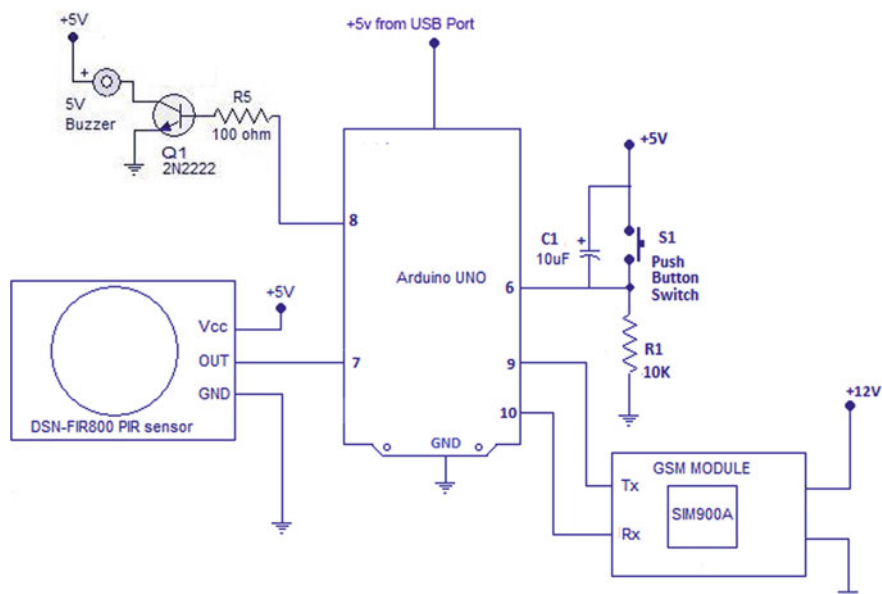


Fig. 4 Circuit diagram

The most important phase in development of proposed system is to place components at right position and connect their pins to microcontroller pins correctly in accordance with the circuit diagram. The circuit diagram for the proposed system is shown in Fig. 4.

After connecting all the components, next important thing is to program the microcontroller to get the desired functions. In general, Arduino Uno microcontroller uses Arduino IDE to program it. It can also be programmed using C programming language. Being friendly to use, C programming language is used in the development of proposed system.

4 Working of Proposed System

The above implemented devices may be installed on trees and poles in the agriculture fields at the points of possible intrusions and may be powered by some power source or replaceable batteries. The device will detect the intrusions of wild animals crossing the PIR sensor sensing area, and process and communicate it in form of predefined SMS to the farmer through GSM module. It also activates the buzzer for programmed duration to alert farmer as well as scares the wild animals to run out of agriculture fields. The working of proposed security system is shown in Fig. 5.

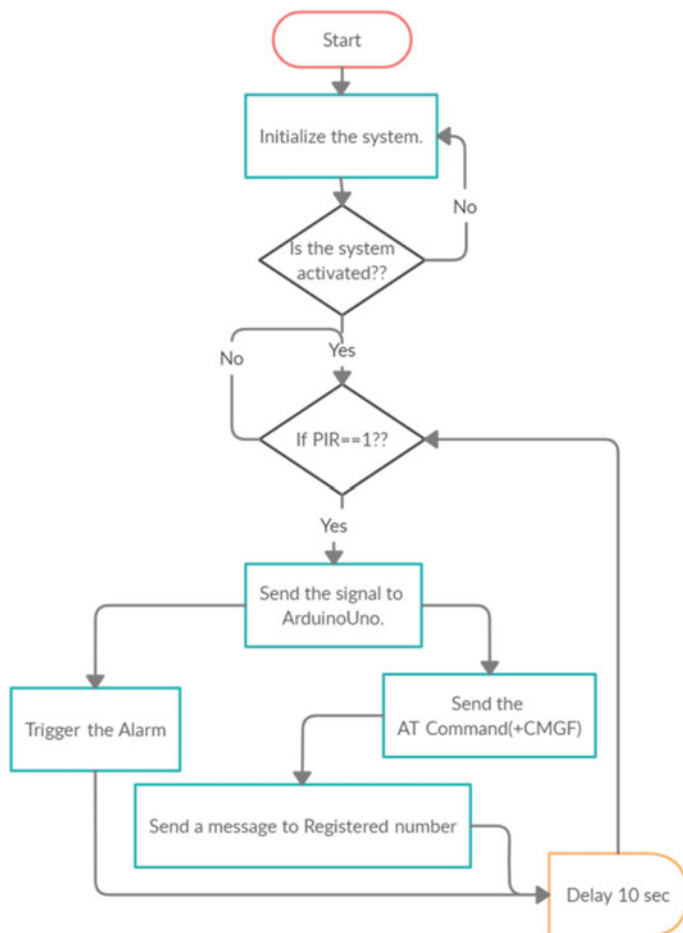


Fig. 5 Flowchart of security system

A PIR sensor is the most essential component of the proposed device to detect presence of an object and inform the microcontroller to perform the desired security system functions. The range and detection accuracy of the device depends upon the quality of PIR sensor used as well as programming and processing capabilities of microcontroller in use. PIR sensor uses inferred radiation to detect the motion produced by humans, animals, and other moving objects. After detecting an object, it will send the signals to the microcontroller. The microcontroller turns on the GSM module and communicates the predefined message to the farmer's mobile number written into the program. It can also be programmed to make a phone call to the farmer's mobile to overcome chances of delayed checking of message by the farmer. A typical PIR sensor can detect an object within a range of around 30 feet or 6 m. A warmup time of duration 20–60 s is required for proper functioning of

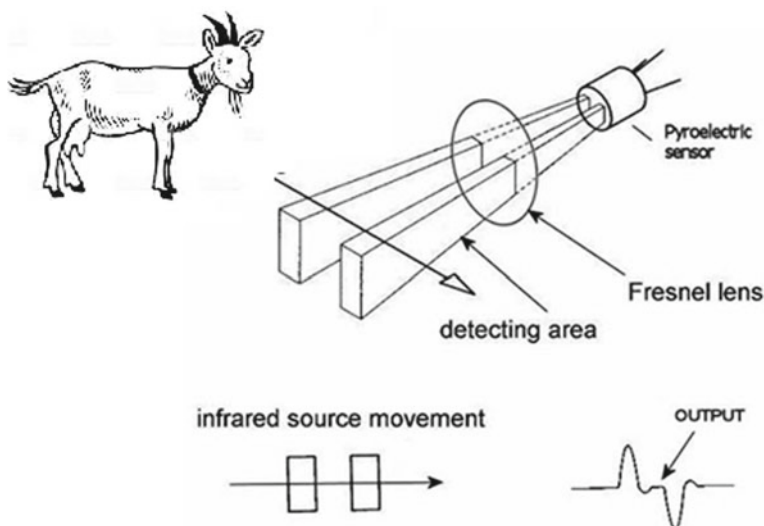
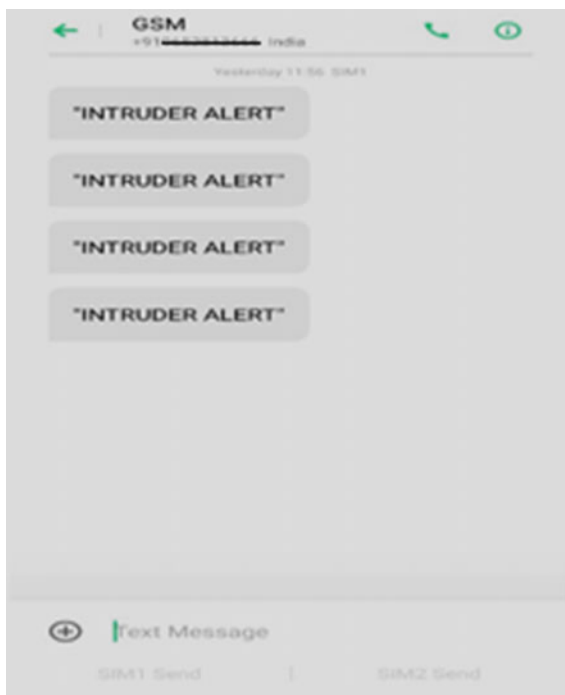


Fig. 6 Working of PIR sensor [14]

the PIR sensor. Actually, this is the settling time for consistent sensor calibration in its environment and to stabilize the IR detector. There are usually 3-pin connectors in PIR modules: +Vcc, Ground, and Output. There may be different pinouts, and it is generally powered through power supply of 5–12 V having own on-board transformer. When it senses some motion, the output becomes high. There is a three pin jumper selection for single/continuous trigger output modes. There are two labels—L and H for these two positions. The sensor is repeatedly re-triggered if the jumper is on H position, while output remains in high state. If the position is L, the output will be high and low whenever the sensor is in triggered state. So, during this mode, there will be endless motion giving repeated high low pulses. There is a Fresnel lens, for focusing the infrared onto sensor element, in front part of PIR sensor module. The working of PIR sensor to detect presence of an object is shown in Fig. 6.

The microcontroller turns on the GSM module and sends the predefined message to the farmer's mobile phone. The intrusion detection alert SMS received on farmer's registered mobile number is shown in Fig. 7. After receiving the message, the farmer may immediately reach the agriculture fields to rush away the wild animals. After sending the message, the microcontroller turns on the buzzer for predefined duration considering power requirement and usability.

Fig. 7 SMS received on mobile phone



5 Conclusions and Future Scope

A smart security system for crop protection in agriculture fields is proposed, developed, and implemented to provide user friendly, low cost, and portable solution to the farmers for protection of their crops from wild animals. It helps in reducing implementation cost through decreased deployment of manpower as well as self-inspections, while the cost of device is limited to few hundred Indian Rupees. It is easy to use due to availability of simple mobile phone interface to access notifications like SMS. It is portable in the sense that the device can be relocated depending upon the particular requirements like field area where the crops are present at a particular time, while the farmer can access notifications on the move. The installation of the device in real field demonstrated working capabilities as well as limitations for possible implementation as well as improvements. As the device detects any moving object like wild animals as well as humans and vehicles, it results in false notifications many a times. A camera can be installed on the device to take photographs of object being detected and can be communicated to farmer as a picture or object name through image processing at device level. The device may be powered through some power source or batteries which require availability of power source or timely replacement of batteries. Uninterrupted power supply or

effective utilization of available batteries is another bottleneck which may be considered for future work. Overall, the proposed system gives an initial prototype having wide possibilities and future scope.

References

1. Rao, K.S., Maikhuri, R.K., Nautiyal, S., Saxena, K.G.: Crop damage and livestock depredation by wildlife: a case study from Nanda Devi Biosphere Reserve, India. *J. Environ. Manag.* **66**(3), 317–327 (2002)
2. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things: a vision, architectural element, and future directions. *Future Gener. Comput. Syst.* **29**(7), 1645–1660 (2013)
3. Vermesan, O., Friess, P.: *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystem*. River Publishers, Denmark (2013)
4. Kodali, R.K., Jain, V., Bose S., Boppana, L.: IoT based smart security and home automation system. In: 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 1286–1289. Noida (2016)
5. Salman, L., Salman, S., Jahangirian, S., Abraham, M., Germah, F., Blair C., Krenz, P.: Energy efficient IoT-based smart home. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 526–529. Reston, USA (2016)
6. Chhabra, J., Gupta, P.: IoT based smart home design using power and security management. In: 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), pp. 3–5. Noida, India (2016)
7. Indumathi, J., Asha, N., Gitanjali, J.: Smart security system using IoT and mobile assistance. In: Krishna, P.V., Obaidat, M. (eds.) *Emerging Research in Data Engineering Systems and Computer Communications, Advances in Intelligent Systems and Computing*, vol. 1054, pp. 441–453. Springer, Singapore (2020)
8. Prasetyo, T.F., Zaliluddin, D., Iqbal, M.: Prototype of smart office system using based security system. In: 2017 4th International Seminar of Mathematics, Science and Computer Science Education, pp. 1–8. Bandung, Indonesia
9. Furdik, K., Lukac, G., Sabol, T., Kostelnik, P.: The network architecture designed for an adaptable IoT-based smart office solution. *Int. J. Comput. Netw. Commun. Secur.* **1**(6), 216–224 (2013)
10. Jha, J., Dubey, P.R., Pradhan, P., Pai, S.N.: IoT-Based home security system with wireless communication. In: Hassanien, A., Bhatnagar, R., Darwish, A. (eds) *Advanced Machine Learning Technologies and Applications, Advances in Intelligent Systems and Computing*, vol. 1141, pp. 525–533. Springer, Singapore (2020)
11. Arduino Project Hub. <https://create.arduino.cc/projecthub>. Accessed on 25 Dec 2021
12. Andriansyah, M., Subali, M., Purwanto, I., Irianto S.A., Pramono, R.A.: e-KTP as the Basis of home security system using Arduino Uno. In: 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), pp. 1–5. Kuta Bali, Indonesia (2017)
13. Monk, S.: *Programming Arduino*, 2nd edn. The McGraw Hill, USA (2012)
14. How Infrared motion detector components work. <http://www.giolab.com/pirparts/infrared.html>. Accessed on 25 Dec 2021

Efficient Clustering of Transactional Data for Privacy-Preserving Data Publishing



Vartika Puri, Parmeet Kaur, and Shelly Sachdeva

Abstract Transactional data is set-valued data which is generated from retail store, healthcare, etc. The data needs to be published to extract useful information from the data. The data contain some sensitive information about the individual, and if leaked, then it will cause serious implications to the privacy of an individual. Therefore, it is required to protect the user's privacy on the published data while ensuring the data should remain useful for analysis purpose. The paper proposes efficient clustering method using ant-colony-based clustering algorithm to bring similar transactions in same equivalence class/cluster. Finally, we can achieve privacy with minimal information loss. The approach has been tested on INFORMS dataset and compared with the Disassociation. The result shows that the more information is preserved as compared to Disassociation approach.

Keywords Ant colony clustering • Clustering • Privacy-preserving data publishing • Relative error

1 Introduction

Privacy-preserving data publishing (PPDP) is the emerging area where data is published to the third party while preserving privacy of individuals whose data is contained in the published data. Transactional data is the real-world dataset generated by the widely used applications such as retail store and healthcare.

V. Puri (✉) • P. Kaur

Department of Computer Science & Engineering and Information Technology,
Jaypee Institute of Information Technology, Noida, India
e-mail: vartika.puri@jiit.ac.in

P. Kaur

e-mail: parmeet.kaur@jiit.ac.in

S. Sachdeva

Department of Computer Science, National Institute of Technology, Delhi, India
e-mail: shellysachdeva@nitdelhi.ac.in

The dataset is of the form $\{\text{id}: a_1, a_2 \dots a_n\}$ where id denotes the identity of user and $a_1, a_2 \dots a_n$ denote the set of attributes belongs to the user.

The primary requirement in PPDP is the protection of identity disclosure [1]. k^m -anonymity [1] is the model which ensures the protection of identity disclosure in transactional data with minimal information loss. K^m -anonymity model ensures every m no. of items should occur in k transactions. There are numerous methods are available to achieve k^m -anonymity. Disassociation [2] is the method which is based on bucketization to achieve k^m -anonymity while incurring less information loss. There are three phases in Disassociation—(i) Horizontal partitioning, (ii) Vertical partitioning, and (iii) Refining.

In first phase, the similar transactions are put into one cluster. In the second phase, the cluster is converted into k^m -anonymous record chunks by placing infrequent item combinations in different record chunks. In any of the privacy-preserving data publishing methods, there are two steps, first, make equivalence classes of similar records, and second, apply anonymization method to anonymize the records in the equivalence class. Therefore, if there are more similar records in a cluster, then there will be less modifications to achieve the desired privacy level and data utility will be maintained. Thus, creation of good equivalence classes/clusters is the main step of PPDP.

Ant colony optimization (ACO) is the technique used by insects existing in adjacent colonies in the search for food. If a source of food is found by any ant team/colony, then some teams of ants follow diverse paths searching this food, leaving behind pheromone trail, a chemical usually excreted by animals, and is of great importance for insects. The pheromone trail directs the other ants, and with its help, other ants follow the way laid down by the ants moving in front of them. Few ant teams will reach the food source prior to the other teams due to the fact that they would have traversed the shortest path, and then they will follow the same path to go back to their colony before the other ant teams. Now this shortest path will have the pheromone trails as the team have traversed this path and came back before other team following another path; therefore, probability of other teams taking the same path over other paths is much higher, lest some other paths (better) are discovered by another teams. Pheromone trail of the shortest path is expected to be more concentrated than the other paths.

Inspiration of the ant-based clustering algorithm comes from the clustering of corpses and larval sorting events found in real ant colonies. Deneubourg et al. [3] have first started the study in this field. He has proposed a basic model in which objects in clusters are randomly moved, picked up, and dropped as per the similarity found in surrounding objects. LF algorithm proposed by Lumer and Faieta [4] which is an extension of basic model, which is applicable for numerical datasets. In this algorithm, ants are considered as agents who travel in a four-sided grid in a random fashion. These agents pick up, transport, and drop the data items scattered within this environment. Operations (picking and dropping) are executed as per the similarity and density of the data items found in the ants' neighborhood: either isolated or data items surrounded by dissimilar ones are likely to be picked up by ants, and ants have a tendency to drop them near the comparable ones. This is how

elements are clustered and sorted in the grid. The ant colony clustering algorithm are more flexible, robust, and decentralized [5–7] than traditional methods.

The paper proposed the use of ant colony clustering algorithm on transactional dataset for making optimized clusters of similar transactions.

The rest of the paper is structured as follows: Sect. 2 presents the related work in this domain. Section 3 proposes application of ant colony clustering algorithm for efficient clustering of transactional data. The results of the implementation of the proposed algorithm and its comparison with related approach are discussed in Sect. 4. Lastly, we summarize and conclude the work followed by future work.

2 Related Work

The application of ACO to solve the clustering problem was introduced by Shelokar et al. [8]. Firstly, the sample data is represented by each string element, and its content signify the cluster number which the sample data allotted to. Each ant in the ACO at that time builds a solution on the basis of string representation. As per [9], the ant algorithm can be segregated into two sets to achieve clustering, ant-based sorting, and ACO based clustering. Ant-based sorting algorithm uses 2D grid. As per that algorithm, foremost the objects are scattered randomly. Afterward, objects dissimilar to its neighborhood are picked up by artificial ants and transfer it to the cluster containing similar objects. The proposed solution was also used in the studies [10–13]. Though a defined cluster number is not required in the beginning by ant-based sorting, the processing time will be high as it requires post-processing to recognize the generated clusters [9]. This was proven in few prior studies where the analysis of the cluster number should be done visually once the clustering is completed [12]. ACO based clustering is another ant algorithm for clustering which uses the same idea of solution string to denote the clustering solution. The solution string is built on each iteration and assessed by the objective function to discover the most optimal one. Although a defined cluster number is a prerequisite, ACO based clustering is more efficient in computation than ant-based sorting. Also, once the clustering is done, it does not require post-processing [9]. Apart from ACO, some of the proposed clustering algorithms also practice the same concept of solution string as ACO based clustering [14–16]. ACOC [17] is the first implementation of ACO based clustering. After that, ACOC has been enhanced in some studies such as [18] which revised the original ACOC by keeping the identified best solution as the initial solution for the next iteration and adding the ability to determine the optimal cluster number automatically using Jaccard index. The study has demonstrated that the algorithm takes more time to run. The research [17] have adopted another methodology by combining the ACOC with k-means algorithm. In this, the ACO explores the initial solution generated by k-means. However, the algorithm was only tested on financial services data processing. Besides, in research [19], ACO based clustering concept was used; however, it builds the classification model according to the training dataset which is clustered using ACO. The fast ant

colony optimization for clustering (FACOC) improves the efficacy of computation in ACOC [20]. In FACOC, the threshold value is used to define whether a cluster number turn out to be common for an object once it is being selected for multiple times. If a cluster number for an object turns out to be common, then that cluster number will be selected without computing the probability in the next iteration for that particular object. With this, the redundant computations can be reduced, enhancing the execution time. In addition, local search will not affect the object with common cluster number. However, the result indicates that FACOC outputs have inferior clustering quality than ACOC.

3 Proposed Approach: Application of Ant Colony Clustering Algorithm for Efficient Clustering of Transactional Data

We propose an algorithm in which efficient partitions are created using ant colony clustering algorithm and then utilizes VERPART algorithm [21] to finally achieve k^m -anonymity. The clusters are initialized using HORPART algorithm [21]. HORPART algorithm selects the most frequent item “a” in the dataset and splits the dataset into two partitions, the records which contain “a” come in one partition and the rest of the records come in another partition. The process of splitting like this will continue till we get the partitions of predefined size, say $P_1, P_2 \dots P_n$.

At the beginning, an ant m is associated to a partition P_I , and during the iterations, the ant will select the most dissimilar transaction d_i of partition P_I , and another partition P_J is selected at random using a roulette-wheel with probability p_{IJ} , where p_{IJ} depends on the pheromone trail and a local heuristic. Ant will assign d_i to the partition P_J . The value of the pheromone trail is modified according to the rule.

$$\tau_{xy} = (1 - \rho)\tau_{xy} + \Delta\tau_{xy}^k \quad (1)$$

where τ_{xy} is the amount of pheromone deposited for a state transition from partition x to partition y , ρ is the pheromone evaporation coefficient where $\rho \in [0, 1]$ and $\Delta\tau_{xy}^k$ is the amount of pheromone deposited by k^{th} ant.

$$\Delta\tau_{xy}^k = \begin{cases} 1 & \text{if ant } k \text{ transfer a transaction from } x \text{ to } y \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

The local heuristic or short-term visibility is defined as.

$$\eta_{IJ} = \frac{A \cap B}{A \cup B} \quad (3)$$

where A and B are the transactions. If the transaction A is more similar to the transaction B of particular partition, then it gives a big value in order to influence in the probability of assigning it to the partition. If ant m is at partition I , partition J is chosen with probability

$$p_{XY}^k = \frac{(\tau_{XY}^\alpha)(\eta_{XY}^\beta)}{\sum_{z \in \text{allowed}_X} (\tau_{XZ}^\alpha)(\eta_{XZ}^\beta)} \quad (4)$$

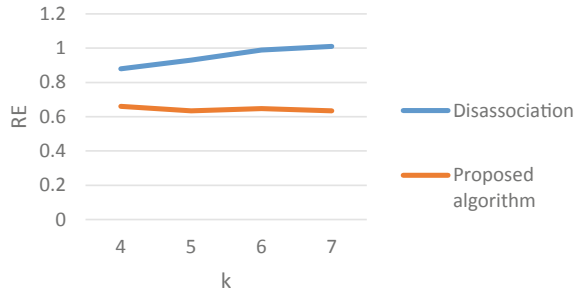
To find whether the obtained solution is better than previous or not, the Jaccard similarity is calculated.

$$B(P) = \sum_{I=1}^n JS(P_I) \quad (5)$$

Then, dissimilar transaction d of partition I is assigned to the partition J .

Algorithm: Proposed algorithm

Input: number of iterations $t_{\max}$, the number of ants M ; the initial value of pheromone τ_0 ; α ; β ; ρ ; Original dataset D .
Output: Anonymized dataset D' .
Initialize $\tau_{IJ} = \tau_0$;
Calculate η according to (3)
Initialize the probabilities p
Initialize partitions $P_1, \dots, P_m$ using HORPART
For $n=1$ to $t_{\max}$:
 For $t=1$ to M do:
 For each p in P :
 Find the most dissimilar transaction d_i in the partition p
 Select a partition P_J according to (4)
 Assign d_i to the partition P_J
 End For
 Calculate the cost $B(P)$ according to (5),
 if $B(P) > B(P_{I-1})$ then
 keep $B(P)$
 else
 keep $B(P_{I-1})$
 Update τ according to (1) and (2)
 End For
End For
For each partition $p \in P$ do:
 Apply VERPART[21] on p .

Fig. 1 Relative error

4 Implementation and Results

The proposed approach is implemented in Python and tested on INFORMS dataset.¹ In ACO, there are five parameters that needs to be fixed. In the literature [22], following conditions have been specified on selecting these values:

- β has to be larger than α ; so that destination cluster should be chosen based on local heuristic, i.e., similarity with the destination cluster instead of deposited pheromone.
- $\alpha, \beta \leq 1$ is better than $\alpha, \beta > 1$;
- $\rho = 0.8$ is better than $\rho = 0.7$ and $\rho = 0.9$ decided by set of experiments.

Considering the above conditions, the following values are considered:

- M = number of clusters
- $t_{\max} = 100$
- $\alpha = 0.8$
- $\beta = 1$
- $\rho = 0.8$
- $\tau_0 = 0.001$

The results are analyzed in terms of information loss while achieving privacy-preserving data publishing. To evaluate information loss, we have used relative error measure [21] which measure the loss in the association of items occurred while anonymization shown in Fig. 1. The relative error is calculated for different values of k ($= 4, 5, 6, 7$) and for the anonymized data using proposed algorithm and Disassociation algorithm, respectively. The result shows that if data is anonymized using the proposed algorithm, it gives lower values of relative error for each k than Disassociation algorithm. The lower value of relative error shows that more items are still associated in the anonymized data and, thus, preserves data utility.

¹<https://sites.google.com/site/informsdataminingcontest/data>.

5 Conclusion

The paper has clearly shown that if we can create the equivalence classes/clusters which have similar records result in less information loss due to anonymization process. Thus, data utility maintained. The proposed algorithm uses ant colony optimization to further refine the equivalence classes/clusters; it shows the significant improvements in equivalence class and, thus, reduces the information loss cause by anonymization. The proposed approach has been tested on INFORMS dataset, and it gives lower relative error than Disassociation algorithm. In future, the applicability of other nature-inspired algorithm can be tested and compared.

References

1. Terrovitis, M., Mamoulis, N., Kalnis, P.: Privacy-preserving anonymization of set-valued data. *VLDB Endowment*, 115–125 (2008)
2. Loukides, G., Liagouris, J., Gkoulalas-Divanis, A., Terrovitis, M.: Disassociation for electronic health record privacy. *J. Biomed. Inform.* **50**, 46–61 (2014)
3. Deneubourg, J.L., Goss S., Franks, N., Sendova-Franks A., Detrain, C., Chretien, L.: The dynamics of collective sorting: robot-like ants and ant-like robots. In: Meyer, J.A., Wilson, S. (eds) *Proceedings of the 1st International Conference on Simulation of Adaptive Behaviour: From Animals to Animals*, pp. 356–365, MIT Press, Cambridge, Mass, USA (1991)
4. Lumer, E., Faieta, B.: Diversity and adaptation in populations of clustering ants. In: *Proceedings of the Third International Conference on Simulation of Adaptive Behaviour: From Animals to Animals*, pp. 501–508, MIT Press, Cambridge, Mass, USA (1994)
5. Bonabeau, E., Dorigo, M., Theraulaz, G.: *Swarm intelligence: from natural to artificial system*. Oxford University Press, New York, NY, USA (1999)
6. Ghosh, A., Halder, A., Kothari, M., Ghosh, S.: Aggregation pheromone density based data clustering. *Inf. Sci.* **178**(13), 2816–2831 (2008)
7. Gao, W., Yin, Z.X.: *Modern intelligent bionics algorithm and its applications*. Science Press, Beijing, China (2011)
8. Shelokar, P., Jayaraman, V.K., Kulkarni, B.D.: An ant colony approach for clustering. *Anal. Chim. Acta* **509**(2), 187–195 (2004)
9. Jabbar, A.M., Ku-Mahamud, K.R., Sagban, R.: Ant-based sorting and ACO-based clustering approaches: a review. In: *2018 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)* (2018)
10. Gao, W.: Improved Ant Colony Clustering Algorithm and Its Performance Study. *Computational Intelligence and Neuroscience* **2016**(19) (2016)
11. Yang, Y., Kamel, M.S.: An aggregated clustering approach using multi-ant colonies algorithms. *Pattern Recogn.* **39**(7), 1278–1289 (2006)
12. Kuo, R.J., Wang, H.S., Hu, T.L., Chou, S.H.: Application of ant K-means on clustering analysis. *Comput. Math. Appl.* **50**(10–12), 1709–1724 (2005)
13. Korurek, M., Nizam, A.: A new arrhythmia clustering: technique based on ant colony optimization. *J. Biomed. Inform.* **41**(6), 874–881 (2008)
14. Tao, W.A., Ma, Y., Tian, J.H., Li, M.Y., Duan, W.S., Liang, Y.Y.: An improved ant colony clustering algorithm. In: Zhu, R., Ma, Y. (eds) *Information Engineering and Applications*, vol. 154. *Lecture Notes in Electrical Engineering*, pp. 1515–1521, Springer, London, UK (2012)
15. Inkaya, T., Kayaligil, S., Ozdemirel, N.E.: Ant colony optimization based clustering methodology. *Appl. Soft Comput. J.* **28**, 301–311 (2015)

16. Chaturvedi, A., Green, P.E., Carroll, J.D.: k-Modes clustering. *J. Classif.* **18**(1), 35–55 (2001)
17. Handl, J., Knowles, J., Dorigo, M.: Ant-based clustering and topographic mapping. *Artif. Life* **12**(1), 35–62 (2006)
18. Wu, B., Zheng, Y., Liu, S., Shi, Z.Z.: CSIM: a document clustering algorithm based on swarm intelligence. In: *Proceedings of the Congress on Evolutionary Computation (CEC '02)*, pp. 477–482, Honolulu, Hawaii, USA (2002)
19. Yang, Y., Kamel, M.S., Jin, F.: Topic discovery from document using ant-based clustering combination. In: *Web Technologies Research and Development—APWeb of Lecture Notes in Computer Science*, pp. 100–108, Springer, Berlin, Germany (2005)
20. Ramos, G.N., Hatakeyama, Y., Dong, F., Hirota, K.: Hyperbox clustering with ant colony optimization (HACO) method and its application to medical risk profile recognition. *Appl. Soft Comput. J.* **9**(2), 632–640 (2009)
21. Terrovitis, M., Liagouris, J., Mamoulis, N., Skiadopoulos, S.: Privacy preservation by disassociation. *VLDB Endowment* **5**, 944–955 (2012)
22. Trejos, J., Murillo, A., Piza, E.: Clustering by Ant Colony Optimization. *Classification, Clustering, and Data Mining Applications* (2004)

Passive Video Forgery Detection Techniques to Detect Copy Move Tampering Through Feature Comparison and RANSAC



Jatin Patel  and Dr. Ravi Sheth

Abstract With the advancement of innovation, these days respectability of digitized information has been addressed from various perspectives. With the assistance of innovation, the integrity level of advanced video can be disturbed from various perspectives. Video tempering performs with two different ways: one is frame level and other is changing the sequence of frames to hide or highlight the specific aim of the original video. In some cases, the original information of video frames is altered and afterward pasted at some other area of the same video. The proposed framework completed two stages of calculation to distinguish the doctored frames. Feature extraction is executed as the initial steps of the proposed framework. Correlation of separated features will assist with distinguishing the altered frames. In the subsequent advance, each frame will be compared with one before and after frames with the assistance of extricated highlights to check the measure of changes in the tempered frames all through the video stream. To check the uprightness of a video, include correlation and RANSAC strategies are utilized and it shows huge outcomes distinctive when checked with the video which altered and not altered. With the utilization of this strategy, we can ensure the originality of the advanced video when it assumes a significant part as proof or verification in specific conditions.

Keywords Video forgery detection • Copy-move forgery • Spatiotemporal tampering • Feature comparison • RANSAC

J. Patel (✉) • Dr. R. Sheth
Rashtriya Raksha University, Gandhinagar, Gujarat, India
e-mail: jatin.patel@rru.ac.in

Dr. R. Sheth
e-mail: ravi.sheth@rru.ac.in

1 Introduction

Because of wide progression in advanced correspondence, now daily's video information has gotten more mainstream. Henceforth, numerous frameworks depend on the integrity of such video correspondence. In the present advanced time accessibility of practical equipment and straightforward video preparing, programming instruments have made a video recording and altering easy. Ordinarily content accessible is not accurate and more often than not, a few recordings are altered deliberately to pass on wrong data. Checking the integrity level of any video is a challenge for an examiner or any layman.

Altered recordings can make sway on political perspectives, lawfulness, and contention among nations just as it may create social strains in a tranquil society. In such cases, it is hard to distinguish an altered recording. Subsequently, proving the authenticity of the video dataset is a challenging task in today's era [1].

Video forgery is classified into two categories: one is an interframe forgery and another one is intraframe forgery. In the case of interframe forgery, the frame, in general, goes through an altering cycle, while in intraframe, only a specific portion of the video frames is altered. The first category of video tempering is further characterized by deletion, insertion, duplication, rearranging, and recompression of video frames. Frame deletion manages the occasion's evacuation from the recording by eliminating the edges concerned. While in frame insertion, the specific portion of the video replicated from the video and pasted into another location or maybe in a different recording. Duplication of the frames includes replicating a specific portion of the video and embedding at other fleeting areas of a similar file. Frames rearranging is a subcategory of edge replica where the replicated video frames are rearranged transiently before addition. Insertion, duplication, and rearranging of the video frames can be utilized to fill the hole of erased content of the original video. Altering any unique video can be performed at two distinct stages which are tampering during recording or tampering in the wake of recording.

Video altering detection is a child category of forensics that looks at the content adjustments of digital data and may find the spatial or temporal areas of video tampering [2]. These forensics methodologies are subdivided into active and passive dependent on the accessibility of earlier data of the video viable. Passive or blind video altering identification techniques do not need earlier data for ordering a video as altered or not. Anyway on account of active methodology, authenticator takes the help of advanced watermark or digital signature to identify tempering in advanced recordings. Here, advanced watermarking or digital signature or hash esteem is an equipment-based element and accordingly it is restricted to less number of users.

The rest of the paper is organized as follows: Sect. 2 quickly clarifies the different kinds of assaults in the copy-move type of forgery. In Sect. 3, survey of existing techniques was carried out, Sect. 4 characterizes the recent concerns in the current framework, and Sect. 5 features the proposed strategy, at long last in Sect. 6 outcome examination and area Sect. 7 conclusion.

2 Types of Video Tampering

Altering of any video file should be possible differently. Copy-move forgery is one of the common techniques of video tempering, where the specific subpart of the video frames is adjusted or the changes are performed in the succession of video frames. First category of forgery is called spatial-temporal while the second one is known as temporal altering [3, 4].

2.1 Spatial Tampering

An attacker can alter source recordings spatially by changing the pixel esteems in a specific frame only or in the next available frames [5, 6]. In such type of imitation, following prospects are considered:

- A specific portion of the frame is copied and is glued in different areas of a similar casing to shroud objects.
- A specific portion of the one frame might be pasted in a different frame of similar group of picture (GOP) or other GOP.

2.2 Temporal Tampering

Temporal-temporal altering kinds of fabrication fundamentally influence the arrangement of a specific scene caught by the camera [5, 6]. Such kind of forgery has the following prospects:

- Video frames are reordered in a similar GOP.
- Video frames are reordered in other GOP.
- It is additionally conceivable that the sequence of frames is changed and afterward pasted at some other area.

2.3 Spatiotemporal Tampering

Such type of altering is considered as mixing of spatial and temporal altering. The sequence of the frames is adjusted just as the visual substance of the edges is altered in a similar video [5, 6]. Figure 1 shows the pictorial representation of the above-mentioned video forgery attacks.

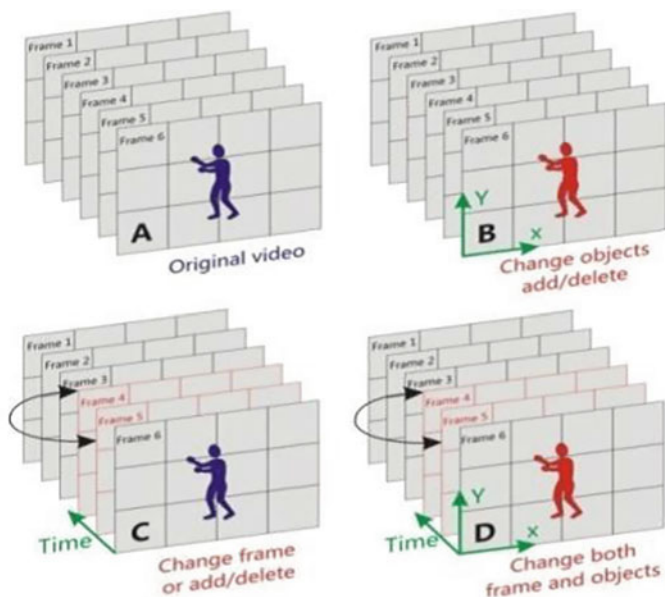


Fig. 1 Graphical representation of video forgery types [7]

3 Literature Review

To identify the research gap, here we have analyzed various standard research papers from well-known journals. The following papers define their capability and limitations.

C. Long, A. Basharat, and A. Hoogs have proposed a profound learning approach to define the duplication of video frame location at both edge level and video level, just as for the video transient limitation. An I3D network is utilized to deliver a sequence-to-grouping framework and decide the competitor frame arrangements at the coarse-search stage. In the next step, a Siamese network is used to define the fine-level search to define whether frame duplication exists or not. In the last phase, an irregularity finder is applied to additionally recognize copied outlines from chosen outlines. Proposed procedure cannot work on multistream 3D neural organizations for both edge drop, outline duplication [8].

In another methodology, M. Raveendra and K. Nagireddy have proposed a DNN-based moth search optimization strategy in which at first the input video is decompressed to identify the double compression. Double compression measurement based on the Markov insights is applied to the video. The frames which have a double compression are then given as a contribution to the SLIC superpixel. This approach based on SLIC is utilized to play out the division cycle in double compressed frames. Here, these extracted frames are portioned into various locales by SLIC superpixel division measure. Now the extracted frames are given as an input

to the Gabor scale channel, which uses the scale data for highlight extraction. In the last phase, highlighted frames are passed into DNN for falsification detection. In light of these extricated highlights, the fashioned casings are distinguished by this DNN classifier. The exactness of this proposed forgery discovery measure is discovered to be 94.37% [9].

In the proposed strategy [10], the input video is divided into multiple frames in the pre-handling stage. Frames are classified into specific groups as per the extracted features. The probabilities are arrived at the midpoint of the post-preparing stage to get the end product. The excess parts are built a similar route as to when the information is a picture. In the pre-preparing stage, faces are identified and scaled to 128×128 . Creator has utilized a piece of the VGG19 network to separate the dormant highlights, which are the contributions to the case network. Now they have taken the yield of the third max pooling layer rather than three yields before the ReLU layers. In the proposed network, there are three primary capsules and two output capsules, one for original data and another for counterfeit pictures. The inactive highlights separated by part of the VGG-19 network are the information sources, which are conveyed to the three primary capsules. The yields of the three capsules ($u_j|i$) are powerfully directed to the output (v_j) for reemphases utilizing the algorithm. The proposed technique is not compatible to oppose antagonistic machine assaults, and it cannot forestall against blended assaults.

An interframe falsification location conspires dependent on 2D stage congruency, and k -implies bunching was proposed for reconnaissance video. Creator has determined 2DPC for each edge initially. At that point, the connection coefficients of adjoining outlines and the variety of continuous relationship coefficients are obtained. At long last, the discontinuous focus brought about by altering is distinguished by utilizing k -implies grouping calculation. Here, deleting outlines show up toward the start or the finish of the video, and the location technique is inconceivable [11].

S. Jia, Z. Xu, H. Wang, C. Feng, and T. Wang determined optical flows (OF), and their high and stable relationship in duplicate move altered recordings offers a reason for effective recognition. For computation cost reasons, the consistency of OFs is dissected first to find speculated altered positions. This cycle will assist with lessening numerous counts and examinations of relationship lattices, however, may prompt all the more bogus locations. Fine discovery dependent on OF relationship is then proposed to define the set of copied frames, and a decrease of false-positive rate dependent on approval checks will be directed further for exactness. In the event that vitality, the copied succession can be separated and erased to acknowledge video recuperation. The proposed strategy may not distinguish some copy-move forgery that does not affect optical flow integrity consistency, for example, altered recordings with a generally static scene and different kinds of care-completely arranged control [12].

S. Kingra, N. Aggarwal, and R. D. Singh depend on the way that expectation leftover and optical progression of back-to-back P frames fluctuate extraordinarily at the area where outline altering has been performed. Wanted highlights are carried out after the extraction of frames (I and P) from the video. These registered highlights are then contrasted with limits which create spikes for bigger extents of PRG and OFG

highlights. Now in the next step, performance on the total number of count and progression in these spikes to unmistakable unique and manufactured recordings. The strategy for figuring chosen highlights and technique of identifying falsification by contrasting these chosen highlights and edges utilizing two unique algorithms. On the off chance that progression check gives negative outcomes in Algorithm 1, at that point concerning video succession is retested utilizing Algorithm 2. On the off chance that the video creates broken spikes, at that point that shows that the video is authentic-spasm. Non-stop spikes, nonetheless, show the location of imitation. Interframe falsification with normal precision is of 83%. Substitute piece rates for recording and reproducing a video do not influence the identification consequences of this strategy except if the objective piece rate is incredibly high or very low [13].

L. Su, C. Li, Y. Lai, and J. Yang proposed algorithm which principally comprises the accompanying four phases: (1) highlight extraction, (2) block coordinating, (3) finding the tempered location in the current frame, and (4) following the produced zones in the ensuing edges. The principal phase of the calculation removes EFMs from each square utilizing an IM-demonstrated component extraction strategy. The subsequent stage applies another square coordinating strategy to look for likely coordinating squares, which altogether lessens the computational cost. In the third stage, the PVS technique is intended to take out falsely coordinated combines and find the altered zones in the current edge. In the last stage, AFCT calculation is adjusted to gain proficiency with the altered zones recognized in the current casing and track the produced districts in ensuing edges. Proposed technique is incapable to identify more perplexing kinds of video forgery or combine video falsification [14].

I. Bozkurt, M. H. Bozkurt, and G. Ulutaş proposed a strategy for forgery discovery dependent on the forgery line. The technique separates binarized DCT highlights from the casings and speaks to the closeness between them to be a connection picture. Components of the connection picture give a thought regarding the similitude between comparing outlines. The technique at that point researches a line called a falsification line on the connection picture, to decide the area of the fabrication line in a coarser way. The Hough change is applied to the picture to decide the area of the line. Besides, the proposed technique recommends two new methods, contracting and extending, to find the imitation line in a better way. The number esteemed focuses on the line show the comparing record estimations of manufactured edges proposed strategy cannot work adequately against outline reflecting assault [15].

4 Current Issues

The quick innovative progression makes the advanced information assume an essential part in moving and tending to thoughts all the more agreeably. This has driven toward finding a fitting component for looking at and recognizing picture and video fraud in this computerized period.

Numerous researchers chipping away at recognition methods accept that extra noise, surface and shading changes would have been made in the additional locale and these regions can be recognized by contrasting the areas and the whole picture. Still epic falsification location strategies cannot adapt up to the most developed sort of malevolent exercises that are done by counterfeiters by changing the calculation of the picture highlights. Subsequently, there is a requirement for the most reformist discovery method to recognize the despicable activities on advanced proof [9].

Recordings are in compacted design. Subsequently, when a unique video goes through certain sorts of object-based fraud, the first step is to decompress it into an arrangement of individual frames and each frame can be viewed as a still picture. At that point, the frames in the selected sections of the succession are altered while the rest frames stay immaculate. After all the modifications are finished, the subsequent framing arrangement is repacked to produce a manufactured form. For this situation, the specialist needs to recognize the frames which went through some noxious movement and separate the frame [16].

- **High calculation multifaceted nature.** Straightforwardly or in a roundabout way connection or dependent on pixel approaches required high computational recognition component to discover forgery. Now and again it is tedious to look at countless frames in recordings with an immense measure of information far more prominent than that of still pictures.
- **Unstable discovery result.** Various strategies are accessible which are dealt with picture highlights, including surface, shading modes, commotion, and pixel dark qualities. A significant number of them are helpless against normal assaults or post-handling on recordings, as an illustration auxiliary pressure and added substance clamor. Here not many existing discovery approaches consider the location power as a record, and for the most part set fixed static boundaries for identification of forgery.
- **Limited pertinence.** Hardly any techniques work on a particular sort of falsification as it were. They are not sufficiently able to distinguish the complex type of forgery. A strategy that is competent to recognize entomb frame fraud may not distinguish intra frame forgery from object-based forgery. Indeed, even the technique which can recognize the frame removing cannot distinguish the framing insertion [17].

As mentioned above, there are various techniques available to check the integrity of the video but they may have some limitations to define the complex or dynamic forgery of digital video. The proposed method is capable enough to define the exact tampering location with the types of video forgery, i.e., temporal tampering or spatiotemporal tampering. In the proposed method, we have defined the copy-move forgery at frame level and the entire flow of the video.

5 Proposed Method of Forgery Detection

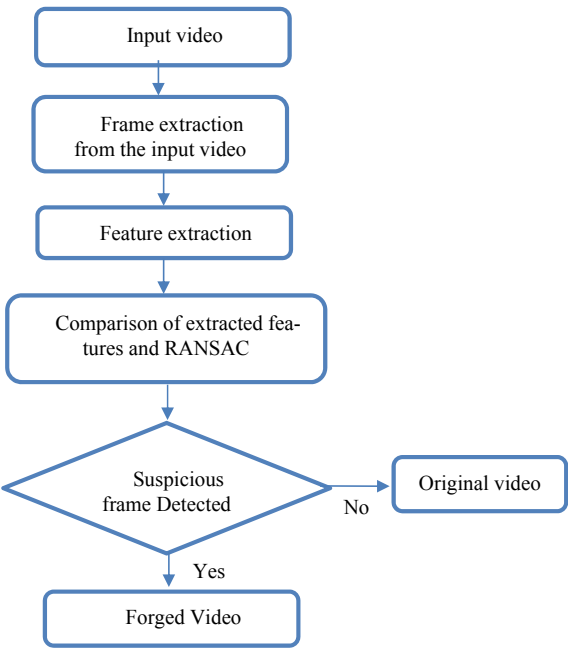
The first step of the proposed system is to extract frames from the input video and then features are extracted from the given video. To extract the features from the input video, here we have implemented a new transformation function which is applied on the partitioned block of the given video.

Discrete transformation assists with changing over spatial domain into the frequency of the picture. This operation is performed while utilizing the orthogonal polynomial [18, 19]. Here, the survey of video signals is performed in specific domains and provides a huge move to its high computing capacity to investigate the pieces of shifted signals [18, 20]. The discrete Tchebichef change (DTT) and discrete Krawtchouk change (DKT) zone unit made upheld the OP portions of the KP and TP, severally. As of late, DTT and DKT polynomials are encouraged by analysts, explicitly Krawtchouk-Tchebichef polynomials (KTP) [21] and Tcheb-ichef-Krawtchouk polynomials (TKP). KTP and TKP portions region unit acclimated change the sign from the special area to the second space, explicitly discrete Krawtchouk-Tchebichef change (DKTT) and Tchebichef-Krawtchouk change (DTKT), severally [22].

The steps of the proposed method are shown in Fig. 2.

The output of the KTP and TKP sets indicated momentous attributes as far as to highlight extraction and localization properties contrasted and different existing genuine transformations [23]. DTKT and DKTT can separate highlights from a

Fig. 2 Flowchart of the proposed method



particular segment of the picture by the benefits of the confinement property in existence spaces.

The overall expenses of computation for separating the predominant features from the input image in the DKTT is not as much as compared to DTKT. Consequently, in this paper, we have used DKTT to extricate highlights from the operated video frame.

As mentioned in the equations, we have performed the mathematical calculation of KTP. Here, $Rn(x)$ is the n th order of KTP and it is given by [21]:

$$Rn(x) = \sum_{i=0}^{N-1} Ki(n; p, N-1) \cdot ti(x) \quad (1)$$

$$x, n = 0, 1, \dots, N-1,$$

$$N > 0; \quad p \in (0; 1)$$

where $ti(x)$ is the TP of the i th order [24].

In conventional strategy, the frame I of size $N1 * N2$ pixels is separated into number square size $B1 * B2$. All out number of squares is $v1 * v2$, where $v1 = N1/B1$ and $v2 = N2/B2$. Here, $BL_{i,j}$ is considered as a picture block in the I and j course. Presently, the change work is applied on each square with the accompanying equation:

$$\Psi BL_{i,j} = R_{B1} BL_{i,j} R_{B2}^T \quad (2)$$

$$i = 1, 2, 3 \dots v1,$$

$$j = 1, 2, 3 \dots v2$$

where $RB1 \in ROrd * B1$ and $RB2 \in ROrd * B2$ are the change grids that define the transformation function. $()^T$ characterizes the render of the lattice, and Ord is the sequence for the transformation. Here, $\Psi BL_{i,j}$ is determined for each edge of the video. To separate the features of the whole video document, the previously mentioned computation is rehashed for $v1 * v2$ times which is not successful from the speed and cost viewpoint.

To beat the previously mentioned issue, another technique for feature extraction from the video record is performed while utilizing one bunch of matrix multiplication ($P1 \ I \ P2T$). The change highlights of the whole frame are joined in one matrix.

$$\Psi = \begin{bmatrix} R_{B1} BL_{1,1} R_{B2}^T & R_{B1} BL_{1,2} R_{B2}^T & \cdots & R_{B1} BL_{1,v2} R_{B2}^T \\ R_{B1} BL_{2,1} R_{B2}^T & R_{B1} BL_{2,2} R_{B2}^T & \cdots & R_{B1} BL_{2,v2} R_{B2}^T \\ \vdots & \vdots & \ddots & \vdots \\ R_{B1} BL_{v1,1} R_{B2}^T & R_{B1} BL_{v1,2} R_{B2}^T & \cdots & R_{B1} BL_{v1,v2} R_{B2}^T \end{bmatrix} \quad (3)$$

Here, the output worth $\Psi \in R\text{Ord} \cdot v1 * \text{Ord} \cdot v2$ is considered as the separated element for the whole casing. As demonstrated in Eq. (3), $RB1$ and $RB2$ are two orthogonal polynomial and they are multiplied with each square of image ($BL_{i,j}$). Here, while utilizing Kronecker item Eq. (3) can be revamped as:

$$\Psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ [v1 * v1] \end{pmatrix} \otimes \begin{pmatrix} R_{B1} \\ [Ord * B1] \end{pmatrix} * \begin{pmatrix} I \\ [N1 * N2] \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ [v2 * v2] \end{pmatrix} \otimes \begin{pmatrix} R_{B2}^T \\ [Ord * B1] \end{pmatrix} \quad (4)$$

where $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix, and $\otimes$ is the Kronecker product. Equation (4) defines the transposition property of Kronecker [25], and it can be written as follows:

$$\begin{aligned} \Psi_{[Ord \cdot v1 * Ord \cdot v2]} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ [Ord \cdot v1 * v1 \cdot B1] \end{pmatrix} \otimes R_{B1} \\ &* \begin{pmatrix} I \\ [N1 * N2] \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ [Ord \cdot v2 * v2 \cdot B1] \end{pmatrix}^T \quad (5) \end{aligned}$$

$$= \begin{matrix} P_{B1} \\ Ord \cdot v1 * N1 \end{matrix} * \begin{matrix} I \\ [N1 * N2] \end{matrix} * \begin{matrix} P_{B2}^T \\ Ord \cdot v2 * N2 \end{matrix} \quad (6)$$

In the above equation, P_{B1} and P_{B2} are two matrices that are constructed from R_{B1} and R_{B2} , respectively. Matrix P_B is an orthogonal matrix that satisfies the orthogonality condition [19]:

$$\sum_{x \in X} P_B(n, x) P_B(m, x) = \delta_{nm} \quad (7)$$

$$n, m = 1, 2, \text{Ord}$$

Here, δ_{nm} is defined as the Kronecker delta and it is defined as a symbol of the orthonormal representation of orthogonal polynomials and is defined by:

$$\delta_{nm} = \begin{cases} 1 & n = m \\ 0 & n \neq m \end{cases} \quad (8)$$

Image reconstruct is performed using two orthogonal matrices P_{B1} and P_{B2} , and it is represented as follows:

$$I = P_{B1}^T \Psi P_{B2} \quad (9)$$

From Eq. (6), it is extremely evident that the future extraction from the given info video is performed for each square of the picture without isolating the picture into various squares. Here, we have utilized just one bunch of matrix multiplication.

Presently, in the following period of usage extracted highlights were put away and determined the invariant highlights of the image. Highlights are localized and separated, keeping exclusively the individuals who are without a doubt to remain stable over relative changes, having satisfactory differentiation, and do not appear to be on edges. At long last, the central issue descriptor is made by inspecting the sizes and directions of the picture angle in a fix around the distinguished element. Here, each info picture is changed over into a grayscale picture. Extracted highlights arranged as dubious highlights and trustworthiness highlights of the video frames.

5.1 Comparing of Features Extraction with Suspicious Frame

Features of the suspicious frames are given as input training data. Extracted features of each picture contrasted and the test input information. So here RANSAC homography comparison method is utilized for ascertaining the coordinating distance between the test input and the current edge of the video individually. Here, score has been created dependent on the coordinating substance of the video with the dubious features. Edge which contains most elevated coordinating with the dubious features is to be highlighted as produced outline in a succession.

5.2 Comparison of Extracted Features Using RANSAC

For i th ($I = 1: N$) assessment arbitrarily pick four correspondences. Here we have checked if these focuses are collinear. If it is there, retry the above advance. Presently, the holography is computed. Now distance d_i was calculated and the Hcurr by standardized DLT generated from the four-point sets for each putative correspondence. At that point, the standard deviation (Sd) of the inlier distance curr, std is calculated. Here the total number of inliers m is counted which has the overall distance d_i less than the threshold value.

5.3 *Decision Making Based on the Feature Matching*

The image which has the highest matching with the extracted feature of the forged image is removed from the sequence. Such an image is defined as a most probable forge or tempered image into the video file.

While the proposed strategy does not require picture dividing, nor amassing the outcome, here there is a requirement of one set of matrix convolution. Subsequently, any kind of transmission, for example, orthogonal polynomials, can be actualized utilizing the proposed method for the feature extraction, and RANSAC utilized as an ultimate conclusion to characterize the tempering dependent on the matching of the extracted features.

5.4 *Details of Forgery*

The original frame sequence number 109–123 is shown in Fig. 3. Figure 4 shows a similar edge grouping with the spatiotemporal forgery. Here as appeared in Fig. 4, a picture of someone else is added to characterize the item-based fraud just as edge grouping is likewise changed which characterizes the fleeting altering of the source video.

Edge number 23–37 of a similar video was duplicated and it was stuck at frame number 109–123. Figure 5 characterizes the recurrence dispersion of unique videos. Figure 6 characterizes the beginning and finishing point of the tempered area.



Fig. 3 Original frame sequence from 109th to 123rd location



Fig. 4 Spatiotemporal tempering frame sequence from 109th to 123rd location

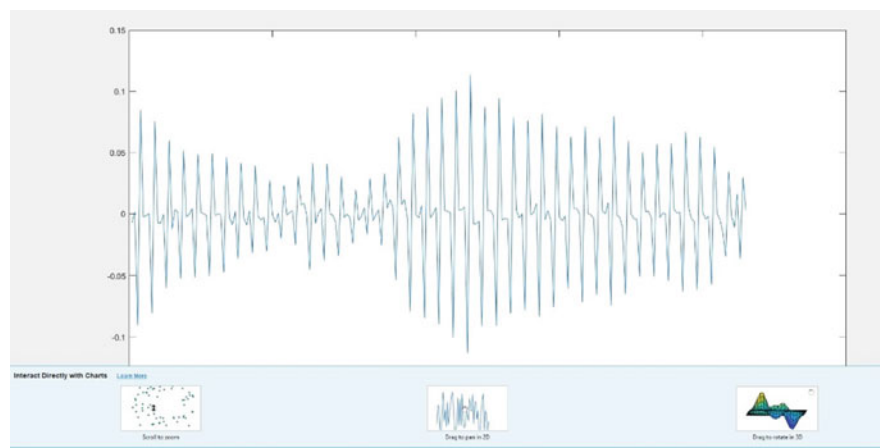


Fig. 5 Frequency distribution of original video frames

6 Experimental Result

As appeared in Fig. 6, our proposed strategy characterizes unexpected pick an incentive in the diagram which characterizes the beginning and finishing area of the manufacture casing of the video. Here, we can characterize the specific area of the manufacturing district of the video. After concluding the produce district of the picture, separated highlights contrasted and the current edges of a similar video. Highlight correlation of dubious framing assists us with distinguishing the kinds of video forgery.

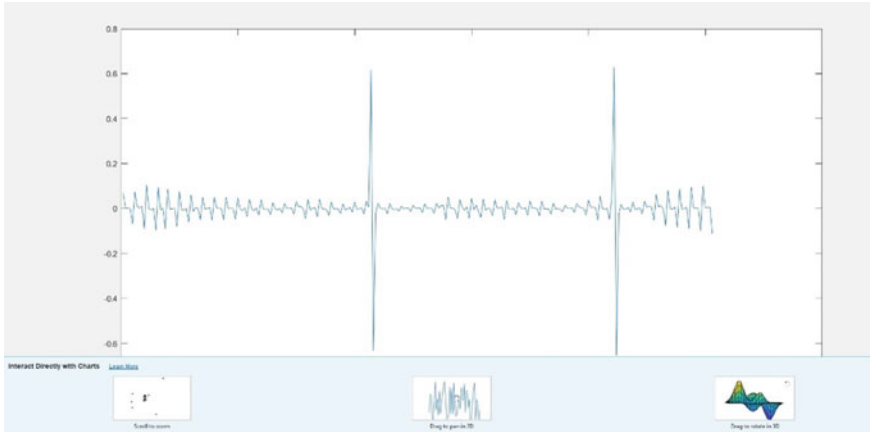


Fig. 6 Frequency distribution of forge video frames

6.1 Video Dataset Used for Testing

The greater part of the works on copy-move forgery recognition depends on the extraction and correlation of the video frame features. On account of this single source of video informational collection was not accessible to characterize the two kinds of video tempering so we took a video dataset from SULFA [25], IVY Lab [26], and YouTube. There are around 120 recordings from SULFA gathered from three distinctive camera sources (Canon SX220, Nikon S3000, and Fujifilm S2800HD). Every video is 10–20 s in length and the goal of the edge was 320×240 with an outline rate somewhere in the range of 29.97 and 30 fps. There are a total of three recordings taken from Ivy Lab. The primary video contains the 729 casings with a resolution of 722×578 and 25 fps; the subsequent video contains a total of 662 frames with a resolution of 767×578 and 30 fps; the third video has 708 edges with a resolution of 704×576 and 30 fps.

6.2 Robustness of the Proposed Method

To legitimize the precision level of the proposed technique, the true positive (TP) rates (e.g., forged is identified as forged), false positives (FP) (e.g., forged is distinguished as credible), true negatives (TN) (e.g., true is recognized as false), and false negatives (FN) (for example genuine is distinguished as valid) are determined. Our strategy is precise under double compressor with false alert 2.8%, fixed GOP with false caution 2.7%, and differing GOP with false caution 6.3%.

Table 1 shows the details of forgery detected on the tested database.

Table 1 Details of video forgery

Video	Types of forgery	Total frames	Forgery location and details
1	Temporal	729	Frame number 129th–164th copied and pasted at 225th–260th location
2	Temporal	663	Frame number 223th–254th was copied and pasted at 495th–526th location
3	Temporal	256	Frame number 229–248 copied and pasted at 125th–144th location
4	Spatiotemporal	255	The object of the 3rd frame is copied and pasted at 16th–19th location
5	Spatiotemporal	219	The object of the 239th frame is copied and pasted at 349th. Another object from 236th was copied and pasted at the 389th location
6	Spatiotemporal	432	An object from 165th frame copied and pasted at 234th–256th location

7 Conclusion and Future Work

In this paper, we have proposed feature extraction and examination-based tempering identification method for copy-move transient and spatiotemporal altering location. The proposed system utilizes feature extraction while utilizing transform matrices (*RB1* and *RB2*) created by the latest transform which is DKTT and RANSAC to discover the copy-move frame tempering in test video succession. We have tried different sports videos with the most extreme movement action. For every video, at least one edge is reordered at different areas in the succession, and objects are reordered at different areas in the video. Other than that, few frames are altered and pasted at other locations in a similar grouping. The results of the proposed simulation demonstrate that the proposed method is very proficient; it can identify all tempered locations and frames sequence with 100% precision. The proposed strategy is additionally equipped for locating the tempered frames in a given video grouping. In the future, we will test our strategy with various sorts of recordings with countless altered frames to check the robustness of the technique. Additionally, execution boundaries have not been investigated in this examination as the dataset is restricted. The work will be stretched out to address different sorts of unpredictable and dynamic assaults. We will try to develop a robust method to detect all the above-mentioned video tempering in a single digital video.

References

1. Wahid, A., et al.: Passive video forgery detection techniques : a survey. Statistical correlation of video feature international conference on information assurance and security (IAS). In: 2014 10th International Conference on Information Assurance and Security, pp. 29–34 (2014)
2. Yao, Y., Cheng, Y., Li, X.: Video objects removal forgery detection and localization. In: Proceedings of NICOGRAPH International 2016, Nicolnt 2016, p. 137 (2016)
3. Gavade, J.D., Chougule, S.R.: Passive blind forensic scheme for copy-move temporal tampering detection. In: 2018 International Conference on Advanced in Communication and Computer Technology ICACCT 2018, pp. 155–160 (2018)
4. Patel, J.J., Bhatt, N.: Review of digital image forgery detection. *Int. J. Recent Innov. Trends Comput. Commun.* **5**(7), 152–155 (2017)
5. Upadhyay, S., Singh, S.K.: Video authentication: issues and challenges. *Int. J. Comput. Sci. Issues* **9**(1), 409–418 (2012)
6. Upadhyay, S., Singh, S.K.: Video authentication—an overview **2**(4), 75–96 (2011)
7. Al-Sanjary, O.I., Sulong, G.: Detection of video forgery: a review of literature. *J. Theor. Appl. Inf. Technol.* **74**(2), 207–220 (2015)
8. Long, C., Basharat, A., Hoogs, A.: A Coarse-to-fine Deep Convolutional Neural Network Framework for Frame Duplication Detection and Localization in Forged Videos (2018)
9. Raveendra, M., Nagireddy, K.: Dnn based moth search optimization for video forgery detection. *Int. J. Eng. Adv. Technol.* **9**(1), 1190–1199 (2019)
10. Huy, I.E., Nguyen, H., Yamagishi, J.: Capsule-Forensics: Using Capsule Networks to Detect Forged Images and Videos, and Isao Echizen SOKENDAI (The Graduate University for Advanced Studies), Kanagawa , Japan National Institute of Informatics, Tokyo, Japan The University of Edinburgh, ed. IEEE International Conference Acoustics Speech Signal Process, pp. 2307–2311 (2019)
11. Li, Q., Wang, R., Xu, D.: An inter-frame forgery detection algorithm for surveillance video. *Information* **9**(12) (2018)
12. Jia, S., Xu, Z., Wang, H., Feng, C., Wang, T.: Coarse-to-fine copy-move forgery detection for video forensics. *IEEE Access* **6**, 25323–25335 (2018)
13. Kingra, S., Aggarwal, N., Singh, R.D.: Video inter-frame forgery detection approach for surveillance and mobile recorded videos. *Int. J. Electr. Comput. Eng.* **7**(2), 831–841 (2017)
14. Su, L., Li, C., Lai, Y., Yang, J.: A fast forgery detection algorithm based on exponential-fourier moments for video region duplication. *IEEE Trans. Multimed.* **20**(4), 825–840 (2018)
15. Bozkurt, I., Bozkurt, M.H., Ulutaş, G.: A new video forgery detection approach based on forgery line. *Turkish J. Electr. Eng. Comput. Sci.* **25**(6), 4558–4574 (2017)
16. Chen, S., Tan, S., Li, B., Huang, J.: Automatic detection of object-based forgery in advanced video. *IEEE Trans. Circuits Syst. Video Technol.* **26**(11), 2138–2151 (2016)
17. Deshpande, R.G., Ragha, L.L.: Performance analysis of various video compression techniques. *Int. J. Sci. Res.* **2**(8), 335–338 (2013)
18. Mahmmmod, B.M., Ramli, A.R., Abdulhussain, S.H.: Low-Distortion MMSE Speech Enhancement Estimator Based on Laplacian Prior, pp. 1–15 (2017)
19. Abdulhussain, S.H., Ramli, A.R., Mahmmmod, B.M., Jassim, W.A.: Image edge detection operators based on orthogonal polynomials. *Int. J. Image Data Fusion* **00**(00), 1–16 (2017)
20. Abdulhussain, S.H., Ramli, A.R., Mahmmmod, B.M., Jassim, W.A.: Methods and challenges in shot boundary detection: a review, pp. 1–42 (2018)
21. Mahmmmod, B.M., Abdulhussain, S.H., Al, S.A.R., Jassim, W.A.: Signal compression and enhancement using a new orthogonal-polynomial-based discrete transform, pp. 129–142 (2017)
22. Abdulhussain, S.H.: A fast feature extraction algorithm for image and video processing. In: 2019 International Joint Conference on Neural Networks, pp. 1–8 (2019)

23. Saripan, M.I., Al-Haddad, S.A.R., Jassim, W.A.: Shot boundary detection based on orthogonal polynomial (2019)
24. Abdulhussain, S.H., et al.: A fast feature extraction algorithm for image and video processing. In: Proceedings of International Joint Conference on Neural Networks, pp. 1–8 (2019)
25. Zhang, H., Ding, F.: On the Kronecker Products and Their Applications (2013)
26. Sohn, H., Neve, W.D., Ro, Y.M.: Privacy protection in video surveillance systems: analysis of subband-adaptive scrambling in JPEG XR. *IEEE Trans. Circuits Syst. Video Technol.* **21** (2), 170–177 (2011). Available at <http://ivylab.kaist.ac.kr/demo/vs/dataset.htm>

Evaluation and Performance Analysis of Apache Pulsar and NATS



Vanita Jain, Aarush Ahuja, and Dharmender Saini

Abstract Messaging systems are a crucial part of many distributed systems. Various implementations of open-source message brokers, message queues, and messaging protocols are in wide use to facilitate highly available and reliable messaging. We evaluated the architectures of two popular open-source message brokers used in the cloud: Apache Pulsar and NATS, studying qualitative differences like broker distribution, client architecture, messaging features, etc., and benchmark the two message brokers in realistic deployments.

Keywords Message-oriented middleware · Performance evaluation · Benchmarking

1 Introduction

Message brokers allows independent applications on a distributed system to communicate with each other using messages. They are useful for processing streaming data like analytics, IoT sensors, microservice communication, remote procedure calls, cloud messaging, command and control, telemetry, etc. The software architecture of message brokers consists of named message queues and protocols to transfer data efficiently. Message brokers offer various messaging transmission semantics like at-least-once, at-most-once, etc., making them reliable for critical systems. They are often deployed as a distributed system, a cluster of highly available, reliable, and fault tolerant systems. We aim to compare two message brokers: Apache Pulsar [1] and NATS [2], with NATS Streaming. A technical comparison of Apache Pulsar and NATS is pursued on the basis of design and performance, while both are message brokers and essentially promise similar functionality, i.e., a publish/subscribe messaging model. The underlying design in both is wildly different, Pulsar is a heavyweight messaging system with a variety of

V. Jain (✉) · A. Ahuja · D. Saini
Bharati Vidyapeeth's College of Engineering, New Delhi, India
e-mail: vanita.jain@bharativedyapeeth.edu

features, and NATS is a lightweight system focusing only on providing the messaging system. We compare the architecture of Apache Pulsar and NATS on the basis of messaging protocol, partitioning, persistence, clustering, clients, messaging semantics, etc. Both of them are also open source and heavily documented, we aim to compare the design and implementation of both the message brokers objectively. Using the OpenMessaging standard, an industry standard for messaging systems, we aim to identify the key performance indicators (KPIs) for message brokers and benchmark the performance of Apache Pulsar and NATS for a quantitative comparison in similar configurations.

2 Related Work

Work on evaluation of message-oriented middleware since the 1990s has produced research focusing on qualitatively and quantitatively comparing legacy messaging systems. Eugster et al. [3] sets up a conceptual base for publish-subscribe message patterns [4] presenting its various forms such as topic-based pub/sub, content-based pub/sub, type-based pub/sub implemented via RPC, message passing, notifications, etc. It presented a qualitative comparison of two early message-oriented middleware TIBCO's TIB/RV and IBM's MQ series on factors like software architecture, message persistence, reliability, etc. Maheshwari et al. [5] evaluate TIBCO's TIB/RV and progress SonicMQ, high-lighting the major difference in TIB/RV's P2P-based architecture and SonicMQ's broker-based architecture support java messaging system (JMS). It studies publish-subscribe and point-to-point messaging on both middleware benchmarking them on message throughput, message latency, and resource utilization. Sachs et al. [6–11] present SPECjms2007 and SPECjms2009-PS standardized benchmarks for JMS-based message-oriented middleware. It simulates a real-world application employing the middleware throughout a supply chain modeled after a supermarket's supply chain where orders, shipments, and sales constantly go through the system. The SPECjms2007 benchmarks effectively tested point-to-point messaging capabilities in JMS-based middleware but lacked in testing publish-subscribe messaging. SPECjms2009-PS was developed with focus on testing publish-subscribe messaging capabilities in JMS-based middleware. Folkerts et al. [12] lay out the requirements for benchmarking and evaluation of cloud infrastructure posing many essential question toward building a benchmark for the cloud. It identifies the requirements of a benchmark to be portable, fair, highly configurable, scalable, representing the real-world and applies the requirements to the layers of a cloud considering example platforms like an online gaming platform deployed in the cloud and analytical platforms deployed in the cloud. It suggested metrics important for the cloud like 99%ile wait time and 99%ile dropped requests. Importantly, the research considered factoring in pricing, elasticity, SLAs, and scalability into development of benchmarks for cloud infrastructure. John et al. [13] consider the case of two distributed message-oriented middleware RabbitMQ [14] and Apache Kafka. It

presents a study of AMQP and Kafka comparing their software design, messaging capabilities and benchmarking the two based on latency and message throughput. The paper concluded Apache Pulsar to be a more effective system compared to RabbitMQ in terms of both latency and throughput.

3 Architectural Overview of Apache Pulsar and NATS

Apache Pulsar and NATS are two popular open-source distributed message-oriented middleware developed to fulfill large-scale computing requirements in the cloud where scalability, performance, and security are most important. The software also highlights two different open-source software engineering philosophies as Apache Pulsar is under the Apache Software Foundation, while NATS is hosted under the Cloud Native Computing Foundation [15]. Even though both software provide similar features like Publish/Subscribe, wide client compatibility and multi-tenancy across clusters, their underlying design brings out differences in terms of clustering, topic storage, security, etc.

In the following sections, we qualitatively describe and compare the design of Apache Pulsar and NATS on the basis of messaging patterns, distribution capabilities, software architecture, and areas of applications. In the case of NATS, we will also include NATS Streaming to be part of the system as the features provided by NATS Streaming enables a fairer comparison with Apache Pulsar.

3.1 *Apache Pulsar*

Apache Pulsar is a multi-tenant messaging solution for server-to-server messaging hosted under the Apache Software Foundation. It is developed focusing on large-scale clustering capabilities with geo-replication across clusters, introducing very low overhead and latency for messaging publishing, scaling to millions of topics streaming data, and providing wide client compatibility with clients in many languages like Java, Go, Python, and C++. Apart from typical messaging features like topic-based messaging, Pulsar also offers a special Pulsar Functions framework to build a serverless computing system for streaming data in and out of Pulsar [1]. Apart from typical messaging features like topic-based messaging, Pulsar also offers a special Pulsar Functions framework to build a serverless computing system for streaming data in and out of Pulsar [1].

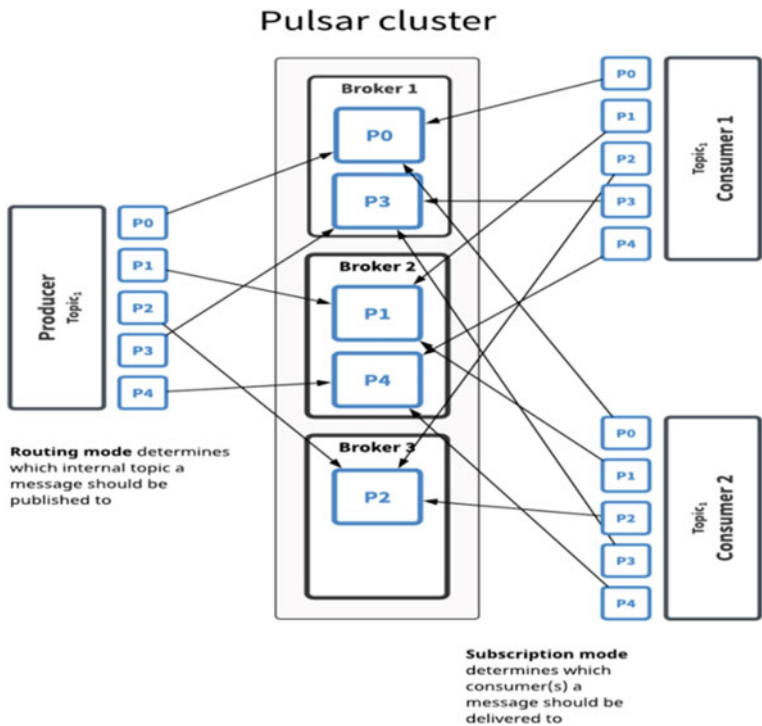


Fig. 2 Topic partitioning in an Apache Pulsar cluster

Messaging Pulsar is built to fulfill publish-subscribe requirements, using the familiar terminologies of producers which publish messages to topics and consumers which can subscribe to those topics. Messages can be processed by implementing clients for a target programming language and subscribing to a topic as a consumer. Messages in Pulsar are always retained in storage unless acknowledged by a consumer; if a consumer fails, then Pulsar will stream messages to them on reconnection. Messages are the basic level of abstraction in Pulsar, messages are published in topics, and consumers receive messages on subscription. Pulsar messages are made to transport raw bytes along with support for typed data schema. A producer can publish messages with inbuilt compression options to save bandwidth. Pulsar Consumers receive messages from the Pulsar Broker and send acknowledgments back to the broker, and acknowledgments can be either for a single message or cumulative for many messages. Messages can be negatively acknowledged to make the broker redeliver the message. Topics in Pulsar are named channels for producers to publish message to and for consumers to subscribe to. Pulsar provides both persistent and non-persistent topics which can be divided into namespaces distributed across clusters.

Namespacing topics are a handy system for defining topics across different tenants and clusters. Three major message subscription modes are provided in

Apache Pulsar: exclusive, shared, and failover. Exclusive grants only one consumer access to a subscription, failover maintains connection to an extra consumer in case of failure, and shared mode shares a single subscription among consumers transmitting to all of them. To increase topic throughput, Pulsar topics are partitioned across multiple broker instances, N internal topics are used to partition a single external topic across instances, and published messages are routed to a partition by either randomly selecting a partition or using round robin. Message ordering guarantees in Pulsar can be maintained per-key-partition and per-producer, and this part of Pulsar is still constrained as it cannot scale against multiple consumers, topics, and producers.

Special Features Pulsar supports defining data schemas for messages transmitted via the broker, and data schema is accessible to the server via a global schema registry.

A lightweight but powerful serverless computing framework called Pulsar Functions is inbuilt into Pulsar which can be used to build serverless stream-native workloads inside Pulsar working on data flowing through Pulsar. For security, Pulsar implements pluggable authentication mechanisms having built-in support for role-based tokens, Kerberos-based authentication, TLS authentication, JWT-based authorization, and Athenz [18] which is an open-source RBAC system.

3.3 *NATS and NATS Streaming*

NATS is a fire-and-forget messaging system built to fulfill the requirements of large-scale distributed computing. NATS Core is a simple and lightweight messaging solution hosted under the Cloud Native Computing Foundation. It is aimed to be applied in the areas of telemetry collection, building service meshes and microservices, deployment on the edge, etc. Similar to Apache Pulsar, NATS offers high performance, availability, wide client compatibility, etc. NATS itself is very limited in terms of what it offers, a sibling system NATS Streaming extends the core NATS API and enhances its capabilities bringing message delivery guarantees, message persistence, etc., bringing it closer to be compared to a typical messaging system like Apache Pulsar. Comparable to Apache Pulsar, NATS also has client implementations for many programming languages including Python, JavaScript, Golang, Rust, etc.

NATS, also known as NATS Core, is the essential component of the middleware responsible for listening to and publishing messages and provides core capabilities like topics, publish-subscribe messaging, message acknowledgments, load balancing, etc. NATS abstracts messaging topics as subjects, these are strings which represent names a publisher, and subscriber can use to identify themselves. In NATS, subscribers connect to subjects to listen for messages and publishers send messages to a subject which is received by any active subscriber. NATS also supports the request-reply messaging pattern where the server uses the

publish-subscribe system to create unique “inboxes” for subscribers to publish replies to. NATS provides a built-in client-side load balancing technique called “Queue Groups” which is an implementation of a distributed queue. Multiple subscribers can connect to a single “Queue” forming a queue subscription, and NATS will balance messages between the subscribers of this queue, scaling messaging for the client becomes as simple as adding more subscribers (i.e., client processes) to the system. NATS Core supports clustering and forms a mesh overlay between all the nodes by using a gossip protocol, and this clustering support can be used to create a HA configuration of the NATS server. NATS messaging follows at-most-once semantics and to ensure message delivery in unreliable networks, and NATS provides built-in request timeouts and message acknowledgements. These simple features bring reliability in NATS messaging letting the sender implement various messaging patterns like request-reply, scatter-gather, point-to-point, etc. Compared to Apache Pulsar, which is a heavyweight compared to NATS with various dependencies and extraordinary features, NATS is a minimal open-source message broker [19] implemented in Golang only focusing on high performance topic-based messaging rather than providing a plethora of features. Implementation in Golang also lets NATS be released as a single compiled binary.

NATS Streaming extends NATS Core and brings advanced messaging capabilities to NATS. NATS Streaming is open source under the Apache-2.0 license and adds fault-tolerance, high availability, data replication, message and subscription persistence, topic partitioning, etc. The underlying messaging protocol is based upon protocol buffers [20] transmitted as binary payloads over the NATS Core messaging protocol. NATS Streaming is essentially a client to a NATS Server, and a NATS Streaming binary embeds the NATS Server through which all messaging happens with NATS Streaming clients. NATS Streaming implements topics-based messaging via channels extending subjects in NATS Core. Each channel is a FIFO queue, thus creating a message log for all messages received to the subject. A special type of durable subscriptions is possible in NATS Streaming which enables resuming message consumption by a subscriber in the case of server or subscriber failure. Channels support at-least-once message delivery semantics using NATS message acknowledgements with the ability to perform redelivery of messages as required (Fig. 3).

NATS Streaming nodes are clustered using the RAFT consensus algorithm [21] to manage message and channel replication among nodes, and clusters can be pre-configured or an initial “seed” node can start the service discovery process to let any new nodes join the cluster. Similar to topic partitioning in Apache Pulsar, NATS Streaming supports channel partitioning which is incompatible running simultaneously with the clustering mode as clustering requires replication of channels across all nodes in the cluster, channel partitioning can share the load of channels among various NATS Servers, every server is assigned a cluster ID in a NATS Network, and a group of NATS Servers with the same cluster ID can share the network handling their own partition of channels. NATS Streaming also has

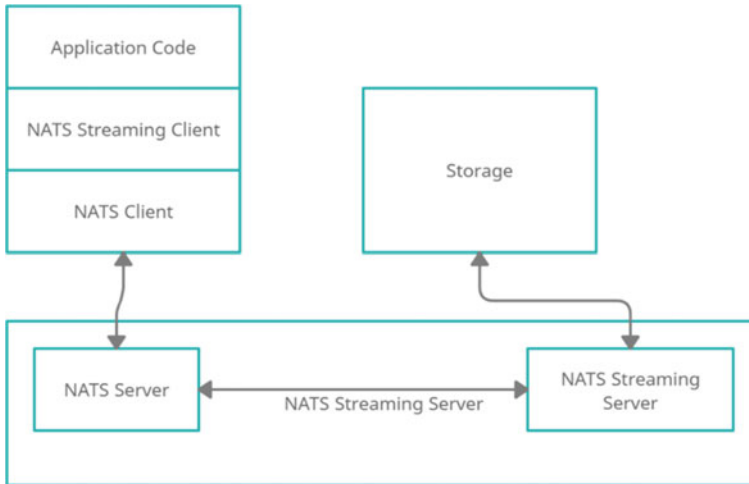


Fig. 3 NATS streaming is an advanced messaging system built on NATS core

inbuilt REST API endpoints for monitoring the system thus allowing ingestion of metrics into any monitoring framework with appropriate data collection tools (Fig. 4).

4 Benchmarking and Results

We designed the benchmark to objectively measure the performance of Apache Pulsar and NATS in realistic cloud deployments. For the server, we deployed NATS, NATS Streaming, and Apache Pulsar on a DigitalOcean Kubernetes cluster with 12 virtual CPUs and 24 GB of RAM running Kubernetes 1.16. For the client, A DigitalOcean server with 2 virtual CPUs and 4 GB RAM running Ubuntu 18.04 was used. The benchmark is based on an open-source project bench [22] which was modified to include NATS [19] v2.14, NATS Streaming [23] v0.17 and Apache Pulsar [24] v2.5.0 clients. The benchmark was run with Go clients of NATS [25] v1.9.1, NATS Streaming [26] v0.6.0, and Apache Pulsar (which are bindings for the C++ client) [24]. We found the Go clients for NATS and NATS Streaming easier to use compared to Apache Pulsar's, especially due to its non-portable nature being bindings for the C++ Apache Pulsar client. Also, TLS was enabled for communication on both NATS and Apache Pulsar. The benchmark involves publishing and subscribing messages from the client server to message brokers deployed in the Kubernetes cluster over the Internet simulating a client of the system. We benchmarked the message brokers considering three major factors: message payload size, message throughput rate, and round-trip latency. For latency benchmarks, we varied the payload size from 256 B up to 1 MB fixing the

Features	Apache Pulsar	NATS Streaming
System Architecture	Mutiple Moving components(Broker, BK, ZK)	Single executable server
Replication and Clustering	Using BookKeeper and ZooKeeper	Using Raft
Messaging Format	Custom Binary Protocol	Google Protobuf based protocols based on top of NATS Protocol
Security	TLS Authentication, JWT and Athenz, Kerberos	TLS Authentication, PKI
Multi Tenancy	Individual Authentication and Authorized streams via namespaces	Using Decentralized JWT authentication and authorization
Message Ordering Guarantee	Ordering guarantee per key partition and per producer	No guarantee of order in case of multiple subscribers
Client Libraries	C++ library and bindings for Python, Golang, etc.	Native Clients for Golang, JS, Rust etc.
Partitioning	Partitioning and replication can Work together	Either only Partitioning or Replication can work

Fig. 4 Feature comparison between subject frameworks

maximum message rate at 1500 messages/s. For throughput benchmarks, we varied the payload size from 256 B up to 50 KB and measured the publish and subscribe throughput of 50,000 messages.

The NATS Cluster was deployed with three nodes, each node being a single Kubernetes pod of NATS Server [19] containers. A Kubernetes service for the NATS cluster was exposed to the Internet by a Digitalocean Kubernetes load balancer. Similarly, a NATS Streaming cluster of three nodes was deployed with channel persistence and data replication. Both NATS and NATS Streaming clients are connected to the cluster via the load balancer.

Apache Pulsar was deployed in a minimal configuration due to the restrictions of the cluster with 1 ZooKeeper instance, 2 BookKeeper instance, and 2 Pulsar Broker instances. Similar to the NATS approach, the broker was exposed to the Internet using a load balancer and a Kubernetes service. Pulsar is meant to be a server-to-server first messaging solution and is thus heavyweight in the number and resource requirements of components, individual ZooKeeper, BookKeeper, and broker instances require a lot of CPU time, and the JVM applications consume a lot of memory. This especially, when compared to NATS which can work directly as a compiled native binary, puts Pulsar at a disadvantage for developer environments with limited resources. To deploy Apache Pulsar in Kubernetes, nodes with large amounts of RAM, powerful CPUs, and expansive disk are recommended.

We take a look at publish-subscribe round-trip latency between NATS, NATS Streaming, and Apache Pulsar varying the payload sizes between 256 bytes upto 1 megabyte apt for representing workloads like transmitting minimal RPC messages and large data files across the brokers. We should notice that both Pulsar and NATS Streaming brings both topic persistence and replication, whereas NATS is a fire-and-forget system. NATS for smaller payload sizes: 512 B and 1 KB had 99%ile latencies of 2 ms and 7 ms, respectively, with tail latencies worsening up to 15 ms and 25 ms, respectively. For larger payload sizes upto 1 MB, the latencies increased to 21 ms at 99%ile and further tail latencies upto 50 ms. NATS Streaming, for small payload sizes: 512 B and 1 KB, had 99%ile latencies of 245 ms and 170 ms, respectively, with further tail latencies up to 270 ms, respectively, for both, we note the increased latencies compared to NATS due to disk persistence and replication. For larger payload sizes up to 1 MB, the latencies increased to 351 ms at 99%ile and further tail latencies up to 820 ms. Apache Pulsar, for small payload sizes: 512 B and 1 KB, had 99%ile latencies of 360 ms and 260 ms, respectively, with further tail latencies up to 650 ms and 350 ms, respectively. For larger payload sizes up to 1 MB, the latencies increased to 740 ms at 99%ile and further tail latencies up to 980 ms. In conclusion, NATS is especially performant in terms of latencies at both smaller and larger payloads.

Apache Pulsar and NATS Streaming both suffer in latency due to presence of disk-based persistence and data replication, while NATS only uses in-memory persistence of messages (Figs. 5 and 6).

We compare message throughput in NATS and NATS Streaming which highlights the overhead disk-based persistence incurs compared to in-memory persistence. We vary the payload sizes from 256 bytes up to 50 KB and transmit 50,000 messages. For small payload sizes, 512 bytes and 1 KB, NATS turned out far superior having a throughput of 78,000 messages/s and 45,000 messages/s, respectively, compared to NATS Streaming having 13,000 messages/s and 7000 messages/s. Though, on a larger 50 KB payload size, the overhead of disk-based persistence becomes less visible with NATS having a throughput of 1000 messages/s and NATS Streaming with a throughput of 700 messages/s (Table 1).

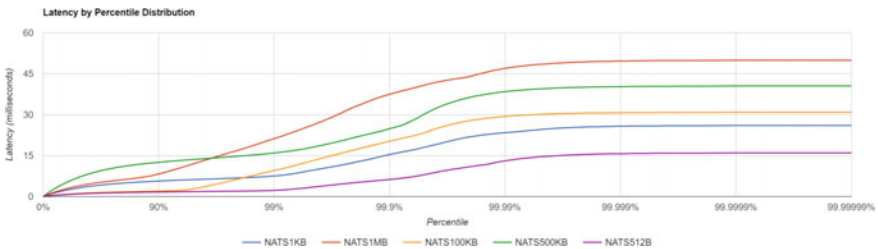


Fig. 5 NATS latency

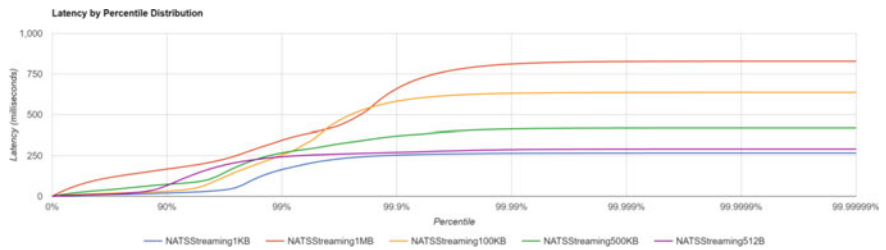


Fig. 6 NATS Streaming latency

Table 1 Throughput with different message sizes

Size	0.5 KB	1 KB	100 KiB	500 KiB	1 MiB
NATS	564.21	560.72	441.15	61.17	
NATS streaming	74.57	69.44	47.73	22.39	9.45
Apache Pulsar	102.85	103.1	63.35	21.14	13.23

5 Conclusion

The benchmarks show clear performance differences in the three systems, namely NATS (Core), NATS Streaming, and Apache Pulsar. Using file-based persistence to store messages and replication capabilities in the messaging system introduces a trade-off for both latency and throughput as writing to files is an expensive operation, which can be possibly improved by using faster disks in the form of storage-optimized instances in deployments. In our benchmarks, while NATS, obviously, was superior to NATS Streaming and Apache Pulsar in terms of throughput and latency. In a fairer comparison, NATS Streaming and Apache Pulsar can be seen to perform similarly in terms of the presented latency benchmark. NATS, extendable by NATS Streaming, is a very lightweight messaging option giving flexibility for both development and production environments, giving the choice between both NATS and NATS Streaming as requirements change, high throughput, low latency, wide client support (especially, first-class Go client support, in our case). Apache Pulsar is a heavyweight system designed for high performance server-to-server messaging systems with large amounts of resources, and this high resource requirement also provides expansive capabilities compared to NATS and NATS Streaming in the form of its serverless function framework Pulsar Functions, extensive topic partitioning and namespacing options, large-scale geo-replication support, and a scalable configuration due to its modular battle-tested components like ZooKeeper individually scalable at will.

References

1. Pulsar Homepage. <https://pulsar.apache.org/docs/en/concepts-overview/>
2. NATS Homepage. <https://docs.nats.io>
3. Eugster, P.T., Felber, P.A., Guerraoui, R., Kermarrec, A.-M.: The many faces of publish/subscribe. *ACM Comput. Surv. (CSUR)* **35**(2), 114–131 (2003)
4. Fidler, E., Jacobsen, H.A., Li, G., Mankovski, S.: Publish/subscribe system. *Feature Interact. Telecommun. Softw. Syst.* **VIII** (2005)
5. Maheshwari, P., Pang, M.: Benchmarking message-oriented middleware: TIB/RV versus SonicMQ. *Concurrency Comput. Pract. Exp.* **17**(12), 1507–1526 (2005)
6. Appel, S., Sachs, K., Buchmann, A.: Towards benchmarking of AMQP. In: *Proceedings of the Fourth ACM International Conference on Distributed Event-Based Systems*, pp. 99–100 (2010)
7. Sachs, K., Appel, S., Kounev, S., Buchmann, A.: Benchmarking publish/subscribe-based messaging systems. In: *International Conference on Database Systems for Advanced Applications*, pp. 203–214. Springer, Berlin, Heidelberg (2010)
8. Sachs, K., Kounev, S., Appel, S., Buchmann, A.: Benchmarking of message-oriented middleware. In: *Proceedings of the Third ACM International Conference on Distributed Event-Based Systems*, pp. 1–2 (2009)
9. Sachs, K., Kounev, S., Bacon, J., Buchmann, A.: Performance evaluation of message-oriented middleware using the SPECjms2007 benchmark. *Perform. Eval.* **66**(8), 410–434 (2009)
10. Sachs, K., Kounev, S., Appel, S., Buchmann, A.: A performance test harness for publish/subscribe middleware. In: *Sigmetrics/Performance* (2009)
11. Sachs, K., Kounev, S., Bacon, J., Buchmann, A.: Workload characterization of the SPECjms2007 benchmark. In: *European Performance Engineering Workshop*, pp. 228–244. Springer, Berlin, Heidelberg (2007)
12. Folkerts, E., Alexandrov, A., Sachs, K., Iosup, A., Markl, V., Tosun, C.: Benchmarking in the cloud: what it should, can, and cannot be. In: *Technology Conference on Performance Evaluation and Benchmarking*, pp. 173–188. Springer, Berlin, Heidelberg (2012)
13. John, V., Liu, X.: A Survey of Distributed Message Broker Queues. *arXivpreprint arXiv:1704.00411* (2017)
14. RabbitMQ Homepage. rabbitmq.com
15. CNCF Homepage. <https://www.cncf.io/>
16. Zookeeper Homepage. <https://zookeeper.apache.org/>
17. Bookkeeper Homepage. <https://bookkeeper.apache.org/>
18. Athenz IO. <https://www.athenz.io/>
19. Nats-Io Server Github. <http://github.com/nats-io/nats-server>
20. Protocol Buffers. <https://developers.google.com/protocol-buffers>
21. RAFT Consensus Algorithm Paper. <https://raft.github.io/raft.pdf>
22. Tykter Github. <https://github.com/tykter/bench>
23. Nats Streaming Server Github. <https://github.com/nats-io/nats-streaming-server>
24. Apache Pulsar Github. <https://github.com/apache/pulsar>
25. Nats-Io Github. <https://github.com/nats-io/nats.go>
26. Stan-Go Github. <https://github.com/nats-io/stan.go>

Problems of Providing Access to a Geographic Information System Processing Data of Different Degrees of Secrecy



Vitaly Gryzunov and Darina Gryzunova

Abstract Geographic information systems contain data of varying degrees of secrecy. Access to data is regulated by different documents. The data is loaded and processed in real time and booked in several hundred layers. On the other hand, geographic information systems are integrated into almost all existing information systems and tend to evolve into spatial data infrastructure. This circumstance imposes strict requirements on ensuring the integrity, confidentiality, and availability of data, makes it extremely difficult to make a decision on granting access of subjects to data, on the allocation of appropriate access rights. The article analyzes the problems of providing access to geographic information systems and suggests approaches to their solution.

Keywords Secure geographic information systems • Security of spatial data • Safe processing of spatial data • Geographic information system • Information security

1 Introduction

Geographic information systems penetrate all spheres of human activity: investigation of crimes and creation of safe conditions for the existence of the population [1], automation of delivery vehicles to consumers and the transition to Industry 4.0 [2, 3], the use of weapons, and other closed technologies.

Some authors believe that in the near future, all information systems will contain geographic information systems (GIS) or be based on them [4].

GIS is an information system operating with spatial data [5]. A high degree of GIS integration with other information systems, a variety of tasks to be solved, and

V. Gryzunov (✉)

Department of Information Technology and Security Systems, Russian State Hydrometeorological University, Saint-Petersburg, Russian Federation

D. Gryzunova

Legal Regulation of Economic Activity, Financial University Under the Government of the Russian Federation, Moscow, Russian Federation

a large number of heterogeneous users suggests the following features of the GIS application:

- work in real time or close to real time;
- a persistence increase in the number of layers provided by technical systems of different ministries, departments, commercial companies, and personal devices of individual: today GIS has several hundred layers;
- layers available in GIS contain information with varying degrees of secrecy;
- GIS users have different rights to access GIS layers;
- use of cloud computing and application of fog computing [6];
- GIS elements are both stationary and mobile means;
- usually, GIS itself is not used and does not perform any actions, but provides data for analysis, allocation of money, geomonitoring, investigation of computer crimes, etc. [7, 8], so in fact, it is an element of the support and decision-making system [9, 10] or “smart card” [11].

These features allow us to say that GIS is being transformed into a flexible infrastructure of spatial data [12], continuously changing its structure and functions, which, firstly, opens up GIS for a wide range of users and dramatically increases the amount of processed data, and secondly, makes GIS an object of malicious actions on the part of computer hooligans, criminal gangs, special services, etc. Both of these destabilize the work of GIS, so reduces the likelihood of achieving the set goals and leads to financial, environmental, social, and moral damage [13]. The foregoing determines the relevance of issues of providing access to information and GIS services.

The purpose of this study is to analyze the existing problems of providing access to information in GIS and propose ways to solve them. The analysis is carried out on the basis of the current legislation of the Russian Federation and experience in the design, implementation, and operation of complex information systems.

Let's consider who exactly is the consumer of GIS services and what information the GIS works with.

2 Consumers of GIS Services and the Information that GIS Works With

The following information is processed in GIS with different requirements in access control: cartographic data; coordinates of objects and routes of movement; coordinate of users, search queries, preferences, etc. Then properties of objects: financing, cost, size, number, etc.; personal data of users of all categories; medical data on foci of diseases and rates of their spread; meteorological situation; data protected by copyright; other data.

Classification of GIS information regarding the access mode according to the legislation of the Russian Federation is shown in Fig. 1.

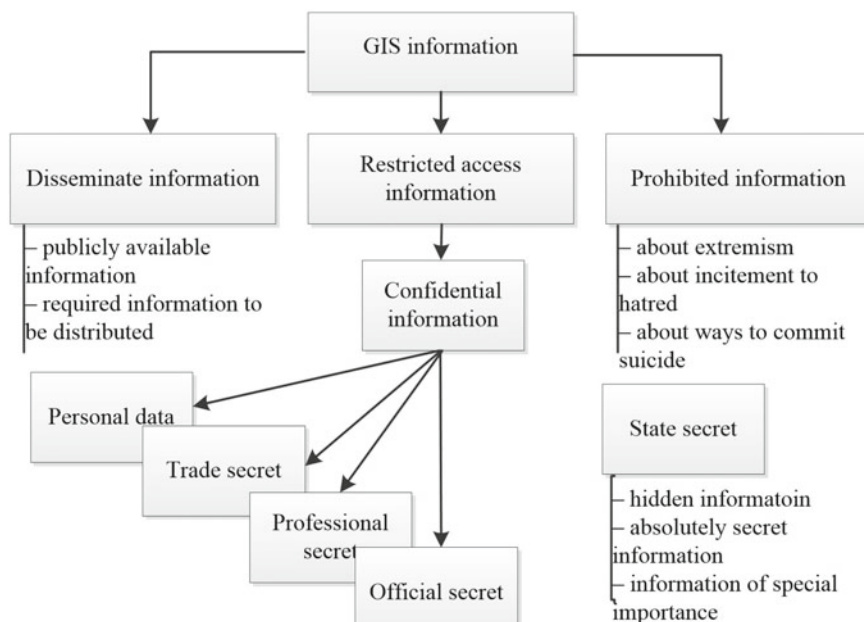


Fig. 1 Classification of GIS information by access mode

Each type of information has its own requirements for access control, which determines the specific requirements for GIS.

From the point of view of organizing information security and providing access to information, the following types of GIS are interesting: state and non-state organizations; public and private; commercial and free.

Information security in state GIS and public GIS is strictly regulated by regulatory documents.

A public information system is an information system in which participants in electronic interaction make up an indefinite circle of persons and the use of which cannot be denied to these persons [14].

Commercial GIS organize information security at their own discretion, if the processed information does not belong to government agencies.

Individuals only have access to the level of information security provided by the GIS owners.

Everyone can attack GIS to use it illegally [15].

In GIS as such, all information is processed, which means that for each specific GIS implementation, there will be its own set of information security threats, its own set of protective measures, its own implementation of the mechanism of the access control. For example, for GIS that fall under the definition of public information systems, the most important is accessibility [16]; for GIS containing information constituting a state secret, confidentiality is primarily required. It is important for all GIS to ensure the authenticity of the incoming data [17].

There is a contradiction between the need to delimit access to information in GIS and provide access to a wide range of people. It is possible, for example, to solve this contradiction by designing and certifying the GIS for the most rigid security class 1A [18]; but in this case, the cost of the GIS will be so great that no one will undertake to implement it, and the GIS will be so inconvenient that users will not be able to operate normally Services.

Classically, the problem is solved either from above, by forced division of GIS into segments, or from below,—GIS segments are generated stochastically and then integrated into a single spatial data infrastructure.

The granting of access is decided for each segment separately and consists of authentication, identification, and authorization in the GIS.

3 GIS User Authentication and Identification

GIS provides access to its information and services using a thin client and through an API interface. There are well-developed authentication protocols for all access options [19]: password authentication; forms authentication; authentication by certificates; one-time password authentication; authentication by access keys; authentication by tokens; using mandates; many others.

The main problem with all the described protocols is that they are suitable for a centralized system. This means that there is an element determining who can use the system and with what authority and who cannot.

If the GIS is segmented and there are several such centers, then relations of trust and delegation of authority are set up between them. One option is to create a GIS public key infrastructure and use certification authorities. In this case, the following methods of spreading trust between segments are available:

- (1) determination of the main element in all GIS and the subordination of all others to this element;
- (2) cross-certification. GIS segment owners decide with whom and what trust to establish. Moreover, if A trusts B, and B trusts C, then this does not mean that A trusts C. Or that C trusts B, or B trusts A. Each trust is established separately;
- (3) bridge scheme. The central element is formally assigned. Technically, trust relationships are established by option 2 and legally by option 1;
- (4) distribution of trust through CTL (certificate trusted list). Each segment has a master electronic key that determines who and what with authority can work in the system. Keys of all segments are collected in a single trusted list that is distributed across all GIS segments.

Schemes 1 and 3 have been tested and proved by authors [20] their worth when creating a network of trusted certification centers of the Federal Tax Service of Russia, the Pension Fund of the Russian Federation, electronic trading platforms, and customs. The FTS network included more than 400 certification centers and

several million users. The main element of the network is the Ministry of Communications and Mass Media. It seems reasonable to apply the already worked out scheme to create the state infrastructure of spatial data.

It is worth noting that with the expansion of GIS to the international level, problems arise associated with the recognition of the countries participating in the GIS of the applied cryptographic information protection tools, as well as with the existing restrictions on the export of such tools in some countries.

Identification issues while using this scheme are also well-developed for a large number of users with different types of identifiers and do not entail any particular difficulties.

The problem is the identification of GIS services and information. The existing solutions for mapping resources or using attribute certificates and Privilege Management Infrastructure [21] seem to be rather cumbersome for practical implementation and require further study.

4 GIS Users Authorization

User authorization is to allow information access the user with requested permission or reject the access request, if the requested permission exceeds the allowed.

The access mode and, therefore, the degree of secrecy of information are determined by the user-owner of the information, with the exception of the following cases: required information to be distributed; prohibited information, here, often, we are not talking about protecting information from the user, but about protecting the user from information; personal data; professional secret.

For these cases, there is a specific list of what is a subject to protection in accordance with the requirements of current legislation.

This means that the GIS must have mechanisms for differentiating access for all types of information, connected: (1) as directed by the user; (2) automatically, upon detection of compulsory protected information.

In the first case, the responsibility for the differentiation of access lies with the user in terms of deciding on the access mode and on the GIS in terms of implementing the decision made by the user.

In the second case, a settling module is needed, where all the information is initially received, and then, a decision is made what type it belongs to, and its further processing is prohibited or allowed. And the information itself must have clear signs by which it can be attributed to some of the classes without human participation.

Access to information—the ability to obtain information and use it [22]. Classically, GIS provides two types of access: read and write.

The main models for controlling access and the possibilities of their application are analyzed in the works [23, 24]: (1) discretionary model; (2) mandate model; (3) role model; (4) attributed model.

Even with the ideal implementation of the access control model, situations of security breaches of GIS information are possible.

For example, the wrong choice of security policy in a GIS can contribute to a breach of confidentiality. The cultural heritage protection authorities need to preserve the confidentiality of the boundaries of territories in relation to which there are grounds to assume the presence of archeological heritage objects or objects with signs of an archeological heritage object in these territories [25]. And the GIS security policy is to issue open areas of the map without objects of archeological heritage and closed ones containing objects—not. An attacker can query the GIS for all open areas. And those map elements that the GIS does not provide contain some kind of closed objects.

The recommendations set out in [26] will help to avoid a large number of typical mistakes when creating GIS. This is some quintessence of the experience of information security specialists. A similar approach to creating secure GIS is used in other countries [27].

Some problems found during the operation of complex information systems (IS):

- tracking uncontrolled transfer of rights during the operation of IS;
- adding new users and resources;
- removal of unnecessary users and resources and the appointment of new owners;
- giving legal significance to the processed information;
- granting access to special services;
- appointment of administrators of the unified system;
- technical and organizational features of GIS safety control;
- GIS interoperability when integrating with other information systems [28];
- a change in the worth of information, entailing both an increase and a decrease in the secrecy level of the processed information.

5 Conclusion

GIS processes a wide variety of different information types. For some information types, the degrees and access mode is determined by the owner of the information, for some it should be done automatically. GIS should provide both options. Authentication and identification for a decentralized GIS are done using a public key infrastructure. The ideal implementation of access control models does not always guarantee the protection of information, so the development of new models is necessary. Many access control problems are solved by GIS segmentation.

Acknowledgements The reported study was funded by Russian Ministry of Science (information security), project № 08/2020.

References

1. Kudelkin, V.A., Denisov, V.F.: Experience of integration of distributed information systems. *IT Standard* **1**, 24–30 (2017)
2. Stoletov, O.V., Chikharev, I.A., Moskalenko, O.A., Makovskaya, D.V.: Geoinformation support of the mediterranean branch of the silk road. In: *Geoinformational and Cartographical Security of Ecological, Economic and Social Aspects of Sustainable Development*, Part 25, vol. 1, pp. 102–113 (2019)
3. Schwab, K.: Globalization 4.0. new architecture for the fourth industrial revolution. *Eurasian Integr. Econ. Law Polit* **1**(27), 79–84 (2019)
4. Kolbanev, M.O., Palkin, I.I., Tatarnikova, T.M.: The challenges of the digital economy. *Hydrometeorol. Ecol. Sci. Notes RSHMU* **58**, 156–167 (2020)
5. GOST R 52438-2005 Geographical Information Systems Terms and Definitions
6. Gryzunov, V.V.: Dynamic aggregation of pools in military computing systems. *Inf. Control Syst.* **1**, 13–20 (2015)
7. Ananiev, Y.S.: *Geoinformation Systems: Tutorial*. TPU, Tomsk, Russia (2003)
8. Boltachev, E.F.: Visualization of data describing information technologies crimes. In: *Crime in the Sphere of Information and Telecommunication Technologies: Problems of Prevention, Disclosure and Investigation of Crimes*, vol. 1, no. 4, pp. 14–19 (2018)
9. Voronin, A.V., Zatsarinny, A.A.: Geoinformation system as the most important component of management decision making system. *Highly Available Syst. Sistemy vysokoy dostupnosti* **15**(3), 27–33 (2019)
10. Lisitsky, D.V., Katsko, Y.S.: User segment of a single territorial geoinformation space. *Bull. SGUGiT* **4**(36), 89–100 (2016)
11. Yankelevich, S.S., Radchenko, L.K., Antonov, Y.S.: From multi-purpose cartographic resource to “smart map”. *Bull. SGUGiT* **23**(1), 142–155 (2018)
12. Koshkarev, A.V.: Laws and standards for the development of geomatics in the digital economy era. *Vestnik of North-Eastern Federal University. Earth Sci.* **3**(15), 46–54 (2019)
13. Nesterowskij, I.P., Yazov, Y.K.: Possible approach to assessment of damage suffered from a threat to security of information being processed in federal information systems. *Cybersecur. Issues* **2**(10), 20–25 (2021)
14. Federal Law of 06.04.2011 N 63-FZ (Revised 10.07.2012) “About the Electronic Signature”
15. Gryzunov, V.V.: Model of purpose aggressive actions on the information-computing system. In: *Third International Conference on Human Factors in Complex Technical Systems and Environments (ERGO)s and Environments (ERGO)*, pp. 300–305 (2018) <https://ieeexplore.ieee.org/document/8443814>
16. Order of FSTEC of Russia of August 31, 2010 N 489 “About Protection of Information Contained in Public Information Systems”
17. Gryzunov, V.V., Ukrainitseva, D.A.: Appearance of the data authenticity protection system of the geoinformation system. In: *Information Security of Russian Regions. Materials of the XI St. Petersburg Interregional Conference*, pp. 172–173 (2019). http://spoisu.ru/files/ibrr/ibrr2019/ibrr2019_materials.pdf
18. GOST R 50922-2006. Information Security Basic Terms and Definitions
19. Overview of Authentication Methods and Protocols in Web Applications. <https://habr.com/ru/company/dataart/blog/262817/>
20. Certificate of Registration of a Computer Program of the Russian Federation. No. 20077613135. Software Complex Information Resource of the Certification Center (“IRUC”)/V.V. Gryzunov (RF), G.M. Dranishnikov (RF), A.V. Kirpichnikov (RF), A.S. Sotenko (RF). No. 2007612892; Declared 07/12/2007; Registered July 25, 2007
21. Sazonov, A.V.: Subject and technology rights management infrastructure in transboundary space. *Inf. Secur. Issues* **3**(98), 83–87 (2012)

22. Guidance Document. Automated Systems. Security Against Unauthorized Access to Information. Classification of Automated Systems and Requirements for Information Protection. Approved by the Decision of the Chairman of the State Technical Commission Under the President of the Russian Federation of March 30, 1992
23. Overview and Comparison of Existing Access Control Methods. Institute of Computing Technologies SB RAS [Electronic Resource]. <http://www.ict.nsc.ru/ws/YM2003/6312/>
24. Kalimoldayev, M.N., Biyashev, R.G., Rog, O.A.: Analysis of the Methods for Attribute-Based Access Control. <https://doi.org/10.17223/20710410/44/4>
25. Asset 9. Federal Law No. 73-FZ of 25.06.2002 (Revised 24.04.2020) “About Objects of Cultural Heritage (Historical and Cultural Monuments) of the Peoples of the Russian Federation”
26. FSTEC. Methodology for Determining Threats to Information Security in Information Systems
27. Ageev, V.O., Shilov, A.K.: Protection in the foreign and domestic system. In: VI All-Russian School-Seminar ‘Perspective-2015’, pp. 313–315, Russia (2015)
28. GOST R 55062-2012. Information Technologies (it). Industrial Automation Systems and Their Integration. Interoperability. Fundamentals

Security Augmented Symmetric Optical Image Cryptosystem Based on Hybrid Transform Employing Rear Mounted Technique Using Three Different Complex Masks



Priyanka Maan, Hukum Singh, and A. Charan Kumari

Abstract This paper presents the utilization of the novel rear mounted triple phase masking procedure to increase the security of traditional double random phase encoding (DRPE) scheme with a variation of hybrid transform. Two chaotic random phase masks and a deterministic phase mask are used in the scheme to enhance its security as opposed to traditional DRPE which uses random phase masks. From the previous studies on cryptanalysis of DRPE, it is clear that the second lens used in it proves to be irrational which leads to cryptanalytic attacks on DRPE. The enhanced framework discards the invalidation of the second lens and therefore reinforces DRPE security. The hybrid transform is a combination of fractional Hartley transform and Gyrator transform that improves the quality of the cryptosystem. The carried out simulations exhibit the efficacy of the designed symmetric cryptosystem.

Keywords Chaotic random phase mask • Deterministic phase mask • Fractional Hartley transform • Gyrator transform • Rear mounted triple phase masking

P. Maan (✉)

Department of Computer Science Engineering, The NorthCap University,
Sector 23 A, Gurugram 122017, India

H. Singh

Department of Applied Sciences, The NorthCap University, Gurugram, India
e-mail: hukumsingh@ncuindia.edu

A. Charan Kumari

Department of Electrical Engineering, Faculty of Engineering,
Dayalbagh Educational Institute, Agra 282005, India

1 Introduction

In data security, cryptography, which scrambles the private and secret data into an encrypted form before transmission to keep away from data revelation, plays a critical role. Due to inherent advantages like multi-dimension encryption qualities, high parallel processing and speed optical cryptosystems are preferred over the digital ones [1–3]. DRPE is a traditional run of the optical image encryption strategy that uses two random phase masks (RPM) for the encoding of an image into a stationary noise [4]. From there on, various variations of the DRPE scheme came in picture based on different transforms and different masks. Every scheme has its own highlights and challenges [5, 6]. The cryptanalysis study of DRPE discovered that it is vulnerable to several attacks like known plaintext, chosen plaintext, chosen cipher text, etc. So to strengthen the security perspective of the DRPE technique, various advancements come in picture like fully phase encoding [7, 8], chaos-based mask generation [9, 10], pixel randomization, extending DRPE in different transforms domain like fractional Fourier transform (FrFT) [11, 12], Fresnel transform (FrT) [13, 14], Gyrator transform (GT) [15, 16], etc., and various asymmetric schemes [17, 18]. Some schemes also make use of combination of different transforms and some new additional techniques like singular value decomposition (SVD), equal modulus decomposition (EMD), etc., for performing image encryption. Later, the encryption is performed on phase images [19, 20] while some use the technique of performing encryption in spectrum domain on spectral images [21] and other uses sandwiched phase code to diffuse random phase masks to perform encryption and decryption [22]. Various researchers have also presented the use of logistic and chaotic map in the field of image encryption [23]. But dismally, these proposed schemes have their drawbacks too and can be cryptanalyzed like DRPE is recently cryptanalyzed using deep learning technique [24]. As known, DRPE is the elementary and the simplest technique, enhancing its security with lesser complexity is yet an appealing issue.

In this paper, the security improvement of the DRPE is strengthened by employing rear mounted triple phase masking technique in the fractional Hartley transform (FHT) and Gyrator transform domain as the encryption strategy and also to overcome the invalidation of second lens in the traditional DRPE. As identified [25, 26], the invalidation of second lens used in Fourier domain in DRPE leads to the cryptanalysis of the encrypted image. So to overcome the effect of this concept, the introduction of one more phase mask called rear mounted phase mask at the output plane is proposed in the discipline of hybrid transform-based DRPE. The three masks leading to triple phase masking scheme are two chaotic random phase masks and one deterministic phase mask which leads to strengthening the security of the proposed method. The proposed algorithm extends the security by exploiting the potential of second lens by adding an extra layer of rear mounted mask. The three complex masks used in the scheme are much more secure and prove to be a great advantage in enhancing its security potential as they are difficult to regenerate without proper information than the random phase mask used in the traditional

DRPE scheme. The use of fractional Hartley transform and Gyrator transform has a reason of providing computational ease and convenient implementation optically. Simulation results provide the validation and efficacy of the proposed cryptosystem.

2 Mathematical Background

The proposed system uses chaotic random phase mask, deterministic phase mask in the FHT, and GT domain employing rear mounted scheme.

2.1 Chaotic Random Phase Mask

Chaotic random phase mask can be formed with the combination of random phase mask and chaotic function. RPMs are used as a secretive key in DRPE-based image encryption. Chaos theory indicates that when a small error in the input calculations can generate a largest possible error in the output, then it can be classified as a chaotic function. Chaotic function portrays nonlinear framework from organized to confused state. A chaotic map is a map that displays some kind of chaotic behavior. Chaotic map can generate tremendous number of random iterative values exhibiting ergodicity, non-correlation, and pseudo randomness kind of nature. RPM can also be likewise built from chaotic function.

A logistic map can be defined as a one-dimensional nonlinear chaos function using the equation below:

$$f(x) = bx(1 - x) \quad (1)$$

where b represents the bifurcation parameter having value in the range $0 < b < 4$. The iterative version of Eq. (1) can be asserted as:

$$x_{n+1} = bx_n(1 - x_n) \quad (2)$$

where x_0 represents the initial value and x_n represents the iterative value with the range $x_n \in [0,1]$.

For generating chaotic random sequence to be use in the encryption process, we first need one-dimensional random value sequence. Using Eq. (2), the one-dimensional random value sequence can be depicted as:

$$X = \{x_1, x_2, x_3 \dots x_{(M \times N) + k}\} \quad (3)$$

where k represents any chosen value of integers and $x_i \in (0,1)$. As images are a two-dimensional function, so the two-dimensional sequence can be generated by rearranging the X as Y which can be depicted as:

$$Y = \{y_{i,j}, |i = 1, 2, \dots, M + k, j = 1, 2, \dots, N + k\} \quad (4)$$

where $y_{i,j} \in (0,1)$. Now, the CRPM can be finally generated using the equation below:

$$\text{CRPM}(x, y) = \exp[i2\pi y_{i,j}(x, y)] \quad (5)$$

where (x, y) represents the coordinated of CRPM. CRPM comprises of three keys, namely x_0, b and n . In the proposed system, two CRPMs are generated CRPM1 and CRPM2 which are depicted in Fig. 3a, b.

2.2 Deterministic Phase Mask

In the proposed system, we have used a deterministic phase mask as the rear mounted key. To generate a DPM [27, 28], firstly we need to set the value of order of encryption parameter ' m ' whose value can be $m = 2, 3, 4$. Now, we decide the number of subkeys (NS) using the parameter m with the help of equation below.

$$\text{NS} = 2^m \times 2^m \quad (6)$$

Then, we split the input image in NS equal sub-blocks. The size of each sub-block can be represented using parameter ' d ' and can be calculated using the equation below.

$$d = \frac{\text{dim}}{2^m} \quad (7)$$

where dim represents input image size.

DPM can now be generated using the continuous combination of sub-masks ($M_{i,j}$) using the following equation:

$$\text{DPM} = \sum_{i=1}^{2^m} \sum_{j=1}^{2^m} M_{i,j}(d \times d) \quad (8)$$

where $M_{i,j}$ represents the number of sub-blocks required for the generation of DPM. $M_{i,j}$ can be defined as:

$$M_{i,j}(p, q) = \exp[i2\pi(u_k.p + v_k.q)] \quad (9)$$

where u_k and v_k range lies between $[1, d]$ in which they are randomly generated. The value of k lies in the given interval $[1, 2^m]$. In our proposed scheme, we have used $m = 2$ for deterministic phase mask generation and for simplicity of the scheme. Figure 3c depicts the DPM used.

3 Methodology

Based on the cryptanalytic attacks possible on the elementary DRPE scheme, an upgraded hybrid transform-based DRPE cryptosystem in the light of rear mounted triple phase masking has been proposed. A supplementary phase mask called rear mounted phase mask has been used which is characterized as DPM, i.e., deterministic phase mask and the other two random phase masks in traditional DRPE has been replaced with chaotic random phase masks, namely CRPM1 and CRPM2. DPM fills in as extra secret key and is used to phase modulate the cipher data again that is generated after the application of hybrid transform-based DRPE. Equation (10) below shows the output of the encryption scheme. The decryption is the reverse of the encryption procedure, and Eq. (11) given below depicts the calculation of the decryption output.

$$C(x, y) = \text{DPM} \cdot \text{GT}^{-\alpha}(\text{CRPM2} \cdot \text{FHT}(p, q)(I(x, y) \cdot \text{CRPM1})) \quad (10)$$

$$I(x, y) = \text{CRPM1}^* \cdot \text{FHT}(-p, -q)(\text{CRPM2}^* \cdot \text{GT}^{\alpha}(C(x, y) \cdot \text{DPM}^*)) \quad (11)$$

where $I(x, y)$ and $C(x, y)$ are the original image and cipher image, respectively. $*$ denotes the conjugate operation. DPM denotes the deterministic phase mask, and CRPM1 and CRPM2 denote the two chaotic random phase masks. GT^{α} represents Gyrator transform with α as rotation angle [14]. $\text{FHT}(p, q)$ denotes the fractional Hartley transform with two order parameters p and q .

The encryption and decryption mechanism has been depicted in Fig. 1a, b, respectively. During encryption, the input image $I(x, y)$ is introduced to the encryption algorithm, and the final output we get is represented by $C(x, y)$. Decryption process is the reverse of the encrypted one, where we apply the decryption algorithm on the encrypted image $C(x, y)$ which has been sent to the receiver after encryption. Firstly, we multiple $C(x, y)$ to the conjugate of rear mounted phase mask DPM^* , and then the product is subjected to Gyrator transform with rotation angle α . Then we multiply the resultant with the conjugate of second chaotic random phase mask CRPM2^* . On the output of this step, we apply fractional Hartley transform with parameters $(-p, -q)$. Finally to get the original image $I(x, y)$ back, we subject the resultant of previous step to the conjugate of first chaotic random phase mask CRPM1^* . In the presented paper, the security potential of the second lens used in the DRPE has been enhanced by the introduction of one more mask at the output plane for the prevention of the realization of the cipher.

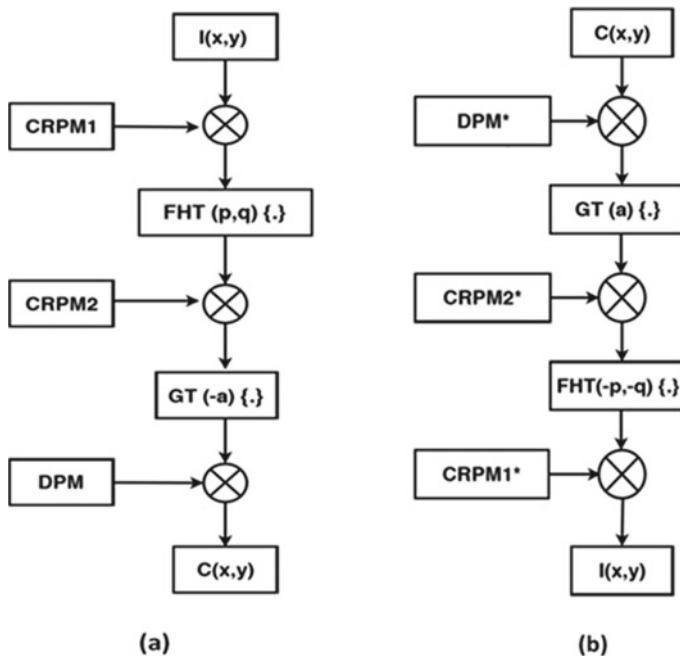


Fig. 1 a Encryption flowchart; b decryption flowchart

4 Simulation Results

MATLAB (R 2019a) 5(9.6.0.117 49 12), L.4066 4799 has been used to carry out the simulation, and the results have been interpreted. Figure 2a depicts the original input image ‘Peppers.png,’ a gray scale image with size 256×256 which is to be encoded. Figure 2b, c shows the encrypted and decrypted images with respect to the original image by employing the presented scheme. After applying encryption algorithm, we get the encrypted image which is a random image from which it is difficult to identify the original image corresponding to it. After applying decryption algorithm with correct parameters, we get the decrypted image. Figure 3a–c depicts the masks that act as the keys during the encryption and decryption process. The presented scheme includes three keys as phase masks, i.e., two chaotic random phase masks (CRPM1, CRPM2) and one deterministic phase mask (DPM) which acts as rear mounted phase mask.

Figure 4a–c depicts the 3D views of original, encrypted, and decrypted images.

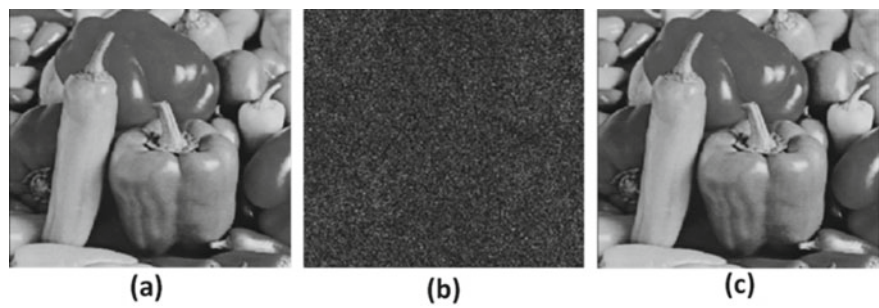


Fig. 2 a Original image; b encrypted image; c decrypted image

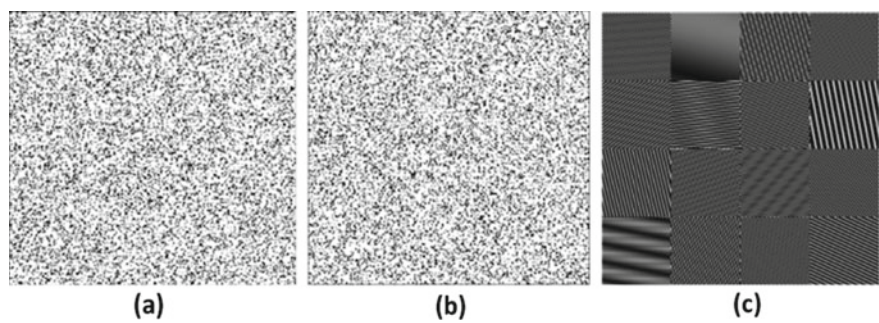


Fig. 3 a CRPM1; b CRPM2; c rear mounted phase mask (DPM)

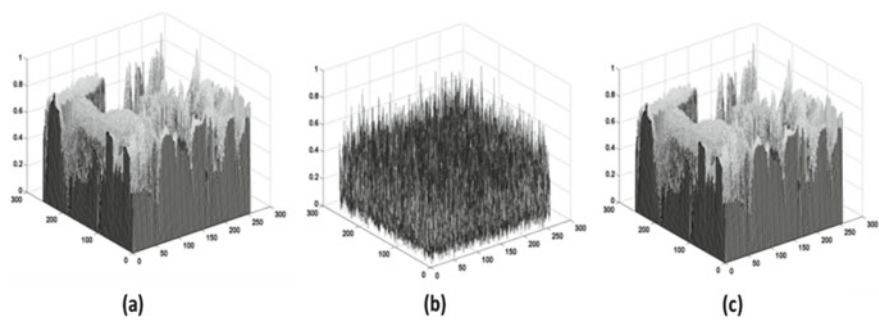


Fig. 4 3D views of a peppers image; b encrypted image; c decrypted image

5 Performance and Security Analysis

5.1 Error Analysis

To check the competency and strength of the proposed algorithm, we calculate the mean square error (MSE) and peak signal to noise ratio (PSNR) [18] values using the formula are given below:

$$\text{MSE} = \frac{1}{M \times N} \sum_{x=1}^N \sum_{y=1}^N |O(x, y) - D(x, y)|^2 \quad (12)$$

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{(N-1)^2}{\text{MSE}} \right) \quad (13)$$

where M and N are the length and width of the images. $O(x, y)$ is the original input image, and $D(x, y)$ is the decrypted image. MSE and PSNR values calculated using the given scheme are 1.50×10^{-24} and 286.34, respectively. Figure 5a, b depicts the plot of MSE and PSNR curves versus fractional order.

5.2 Correlation Coefficient (CC) Analysis

The correlation coefficient analysis has been done for both the original and encrypted images by randomly selecting 10,000 pairs of adjacent pixels in all the three directions, i.e., horizontal, vertical and diagonal. The formula for calculation of CC [28] is given in Eq. (14) below:

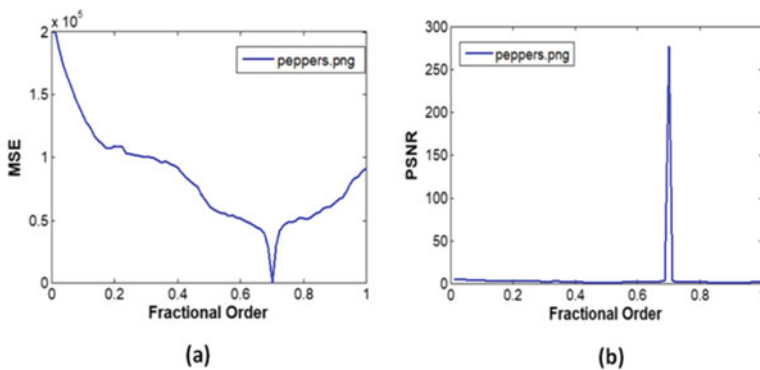


Fig. 5 **a** MSE versus fractional order plot; **b** PSNR versus fractional order plot

$$CC = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\sum_{i=1}^N (x_i - \bar{x})^2\right) \left(\sum_{i=1}^N (y_i - \bar{y})^2\right)}} \tag{14}$$

$$\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \tag{15}$$

$$\bar{y} = \frac{1}{N} \sum_{i=1}^N y_i \tag{16}$$

where $\bar{x}$ and $\bar{y}$ represent the mean values of x_i and y_i , respectively. Table 1 and Fig. 6 represent the CC analysis done for the original and encrypted images.

The CC distribution values of encrypted image in all the three directions as given in the table below show that they are very less correlated as compared to the values of the original image. The scatter plot of encrypted image also depicts that it has random distribution, and after encryption, it is difficult for intruder to identify the original image.

5.3 Key Sensitivity Analysis

To check the strength and robustness of the proposed algorithm, sensitivity analysis has been done for different parameters. Figure 7a displays the output when we use wrong second mask, i.e., CRPM2 for decryption. If we exchange the first and second chaotic random phase masks during decryption, then we get the output as displayed in Fig. 7b. When we use wrong rear mounted phase mask, i.e., DPM for decryption, then also we are not able to get the original image while performing decryption as shown in Fig. 7c. If the rotation angle of Gyrator transform used is wrong, i.e., $\alpha = 0.05 * \pi$ instead of the original one, i.e., $\alpha = 0.05 * \pi$, then we get the decrypted output as shown in Fig. 7d. When we take the wrong values for order parameters (p, q) of fractional Hartley transform, then we get the result as shown in Fig. 7e, f. The original values used in the presented scheme are $p = 0.7$ and $q = 0.4$.

From the analysis, it is positively implicit that the use of wrong parameters produces wrong results. The key space of the presented scheme constitutes rotation

Table 1 Horizontal, vertical, and diagonal directions values of correlation coefficient of original and encrypted image

Image	Original image			Encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Peppers	0.9398	0.8869	0.8274	0.0247	0.0825	0.0575

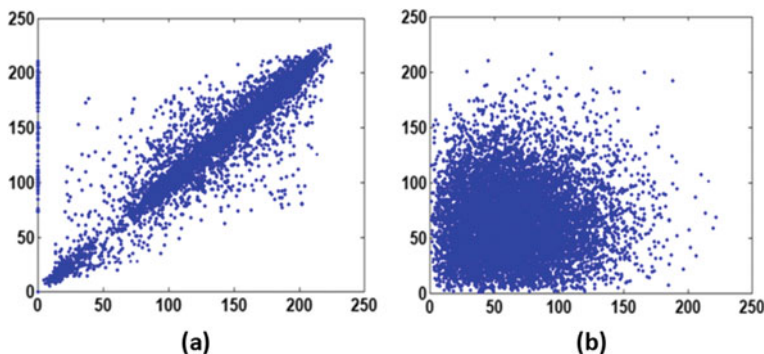


Fig. 6 **a** Correlation distribution of original image; **b** correlation distribution of encrypted image

angle (a) of Gyrator transform, order parameters (p , q) of fractional Hartley transform, and 3 phase masks used. It is evident from the above discussion that even the slight variation in these key parameters produces scrambled result from which we even cannot identify a part of the original image. Thus, it proves the robustness of proposed framework.

6 Conclusion

A security enriched image encryption method in light of fractional Hartley and Gyrator-based hybrid transform utilizing rear mounted triple phase masking has been proposed to overcome the invalidation of second lens in DRPE. The key space constitutes: rotation angle of Gyrator transform (a), 2 order parameters (p , q) of fractional Hartley transform, 2 logistic map parameters, and 3 masks, i.e., CRPM1, CRPM2, and DPM. The enlarged key space resists the brute-force attack on the proposed algorithm. The utilization of DPM as a mask in the third layer of cryptosystem enhances the security potential of the presented scheme. The usage of complex masks and the enhancement in the number of security parameters of the stated algorithm makes it immune against chosen plaintext attack, known plaintext attack, etc. The scheme has been verified on different factors like correlation coefficient analysis, MSE, and PSNR to check its adequacy and strength. The key sensitivity analysis and numerical simulation results mark the security enhancement of the scheme in comparison to the beforehand existing schemes. The developed cryptosystem has an advantage of being a symmetric one which makes it less complex and fast in comparison to the asymmetric ones. This technique highlights the use of rear mounted triple phase masking to build the key space, enhancing the security potential of second lens and makes the scheme troublesome for an eavesdropper to recuperate the original image which affirms the security improvement.

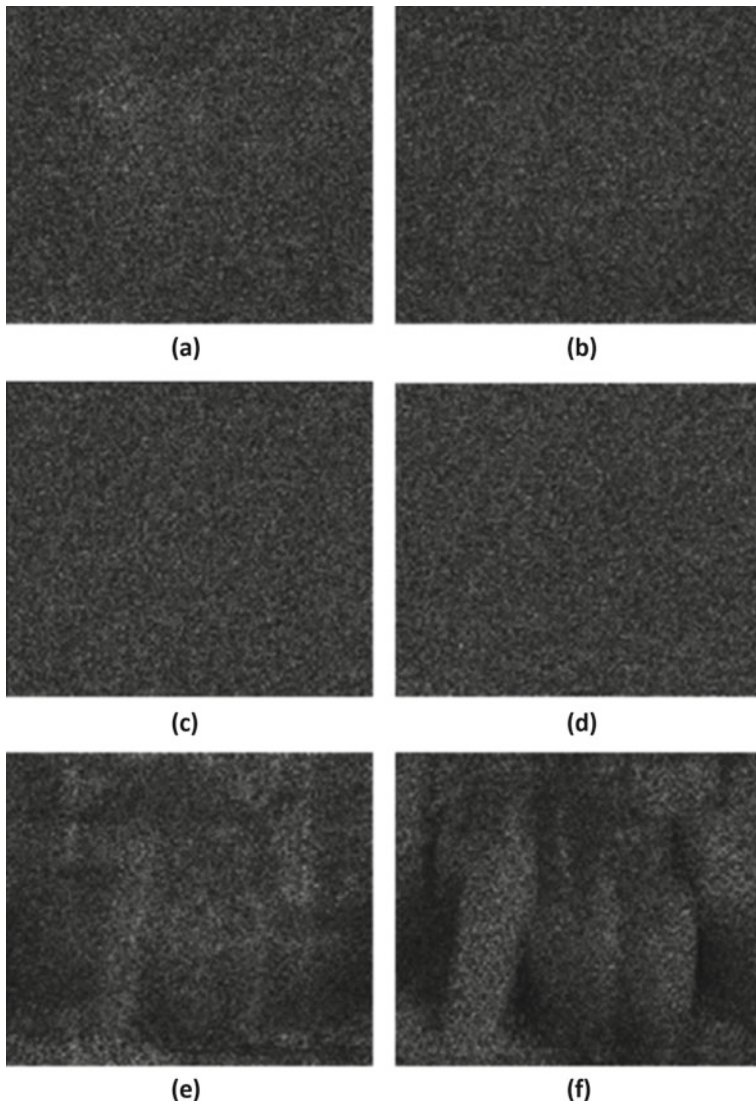


Fig. 7 **a** When second mask (CRPM2) is wrong; **b** when both CRPM are exchanged; **c** when DPM is wrong; **d** when Gyrator angle is wrong ($\alpha = 0.05 * \pi$); **e** when $p = 0.2$ first fractional order is wrong; **f** when $q = 0.2$ s fractional order is wrong

References

1. Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M.S., Javidi, B.: Optical techniques for information security. *Proc. IEEE* **97**(6), 1128–1148 (2009)
2. Chen, W., Javidi, B., Chen, X.: Advances in optical security systems. *Adv. Opt. Photonics* **6**(2), 120–155 (2014)
3. Javidi, B., Carnicer, A., Yamaguchi, M., Nomura, T., Pérez-Cabré, E., Millán, M.S., Nishchal, N.K., Torroba, R., Barrera, J.F., He, W., Peng, X.: Roadmap on optical security. *J. Opt.* **18**(8), 083001 (2016)
4. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**(7), 767–769 (1995)
5. Kumar, P., Joseph, J., Singh, K.: Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures. In: *Linear Canonical Transforms*, pp. 367–396. Springer (2016)
6. Maan, P., Singh, H.: A survey on the applicability of Fourier transform and fractional Fourier transform on various problems of image encryption. In: *Communication and Computing Systems*, pp. 475–480 (2017)
7. Singh, H., Yadav, A.K., Vashisth, S., Singh, K.: Fully phase image encryption using double random-structured phase masks in gyrator domain. *Appl. Opt.* **53**(28), 6472–6481 (2014)
8. Nishchal, N.K., Joseph, J., Singh, K.: Fully phase encryption using fractional Fourier transform. *Opt. Eng.* **42**(6), 1583–1589 (2003)
9. Abuturab, M.R.: Securing multiple information using chaotic spiral phase encoding with simultaneous interference and superposition methods. *Opt. Lasers Eng.* **98**, 1–16 (2017)
10. Enayatifar, R., Abdullah, A.H., Isnin, I.F.: Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt. Lasers Eng.* **56**, 83–93 (2014)
11. Unnikrishnan, G., Joseph, J., Singh, K.: Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **25**(12), 887–889 (2000)
12. Tao, R., Xin, Y., Wang, Y.: Double image encryption based on random phase encoding in the fractional Fourier domain. *Opt. Express* **15**(24), 16067–16079 (2007)
13. Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **29**(14), 1584–1586 (2004)
14. Khurana, M., Singh, H.: Asymmetric optical image triple masking encryption based on Gyrator and Fresnel transforms to remove silhouette problem. *3D Res.* **9**(3), 1–17 (2018)
15. Rodrigo, J.A., Alieva, T., Calva, N.L.: Gyrator transform: properties and applications. *Opt. Express* **15**, 279–284 (2007)
16. Singh, H.: Hybrid structured phase mask in frequency plane for optical double image encryption in gyrator transform domain. *J. Modern Opt.* **65**(18), 2065–2078 (2018)
17. Maan, P., Singh, H.: Non-linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain. *3D Res.* **9**(4), 1–12 (2018)
18. Maan, P., Singh, H., Kumari, A.C.: Optical asymmetric cryptosystem based on kronecker product, hybrid phase mask and optical vortex phase masks in the phase truncated hybrid transform domain. *3D Res.* **10**(1), 1–18 (2019)
19. Singh, P., Yadav, A.K., Singh, K.: Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. *Opt. Lasers Eng.* **91**, 187–195 (2017)
20. Chen, H., Du, X., Liu, Z.: Optical hyperspectral data encryption in spectrum domain by using 3D Arnold and gyrator transforms. *Spectroscopy Lett.* **49**(2), 103–107 (2016)
21. Han, C.: An image encryption algorithm based on modified logistic chaotic map. *Optik* **181**, 779–785 (2019)
22. Hasheminejad, A., Rostami, M.J.: A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. *Optik* **184**, 205–213 (2019)

23. Rakheja, P., Vig, R., Singh, P.: An asymmetric hybrid cryptosystem using hyperchaotic system and random decomposition in hybrid multi resolution wavelet domain. *Multimedia Tools Appl.* 1–26 (2019)
24. Hai, H., Pan, S., Liao, M., Lu, D., He, W., Peng, X.: Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning. *Opt. Express* **27**(15), 21204–21213 (2019)
25. Chen, J., Zhang, Y., Li, J., Zhang, L.B.: Security enhancement of double random phase encoding using rear-mounted phase masking. *Opt. Lasers Eng.* **101**, 51–59 (2018)
26. Khurana, M., Singh, H.: A spiral-phase rear mounted triple masking for secure optical image encryption based on gyrator transform. *Recent Pat. Comput. Sci.* **12**(2), 80–94 (2019)
27. Zamrani, W., Ahouzi, E., Lizana, A., Campos, J., Yzuel, M.J.: Optical image encryption technique based on deterministic phase masks. *Opt. Eng.* **55**(10), 1–9 (2016)
28. Girija, R., Singh, H.: A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition. *Opt. Quantum Electron.* **50**(5), 1–24 (2018)

Security Considerations in the Design of IEEE 802.15.4 Transceiver: A Review



K. Vivek Raj, P. Dinesha, and S. I. Arpitha Shankar

Abstract As internet of things (IoT) is extending internet connectivity beyond standard devices; the secure data transmission between IoT devices becomes more challenging. However, most of the traditional upper layer security schemes are computationally complex and increase the latency. Moreover, the security provided at upper layer is software implemented, and its strength depends on complexity of the encryption algorithm. This is a bottleneck situation for low-power IoT applications. As IoT uses many remote sensors which operate on battery power; IEEE 802.15.4 standard is gaining attention because of low-power consumption. An 802.15.4 protocol defines medium access control (MAC) and physical layer (PHY) specifications, and is designed to allow low-power, low-cost short range communication. Basic encryption and authentication in 802.15.4 are provided by link layer. Hence, considerable attention is required to study 802.15.4 specifications that can be used to provide alternative methods of security. So this paper is motivated to study the importance of 802.15.4 PHY. Firstly, we review the different physical layer security (PLS) schemes. Secondly, we present the concept of physical layer encryption (PLE) and further we analyze and compare the implementation of different PLE schemes in wireless standards. Later, we will try to give insights of 802.15.4 security standards and bring out the drawbacks of AES based link-layer security. Finally, we present the design and implementation aspects of 802.15.4 transceiver hardware architecture by considering performance and security.

K. Vivek Raj (✉)

Department of Electronics and Telecommunication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka 560078, India

P. Dinesha

Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka 560078, India

S. I. Arpitha Shankar

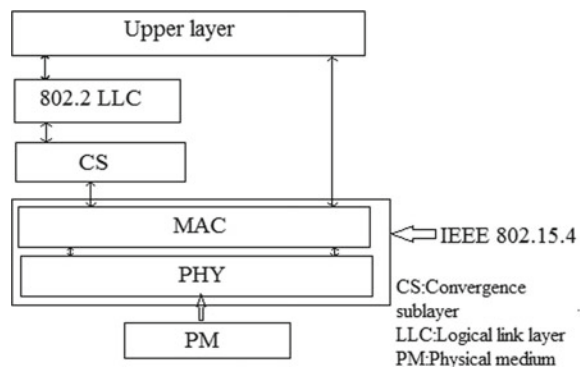
Department of Electronics and Telecommunication, GSSS Institute of Engineering and Technology for Women, Mysore, Karnataka 570016, India

Keywords IEEE 802.15.4 • Computational security • Physical layer security • Internet of things • Physical layer encryption • Transceiver • Medium access control • Authentication

1 Introduction

In recent years, wireless communication is advancing with respect to its infrastructure and services with an aim of meeting rapidly growing demands. Wireless networks are being used for many applications. The International telecommunications Union [ITU] facts and figures in 2020 indicates that in 104 countries, half of the population is now using internet of which 70% are the youth [1]. Extending internet connectivity beyond conventional mobile phones and computers leads to evolution of new technology called internet of things. Currently, IoT is gaining more importance and it is playing important role in most of the fields such as health monitoring, automation, e-cities and so forth. However, secure data communication on IoT technology is more challenging scenario due to many constraints like power consumption, less storage memory and availability of processing power etc. [2]. Due to this, existing cryptographic techniques that are provided at the upper layer are not suitable because of their power consumption and the complexity in implementation. The IEEE 802.15.4 is designed to provide very low-cost communication between nearby devices in wireless personal area network (WPAN). Low-power wireless connectivity of 802.15.4 attracts wide variety of applications especially which operates on battery power. Since IoT employs different sensors which rely on battery, the use of 802.15.4 becomes most common in IoT applications. The structure of 802.15.4 protocol stack is shown in Fig. 1. It defines PHY and MAC layer specifications. PHY sits at the bottom of the protocol stack and transmit data packets. Direct sequence spread spectrum (DSSS) allows two physical layer configurations one works at 868/915 MHz and provides data rate of 20–40 kbps, second operates at 2.4 GHz with 250 kbps.

Fig. 1 IEEE 802.15.4 protocol stack



However, further revision in the standard allows the use of different modulation schemes. MAC layer performs different functions including channel access, frame delivery, synchronization, flow control, error control and it also provides interface between PHY and application layer. 802.15.4 is gaining importance as demand for IoT is increasing and security becomes a major concern. The PHY security technology combines the communication PHY and the security layer; hence, it is important to study the fundamental ability of the 802.15.4 PHY to offer secure wireless communication. In recent times, PLS and PLE are in much attention. Both of these approaches exploit the properties and characteristics of the PHY to provide the security. PLS provide information-theoretic security that is impossible to break by computing power. On the other hand, PLE is based on computational complexity and uses distribution of secret key. Unlike conventional cryptography, encryption in PLE is performed during the modulation process. That is in PLE, the security is provided at signal level. Further, PLE takes advantage of effect of the channel and noise. Hence, it increases the strength of underlying algorithm as it makes difficult in receiving the encrypted text itself. However, there is a clear difference between PLS and PLE.

Some of the characteristics which differentiates PLE from PLS are listed below.

- 1. Unlike PLS, PLE can guarantee secrecy, even if the channel capacity of eavesdropper is better than legitimate channel.
- 2. PLE has low-computational complexity, provides low latency with minimum power consumption and provides long lifetime hence it is best suited for IoT applications.
- 3. PLE provides security at signal level. It uses Boolean algebra therefore it gives much more functions to design and construct secure encryption algorithm.
- 4. In contrast to PLS which only focuses on eavesdropping attack, PLE uses randomness function which can be used to prevent linear and plaintext attacks.

Since our focus is on 802.15.4 protocol, further we concentrate more on the security aspects in the design of 802.15.4 transceiver. Table 1 provides the comparison between PLS, traditional cryptography and PLE and shows that PLE is different than PLS and conventional cryptography.

Table 1 Comparison of PLS, cryptography and PLE

Type	Distribution of key	Type of channel	Type of security	Operate domain
PLS	NO	Noise channel	Perfect secrecy, depends on channel	Complex vector
Traditional cryptography	YES	Perfect channel	Computationally secure	Bit level
PLE	YES	Noise channel	Computationally secure, uses characteristics of channel	Complex vector and signal level

Most of the available upper layer encryption schemes are computationally complex and increases the latency and its strength completely depends on complexity of the encryption algorithm. However, PLS schemes can provide security at the physical layer, but its implementation faces serious problems. PLS cannot guarantee secrecy if the legitimate node has weak channel capacity than eavesdropper or if no channel information of eavesdropper is available. Power consumption is large in PLS as it uses more number of relays or antenna systems. From Table 1, we have seen that PLE schemes have many advantages over other two. It is more practical to use PLE in the design and construction of secure 802.15.4 transceiver.

Rest of the paper is organized as follows. Section 2 presents overview of PLS. In Sect. 3, PLE and its implementation in different wireless systems are discussed. In Sect. 4, different security suits of 802.15.4 protocol is compared. Section 5 gives hardware implementation of 802.15.4 transceiver, and finally Sect. 6 provides conclusion.

2 Physical Layer Security

PLS provides unbreakable, quantifiable and provable secrecy from the information-theoretical point of view. PLS takes an advantage of wireless channel characteristics for improving the reliability and security. In this subsection, we discuss about different PLS schemes such as information-theoretic security, artificial noise generated secrecy, secure beam forming and diversity-assisted security.

2.1 *Information-Theoretic Security*

It is a cryptosystem whose secrecy is derived mainly from an information theory. Basic principle of security schemes was developed by focusing on the properties of mathematical structures. Claude Shannon proposed a security principle as a mathematical transformation of valid plaintext into another set of reliable cryptograms. Here, each transformation is done by encrypting the message, using secret keys. This cryptosystem is unbreakable even though attacker has unlimited computing power. One-time pad is an example of such a cryptosystem. This secrecy system was designed for protection against eavesdropping attacks. Since Shannon model uses distribution of key, key management becomes difficult for wireless networks with no fixed infrastructure [3]. Wyner improved Shannon's model without secret keys and analyzed the performance of a discrete memory less wiretap channel and achieved perfect secrecy, provided if the capacity of a channel of the link spanning from an sender to receiver must be greater than the wiretap link between the sender and the adversary [4] and he proved that secure communications without keys can be realized with channel quality between intended nodes which is

better than the adversary link [5]. However, the use of information theoretic security is not practical because of difficulty in key generation and distribution. Further, secrecy capacity of wireless networks is extremely attenuated because of time varying fading effect. Usually, fading degrades the signal received at the legitimate receiver, which decreases the capacity of the valid channel, and reduces the secrecy capacity.

2.2 Artificial Noise Aided Security

Artificial noise (AN) has been exploited to enhance the security performance by degrading the capacity of the adversary, termed as artificial noise aided security. Basic principle of the noise injection method is to simultaneously transmit the message and the generated noise in order to reduce the performance of the adversary [5]. In AN pre-coding, the source node splits the transmission power between data transmission to legitimate receiver and the noise transmission to the eavesdropper. The transmitter is designed in such a way that only adversary channel is selectively degraded. With this model, certain minimum rate of security can be achieved. However, secrecy cannot be guaranteed, if the eavesdropper channel is better than the recipient [6, 7]. AN pre-coding gives provable security at the PHY, but it comes with an extra cost of additional energy requirements. In this approach, a fraction of transmission power of message signal is taken to produce the AN. It depletes transmission power that can be utilized to improve the capacity of a channel and receiver signal-to-noise ratio (SNR). Hence, it is a compromise between the transmission power and secrecy rate [8].

2.3 Security Oriented Beam Forming

This technique is extensively used in the relay systems; it helps in improving the SNR at the receiver end. It has an ability to control the direction of transmission, it only focuses energy in specified direction and suppresses energy in other direction. This in turn increases the energy efficiency of a system. Consider a model which consists of A, B and C, where A is the transmitter, B is the receiver, and C is the eavesdropper. When A sends information to B in the presence of C, and if C is within the coverage area then C can easily intercept the message sent by A to B. Thus, this can be avoided by using beam forming. Beam forming creates a beam only in the direction of B to maximize the SNR ratio and suppresses the transmission or reception in the direction of the C. One of the main features of beam forming techniques is spatial filtering. The spatial filtering helps in distinguishing the secure and insecure locations for the transmission of information. Beam forming helps in utilizing the wireless medium in order to provide better service with respect to error performance and bit rate at the PHY [7].

However, beam forming faces issues such as fraction of the power being spread through minor side lobes, even though signal is directed toward legitimate node and the transmitted power is concentrated in the beam of main lobe. It creates a loophole for an eavesdropper who is in the coverage area to decode the transmitted information. It is also observed that beam forming only concentrates on improving the quality of the main channel and it neglects the possibility of having favorable channel by eavesdropper. Further, beam forming is computationally expensive and difficult to implement [8].

2.4 Security Diversity Techniques

The diversity technique is usually employed to enhance the transmission reliability which in turn improves the wireless security and also to reduce the duration of fading, experienced at the receiver. The PLS can be improved by various diversity methods which includes MIMO, multiuser and cooperative diversity [9].

MIMO Diversity: In this technique, multiple antennas are used for transmitting and receiving the signal. When the information bearing signal is sent through the channel, it will be transmitted through more than one antenna and, while receiving, it will be received through multiple antennas. Basically, MIMO is considered as an effective method of overcoming wireless fading and thus increases the channel capacity. However, there is possibility that eavesdropper could also utilize the structure of MIMO to improve the capacity of wiretap channel.

Multiuser Diversity: This is obtained by the user scheduling it either at the transmitter or at the receiver. Basically, it uses OFDMA and TDMA. So at any point of time, transmitter will select the best user among different receivers based on the quality of their channel and throughput. Disadvantage of this method is that if the user is far away from the base station and experiences deep fading and worst propagation loss, then the user will not get a chance to access channel. Hence, user fairness needs to be maintained and should provide guarantee that each user will get opportunity to use the channel [10].

Co-operative Diversity: Cooperative diversity is one of the important beam forming techniques against eavesdropping. It is a multiple antenna technique which is employed to improve the legitimate channel capacities for a given set of bandwidth [9]. Cooperative network includes source (s), X relays (r), destination (D) and an eavesdropper (E). X relays (r) is used to help the message transmission between source and destination. The source first transmits the message to X relays that then relay (r) sends the received signal to the destination.

2.5 *Physical Layer Secret Key Generation*

Secret key is extracted by exploring the physical layer characteristics such as channel randomness, independent channel variation over space, channel reciprocity. The randomness is extracted either from amplitude or phase of wireless fading. Key is generated by alternatively sending probe signal and estimating the channel state information (CSIs). Intended nodes can convert their CSI into the same bit strings. The bit discrepancies are corrected using privacy amplification techniques and key reconciliation [11]. Basically, two methods are used to generate key streams, one way is by using received signal strength (RSS) where power of received signal is used and in the other scheme phase of the received signal is used to extract the common randomness. Even though this can provide an alternative approach to the conventional key generation algorithms there are certain limitations which requires an attention. RSS provides a low-key bit generation rate and it faces scalability issues however signal phase based scheme gives good performance the implementation is difficult since it requires analog-to-digital converter which increases hardware complexity [11].

Even after researchers have proposed significant number of mathematical models, algorithms, and solutions, PLS faces challenges in its implementation. Most of the problems which are faced by PLS completely depend on the channel. PLS, cannot guarantee security if the channel capacity of eavesdropper is better than legitimate channel or unavailable eavesdropper's CSI. Increased power requirement in PLS due to the use of MIMO and relay systems [12] is another issue. In addition to this, all the existing work related to PLS is only concentrated on improving the security against eavesdropping attack by completely neglecting the various wireless PHY attacks. Hence, it is important to search alternative techniques to improve security at the PHY.

3 **Physical Layer Encryption**

PLE is yet another method of providing security at the PHY. Unlike PLS, PLE rely on computational complexity and uses distribution of secret key. PLE has no strict requirement on the channel conditions and the number of antennas. Compared to upper layer security schemes PLE resists the influence of noise and the effect of the channel in order to give reliability along with security. PLE provides security at the signal level and makes use of channel error to enhance the secrecy level. PLE schemes are more modulation intended; uses joint design of encryption and modulation, and it varies along with wireless technology. Based on processing of plain text PLE can be categorized into two types: Stream and Block PLE.

Stream PLE: It uses an encryption unit which encrypts binary message sequence using pseudo-random cipher key streams. Key streams are generated by using pseudo-random complex sequence generation function. The encrypted symbol is a

function of message binary sequence and complex sequence. And the complex sequence is calculated based on the initial key. In stream PLE, each plain text symbol is encrypted with the corresponding key symbol. Receiver jointly performs decryption and demodulation to get plaint text back. Security in stream PLE depends on encryption function and the complex sequence. This scheme provides low-propagation error and latency. Disadvantage is low diffusion and lacks symbol overlap. Hence, stream PLE is mostly used in simple and high-speed applications.

Block PLE: This scheme encrypts a fixed size plaintext symbols as one block. Block PLE uses mapping functions which maps fixed block of an input sequence to complex vector based on corresponding key. Different types of mapping functions can used to design PLE and they can be random. In block, PLE encrypted output depends on block of binary sequence, mapping function and a key. Designing a suitable mapping function plays key role. Advantages of block PLE are; it provides high diffusion and is immune to tampering, it suffers with error propagation and slow encryption process.

In recent years, many researchers had proposed PLE implementation techniques in various communication systems like OFDM, MIMO and 802.15.4 so on. In this subsection, we try to present PLE schemes used in different wireless standards. As 5G is in focus, MIMO technology is evolving significantly and there is a need for security. New PLE method is proposed to improve the security in MIMO with spatial modulation [13]. Adding spatial modulation to MIMO provides high energy and spectral efficiency. This paper presents a chaotic-antenna-index-3D modulation and rotated constellation points PLE which effectively makes use of spatial modulation as well as chaotic theory. Key generation algorithm is designed based on chaotic theory. Security can be achieved by protecting the spatial constellation diagram, for this the chaotic sequence generated antenna index is used. The simulation results clearly show that even with infinite MIMO system, eavesdropper cannot recover plaintext. In [14], PLE implemented at the PHY using OFDM is discussed. The encryption method reserves a part of OFDM subcarriers which transmits dummy data used to hide information at subcarrier level and provides randomness. This makes information about subcarriers unclear. Obfuscation of subcarrier makes the transmission secure. Along with obfuscation it also uses re-sequencing of training symbols. The reserved subcarriers used for re-sequencing provides protection to entire packet in physical layer without affecting synchronization and channel estimation between intended user meanwhile it prevents the eavesdropper from doing all these operations. This scheme is implemented on 802.11 OFDM and compared the results with key rate, complexity and search space. Calculated results show that entire data search space is $(48!)^{38}$ and a search space for entire packet is 2.47×10^{173} with this eavesdropper will take 3.74×10^{121} years to break. Key streams are generated using stream ciphers. Key rate can be adjusted by varying 's' OFDM symbol and 'k' reserved subcarrier. With increase in s and k value increases the search space which in turn improves security.

Further Li et al. [15] presented both stream and block PLE for 802.11 OFDM in their work. Two PLE framework designs are developed which can provide security

against known plaintext and chosen-plaintext attacks (CPA). In design framework, reliability and security are considered together. Stream PLE unit have of two parts; pseudo-random complex number generator (PRCNG) which is used to generate pseudo-random complex binary sequences (PRCBS). Both the legitimate user generates same PRCBS using a key. Next part is the design of encryption function, which performs mapping of plaintext symbols into constellation points (complex signal). The mapping is done according to PRCBS. Constellation distance and confusion are taken into account, while designing the mapping function. 3D constellation scheme maps 2 bit message to 3D constellation point and these points are distributed over spherical surface. After mapping, 3D rotation is used to disturb the constellation. This disturbance creates confusion which helps in improving the security. In block, PLE key generation algorithm produces three sub keys K1, K2, K3 which are used at three different stages. Three stages of PLE are bit change stage, modulation stage and block change stage. Bit change disturbs and creates confusion among the binary sequence using first sub key K1. Modulation uses K2 to map confused sequence to complex vector. Block change stage is a function used to make symbols confuse and interlace so that it will be difficult for eavesdropper to get plaintext. At this stage, K3 maps 2 complex vector spaces. Table 2 shows the comparison between different PLE methods used for 802.11 OFDM. Search and key space, CPA security, throughput, BER performance and design complexity are considered for performance analysis. All three PLE schemes give similar results when it comes to bit penalty, key and search space. The subcarriers obfuscate scheme uses a part of transmission power to send dummy bits so its throughput decreases. And since it uses two stream ciphers CPA security relies on stream cipher which it uses. Block PLE and stream PLE provide better throughput performance however CPA security in stream PLE depends on PRCNG which is used to produce PRCBS using keys. All three are linearly complex and these PLE can be software or hardware implemented.

Huo et al. [16] presented a new generalized phase encryption scheme which can be applied to any of the wireless communication standard independent of modulation scheme. XOR encryption uses bitwise XOR between data bits and the corresponding key bit to give encrypted output. Unlike XOR encryption, phase encryption is performed on modulated sequences. Basically, phase encryption

Table 2 Comparison between different PLE methods

Type	Bit penalty	Throughput decrease	Search space	Key space	CPA security	Complexity
Subcarrier obfuscate [15]	NO	Depends on reserved subcarrier	High	High	Relies on stream cipher	Linear
Block PLE [16]	NO	NO	High	High	Good	Linear
Block PLE [16]	NO	NO	High	High	Relies on PRCNG	Linear

neither depends on system or on specific modulation scheme. Security functions provided at upper layers makes added data and the headers of succeeding layers unprotected and it is vulnerable to traffic analysis attacks. Authors proposed PHY structure using phase encryption. Here, two bits are used to encrypt one modulated symbol. First bit represents real part and another bit is used for imaginary part. Modulated symbol consists of $\log_2 M$ bit information where M is the size of constellation. It shows phase encryption is not one to one mapping of plaintext and secret key. N bit symbols are encrypted by a key stream of 2-bits. Further, 1 bit key stream is enough to encrypt modulated symbol in case if it consists of only real component. Once phase encryption is done the modulated discrete symbols and encrypted sequence are given to digital to analog converter. Obtained analog part is up converted into carrier frequency later it is transmitted over a channel. In phase encryption, the cipher text is a complex number and relation between plaintext and cipher text depends on channel coding, source coding and type of modulation is used. Since the encryption is done at physical layer just before the transmission can prevent the traffic analysis attack. Comparison results of both XOR and phase encryption are given in Table 3. From the result, it is shown that phase encryption gives higher encryption efficiency and can be used as a substitution for XOR encryption.

Generalized phase encryption is extended to design the PHY of 802.15.4. [17]. Since PLE is modulation specific considerable attention is required for each wireless standard. Even though different PLE methods are already available, most of them are for OFDM systems [14, 15]. And some schemes are implemented by rotating the constellation points [13]. Paper [16] presented the phase encryption to mitigate traffic analysis. All the above-mentioned methods are concentrated in providing security to 802.11 OFDM systems. But all these schemes are not suitable when it comes to the security of IEEE 802.15.4 because of different operating conditions of its devices. In general, security services like confidentiality, integrity of 802.15.4 is provided via MAC. These security primitives increase the computational energy which cannot be neglected [18]. Hence in [17] authors proposed an efficient phase encryption scheme for PHY of 802.15.4 and analyzed it against energy depletion and traffic analysis attack. During an encryption, phase of the modulated symbol changes with respect to key. The size of key is depends on the underlying modulation method. Each one of the modulated symbols consists of 2

Table 3 Comparison between XOR and phase encryption

Type	Encryption	Encryption efficiency	Cipher text	Mapping
XOR encrypted	Before modulation	Low	Bit level	Bit to bit
Phase encrypted	After modulation	High	Complex number	2 bits used to encrypt 1 modulated symbol

message bits and it is the form (I, Q). Values of I and Q are from the set of {1, -1}. Hence I and Q of key stream also take its values from the set of {1, -1} .cipher text is produced by multiplying the corresponding components of the modulated symbol and key streams.

4 IEEE 802.15.4 Security Suits

In recent years, 802.15.4 standard is becomes popular and an association with an IoT makes its applications even broader.802.15.4 protocol defines low-power, low-complexity and low-data rate communication in WPAN. An 802.15.4 appli- cation includes smart cities, home and industrial automation, health monitoring and military surveillance so on. All these applications need secure transmission of information. Particularly, when it comes to a health and military applications, security is the utmost concern. Hence, it is very important to study the security aspects of IEEE 802.15.4. This section presents the IEEE 802.15.4 security spec- ification. Security requirements of 802.15.4 are frame integrity, confidentiality and access control. Integrity resists the modification of frames; Confidentiality guar- antees that only intended nodes can transmit the secret message. Access control protects the frames against unauthorized users. Sastry et al. [19] extensively dis- cussed about security provisions. In 802.15.4 link-layer security provides confi- dentially, integrity and access control. The 802.15.4 uses two types of packets; data packet which uses a flag to indicate type of packet, security enable and addressing modes. At last 2 bytes of CRC are used for error correction. Acknowledgment packet is used to send acknowledgment by the recipients. In 802.15.4, MAC layer controls the security. In case of security requirement, the application has to explicitly specify that using different control parameters. Application can choose different security schemes which control the security for transmission of message. Security suits of 802.15.4. Specification can be broadly categorized into two types: secure and unsecure mode. Table 4 gives information of security suits supported by 802.15.4. Each scheme offers different aspects of security. Null suit is unsecure where it defines no security. AES-CTR only performs encryption and gives con- fidentiality. AES-CBC-MAC provides data integrity which comes with 3 variations

Table 4 Comparisons between various IEEE 802.15.4 security suits

Security suit	Description
Null	Unsecure
AES-CTR	Only encryption
AES-CBC-MAC-128,64,32	Authentication only. Flexible with different MAC sizes: 128,64, 32 bits
AES-CCM-128,64,32	Authentication and encryption flexible with different MAC sizes: 128, 64, 32 bits

based on size of the MAC bit. Size can be 32, 64 or 128 bits. Each one is considered as separate security suit. Higher the size of MAC bits lower the risk of adversary, but it increases the size of packets. Whereas AES-CCM first provides integrity using CBC-MAC later it encrypts the data by using AES-CTR.

However, the above-mentioned security suits faces serious problems. Implementation of AES-CTR is unsafe because, encryption without authentication introduces significant risk of vulnerability at protocol level. Also it is shown that AES-CTR is more prone to denial of service attacks. Further, none of these security suits gives data integrity to acknowledgment packets. With jamming, this loophole can be used to stop the delivery of packets. This makes acknowledgments untrustworthy. A new method of security enhancement in 802.15.4 Zigbee is proposed [20]. This is done by altering the MAC. This paper also presents security enhancement in application and network layer, and it is implemented by using RFID detector and application gateway. In Zigbee, security is maintained by external service provider interface, which work on every layer. In order to enhance the security, MAC addressing, authentication, security unit is added at MAC layer. RFID detector is integrated at network layer, and APL security is included at application layer. Riverbed modeler is used to implement the zigbee protocol and simulation results shows with the proposed work MAC can block unauthorized devices and performs authentication, network layer blocks illegal packet and application layer block adversary data. Since performance and security compete for same CPU, memory, energy and bandwidth, it is very much necessary to analyze the resource consumption, while giving security. Hence, further we study the impact of security on memory, energy consumption and network performance [21]. To test security, authors used 2Tmotesky motes with 48 kbyte ROM and MSP430 microcontroller operates at 8 MHz with RAM of 10 kbytes. In order to analyze the network performance, full function device (FFD) and reduced function device (RFD) are consider. FFD acts as PAN coordinator which manages network and security. RFD acts as a sender and continuously transmits protected data to the PAN coordinator using a common secret key shared between RFD and FFD. After receiving data packets, PAN coordinator verify data frame and sends back ACK. Memory consumption is compared with and without security sub layer. Obtained results shows that without security FFD function takes 33.2 Kbytes that is (69% of total memory) and the same FFD with security consumes 39.31 Kbytes (81.9%) overall there is around 13% increase.

Similarly for RFD takes 34.43 Kbytes (71.7%) without and 39.85 Kbytes (81.1%) with security, 9.4% increase. By adding security layer the size and complexity of PAN coordinator increases. Table 5 shows how different security suits affect the transmission of frames. When compared to null security suit, 26.2% reduction in frames when only encryption (AES-CTR) is provided. With only authentication (CBC-MAC) 28 to 33.5% of frames are reduced (varies with size of MAC bits) and adding both encryption and authentication (AES-CCM) reduces 28.2 to 33.9% of frames. Size of each frame increase with different security suits as it adds overhead. Cost of energy consumption when implemented security suits is shown in Table 6. Overall energy consumption is split into energy for secure one

Table 5 Security impact on frame transmission

Security suit	Frames	Decrease in frame (%)	Frame size (bytes)
Null	7685.5	–	27
AES-CTR	5671.6	26.2	37
AES-CBC-MAC-4,8,16	5534.8, 5371.6, 5110.3	28, 30.1, 33.5	41, 45, 53
AES-CCM-4,8,16	5514.6, 5374.4, 5082.1	28.2, 30.1, 33.9	41, 45, 53

Table 6 Energy consumption

E (μJ)	V (v)	I	t (ms)	Device
$E1 = 240.54$	3.6	17.4 mA	3.84	CC2420
$E2 = 150.34$	3.6	17.4 mA	2.40	CC2420
$E3 = 2.66$	3	600 μA	1.48	MSP430

frame transmission (E1), energy for encryption and authentication (E2) and energy for security management (E3). As 802.15.4 protocol gaining importance for its low-power, low-complexity nature, and all these parameters discussed above plays an importance role hence one has to look in this direction in the design of efficient and secure 802.15.4 protocol.

After analyzing related work it is clear that there is less research work done toward the implementation of efficient and secure 802.15.4 protocol. As for as IoT applications are concerned the existing security suits using AES is unsuitable. Hence, it is important to search for alternative security methods which meet the low power and low-complexity requirements.

5 Hardware Implementation of IEEE 802.15.4

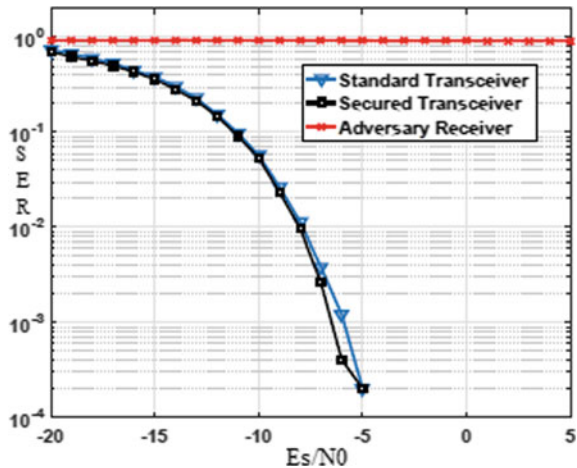
IEEE 802.15.4 defines PHY and MAC layer specifications. PHY is designed to transmit data packets. Physical layer operates at 868/915 MHz and 2.4 GHz. Further revisions in 802.15.4 allow the use different modulation schemes including BPSK, QPSK, O-QPSK, GFSK and UWB. In 802.15.4 data link consists of two parts; link control and MAC. Link control is standard used in all 802 protocols logic. MAC layer is designed to perform various operations like channel access, frame delivery, synchronization; flow control and error control etc. In this sub-section, various hardware implementation techniques of IEEE 802.15.4 are discussed. A small subset of 802.15.4 MAC protocol is designed to provide a point to point communication [22]. Author implemented 2.4 GHz protocol design. Mapping of bit to symbol is done by mapping 4 bit of LSB to first symbol and 4 bit of MSB to next symbol. Later each and every symbol are mapped to 32-chip sequence.

Mapped chip sequences now modulated by using O-QPSK. Modulated signals are then added with 16-bit cosine and sine values. Summed signal is finally transmitted. At the receiver sine and cosine are subtracted. Demodulation is later performed to get original signal. Verilog code is used to design the proposed protocol. Virtex-4 pro FPGA is used for hardware implementation which has a clock speed of 100 MHz. Since the design has to work only at 250 kHz; this hardware is not suitable for optimal zigbee transceiver design. However, clock divider circuit can be used, but it will add additional hardware. 2.4 GHz zigbee receiver is implemented using sparton-3E XC3S500E FPGA kit, which supports clock frequency of 250 kHz and 2000 kHz [23]. The receiver consists of O-QPSK demodulator, chip-synchronization and de-spreading block which are designed using Verilog. Further to optimize, the design all the blocks are integrated into single Verilog module. The proposed system gives data rate up to 250 kbps. In [24], MQAM modulation scheme is used to design 802.15.4 transceiver which operates at 2400 MHz. Proposed system consists of FIR filter, serial in parallel out and parallel in serial out shift registers, up and down samplers and a chip generator block. Verilog is used as a designing language and it is implemented over sparton-3 XC3S200E FPGA. Model-sim is used to simulate the waveforms of transceiver. The clock speed used is 1000 kHz and 8 MHz, even though 802.15.4 standard is designed for very low-power applications, designing energy aware transceiver is very much needed. Elmiligi et al. [25] implemented energy scalable 802.15.4 transceiver using a BPSK modulation which uses 868 MHz frequency band. VHDL is used to design zigbee transceiver and AMIRIX AP1000 for implementation. Recently, a design of fully integrated 802.15.4 zigbee transceiver is implemented on ARTIX-7 using Verilog [26]. Table 7 gives the comparison results of the implementation techniques discussed above.

All the research work discussed above only concentrated on the efficient hardware implementation of 802.15.4 transceiver design and they failed to implement security services to 802.15.4 transceiver along with performance. Nain et al. [17]

Table 7 Comparison between different implementation techniques

References	[23]	[24]	[25]	[26]
Design approach	Verilog	Verilog	VHDL	Verilog
FPGA family	Sparton-3E XC3S500E	Sparton-3 XC3S200E	AMIRIX AP1000	Atrix-7
Modulation scheme	O-QPSK	MQAM	BPSK	O-QPSK
Operating frequency	2.4 GHz	2.4 GHz	868 MHz	2.4 GHz
Clock frequency	250 kHz and 2 MHz	1 MHz and 8 MHz	105.502 MHz	270.1 MHz
LUTs	3,228	2526	284	428
FFs	2993	60	227	179
Slice registers	–	320	229	224

Fig. 2 Comparison of SER

designed and implemented a secure IEEE 802.15.4 transceiver which provides a protection against multiple attacks. Along with the confidentiality and message integrity, proposed scheme provide security to brute-force, cryptanalysis and traffic analysis attacks. Proposed secure transceiver uses a stream PLE scheme using phase encryption which provides a security at physical layer during the modulation. The PHY preamble here uses 8 symbols/256 chips which will be converted to 128 complex samples when it is modulated. Since QPSK is used, one of the 4 phases is used to rotate each sample according to key. This gives 4^{128} possible set of key for 1 preamble. This proposed system resists brute-force attack. Secure 802.15.4 transceiver is designed in Xilinx environment using Verilog. After simulation, results are analyzed in terms of security. Figure 2 gives the comparison of symbol error rate (SER) between standard and proposed 802.15.4 transceiver in noisy environment. The result shows that there is no degradation in SER performance at legitimate node and a very high SER degradation at adversary which increases the difficulty for an attacker to get the plain text.

Proposed system is implemented on Kintex-7 FPGA and ASIC UMC. Synthesis results show that proposed secure PLE based 802.15.4 transceiver uses 132,046 gates compared to the gate count of 104,477 in standard design. 26% increase in the gate count is observed and the implementation on FPGA uses 6507 slices and 15,954 LUTs. However, this resource overhead is because of RC4 cipher.

6 Conclusion

With the growing demand for the IoT applications, IEEE 802.15.4 protocol is gaining much attention in recent times. In this paper, we presented the importance of 802.15.4 PHY and discussed how security can be achieved by exploiting the

characteristics of physical layer. PLS and PLE schemes are studied extensively and distinguished between them. Different PLS schemes are reviewed with their limitations. Next, the concept of PLE is introduced and discussed about stream and block PLEs. Further various PLE implementation techniques are analyzed and compared. However, most of the research works on PLE have been done on 802.11 OFDM. Later, we looked into existing security suits of IEEE 802.15.4 standard and discussed the loopholes in AES based encryption schemes as they failed to provide data integrity to acknowledgment packets. Since performance and security compete for same resources, impact of security on memory, energy and network are analyzed. It is observed that the existing designs consume more memory space and energy. Finally, we reviewed various FPGA implementation of 802.15.4 transceiver design and most of them are only concentrated on performance and the security aspect is completely neglected. After detailed survey, it is observed that a very less research work is done toward the design of hardware based secure and efficient IEEE 802.15.4 transceiver. PLE has low-computational complexity, provides low latency with small power consumption and provides longer lifetime. Future scope of this paper proposes the integration of PLE scheme along with the efficient lightweight key generation algorithm for the design of 802.15.4 transceiver system which can greatly enhance the security and efficiency thereby providing the security to IoT applications.

References

1. ITU, ICT Facts and Figures, 2020. Available on-line at <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>
2. Stankovic, J.A.: Research directions for the internet of thing. *IEEE Internet Things J.* **1**, 3–9 (2014)
3. Zou, Y., Zhu, J., Wang, X., Hanzo, L.: A survey on wireless security: technical challenges, recent advances, and future trends. *Proc. IEEE* **104**, 1727–1765 (2016)
4. Wyner, A.D.: The wire-tap channel. *Bell Syst. Tech. J.* **54**, 1355–1387 (1975)
5. Sun, L., Du, Q.: A review of physical layer security techniques for internet of things: challenges and solutions. In: *Entropy* (2018)
6. Hyadi, A., Rezki, Z., Alouini, M.: An overview of physical layer security in wireless communication systems with CSIT uncertainty. *IEEE Access* **4**, 6121–6132 (2016)
7. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **7**, 2180–2189 (2008)
8. Sanenga, A., Mapunda, G.A., Jacob, T.M.L.: An overview of key technologies in physical layer security. In: *Entropy*, Multidisciplinary Digital Publishing Institute (2020)
9. Johansson, M.: Benefits of multiuser diversity with limited feedback. In: *4th IEEE Workshop on Signal Processing Advances in Wireless Communications—SPAWC*, Rome, Italy, pp. 155–159 (2003)
10. Zou, Y., Zhu, J., Wang, X., Leung, V.C.M.: Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw.* **29**, 42–48 (2015)
11. Ren, K., Su, H., Wang, Q.: Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wirel. Commun.* **18**, 6–12 (2011)
12. Trappe, W.: The challenges facing physical layer security. *IEEE Commun. Mag.* **53**, 16–20 (2015)

13. Wang, S., Li, W., Lei, J.: Physical-layer encryption in massive MIMO systems with spatial modulation. *China Commun.* 159–171 (2018)
14. Zhang, J., Marshall, A., Woods, R., Duong, T.Q.: Design of an OFDM physical layer encryption scheme. *IEEE Trans. Veh. Technol.* **66**, 2114–2127 (2017)
15. Li, W., McLernon, D., Lei, J., Ghogho, M., Zaidi, S.A.R., Hui, H.: Cryptographic primitives and design frameworks of physical layer encryption for wireless communications. *IEEE Access* **7**, 63660–63673 (2019)
16. Huo, F., Gong, G.: Physical layer phase encryption for combating the traffic analysis attack. In: *IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Raleigh, NC (2014)
17. Nain, A.K., Bandaru, J., Zubair, M.A., Pachamuthu, R.: A Secure phase-encrypted IEEE 802.15.4 transceiver design. *IEEE Trans. Comput.* **66**, 1421–1427 (2017)
18. Razvi Doomun, M., Sunjiv Soyjaudah, K.M., Bundhoo, D.: Energy consumption and computational analysis of rijndael-ES. In: *3rd IEEE/IFIP International Conference in Central Asia on Internet*, Tashkent, pp. 1–6 (2007)
19. Sastry, N., Wagner, D.: Security considerations for IEEE 802.15.4 networks. In: *Proceedings of the 3rd ACM Workshop on Wireless Security*, Association for Computing Machinery, New York (2004)
20. Biddut, M.J.H., Islam, N., Sultana, R.S., Sarker, A., Rahman, M.M.: A new approach of ZigBee MAC layer design based on security enhancement. In: *IEEE International Conference on Telecommunications and Photonics (ICTP)*, Dhaka, pp. 1–5 (2015)
21. Daidone, R., Dini, G., Tiloca, M.: On experimentally evaluating the impact of security on IEEE 802.15.4 networks. In: *International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, pp. 1–6 (2011)
22. Bhat, N.S.: Design and implementation of IEEE 802.15.4 mac protocol on FPGA. In: *Innovative Conference on Embedded Systems, Mobile Communication and Computing (ICEMC2)* (2011)
23. Ahmad, R., Sidek, O., Shukri, M.: Implementation of a Verilog-based digital receiver for 2.4 GHZ Zigbee applications on FPGA. *J. Eng. Sci. Technol.* **9**, 135–152 (2014)
24. Supare, V.P., Sayankar, B.B., Agrawal, P.: Design & implementation of MQAM based IEEE 802.15.4/ZigBee transceiver using HDL. In: *International Conference on Smart Technologies and Management for Computing, Energy and Materials (ICSTM)*, Chennai, pp. 455–458 (2015)
25. Elmiligi, H., El-Kharashi, M.W., Gebal, F.: Design and implementation of BPSK MODEM for IEEE 802.15.4/ZigBee devices. In: *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Vancouver, BC, pp. 1–5 (2016)
26. Guruprasad, S.P., Chandrasekar, B.: Design and implementation of 802.15.4 transceiver for wireless personal area networks (WPANs) on FPGA. *Int. J. Innovative Technol. Exploring Eng.* (2020)

An Enhanced Security Framework for Robotic Process Automation



K. Murugappan and T. Sree Kala

Abstract Robotic process automation (RPA) is an emerging field in any industry that takes care of automation of the monotonous jobs. This can help to optimize the resources utilization for the organization, save the cost, time and improve the accuracy and quality of the jobs performed. However, lack of security in the implementation and the management of these RPAs shall affect the business in an adverse way. In the current scenario, privacy has also taken important role, and allowing bots (RPA) to have an access to these privacy applications can lead to regulatory compliance issues and invite heavy penalty to the company, and at certain times, it may result in business shutdown. Hence, in this paper, we explored various security risks associated with the bots automation and provided a proposal to build a holistic security framework for the RPA environment.

Keywords Robotic process automation • Bots • Noncompliance • Regulatory • Policy compliance

1 Introduction

Robotic process automation (RPA) is a software program that imitates human actions when interacting with a computer systems application and accomplishing automation of repetitive, conditional-based processes. This shall be called as a software robot or a bot. These bots also can leverage artificial intelligence and machine learning technologies to improve the experience of organization workforce and customers. While doing so, the bots may have an access to the organization's critical applications and that can be misused by the unauthorized users. Also, mis-configuration and lack of management controls can result in security breaches, data leakage and financial impacts. To counter these potential risks, there is no single end-to-end comprehensive framework available in the IT industry. Since this RPA solution is being embraced by organizations around the world to carry out

K. Murugappan (✉) · T. Sree Kala
VISTAS, Chennai, India

crucial processes across multiple business functions, this paper would help in providing an insight to those security risks and provide a framework to safeguard the organization and its customer assets.

2 Problem Identification

When RPA is interacting with multiple applications (in-house or off-the-shelf), it increases the attack surface. Other problems are manual override of the bot set-up, unauthorized changes, software licence misuses where generic ID is used, weak credentials storage, security incident response is not aligned or designed to cope up with the bot's speed and volume of transaction, no accountability established for the bots used in the network, regulatory noncompliance, a corrupt bot can access sensitive data and move laterally in the network or destroy high value information, security breach can result to disclosure of sensitive information to external parties, a rogue robot can create security vulnerabilities for data at rest or in motion, and Service denials.

3 Proposed Solution

As per a 2018 report by Ernst and Young for RPA implementations, organizations should consider the technical, process and people elements of the entire robotics ecosystem. A secure implementation should be in accordance with the entire product lifecycle starting from requirements, architecture to the ongoing operations. This is well captured in the below sections.

3.1 *Security Framework—Key Pillars*

In Fig. 1, key pillars for building a security framework are provided. This shall be tailored as per the organization's requirement.

Governance: The organization should ensure a governance framework which will build strategy and security requirements from an RPA perspective. This shall explain the management support and its commitment to ensure the data security [1].

Risk Management: Any risks that shall obstruct the RPA objective of the business have to be mitigated based on the priority.

Product and Software Security: Organizations should perform a product architecture risk assessment both internally and externally.

Access Management: Role-based access control is one of the most crucial features to keep in mind while opting for an RPA solution [2]. A credential

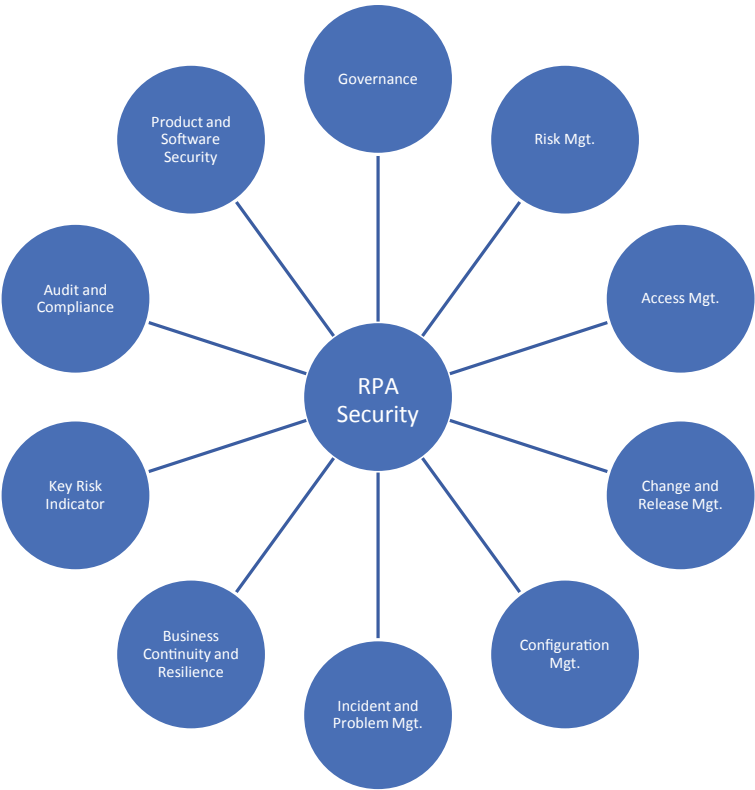


Fig. 1 Security framework

management process must be put in place for the bots to store credentials in a vault and access it as and when needed as per assigned privilege.

Change and Release Management: Any changes to the RPA systems and applications are authorized and implemented accordingly to avoid unauthorized or unnecessary downtime or security breaches.

Configuration Management: All deployed configurations are backed up and version controlled to ensure the timely recovery in case of any operational failure or application or hardware issues [3].

Incident and Problem Management: Focus on any operational and security incident to be addressed and avoid any repeated issues.

Business Continuity Planning (BCP) and Resilience: This will support the business resumption in case of a disaster.

Key Risk Indicators (KRI): This will support the RPA business to take a quick proactive action and avoid any significant impact to the business.

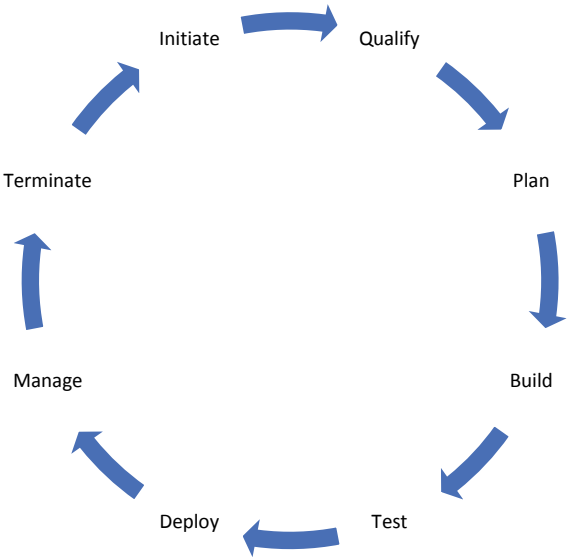
Audit and Compliance: The organization must conduct regular audits to ensure that the bots are compliant to all industry regulations in order to avoid hefty fines and a tarnished brand image.

3.2 *Process Flow*

Figure 2 provides the process flow of the bot establishment in a network that starts from *initiate* step [4]. In this step, the requestor, usually from the business, raises a request, and it is validated by the respective business subject matter expert (SME) for the business value added. Based on the positive outcome of this qualifying activity, the resource planning will kick start. Once the planning is done, the required resources (people, process, technology, location, schedule, cost and quality) will be determined and allocated to the project, and build phase will begin.

During this phase, the actual bot package will be developed, and then, it moves into testing phase. In this phase, test strategy and test cases are tested. If the test results are satisfied, final package would be deployed into the production. After deployment, this is managed for maintenance purposes and minor bug fix or enhancements. Finally, the bot can be terminated after the end of life or once the business objective is achieved.

Fig. 2 Process flow of the proposed work



4 Control Requirements in Each Phase

The control requirements in each phase are listed below. The audit and compliance are applicable for every phase.

Phase	Includes	Control requirement
Initiate	Request creation is restricted to authorized users/limited users only	• Limit the request creation based on job role
Qualify	Requirement is captured or understood clearly from the business	• Risk management • RPA vendor or platform selection • Business and security requirement sign-off
Plan	Proper planning for development estimate, detailed process breakdown, value stream map and estimated savings	• Policy adherence • Return on investment is calculated and accounted for every resource • Project/change request is created
Build	• Code/script development • Bot ID creation request • FTE redeployment • Communication and escalation • Package creation • Version control • Bot reuse • Best practices establishment	• Secure coding or vendor recommended security practices are followed
Test	• Unit test • System integration test (SIT) • Quality assessment test (QAT) • User acceptance test (UAT) • Business sign-off	• Every test case is tested • All significant and high rated errors are fixed • Positive and negative tests conducted • Functional and non-functional tests are performed
Deploy	• Infra requirements (virtual machine/ physical system) • Bot installation and configuration • Code deployment to production • License request and management • ID creation in authentication servers, applications and e-mail systems • Bot console management • Scheduling • SMOKE test • Saving confirmation • Handover to operation • Project closure	• Dedicated deployment team • Deployment team not to have an access to development and testing environment • Release ticket is created • Version control/configuration management
Manage	• User access management • Communication plan • Upgrades (operating system, applications and databases) • Change request (functional /technical)	• Unique account for every bot (attended and unattended) • Log monitoring • Bot task monitoring and traceability • Segregation of duties (SOD)

(continued)

(continued)

Phase	Includes	Control requirement
	• Hot fix • Patch management (OS, applications) • Issue management • Monitoring • Logs management • Backup and archival • Bot inventory and its mapped applications	• Privileged account management • No direct write access to the database • Strong passwords • Least privilege and need to know basis access management • Periodic vulnerability assessment • Penetration test performed at least once in a year or whenever significant change in the environment • Software and bot license management • Regulatory compliance • KRI is established and monitored • Periodic backup • Periodic restoration test • BCP/DR • Security incident and problem management
Terminate	Bot decommissioning	• Periodic bot reconciliation and review process established • Unnecessary or unwanted bots de-commissioned

5 Technical Security Requirements

Data Flow: End-to-end data flow is identified for the bot, and blueprint is created with upstream and downstream applications or interfaces [5].

Data Flow Security: In each stage of the bot, data flow security is ensured. This shall include and not be limited to access control and encryption for achieving confidentiality, hashing for achieving data integrity and backup and recovery control for achieving availability [6].

Encryption: Minimum encryption shall be AES 256 and can be used in data at rest, data in transit and processing stages. The hashing algorithm shall be MD5 or SSH latest version.

Audit Trail: Every activity of the bot is logged and tracked with timestamps [7].

Passwords: Strong passwords for the bots and secured with password/credential vault.

Single Sign-On: Centralized authentication is enabled, and no local authentication is recommended.

Alert Management: In case of security breach, an alert is triggered to the concerned stakeholders/security administrator.

Vulnerability Management: Periodic vulnerability scanning and Threat modelling exercises are established to identify technical vulnerabilities and process gaps.

Security Testing: Identify bot security vulnerabilities by performing static and dynamic testing.

Penetration Testing: If any of the bots is exposed to Internet, then penetration testing is mandatory.

Remote Control: All remote console accesses are to be safeguarded with two-factor authentication.

Security by Design: It is better to ensure the security in each stage of the bot development instead of trying to fix gaps at the later stages.

Accountability: Every bot needs to have unique ID and mapped to a business owner so that accountability is established.

Sensitive Data: Sensitive data are to be wiped out before reassigning the bot to any other business.

Regulatory and Policy Compliance: Every Bot needs to be in compliance with the organization policy, standards and regulatory requirements. For example, Sarbanes–Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

PKI Solution: Public key infrastructure shall be used to secure the bot communication process.

6 Comparative Analysis

In the current industry, there are many commercial RPA platforms available, every player has their own way of developing, implementing and managing the RPA, and this might lead to a platform dependent security and inconsistency in following the security measures when the organization wants to implement the RPA with multiple vendors. This paper provides the comprehensive and holistic approach in implementing the RPA security framework, and consistency shall be maintained across the organization even if multivendor environment exists.

7 Conclusion

The need for RPA is increasing and proliferating in every industry; however, implementing the RPA should not impact the existing systems and services in the adverse way. To strikeout the balance, we need to really consider security versus stability. In this paper, the key pillars, process flow and control requirements are discussed for each phase of the bot lifecycle, and these can help to establish the strong security framework for the organization when implementing the RPA solution.

References

1. Deborah, G.: Robotic Process Automation (RPA) Within Federal Identity Management (2019). <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-gps-robotic-process-automation.pdf>. Accessed, 1 March 2021
2. Gautam, R.: 4 Security Must-Haves for a Safe RPA Solution (2020). <https://www.automationanywhere.com/company/blog/product-insights/four-security-must-haves-for-a-safe-rpa-solution>. Accessed, 1 March 2021
3. CemDilmegani.: Technical Buyer's 11 Point RPA Checklist: In-Depth Guide (2021). <https://research.aimultiple.com/rpa-technology>. Accessed, 1 March 2021
4. UIPATH Best Practices for IT Compliant RPA Implementation (2021). <https://www.uipath.com/resources/automation-whitepapers/information-technology-compliant-rpa-implementation>. Accessed, 1 March 2021
5. Enríquez, J.G., Jiménez-Ramírez, A., Domínguez-Mayo, F.J., García-García, J.A.: Robotic process automation: a scientific and industrial systematic mapping study. *IEEE Access* **8**, 39113–39129 (2020). <https://doi.org/10.1109/ACCESS.2020.2974934>
6. Lewin, A.R.W., Edwards, P.P.: *Open-Source Robotics and Process Control Cookbook*, USA, pp. 222–225 (2005)
7. Sumit, S.: RPA Implementation: Key Considerations (2018). <https://www.pwc.in/assets/pdfs/publications/2018/rpa-implementation-key-considerations.pdf>. Accessed, 1 March 2021

Analysis of the Trust and Resilience of Consumer and Industrial Internet of Things (IoT) Systems in the Indian Context



Akaash R. Parthasarathy

Abstract The Internet of Things (IoT) connects every device possessing some element of computer technology or a digital interface. These devices constitute a global interconnected network that bridges the gap between the physical and virtual worlds. Today, there are two major applications for IoT—Consumer Internet of Things (CIoT), concerned with interactions between consumers and IoT devices, and industrial Internet of Things (IIoT), focussed on the utilisation of IoT for designing industrial systems. With the proliferation of IoT devices for myriad applications, it is becoming increasingly important to investigate and understand the factors essential to securing them against external threats. These factors directly influence the design, functionality and the standards and regulations for IoT devices. This paper defines the trust and resilience of IoT systems and provides unambiguous definitions for key factors (security, privacy, safety, recoverability, reliability and scalability) that directly influence the trust and resilience of IoT systems. Based on the results of a survey conducted amongst IoT consumers and experts, this paper ranks each of these factors in the order of their importance in determining the trust and resilience of CIoT and IIoT systems. These rankings are generated using the analytic hierarchy process (AHP) and a pairwise analysis of the collected data.

Keywords Internet of things • Trust and resilience • Security

1 Introduction

The International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) defines the Internet of Things (IoT) “as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” [1]. IoT broadly refers to the worldwide system of

A. R. Parthasarathy (✉)

The Shri Ram School—Aravali, Gurgaon, Haryana 122002, India

devices that are connected to the Internet and can communicate and exchange data with each other. Today, IoT connects every device that possesses some element of computer technology or a digital interface. These include devices such as Amazon Echoes, which function as smart speakers and assistants, and fitness bands, which track your activity and monitor your health. IoT is responsible for bridging the gap between the physical and virtual world and has been extensively employed in myriad applications ranging from home automation to facility management.

These applications depend on the collection of data through sensors, which can measure physical quantities in the surrounding environment. IoT devices, composed of a multitude of these sensors, are integrated with powerful IoT platforms capable of organizing and manipulating the collected data to perform specific tasks [2]. For example, using IoT technology, smart lights containing proximity sensors are able to turn on or off when they detect the presence or absence of people nearby. More often than not, IoT devices and platforms are enabled with artificial intelligence (AI) to effectively handle and detect patterns in the enormous amounts of incoming data, allowing for enhanced convenience [3]. Using AI, the same smart lights can learn your sleep and work patterns and automatically adjust the lighting to suit your needs.

Historically, consumer devices, home control systems and industrial machines have been offline and not connected to any network. These entities were inherently secure since they could only be compromised through physical access. At the turn of the century, however, there was a significant explosion in computing power and techniques for data analysis, enabling the shift of security and safety systems to virtual platforms [4]. This shift came with its associated risks, both in terms of data leakages and reductions in the integrity of these systems. The past decade saw the emergence of the concept of IoT, associated with an increase in the connectivity of physical devices with each other and with virtual systems. In fact, Gartner forecasts that over 25 billion connected devices will be in use around the world by 2021 [5]. This ever-rising number of IoT devices, which is expected to soon surpass the number of people on the planet, has brought into question their trust and resilience. The immense scale of implementation and the intricacy of the computer systems involved in developing IoT devices leave them vulnerable to malicious hackers and cyber attacks [6]. Each unsecured endpoint serves as a potential location for attacks that can cripple entire IoT systems.

In 2017, Ronen et al. [7] discovered a vulnerability in the Zigbee protocol for IoT devices, allowing them to develop a self-replicating Zigbee worm to exploit Philips Hue smart lamps. This worm could spread to other lamps based on their wireless connectivity and physical proximity. Their research had large implications since similar attacks could be carried out across entire cities, leading to city-wide blackouts. More recently, in February 2020, it was demonstrated that several Philips Hue smart lamps could be hacked with the assistance of drones.

It is evident that device interoperability, trusted communication and the secure sharing and management of data are key aspects that need to be addressed when

designing and analysing IoT systems. Thus, research into developing standards for and enhancing the resilience of IoT systems has gained considerable traction in recent years.

2 Consumer and Industrial Internet of Things

IoT can be categorically divided into consumer IoT (CIoT) and industrial IoT (IIoT). CIoT is the more widely known variant of IoT and broadly encompasses IoT devices used to meet consumer needs and increase consumer convenience. CIoT is mainly focussed on residential and consumer interactions with IoT devices such as smart home appliances and wearable technology. IIoT, on the other hand, is concerned with using IoT devices for industrial applications such as synchronisation of manufacturing equipment and operation of integrated supply chains. IIoT makes use of a combination of sensor-driven computing, data analytics and intelligent machines to promote the efficiency of industrial processes and increase enterprise productivity [8].

Since IIoT systems involve the transmission of vast amounts of confidential data, unauthorized access to this data has far-reaching impacts. Despite being less popular and prevalent, IIoT has made significant progress towards standardisation with the help of industrial consortiums dedicated to the advancement of machine-to-machine communication and the promotion of open standards for security and interoperability [4]. These standards have continuously been revisited and updated for several years.

CIoT devices are independently developed by smart device and application providers through the use of traditional interfaces, which emphasise usability and functionality over trust and resilience [9]. Mechanisms to ensure security, privacy and safety are often incorporated solely on the basis of present consumer needs without appropriate planning for subsequent integrations. These concerns arise due to the absence of well-documented standards for CIoT systems, and as a result of the fact that CIoT devices are marketed directly to consumers with limited knowledge of security protocols. For example, in September 2019, a couple's smart home was compromised by a hacker, who took control of their cameras, played disturbing music and manipulated the heat levels in their house by accessing the Google Nest thermostat. This is just one of the many attacks that have been carried out on CIoT systems.

With the widespread adoption of both CIoT and IIoT devices, it is becoming increasingly important to investigate the issues and challenges related to their trust and resilience. The impact of the various characteristics of trust and resilience on the buying and adoption decisions of consumers and industries is of great significance.

3 Literature Survey

Recently, much research has been conducted in order to identify the security and privacy risks associated with IoT devices. Atlam and Wills [10] analysed the security, privacy and safety requirements for IoT systems. They reviewed the challenges faced in IoT security and privacy and presented a case study revolving around the security threats affecting smart cities. Additionally, they provided details regarding the implementation of security and privacy by design and listed the types of cyber and physical attacks that can affect IoT systems. Papp et al. [11] wrote a primer on hacking the hardware and software of IoT systems, where they analysed the most commonly employed methods and scientific research on IoT hacking.

Prior research has focussed on the development of malware to test the resilience of IoT systems. A few of these attempts have been successful in depicting threats to IoT protocols on a global scale [7, 12]. In an attempt to enhance the recoverability of IoT systems, researchers have also proposed self-recoverable IoT architectures, which employ time synchronisation combined with a novel algorithm to achieve formerly unobtainable results [13].

Within the field of IoT, there has also been research into the specific security threats and concerns related to CIoT and IIoT, with individual analyses having been performed for both CIoT [14, 15] and IIoT [16] systems. In order to achieve significantly higher levels of security and privacy, researchers have explored the viability of applying blockchain to CIoT and IIoT security [17]. Additionally, Wurm et al. [9] analysed and contrasted the security features and concerns in CIoT and IIoT devices. Techniques for enhancing the reliability and scalability of CIoT and IIoT systems have also similarly been investigated.

Research has also been conducted into the standardisation of IoT systems. Reference [4] is a comprehensive document analysing and outlining regulations and standards related to the security framework of IIoT systems from both business and implementational viewpoints. Additionally, [4] defines crucial terms related to the trustworthiness of IIoT systems. Taking a major step in the right direction, the European Telecommunication Standards Institute released the first global standard for CIoT devices, which outlines baseline requirements for internet-connected consumer products, in early 2019. The most recent iteration of this standard was released in June 2020 [18].

3.1 *Research Gap and Contributions*

It is clear that substantial research has been conducted in the field of IoT. Whilst a majority of this research has focussed on individual factors such as security, privacy and safety that impact the functioning of IoT devices, these variables or characteristics have not been comprehensively analysed in terms of their cooperative

functioning. Additionally, these factors have usually been examined for IoT frameworks in general and have not been compared and contrasted across the CIoT and IIoT spaces.

This paper investigates the factors affecting the trust and resilience (see Sect. 3.2) of IoT systems. This paper initially identifies and provides definitions for key factors that influence the trust and resilience of IoT systems according to the current research in the field. Next, it assesses the importance of each of these factors in determining the trust and resilience of CIoT and IIoT systems (both separately and combined) based on the results of a survey conducted amongst IoT consumers and experts. The paper ranks the factors against each other based on a pairwise analysis of the collected data. Using the survey results, this paper makes recommendations to enhance the trust and resilience in both the CIoT and IIoT spaces, thereby providing logical steps to follow as the IoT market enlarges.

The remainder of this paper is organised as follows: Sect. 3.2 introduces the concept of trust and resilience and presents key definitions of certain factors that describe the trust and resilience of IoT systems. Section 4 describes the methodology of the study utilised to analyse the impact of each of these factors on the trust and resilience of both CIoT and IIoT systems. The results of the study are presented and analysed in Sect. 5. Conclusions are drawn in Sect. 6, and the future scope of the work is discussed in Sect. 7.

3.2 Trust and Resilience of IoT Systems

IoT systems, like all other information systems, have key features and elements that define their trust and resilience (T&R). T&R of IoT systems is particularly important due to our continuously increasing dependence on them. A system is said to be resilient to a fault if its core capabilities are unhindered in the presence of that fault. T&R of an IoT system can be defined by its capacity to “withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time” [19]. This encompasses resistance to both external attacks and internal failures, and adaptation to continual change in global policies and standards.

Whilst no system can be fully trustworthy and resilient, laws and standards assist in maintaining their T&R to a certain degree by creating a balance between functionality and compliance. Although creativity and innovation can lead to the development of novel products and services, improper maintenance and failure to adhere to standards can result in issues such as data and identity theft. It is imperative to establish thorough guidelines and standardisation techniques in order to streamline processes related to the collection and transmission of data, and enhance the interoperability of IoT devices.

However, developing effective regulations necessitates an understanding of the different facets of the subject you are dealing with. In this subsection, six key characteristics that comprise T&R of IoT systems—security, privacy, safety,

recoverability, reliability and scalability—have been defined based on the current research in IoT [4]. All further mentions of these characteristics will adhere to the definitions in this subsection.

Security. Collins Dictionary defines security as “all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it” [20]. A similar definition can be extended to IoT systems: Security in an IoT system refers to the countermeasures that can be put in place to prevent any individual or group from exploiting the system. Systems have vulnerabilities or security risks that may be exploited and thus, need to be kept secure and protected from unauthorised access. The security of a system is defined by the CIA triad: confidentiality, which deals with unauthorised disclosure of information, integrity, which deals with unauthorised modification or deletion of data, and availability, which deals with reliable access to systems and data by authorised personnel [4].

Privacy. For the purposes of this paper, Adam Moore’s [21] definition of privacy, wherein privacy is defined as an “access control right over oneself and to information about oneself”, has been adopted. Privacy is the right of an individual or a group to decide how information concerning them should be utilised. This includes control over who has access to this personal information and the methods involved in collecting, processing and storing the information [4]. In terms of IoT, privacy refers to preventing the unauthorised access of personal information of an individual or a group in an IoT system. Privacy is ensured if this data is handled by an entity and in a manner that said individual or group has lawfully agreed to. With the growing popularity of IoT and the spike in the amount of personal information being handled and analysed by IoT systems and devices, manufacturers and service providers are required to become increasingly sensitive to consumer privacy and data protection. As such, major steps are being taken towards redefining the current techniques for ensuring privacy and aligning them with global standards [22].

Safety. An IoT system is said to be safe when it can operate without putting people at risk beyond specified acceptable limits. An IoT system must operate without endangering the lives of or causing physical harm to its users [4]. Device malfunctions and transmission of incorrect data may affect health, cause bodily harm or even be life threatening. Safety of IoT systems encompasses the measures taken to prevent such occurrences.

Recoverability. The recoverability of an IoT system is its ability to be restored to a stable state once the failures acting on it cease [23]. Recoverability is closely related to fault tolerance which aims to ensure the attainment of system goals even in the presence of unfavourable conditions and errors [24]. They are focussed on providing certain service level guarantees despite the occurrence of faults. A system is said to be recoverable to a fault if “there exists a control law such that the post-fault system satisfies the design specifications” [24].

Reliability. Reliability is the ability of an IoT system to consistently perform as it is expected to. Reliability determines whether an IoT system is capable of performing its assigned tasks for an extended period of time [4]. Reliability is applicable not only to IoT devices and their data collection techniques but also to the

utilised communication frameworks. It is an essential factor in building trust in both commercial and industrial applications.

Scalability. As defined by Gupta et al. [25], scalability is “the ability of a device [or system] to adapt to changes in the environment and meet changing needs in the future”. In terms of IoT, scalability refers to the capability of IoT systems to “support an increasing number of connected devices, users, application features and analytics capabilities, without any degradation in the quality of service” [26]. In this increasingly virtual and hyper-connected world, ecosystems must possess the ability to scale and plan for unusual spikes in requests. It is important for IoT systems to adapt to changing volumes of work due to factors such as seasonal demands.

4 Methodology

In order to analyse the influence of each of the T&R factors on the T&R of CIoT and IIoT systems, an online survey was conducted amongst more than 90 consumers and industry and corporate experts from across the world (however, a majority of the survey respondents were from India) using the SurveySparrow platform. The survey explicitly defined each of the T&R factors in order to reduce any ambiguity resulting from the wording of the questions.

The survey was divided into two sections—one for CIoT systems (see Fig. 1) and one for IIoT systems. Both of the sections contained the same questions, but were specific to the respective system. For each pair of factors, survey respondents were asked which factor they believed is more important in determining the T&R of the relevant type of IoT system. These choices were to be made under the assumption that the remaining 4 factors were stable or perfectly implemented. Respondents were additionally asked to take into account the impact of the remaining 4 factors on the factors under consideration, whilst making their choices. Figure 2 details the instructions for answering the questions in the CIoT section of the survey (Fig. 3).

Trust and Resilience Factors in Consumer IoT (CIoT) Systems

CIoT is the more widely known category of IoT and involves the use of smart devices to increase convenience for consumers. Examples of CIoT devices include smart speakers and smart lights. This section will ask you questions about how the preceding six factors affect the trust and resilience of CIoT systems.

Fig. 1 Survey section on T&R factors in CIoT systems. *Source* SurveySparrow

Section Instructions

For each pair of factors displayed (eg. Security vs Privacy), please select the factor that you believe is more important in determining the trust and resilience of CIoT systems.

Choose one of these factors assuming that the other four factors are stable (eg. If the question is Security vs Privacy, assume that the system is perfectly safe, recoverable, reliable and scalable).

Consider the following example: although you may believe that security is more important than privacy, you may decide that privacy is more important than security when integrated with safety, recoverability, reliability and scalability.

The last question in this section asks you to rank all six factors in the order of their importance.

Fig. 2 Section instructions for survey section on T&R factors in CIoT systems. *Source* SurveySparrow

Security vs Privacy

Which factor do you believe is more important in determining the trust and resilience of CIoT systems?

Security

A

Privacy

B

Fig. 3 A sample question from the CIoT section of the survey. *Source* SurveySparrow

The collected data was examined using the SpiceLogic AHP Software v2.2 [27]. The technique used to analyse the data was the analytic hierarchy process (AHP) for multi-criteria decision making (MCDM). Initially, as shown in Fig. 4, the objectives for the AHP were added, with the aim to maximise each T&R factor in the IoT system. Then, a pairwise analysis was conducted on the data, taking into each account each possible pair of factors. The percentages of survey respondents who chose each factor in the survey were inputted as weights in order to calculate the priority trade-off for each pair.

This procedure was followed for the responses for both CIoT systems and IIoT systems. Additionally, a pairwise analysis was performed on the combined data for both types of systems.

Objective	Attribute Type	Range	Relative Priority
1. Maximize Security	Subjective	0 to 100	24.77%
2. Maximize Privacy	Subjective	0 to 100	19.51%
3. Maximize Safety	Subjective	0 to 100	24.46%
4. Maximize Recoverability	Subjective	0 to 100	9.26%
5. Maximize Reliability	Subjective	0 to 100	17.84%
6. Maximize Scalability	Subjective	0 to 100	4.15%

Fig. 4 Maximisation objectives and their relative priorities. *Source* SpiceLogic Analytic Hierarchy Process Software v2.2

5 Results

The pairwise analysis conducted on the survey responses yielded a chart of the relative priority numbers of percentages of each of the T&R factors. These percentages indicate the importance of each of the T&R factors to the respective IoT system when stacked against each other. Based on the results from the AHP software, bar charts were created using Excel for the relative priorities of the T&R factors for CIoT systems, IIoT systems and the two when considered as a whole (Fig. 5).

As depicted in Fig. 6, security assumed the highest priority for CIoT systems with a relative priority number of nearly 25%, followed closely by safety. The subsequent levels of importance were occupied by privacy and reliability, respectively, whilst recoverability and scalability were considered to be the least important T&R factors by a margin of almost 9%.

As shown in Fig. 7, security was similarly assigned the highest relative priority number for IIoT systems. The generated relative priority number for safety was



Fig. 5 Priority trade-off for maximisation of security and maximisation of privacy. *Source* SpiceLogic Analytic Hierarchy Process Software v2.2

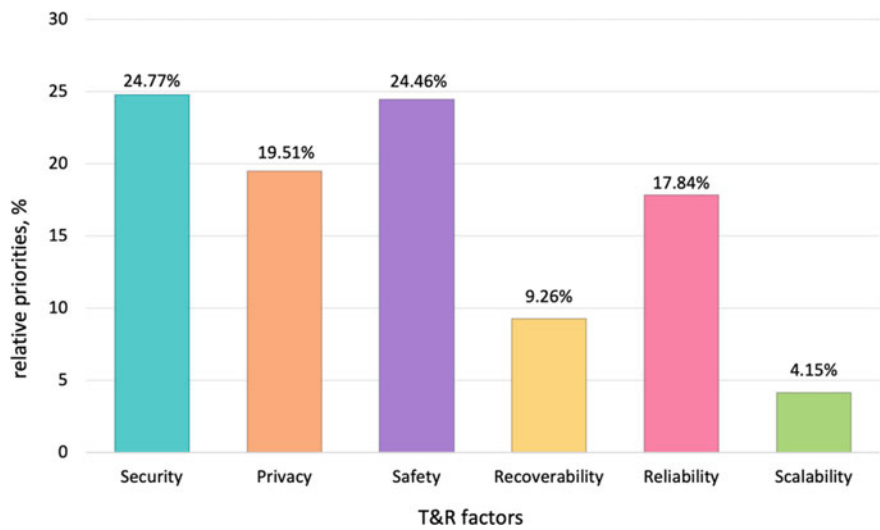


Fig. 6 Relative priorities of T&R factors for CIoT systems

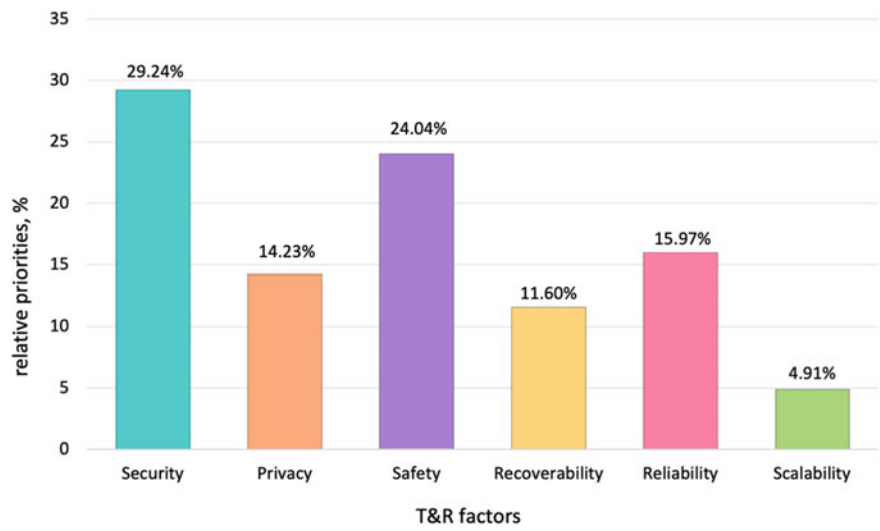


Fig. 7 Relative priorities of T&R factors for IIoT systems

similar to that in CIoT systems. Recoverability and scalability were again deemed to be the least influential in terms of the T&R of IIoT systems.

Comparing the two charts in Figs. 6 and 7, it is apparent that although security and safety occupied the highest two ranks for both types of systems, survey respondents considered security more important in determining the T&R of IIoT

systems as opposed to CIIoT systems. This is reasonable given the fact that IIoT involves access to greater amounts of confidential data and the coordination of many more physically adjacent systems. These systems must additionally be accessible to authorised staff at all times, failing which severe consequences such as the shutting down of entire factories could be observed.

Privacy and reliability were found to be less important to IIoT systems than to CIIoT systems. One reason for this could be concern surrounding personal data in view of relatively recent data leaks such as the Facebook-Cambridge Analytica data scandal. Further, although privacy was considered more important than reliability for CIIoT systems, reliability was considered more important in relation to IIoT systems.

Recoverability was more important to IIoT systems, indicating the need for the development of more fault-tolerant IIoT systems, whilst scalability remained the least important T&R factor with no major changes in its relative priority number across IoT systems.

On performing a combined pairwise analysis (see Fig. 8) of T&R factors for both CIIoT systems and IIoT systems, a similar trend was observed. An important detail to note is that security was indisputably assessed to be the most important T&R factor across IoT systems. Further, despite the aforementioned reflection regarding reliability and privacy, overall, reliability fared marginally better than privacy.

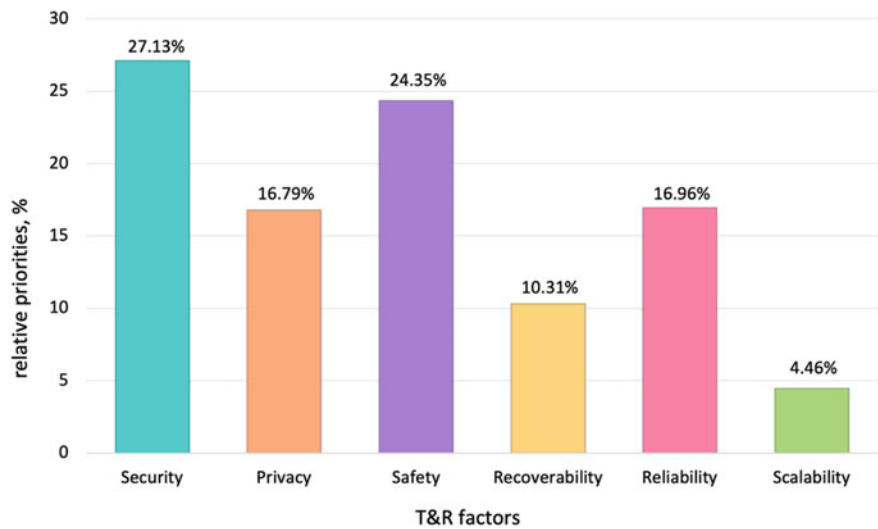


Fig. 8 Relative priorities of T&R factors for combined analysis (both CIIoT and IIoT systems)

6 Conclusion

With the recent surge in IoT, many concerns have been raised as to its long-term feasibility. It is becoming increasingly necessary to address the issues surrounding the security and privacy of IoT, amongst other factors. This paper collectively laid down concise definitions for six key terms (security, privacy, safety, recoverability, reliability and scalability) influencing the T&R of IoT systems with the aim of analysing these factors with respect to the CIoT and IIoT spaces. Specifically, it utilised pairwise comparisons as part of the Analytic Hierarchy process to rank the factors according to their importance in determining the T&R of IoT devices. It compared and analysed results, obtained from a survey conducted amongst IoT experts, between CIoT and IIoT systems. It established that security is the most important factor influencing the T&R of IoT systems and, in the future, special emphasis must be placed on enhancing the security features of IoT systems in order to defend against the onset of ever-increasing cyber attacks.

7 Future Scope

Although this study was limited to a small sample and the results may not be representative of the general consensus regarding the T&R of CIoT and IIoT systems, going forward the study could be extended to a larger sample to validate its findings.

The results of this study could be used to perform case studies comparing the T&R of different IoT products. The AHP software generated a multi-criteria utility function based on the relative weights of the T&R factors using a weighted sum model. For example, the combined utility function (U) for CIoT and IIoT was given by:

$$\begin{aligned}
 U = & 0.27 * [\text{Security}] + 0.17 * [\text{Privacy}] + 0.24 * [\text{Safety}] \\
 & + 0.10 * [\text{Recoverability}] + 0.17 * [\text{Reliability}] \\
 & + 0.04 * [\text{Scalability}]
 \end{aligned} \tag{1}$$

This function could be used to compare multiple IoT product alternatives and generate rankings for them.

Additionally, whilst the AHP operated under the assumption that each of the T&R factors were independent, a method such as the analytic network process (ANP) could be later used to consider the interdependence between the factors, whilst developing IoT systems.

Acknowledgements I would like to thank Dr. Dinesh Likhi, adjunct professor at the Indian Institute of Technology, Roorkee, for guiding me throughout this research, Dr. Akanksha Upadhyaya, Associate Professor, Rukmini Devi Institute of Advanced Studies, New Delhi for her review and comments on the paper, and Dr. Kavita Khanna, Associate Professor and the Head of the Department of Computer Science and Engineering, The NorthCap University, Gurgaon for guiding me and giving me the opportunity to present my paper at the ICCSDF 2021 conference at The NorthCap University. I would also like to thank my parents for their constant guidance and support.

References

1. International Telecommunication Union.: ITU-T Y.4000/Y.2060 “ITU-T recommendations”. <http://handle.itu.int/11.1002/1000/11559>. Last accessed 20 Jan 2021
2. IBM.: What is the Internet of Things (IoT)? <https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/>. Last accessed 26 Jan 2021
3. Norton.: What is the Internet of Things? How the IoT Works, and More. <https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html>. Last accessed 26 Jan 2021
4. Industrial Internet Consortium.: IIC:PUB:G4:V1.0:PB:20160919 “Industrial Internet of Things Volume G4: Security Framework”. https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf. Last accessed 24 Jan 2021
5. Gartner.: Gartner Identifies Top 10 Strategic IoT Technologies and Trends. <https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends>. Last accessed 20 Jan 2021
6. Ngo, Q.-D., Nguyen, H.-T., Le, V.-H., Nguyen, D.-H.: A survey of IoT malware and detection methods based on static features. *ICT Express* (2020). <https://doi.org/10.1016/j.icte.2020.04.005>
7. Ronen, E., Shamir, A., Weingarten, A.-O., OFlynn, C.: IoT goes nuclear: creating a ZigBee chain reaction. In: *IEEE Symposium on Security and Privacy (SP)*, pp. 195–212. IEEE (2017). <https://doi.org/10.1109/sp.2017.14>
8. Panchal, A.C., Khadse, V.M., Mahalle, P.N.: Security issues in IIoT: a comprehensive survey of attacks on IIoT and its countermeasures. In: *IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 124–130. IEEE (2018). <https://doi.org/10.1109/gcwc.2018.8668630>
9. Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., Jin, Y.: Security analysis on consumer and industrial IoT devices. In: *21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 519–524. IEEE (2016). <https://doi.org/10.1109/aspdac.2016.7428064>
10. Atlam, H.F., Wills, G.B.: IoT security, privacy, safety and ethics. In: *Digital Twin Technologies and Smart Cities*, pp. 123–149. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-18732-3_8
11. Papp, D., Tamás, K., Buttyán, L.: IoT hacking—a primer. *Infocommun. J.* **11**(2), 2–13 (2019). <https://doi.org/10.36244/ICJ.2019.2.1>
12. Vaccari, I., Cambiaso, E., Aiello, M.: Remotely exploiting AT command attacks on ZigBee networks. *Secur. Commun. Netw.* 1–9 (2017). <https://doi.org/10.1155/2017/1723658>
13. Qiu, T., Liu, X., Han, M., Li, M., Zhang, Y.: SRTS: a self-recoverable time synchronization for sensor networks of healthcare IoT. *Comput. Netw.* **129**, 481–492 (2017). <https://doi.org/10.1016/j.comnet.2017.05.011>
14. Alladi, T., Chamola, V., Sikdar, B., Choo, K.-K.R.: Consumer IoT: security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* **9**(2), 17–25 (2020). <https://doi.org/10.1109/mce.2019.2953740>

15. Loi, F., Sivanathan, A., Gharakheili, H.H., Radford, A., Sivaraman, V.: Systematically evaluating security and privacy for consumer IoT devices. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 1–6 (2017)
16. Bakhshi, Z., Balador, A., Mustafa, J.: Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In: 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 173–178. IEEE (2018). <https://doi.org/10.1109/wcncw.2018.8368997>
17. Wang, Q., Zhu, X., Ni, Y., Gu, L., Zhu, H.: Blockchain for the IoT and industrial IoT: a review. *Internet Things* **10**, 100081 (2020). <https://doi.org/10.1016/j.iot.2019.100081>
18. European Telecommunication Standards Institute: ETSI EN 303 645 “ETSI Releases World-Leading Consumer IoT Security Standard”. <https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard>. Last accessed 27 Jan 2021
19. IGI Global: “What is System Resilience?” <https://www.igi-global.com/dictionary/cyber-threats-to-critical-infrastructure-protection/51260>. Last accessed 26 Jan 2021
20. Collins Dictionary.: Definition of ‘Security’. <https://www.collinsdictionary.com/dictionary/english/security>. Last accessed 26 Jan 2021
21. Moore, A.D.: Defining privacy. *J. Soc. Philos.* **39**(3), 411–428 (2008)
22. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaidar, M.: IoT privacy and security: challenges and solutions. *Appl. Sci.* **10**(12), 4102 (2020). <https://doi.org/10.3390/app10124102>
23. Nykyri, M., Kuisma, M., Karkkainen, T.J., Hallikas, J., Jappinen, J., Korpinen, K., Silventoinen, P.: IoT demonstration platform for education and research. In: IEEE 17th International Conference on Industrial Informatics (INDIN), vol. 1, pp. 1155–1162. IEEE (2019). <https://doi.org/10.1109/indin41052.2019.8972280>
24. Yang, H., Jiang, B., Staroswiecki, M., Zhang, Y.: Fault recoverability and fault tolerant control for a class of interconnected nonlinear systems. *Automatica* **54**, 49–55 (2015). <https://doi.org/10.1016/j.automatica.2015.01.037>
25. Gupta, A., Christie, R., Manjula, R.: Scalability in Internet of Things: features, techniques and research challenges. *Int. J. Comput. Intell. Res.* **13**(7), 1617–1627 (2017)
26. Tata Consultancy Services: “Build a Scalable Platform for High-Performance IoT Applications”. https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/Research-and-Innovation/Build_a_Scalable_Platform_pdf.pdf. Last accessed 26 Jan 2021
27. SpiceLogic Inc.: Analytic Hierarchy Process Software v2.2. <https://www.spicelogic.com/Products/ahp-software-30/>

A Comprehensive Study on Vulnerabilities and Attacks in Multicast Routing Over Mobile Ad hoc Network



Bhawna Sharma and Rohit Vaid

Abstract MANET is an autonomous collection of mobile devices. They need the features of infrastructure-less network, flexibility, random mobility, and they do not require any base station or centralized device for the communication process. Rather than this, each device in MANET acts as a client and server. So it becomes a hot research topic among researchers. Communication between nodes is completed by intermediate nodes. Sometimes the intermediate nodes act as malicious nodes by implementing any abnormal function. So we would like to guard the traditional nodes. Therefore, we examine some routing attacks, and how they drastically affect the MANET communication process.

Keywords Network security • Ad hoc network • Denial of service • Route request • Route reply • Attacks • Secure routing protocols

1 Introduction

Mobile Ad-hoc networks (MANET) are the organizations of portable processing gadgets joined remotely with no help of fixed cooperation. There are a few attributes of MANET, which are as per the following:

- No requirement of fixed street and rail organization.
- Network of the organization is dynamic.
- Two nodes be in contact straightforwardly on the off chance that they are inside radio reach.
- Less secure than wired organization.
- MANET is an independent arrangement of portable nodes. It can work in disengagement or may have doors to and interfaces with a fixed organization.
- There are bandwidth constraints and energy constraints.
- Distributed nature of action for security, controlling, and have arrangements.

B. Sharma (✉) · R. Vaid

Department of Computer Science and Engineering,
MMEC, MM (Deemed To Be University), Mullana, Ambala, India

- More adaptable than fixed network.
- High client thickness and enormous degree of client portability.
- Nodal network is irregular.

In Fig. 1, design of MANET has been appeared in which a bunch of cell phones is associated together to shape a portable impromptu organization. The gadget with high calculation capacity and more battery force can be chosen as the gathering chief, who is dependable, the general administration of gathering correspondence inside the organization.

In MANET, there are different types of routing—unicast routing and multicast routing. The unicast routing is used for one-to-one communication, whereas multicast routing is used for one-to-many communications [2]. Broadcast conveys a message to all or any hub inside the organization. Multicast conveys a message to a bunch of hubs that demonstrate revenue in accepting the message. Anycast conveys a message to anybody out of a bunch of hubs, as a rule of the one nearest to the source. Geocast conveys a message to a geological area [3] (Fig. 2).

2 Multicasting

Multicasting correspondence fills in as one basic activity to help numerous uses of mobile Ad hoc networks (MANETs) that accomplishes bunch correspondence as opposed to sets of people. Multicast steering conventions turns out to be progressively significant in MANETs since they adequately arrange a lot of nodes [4]. Moreover, it gives viable coordinating to blended media applications, for instance, video social occasions, military, and rescue errands (Fig. 3).

2.1 Routing Protocols

There are many routing protocols in MANET. At whatever point a hub needs to talk with target hub, it broadcasts its current status to neighbors. Guiding shows can be arranged into proactive, reactive, and hybrid directing show.

Fig. 1 Structure of mobile Ad hoc network [1]



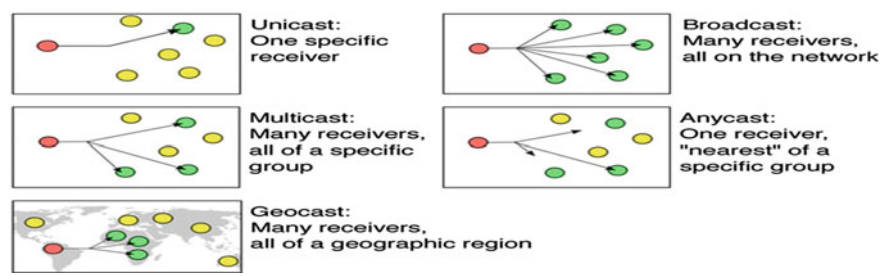


Fig. 2 Different types of routing

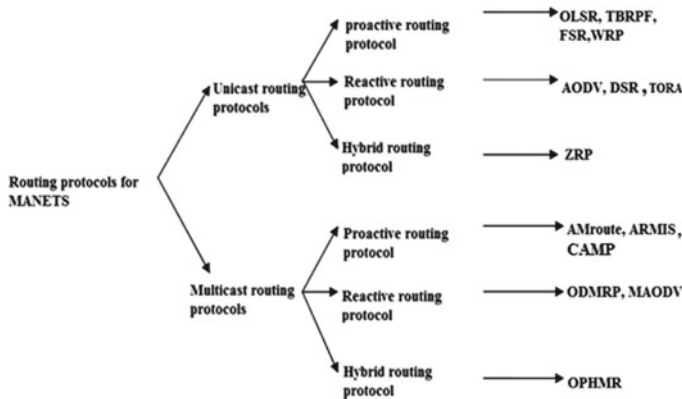


Fig. 3 Classification of routing protocols in MANET [5]

Proactive Routing Protocol:

This is a table-driven coordinating show. Each hub keeps a coordinating table which not only contains record of bordering hubs and reachable hubs, but also the amount of hops. If the size of association extends, the overhead furthermore increases which achieves decline in execution. Target sequenced distance vector (DSDV) and optimized interface state coordinating (OLSR) are proactive shows.

Reactive Routing Protocol:

This convention is likewise approached as request directing convention. At the point when a node needs to send information bundle, the responsive convention began. The preferred position of this convention is that squandered data transmission incited from consistently broadcast gets decreased. The primary weakness of this convention is that it prompts bundle misfortune. Ad hoc on-request distance vector (AODV) and dynamic source routing (DSR) are the cases of responsive directing convention. In AODV, every node records the data of next bounce in its steering table. The course revelation measure is executed at the point when the objective node cannot be reached from source node. The source node

communicates the course demand (RREQ) bundle to begin course disclosure measure. All the nodes get the RREQ packet send the course answer (RREP) parcel to the source node if the objective node data happened in their directing table. Course maintenance measure is begun when the organization geography has changed or the association has fizzled. The source node is educated by a course mistake (RRER) bundle. In DSR, nodes keep up their course store from source to objective node. Execution of DSR diminishes with the portability of organization builds, a lower bundle conveyance apportion inside the higher organization.

Hybrid Routing Protocol:

This convention contains the upsides of proactive, what is more, responsive convention. Proactive convention is utilized to accumulate the new steering data. At that point, responsive convention is utilized to keep up the steering data when geography changes. Zone routing protocol (ZRP) and temporally requested routing calculation (TORA) are the cases of crossover convention.

2.2 Security Services

MANETs are to give security administrations, for example, authentication, confidentiality, integrity, anonymity, and availability, to mobile users [5].

Confidentiality: Protection of any information from being introduced to unintended substances. In off-the-cuff associations, this is all the more difficult to achieve, considering the way that intermediate hubs get the packs for various recipients, so they can without a doubt tune in the information being coordinated.

Availability: Services should be available at whatever point required. There should be an affirmation of survivability, paying little heed to a denial of service (DOS) attack. On physical and media access control layer, the assailant can use adhering techniques to intrude with correspondence on real channel. On association layer, the attacker can upset the coordinating show. On higher layers, the attacker could chop down raised level organizations.

Authentication: Assurance that an element of concern or the cause of a correspondence is the thing that it professes to be or from. Without which, an aggressor would mimic a node in this manner, picking up unapproved admittance to asset and touchy data, and meddling with activity of different nodes.

Integrity: Message being sent is rarely adjusted.

Non-disavowal: Ensures that sending and getting gatherings can never deny truly sending or getting the message.

3 Literature Review

Jhaveri [6] proposed an MR-AODV convention which is an adjustment of R-AODV. MR-AODV not just distinguishes the dark opening and dim opening hubs, but additionally builds up free from any danger course for information transmission during the course disclosure measure.

Dhurandher et al. [7] proposes GAODV convention which is an altered AODV convention. Here, the presence of dark opening can be identified by utilizing critical control parcels CONFIRM, REPLYCONFIRM, and CHCKCNFRM. The source hub communicates RREQ message, and the middle hubs send RREP message to source, and afterwards, they unicast CONFIRM bundle to objective hub.

Karthikkannan et al. [8] proposed the grouping number distinguishing proof technique to keep away from the dark opening assaults in MANET. Here, an extraordinary grouping number will be given to every data parcel and the new bundle should have an arrangement number more noteworthy than that of pervious parcel.

In MANET, major focus was on increasing performance parameter values by developing new and updated mechanisms, and for this, several methodologies were offered. But, along with performance, security is also an important concern that must be taken care of [9]. In MANET, several attacks were found out due to which security of information can be compromised. Unauthenticated or malicious nodes are performing their attempts to be successful so that vulnerabilities can be found out in system, and accordingly, attack can also be imposed on network [10]. Each layer faces distinctive sort of assaults. Table 1 shows the normal assaults on different layers of MANETs [11].

4 Classification of Security Attacks on MANET

Making sure about MANETs is an exceptionally testing issue inferable from its existing engineering weaknesses. Assaults can be focused at steering conventions or even at security instruments conveyed in networks. Traded-off nodes can be

Table 1 Type of attacks on layers [13]

Layer	Attacks
Physical layer	Jamming, interceptions, eavesdropping
Data link layer	Traffic analysis, monitoring
Network layer	Wormhole, black hole, gray hole, message tempering, Byzantine, flooding, resource consumption, location disclosure attacks
Transport layer	Session hijacking, SYN flooding
Multiple layer	Denial of service (DoS), man-in-the-middle attack

available outside also as within the organization. Assaultants can disturb typical organization steering, confine node(s), may burn through imperative assets.

4.1 Internal Attacks

This sort of assaults are started by approved (real) nodes inside an organization. An inside node may get undermined by an outer aggressor, or it might carry on ego-tistically to spare its assets. Inward assaults are extremely difficult to recognize.

Ex: Byzantine attacks.

4.2 External Attacks

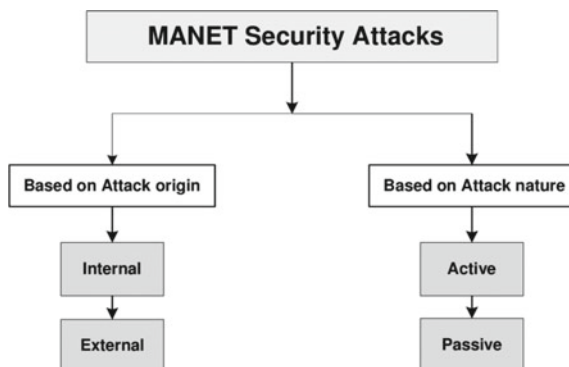
This sort of assault is started by non-approved (non-legitimate) nodes which are not a piece of the organization. Outside bargained nodes can seriously upset organization's directing and can cause blockage in different pieces of the organization (Fig. 4).

Ex: eavesdropping.

4.3 Passive Attacks

In this assault, an aggressor just tunes in or monitors information of data that is being moved between two parties. No change and manufacture is finished. Instances of latent assaults are snooping and traffic analysis. Assaultants can undoubtedly get all the data about the organization that is helpful in

Fig. 4 Classification of security attacks in MANET



commandeering or infusing an assault in the network. It is very difficult to identify inactive assaults when contrasted with dynamic assaults [12].

Ex: eavesdropping, traffic monitoring and analysis.

4.4 Active Attacks

In this assault, an aggressor endeavors to adjust or modify the information being traded in the organization. It might disturb the ordinary working of the organizations. In dynamic assault, the interlopers can change the bundles, infuse the parcels, drop the parcels, or it can utilize the different component of the organization to dispatch the assault.

Ex: spoofing, denial of services, wormhole, black hole, sinkhole, Sybil, etc.

Wormhole Attack: In this assault, an assailant records parcels at one area in the organization and passages them to another area. This passage between two plotting assailants is alluded as wormhole. Directing can be disturbed when steering control message are burrowed [14]. Wormhole assault is utilized against on-demand routing protocol the assault could forestall the disclosure of any courses other than through the wormhole. Tunneling is used by the attacker [15].

Black-hole Attack: In this assault, a black opening is a vindictive node that erroneously answers for course demands without having a functioning course to the objective and endeavors the directing convention to promote itself as having a most brief course to objective. By promoting the most limited course, source station begins sending information through the black opening node, and it become the dynamic component in the course (Fig. 5).

Byzantine Attack: In this attack, a sabotaged temporary hub works alone, or a lot of haggled center hubs works in plan and complete attacks. These assailant hubs make controlling circles, sending groups through non-ideal ways, or explicitly dropping packs, which achieves interference or debasement of the guiding organizations.

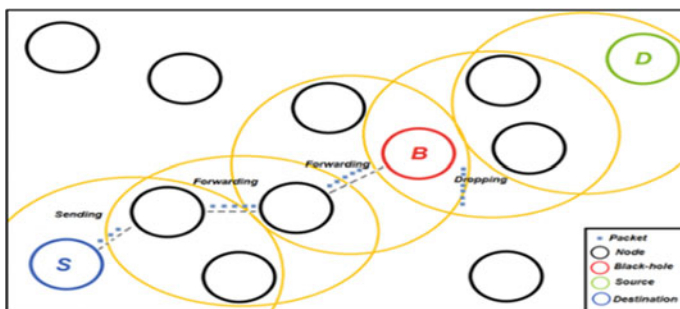


Fig. 5 Illustration of black-hole attack in MANET [16]

Traffic Monitoring and Analysis: In MANET composing, it is moreover named as location disclosure attack. In this kind of attack, the noxious hub screens, the conveyed groups, and examinations in this traffic which may reveal information, for instance, zone of sender–gatherer, sender collector pair, network topography, network coordinating structure, traffic rate, presence, zone of other genuine hubs, etc. A couple of association gadgets exist in the Web which can be used, thus, for instance, NetStumbler. Using this divulged information, other malicious hubs may similarly configure further attack circumstances in coordination. The attacker can even record, change, and retransmit changed packages to other veritable hubs remaining absolutely vague. Spillage of such information can be wrecking in security fragile conditions.

Eavesdropping: In this type of assault, the malevolent node captures the bundles sent or got, and it may uncover some classified data, for example, area of sender/beneficiary, mystery keys, passwords, and so on which might be generally left well enough alone during the correspondence between approved clients [17]. This is an aloof type of assault which owes itself because of simple tapping of remote nature of correspondence medium in MANETs.

Gray Hole Attack: In this sort of assault, a scornful node does not take an interest in course revelation instrument that is started by different nodes and is consequently not a piece of dynamic course. Such contemptuous nodes would build the course revelation disappointment and damage the general organization execution [18]. Another goal of such assailants is to moderate their energy by deciphering the message planned for them just and else they do not help out different nodes, which at last debase the presentation of the organization.

Jellyfish Attack: In this assault, the vindictive node first turns into a piece of the organization, and afterward, it might reorder the arrangement of got bundles, create undesirable postponements in bundle sending, or drop parcels [19]. This assault is like black-hole assault in any case; here, recognition is more troublesome in view of inclination of assailant to act as per convention rules. This makes the making trouble node yield very good quality to-end delay, high jitter and fundamentally influences the throughput of the organization.

Impersonation Attack: In impersonation attack, attacker node impersonates itself as authentic hub and sends bogus directing data and veils itself as sending from confided in hub [20].

Sybil Attack: Sybil attack shows itself by faking various characters by professing to involve various hubs in the association. So one single hub can anticipate the capacity of different hubs and can screen or hamper various hubs at the same time [21]. In case Sybil attack is performed over a blackmailing attack, by then degree of interference can be high. Achievement in Sybil attack depends on how the characters are created in the structure [22]. This may assist the aggressor with breaking required edge [23].

Resource Consumption Attack (RCA): Resource consumption attack (RCA) is against on-request directing convention. It is the one of DOS assaults, in which the aggressor abuses the course revelation process. During the course disclosure measure when the source node sends the RREQ parcel, at that point assailant node

kept this bundle with an alternate ID, to adjust the cycling ID of every node ceaselessly and devour its restricted energy of asset, memory, and bandwidth is appeared. The primary reason for RCA is to burn through the energy of genuine hubs and to locate the accessible connection all through [24].

Flooding Attack: Flooding assault is dispatched by flooding the organization with counterfeit RREQ’s or information bundles prompting the blockage of the organization and decreases the likelihood of information transmission of the approved hubs [25]. The identification of assault is exceptionally hard, and it debilitates the organization assets (Table 2).

Table 2 Summary table

S. No.	Name of attack	Attack effect
1	Wormhole attack	• Packet drain/rope methods • MAD convention and OLSR convention • Directional reception apparatuses • Multi-dimensional scaling calculation (versatility) • Using nearby neighborhood data • DAWWSEN convention • Designing appropriate steering conventions (grouping-based and topographical steering conventions) • Leveraging worldwide information
2	Black-hole attack	• Approval and monitoring • Redundancy • Using another course • Multipath steering
3	Byzantine attack	• Prevent the route establishment • Create loops, forwards packets through non optimal paths [26]
4	Traffic monitoring and analysis	• Access control • Reduction in detected information subtleties • Distributed handling • Strong encryption methods • Sending faker bundles persistently and normal checking
5	Eavesdropping	• Access control • Reduction in detected information subtleties • Distributed preparing • Access limitation • Strong encryption procedures
6	Gray hole attack	• Cautious instruments of black-hole assault, aside from excess also, utilizing worldwide information
7	Jellyfish attack	• Compliance with all data and control protocols • Affects mainly closed-loop flows [27]
8	Impersonation attack	• Strong and legitimate verification methods • Using solid information encryption

(continued)

Table 2 (continued)

S. No.	Name of attack	Attack effect
9	Sybil attack	• Certificate authority (CA) and using personality endorsements • Limiting the quantity of hub's neighbors • Physical insurance of gadgets • Changing key consistently • Resetting gadgets and changing meeting keys (network layer) • Authentication, interface layer encryption, and worldwide shared key procedures [28]
10	Resource consumption attack	• Consumes the energy of legitimate nodes and to find the available link throughout [24]
11	Flooding attack	• Customer puzzles • AODV (Ad hoc on-request distance vector) convention • Limiting the quantity of hub's associations • Routing access restriction • Key the board

5 Conclusion

Security is the standard concern in MANETs. Because of their basic properties, for instance, dynamic topography, nonattendance of central position, confined resources and open access medium Remote exceptionally named associations are introduced to being attacked or harmed. These basic credits familiarize new troubles with interference disclosure advancement, so it is difficult to achieve security in Ad hoc network when stood out from wired organizations. In this paper, we first briefly summed up the MANET and mainstream steering conventions in it. At that point, kinds of assaults alongside a most recent review of existing arrangements are examined. Various creators have given different expert throbs for discovery and counteraction of vindictive assault in MANET, yet every methodology has its own restriction. The malignant assault is as yet a functioning research zone in MANET. In the future, assessment fuses intend to develop such a security computation, which will be presented in header of each center point that helps in acknowledgment and expectation of malicious attacks.

References

1. Chander, D., Kumar, R.: Analysis of scalable and energy aware multicast routing protocols for MANETs. *Ind. J. Comput. Sci. Eng. (IJCSE)* **8**(3) (2017)
2. Jain, S., Agrawal, K.: Prevention against rushing attack in mobile Ad hoc networks. *Int. J. Comput. Sci. Technol. (IJCST)* (2014)
3. Gridher, V., Jain, S.: Review paper on an optimized approach for attack detection and prevention in wireless sensor networks. *Int. J. Comput. Sci. Technol. (IJCST)* (2017)

4. Qabajeh, M.M., Abdalla, A.H., Khalifa, O., Qabajeh, L.K.: A tree-based QoS multicast routing protocol for MANETs. In: 4th International Conference on Mechatronics (ICOM) (2011)
5. Sliman, K.A., Yaklaf, A., Abdurrezagh, S.E., Ekreem, N.B., Abosdel, A.A.M.: Security routing protocols in Ad hoc networks: challenges and solutions. In: Proceedings of the International Conference on Recent Advances in Electrical Systems, Tunisia (2016)
6. Jhaveri, R.H.: MR-AODV: a solution to mitigate blackhole and grayhole attacks in AODV based MANETs. In: 2012 Third International Conference on Advanced Computing & Communication Technologies, pp. 254–260. IEEE (2012) (978–0–7695–4941)
7. Dhurandher, S.K., Woungang, I., Mathur, R., Khurana, P.: GAODV: a modified AODV against single and collaborative black hole attacks in MANETs. In: 2013 27th International Conference on Advanced Information Networking and Applications Workshops, pp. 357–362. IEEE (2013) (978–0–7695–4952)
8. Karthikkannan, P., Lavanya Priya, K.P.: Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks. IEEE (2013)
9. Kumar, A.: Security attacks in MANET—a review. In: IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (2011)
10. Kumar, A., Singh, J.: Security attacks in mobile Ad hoc networks (MANET): a literature survey. *Int. J. Comput. Appl.* **122**(20), 31–35 (2015)
11. Mohammad, S.N.: Security attacks in MANETS (survey prospective). *Int. J. Eng. Adv. Technol. (IJEAT)* **6**(3) (2017). ISSN: 2249–8958
12. Dobhal, N., Pundir, D.: An investigative survey of different security attacks in MANETs. *Int. J. Comput. Appl.* (0975–8887) **126**(1) (2015)
13. Goyal, M., Poonia, S.K., Goyal, D.: Attacks finding and prevention techniques in MANET: a survey. *Adv. Wirel. Mobile Commun.* **10**(5), 1185–1195 (2017). ISSN 0973–6972
14. Rajkumar, K., Prasanna, S.: Complete analysis of various attacks in MANET. *Int. J. Pure Appl. Math.* **119**(15), 1721–1727 (2018)
15. Majumder, S., Bhattacharyya, D.: Mitigating wormhole attack in MANET using absolute deviation statistical approach. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 317–320. IEEE (2018, January)
16. Yasin, A., Abu Zant, M.: Detecting and isolating black-hole attacks in MANET using timer based baited technique. In: Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 9812135
17. Goyal, U., Gupta, M., Kaur, K.: Meliorated detection mechanism for the detection of physical jamming attacks under AODV and DSR protocols in MANETs. *IJAIEEM* **3**(10) (2014)
18. Alkathairi, M.S., Liu, J., Sangi, A.R.: AODV routing protocol under several routing attacks in MANETs. *IEEE* (2011) 978–1–61284–307–0/11
19. Sachdeva, S., Parneet Kaur, M.: Routing attacks and their countermeasures in MANETs: a review. *Int. J. Adv. Res. Comput. Sci.* **7**(4) (2016)
20. Latha, R., Sasikala, S.: A survey of routing attacks in Manet. In: Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015
21. Singh, R., Singh, J.: A novel Sybil attack detection technique for wireless sensor networks. *IEEE J. Sel. Areas Commun.* **10**, 185–202 (2017)
22. Saha, H.N., Bhattacharjee, D.: Different Types of Attacks in Mobile Ad hoc Network: Prevention and Mitigation Techniques. <https://arxiv.org/ftp/arxiv/papers/1111/1111.4090.pdf>
23. Rajakumar, P., Prasanna, V.T., Pitchaikannu, A.: Security attacks and detection schemes in MANET. In: 2014 International Conference on Electronics and Communication Systems (ICECS), pp. 1–6. IEEE (2014, February)
24. Jain, S., Agrawal, K.: The impact of resource consumption attack on signal-stability based adapting routing protocol in MANET. In: International Conference on Recent Developments in Science, Engineering and Technology (IJST) (2016)
25. Nithya, S., Prema, S., Sindhu, G.: Security issues & challenging attributes in mobile ad-hoc networks. *Int. Res. J. Eng. Technol. (IRJET)* **03**(01), 1083–1087 (2016)

26. Manohar, B., Kumar, M.: Review on Byzantine attack in MANET and solution to avoid. *Int. Res. J. Eng. Technol. (IRJET)* **6**(1) (2019). e-ISSN: 2395–0056
27. Kaur, M., Rani, M., Nayyar, A.: A comprehensive study of jelly fish attack in mobile Ad hoc networks. *Int. J. Comput. Sci. Mob. Comput.* **3**(4), 199–203 (2014). ISSN 2320–088X
28. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor networks: analysis & defenses. *Cent. Comput. Commun. Secur.* (2004)

An Offensive Approach for Hiding Malicious Payloads in an Image



Keshav Kaushik  and Sneha Surana

Abstract Steganography is the oldest technique that is been used from century, steganography purpose has not changed, i.e., all these techniques aim at hiding data or protecting data. With the help of steganalysis, the media can be analyzed to check for the presence of any secret information. Nowadays, attackers are making the use of advanced steganography approaches to conceal the secret information and communicate in a stealth manner. In this paper, the authors have discussed about the novel approach to hide malicious payload into image metadata. Therefore, metadata is a data that describes about the image rights and its administration. Hacker generally uses this metadata to perform various malicious attacks such embedding malicious script inside the image metadata and many more.

Keywords Steganography · Steganalysis · EXIF · Payload · Metadata · Image steganography · Stager · Cybersecurity · Digital forensics · Cyber forensics

1 Introduction

With the increase of Internet usage, people uploading and downloading pictures activity have increased. Now hackers are taking advantage of these activities and performing attacks. Once such type of attack is hiding payload in the image, it is actually steganography. Steganography is the art of concealing or hiding data within another object. The message can be hidden in physical objects or in reference of electronic, it can be an image, video, audio. Now the message is payload for hackers, they generally try to embed the malicious script when the image is downloaded on the victim system, it will execute on the system and run the process or delete the files or spread of malware, viruses, etc., ultimately leading to damage

K. Kaushik (✉)

Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

S. Surana

University of Petroleum and Energy Studies, Dehradun, India

or loss of the victim. Image steganography is majorly classified based on two main methods that are spatial domain and transform domain. Others types of steganography includes masking, filtering, and distortion techniques.

2 Related Work

In [1], research paper describes an approach a technique named hue–saturation–intensity (HSI) color space, which depend upon the least significant bit (LSB). This technique is assessed both on subjective and objective part. In the technique proposed, using LSB method, the message that is to be hidden is embedded in I-Plane of HIS color space model. The outcome image is retransformed to RGB color model to develop the stego-image. This technique adds the extra level security to image making difficult for an attacker to detect the whether the data is hidden in the image or not.

In [2], research paper discusses about the technique for hiding an image in audio file using least significant bit (LSB) substitution techniques for implementing image and audio steganography. This technique proposed converts the normal colorful image into grayscale image and use a 16-bit AES algorithm to encrypt a grayscale image. The secret audio is embedded in the grayscale image and 16 bits key in any frame in the video file in which data is to be hidden with the help of LSB substitution technique. The audio and video on which steganography is performed can easily transmit to receiver over the network.

The Android malware clustering is identified through mining of malicious payload in [3]. The research paper discusses keeping the malicious code separate from legitimate library code from malware in Android. It implements robust technique to determine if malware samples having the same version as malicious payload. The method uses tradition hierarchical clustering and fuzzy hashing fingerprint. The techniques improve the performance and scalability on examining of large malware families, and accuracy is also maintained. It can determine that if library is having old version and whether it shares the name with a bogus library.

The STEGANOGAN [4], end-to-end model that is based on deep learning, mitigates vanishing gradient problem for image steganography. Using this model, a 4.4 bits per pixel relative payload is achieved and evades the detection of steganography in the image. This technique is efficacious on images using multiple datasets. STEGANOGAN is an open-source library to enable fair comparisons. This technique [5] uses generative adversarial networks to hide binary data in images to enhance the quality of images produced by this model.

3 Working Methodology

The authors will add a malicious script to the image EXIF [6] metadata. The malicious script (Payload) will be directly embedded into the EXIF metadata using the tool. The image will be available online, and it will be easily accessible. Generally, when the image is open and the payload will execute itself, but, in this case, the stager will be required to execute the payload in the image. So firstly, the stager will download the image from the Web site, and after that, it will extract the payload from image EXIF metadata. Once the payload is extracted, the stager will execute it. Therefore, a stager can be written in short length let us say 100 characters and it will not take much space on disk.

Following tools will be used like curl, Exiftool, bash, and grip.

First step, the image is downloaded, as it is the medium for attack. The image will not be saved on the system or target computer. For downloading the image, the tool will use named Wget [7] that is non-integrated tool network downloader that even download the file from the server whether user is logged on to the system or not. Wget tool can work without hampering the process that is currently working in the background. Wget has various flags like -h flag that displays the information about other various flags, and here, the authors will use -O flag to write documents to file and will save the file to particular directory say in /tmp directory.

Here, the image is being downloaded and saved that file with name image.jpeg in tmp folder (Fig. 1).

Now the **second step** is generating payload, in reference to a cyberattack [8], it is that component of the attack that harms the target system. It can be any virus, worms, malware, or any malicious payloads that can drastically affect the target computer. In this step, the utility named Mate calculator in Kali Linux will be trying to open. The steps are performed, so that it can be run through the terminal. Therefore, whenever payload is executed, Mate calculator will be opened through stager. Here, any type of bash script can be used to perform any operations. Here, the combination printf, base64, and tr commands will be used to encode the payload. The printf command displays the passed formatted text on a terminal in Linux. The base64 is the command in Linux that encodes the text the base64 and decodes base64 encoded text to normal text. The tr is a utility in Linux that translates and

```
root@kali:~# wget https://www.gardeningknowhow.com/wp-content/uploads/2008/07/tulips-400x300-  
.jpg -O image.jpg  
--2021-01-10 23:31:14-- https://www.gardeningknowhow.com/wp-content/uploads/2008/07/tulips-  
400x300.jpg  
Resolving www.gardeningknowhow.com (www.gardeningknowhow.com)... 151.139.128.11  
Connecting to www.gardeningknowhow.com (www.gardeningknowhow.com)[151.139.128.11]:443... con  
nected.  
HTTP request sent, awaiting response... 200 OK  
Length: 40352 (39K) [image/jpeg]  
Saving to: 'image.jpg'  
  
image.jpg 100%[=====] 39.41K --KB/s in 0.007s  
  
2021-01-10 23:31:15 (5.16 MB/s) - 'image.jpg' saved [40352/40352]
```

Fig. 1 Downloading image for steganography

deletes characters and supports transformations like uppercase to lowercase, deleting characters. The command be written as this (Fig. 2).

The **third step** will payload embedding into the image, and here, the authors will be modifying the EXIF metadata [9] of the image to embed the above results in it using a tool named Exiftool. Exiftool is an open-source tool for manipulating and writing audio, image, video, and PDF metadata. Now, install that tool in Linux [10] using this command (Fig. 3).

Now, after the installation, it clears all the EXIF metadata that can be in an image using this command (Fig. 4).

Now, the payload is added to the metadata of the image by using Exiftool tag—and certificate tag is only for demonstration purpose (Fig. 5).

Now to verify whether certificate tag is added to the image or not, the authors will use below displayed command (Fig. 6).

See certificate tag in the image in the above image. Now **fourth step** is uploading image on the Web site. It might look easy, but one should upload the image by taking the following factors in mind:

Web Traffic Irregularities—The image should be uploaded on the Web site [11] that is regularly visited by the target. For example, if the target visited a particular news Web site daily, it would not appear suspicious to sysadmin, which

```
root@kali:~# printf "m0te-c4lculat0r" | base64 | tr -d '\n'
bWFOZSljYWxjdWxhdG9yroot@kali:~#
```

Fig. 2 Preparing payload and encoding it

```
root@kali:~# apt-get install exiftool
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libimage-exiftool-perl' instead of 'exiftool'
libimage-exiftool-perl is already the newest version (12.13+dfsg-1).
0 upgraded, 0 newly installed, 0 to remove and 967 not upgraded.
```

Fig. 3 Updating the packages and installation of Exiftool

```
root@kali:~# exiftool -all= /tmp/image.jpg
Warning: ICC Profile deleted. Image colors may be affected - /tmp/image.jpg
1 image files updated
root@kali:~#
```

Fig. 4 Cleaning metadata of the image using Exiftool

```
root@kali:~# exiftool -Certificate='bWFOZSljYWxjdWxhdG9y' /tmp/image.jpg
1 image files updated
root@kali:~#
```

Fig. 5 Embedding of payload to the image using Exiftool

Fig. 6 Payload is embedded using Exiftool

```
root@kali:~# exiftool /tmp/image.jpg
ExifTool Version Number      : 12.13
File Name                    : image.jpg
Directory                    : /tmp
File Size                     : 42 KiB
File Modification Date/Time   : 2021:01:13 22:05:13+05:30
File Access Date/Time        : 2021:01:13 22:05:13+05:30
File Inode Change Date/Time   : 2021:01:13 22:05:13+05:30
File Permissions              : rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
XMP Toolkit                   : Image::ExifTool 12.13
Certificate                   : bWF0ZS1jYWxjdWxhdG9y
Image Width                  : 400
Image Height                 : 300
Encoding Process              : Progressive DCT, Huffman coding
Date-Time Created            : 2021:01:13 22:05:13+05:30
```

monitor network traffic. The main idea is to make traffic look normal or ordinary to the victim Web behavior.

Avoid EXIF Data Sanitization [12]—Generally, when images are uploaded on popular Web site like Twitter, Instagram, etc., image metadata is deleted to protect the user GPS coordinates that are coincidentally uploaded with photographs, and these GPS coordinate can be source for a cyberstalker to perform attacks or harass people. Therefore, uploading the image on a mainstream Web site [13] that contain payload be a waste, as EXIF metadata will be deleted.

Website Encryption—The Web site on which image will be hosted should be HTTPS, as this will prevent sysadmin network monitor to analyze the GET request with surgical precision. Therefore, transport layer security is a necessary part in making this attack obscure.

Now, the last step is generating the stager; in this step, stager will download the image from the Web site, and then, it will extract the payload from the image and execute it (Fig. 7).

Therefore, this last step is further broken into further steps to understand the role of stager easily:-

- **p = \$(...):** This variable that is used to store the results of commands [14] that are used are executed and it is known as “p,” p refers to payload. This is done, so that the image is not directly saved to Linux hard drive. Since the payload is stored in the variable after the commands like to curl, grep, sed, and base64 are being executed, so that it can be payload that contain certain scripts that executed further.
- **curl -s https://127.0.0.1/image.jpg:-** Curl is the utility in Linux that uses several protocols, so that data can be transferred from the server. Here, the curl will be used with flag “-s,” so that the image is downloaded silently, so victim do not know that script is executed. After the flags, the URL have added for image downloading purpose. For demonstration purpose the image is been hosted on

```
root@kali:~# p=$(curl -s http://127.0.0.1/image.jpg | grep Certificate -a | sed 's/<[^>]*>/\n/g' | base64 -d -i );eval $p
```

Fig. 7 Generation of stager

localhost server. The output of curling image from the server will be in the binary form. Now output of this command is piped to grep command.

- **grep certificate -a:** grep command is used to search a mentioned word in input files or in the standard input. As default, grep prints the lines that are matched. The output of the curling image from the server will be in the form binary form. If grep is used with -a, it is used to process or search the given input in the binary files like these binary files are containing text. Therefore, in the above command mentioned, grep will search the input keyword certificate in the binary output that has been obtained from binary files. Now output of this command is piped to sed command.
- **sed 's/<[^>]*>//g':** sed is a basic text editor that is used on input stream that be a file or pipeline input. So as text editor, it performs operations like finding, searching, and replacing. The output of grep command is surrounded by xml data type [15], so to extract payload from this output, it is necessary to use sed command. Here, the “s” in the single quotes in this command stands for substitution operation. The “/” refers to delimiters, and “g” refers to substitute flag that replaces all occurrences of a string in the line. So here, the command used is replacing all xml data types with leaving empty, and only payload data are extracted by using sed command. Now output of this command is piped to base64 command.
- **base64 -d -i:** base64 is utility in the command line that is used for encoding a text into base64 encoding and decode the base64 encoding to normal text. Here, base64 command is being used to decode the payload that extracted from the image. Here “-d” flag stands for decode data, and “-I” flag stands for ignoring garbage like non-alphabet characters while decoding. The final output from this command is stored in variable “p.”
- **eval \$p:** eval is utility in Linux that concatenates the arguments into a single string and take it as input and execute the commands. This command is being used to execute the payload which is extracted from the image on the terminal.

The results can be verified that Mate calculator utility is open on the screen while executing the payload. For the demonstration purpose, an open Mate calculator is opened from terminal by executing the payload. The Mate calculator is utility, i.e., present in Kali Linux (Fig. 8).

4 Result and Discussion

The authors are successful in implementing execute the payload which was embedded in the image by using stager. The payload was first encoded with base64 encoding, and then, using Exiftool, all metadata of the image was cleared. The encoded payload was added to the image using Exiftool to the metadata of an image by assigning tag to payload in this tag was named as “certificate.” After that stager was written, curl the steganography [16] image from the server and extracted

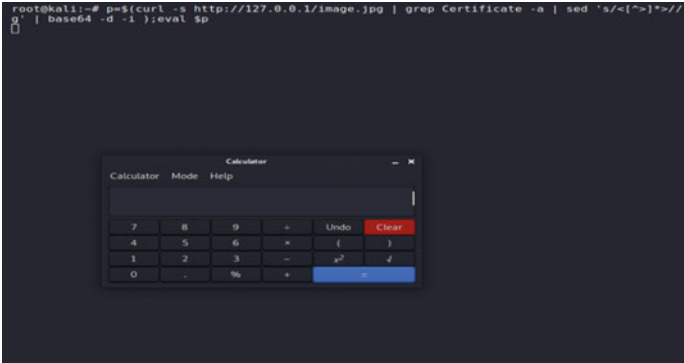


Fig. 8 Triggering Mate calculator after execution of payload using stager



Fig. 9 Procedure of embedding the payload and its execution

encoded payload from binary image data by using `grep` and `sed` utility in Linux. The encoded payload was decoded and executed it by assigning payload to a variable and executing variable using `eval` command in Linux and further executed that variable. For demonstration purpose, the Mate calculator (utility) was opened. We can use various types of payload such as it consists of malware or script that count keystroke or to open software. Once these payloads are executed, they are successful in implementing the things that were assigned to them. It tells the importance of image sanitization and network sanitization to prevent these kinds of attacks in future (Fig. 9).

5 Conclusion

This paper has highlighted the use of steganography in cyberattacks and cyber-crimes. Although, steganography is an ancient technique, it is predominant in many cyberattacks with some advanced mechanism and approaches. This paper also focused on the hiding of some malicious payload in the metadata of an image. Likewise, any image can be used for this purpose and later on can be used for performing specialized type of cyberattack. The main motive of this paper was to make the readers and cybersecurity enthusiasts aware about such type of approaches that are in practice in the current scenario. Furthermore, the payload may contain any type of costumed malicious scripts that may be capable of damaging the

entire organization with the help of an image only. In future aspect, the metadata of the image can also be used for hiding some payment related QR codes that may trigger some financial transaction from some mobile app. The authors will also look forward to extend this work in near future.

References

1. Muhammad, K., Ahmad, J., Farman, H., Zubair, M.: A novel image steganographic approach for hiding text in color images using HSI color model. arXiv preprint [arXiv:1503.00388](https://arxiv.org/abs/1503.00388) (2015)
2. Rawde, M., Kumbhare, M., Chaudhari, S., Bhongade, S., Bhagat, V.: Novel approach towards higher security using crypto-stego technology. *Int. J. Emerg. Trends Technol. Comput. Sci. (IJETTCS)* **4**(1) (2015)
3. Li, Y., Jang, J., Hu, X., Ou, X.: Android malware clustering through malicious payload mining. In: *International Symposium on Research in Attacks, Intrusions, and Defenses*, pp. 192–214. Springer, Cham (2017)
4. Zhang, K.A., Cuesta-Infante, A., Xu, L., Veeramachaneni, K.: SteganoGAN: high capacity image steganography with GANs. arXiv preprint [arXiv:1901.03892](https://arxiv.org/abs/1901.03892) (2019)
5. Hosam, O., Ben Halima, N.: Adaptive block-based pixel value differencing steganography. *Secur. Commun. Netw.* **9**(18), 5036–5050 (2016)
6. Alwan, I.M., Mohammed, F.J.: Image hiding using discrete cosine transform. *J. College Edu. Women* **27**(1), 393–399 (2016)
7. Hamid, I.: Image steganography based on discrete wavelet transform and chaotic map. *Int. J. Sci. Res. (IJSR)* **7** (2018)
8. Deshpande, S., Mallayyanavarmath, S.: Complete study on steganography [online]. Ijraset.com. Available at: <https://www.ijraset.com/files/serve.php?FID=8366> (2017). Accessed 11 Jan 2021
9. Hacking MacOS: How to hide payloads inside photo metadata [online]. Available at: <https://null-byte.wonderhowto.com/how-to/hacking-macos-hide-payloads-inside-photo-metadata-0196815/> (2019). Accessed 11 Jan 2021
10. Kernel.org.: The linux man-pages project [online]. Available at: <https://www.kernel.org/doc/man-pages/> (n.d.). Accessed 11 Jan 2021
11. En.wikipedia.org.: Steganography [online]. Available at: <https://en.wikipedia.org/wiki/Steganography> (n.d.). Accessed 11 Jan 2021
12. Data Sanitization Terminology And Definitions—International Data Sanitization Consortium [online]. Available at: <https://www.datasanitization.org/data-sanitization-terminology/> (n.d.). Accessed 11 Jan 2021
13. LSB Based Image Steganography Using MATLAB—Geeksforgeeks [online]. Available at: <https://www.geeksforgeeks.org/lsb-based-image-steganography-using-matlab/> (2020). Accessed 11 Jan 2021
14. The Types and Techniques of Steganography Computer Science Essay [online]. Available at: <https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php> (n.d.). Accessed 11 Jan 2021
15. Kaur, S., Bansal, S., Bansal, R.K.: Image steganography for securing secret data using hybrid hiding model. *Multimedia Tools Appl.* 1–21 (2020)
16. Zhou, Z., Mu, Y., Wu, Q.J.: Coverless image steganography using partial-duplicate image retrieval. *Soft. Comput.* **23**(13), 4927–4938 (2019)

A Review of Anti-phishing Techniques and its Shortcomings



Bhawna Sharma and Parvinder Singh

Abstract Phishing has become one of the most common activities observed over the Internet quite often. To investigate the methods through which phishing can not only be detected but can also be controlled, a lot of researchers have contributed and have opened gates for the industry. This paper illustrates the types of phishing attacks and ways to optimize the anti-phishing architecture. The highlights of this paper are listing down the ways to detect phishing activities over web services. The analyzed techniques are compared on the basis of suitable comparative parameters listed in reputed articles.

Keywords Information security • Phishing • Phishing countermeasures • Phishing identification • Assessment measurements

1 Introduction

The revolution of the Internet can be analyzed from our daily life. Due to the wide use of digitized systems, data security is of main concern. Security means that users should take necessary precautions while using technologies. Phishing is a social engineering attack. Phishers maliciously gather user's confidential data like credit card numbers, bank account details, and passwords [1]. The phisher introduced several attacks every day to attack the authentic site and misled the user by sending malicious code. Phishing can be done on a single user or a number of users. If phishing is done on specific users, then it is termed spear phishing. Today, phishing is a critical challenge. However, several methods have been introduced by the

B. Sharma (✉)

Deenbandhu Chhotu Ram University of Science and Technology,
Murthal, Sonapat, Haryana 131039, India

P. Singh

Department of Computer Science and Engineering, Deenbandhu Chhotu Ram University
of Science and Technology, Murthal, Sonapat 131039, India

e-mail: parvindersingh.cse@dcustm.org

researchers to prevent phishing attacks or anti-phishing techniques. Phishing may prompt money-related misfortune, information misrepresentation, sensitive data loss, spoliation of reputation, and reduction of trust in the web [2]. Phishing smartly removes the security measures taken by any organization to prevent phishing activity from the hacker. Phishing and legitimate sites seem to be visually alike. Phishing attacks mainly target financial organizations. Phishing is carried out via emails, websites, and instant messengers.

This paper starts by showing the phishing issue in Sect. 2 and portraying distinctive anti-phishing techniques in Sect. 3. Section 4 focuses on evaluation metrics. The conclusion is drawn in Sect. 5 which concludes this paper.

2 The Phishing Problem

A. History

The term phishing came into account in 1996 in America. Fishers (e.g., attackers) use a trap (e.g., fake email tempting users for entering sensitive information) to catch a fish (i.e., to befool a user). **Phone phreaking** was the earliest form of hacking. So the character “f” of fishing was replaced by “ph,” and the term “phishing” came into the picture [3]. “Phishing” takes after “angling” in a way that fishers (e.g., attackers) utilize a snare (e.g., socially designed messages) to angle (i.e., to take client's delicate data). The oldest kind of hacking was known as phone phreaking. It was utilized for phone systems.

B. Definition

Phishing is an assault in which the aggressor misuses social designing methods to perform data fraud. It is the illegal activity that hackers take to steal crucial data of the user such as details of bank, passwords, unique identification, and other sensitive data.

It occurs when the attacker concealments his identity and acts as an authentic person and fools the users by fake message or text, including malicious connection. This attack consequence in respect of ingathering funds and steal personal details.

Figure 1 displays the mechanism of the phishing attack to steal crucial data of the authentic user using phishing website when users log in to the original website. It mainly happens when the user clicks on the malicious link that makes by the phisher, and the user redirects to the phishing website, so the phisher takes control over it. Phishing customarily works by sending an email, mirroring an online bank, closeout, or installment destinations, controlling clients to a fake website page, which is cautiously intended to resemble the login to the certified webpage. Phishing means gathering touchy and personal information by imitating an authentic entity [4]. Portray a phishing assault in three different ways: (1) a simple site must be picked; (2) a phishing site must be made so that it has a comparative look-and-feel as that of the real site, and (3) delicate data of the client must be

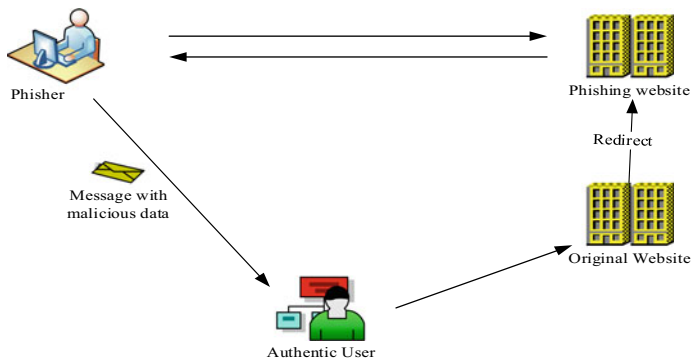


Fig. 1 Mechanism of phishing attack

gathered. Phishing assaults could have genuine ramifications for their exploited people, for example, the loss of protected innovation and sensitive data, monetary misfortune, and the trade-off of national security, just as general debilitating trust.

Different types of phishing attacks as discussed by authors are as follows (Fig. 2):

1. **Deceptive Phishing:** It is a kind of phishing. It happens by sending emails and links to the malicious website that makes to tackle the user and theft the sensitive data of the user. Mainly, these phishing attacker occurs by requesting to users to verify the details of the account, re-enter data like password or logins details and steal the sensitive data of the authentic user.
2. **Malware-Based Phishing:** This phishing attack happens through malicious software on the system of the user. The attacker sends the attachment or as a downloadable document manipulating vulnerabilities of security. It is more problematic for medium and small businesses who unsuccessful in updating their software of the system.
3. **SMiShing:** It utilizes text messages or SMS on cellular mobile or smartphone to tackle the user for the purposes of stealing data of the user. In this process, the attacker tries to trick the customer into providing them crucial data of the customer through the text message.
4. **Vishing:** It is the form of the attack that is derived from phishing and voice. It is the experience of leveraging technologies of IP-based voice messaging to engineer the intended user into giving financial, personal, socially, or other crucial data for financial reward. This attack utilizes the phone calls to mislead the user or trick to user into providing details of the user.
5. **Web Trojan:** It is the kinds of phishing attack that involves malicious code or software that seems to be authentic to steal the sensitive data of the customer. It pops up when the consumer wants to log in to a significant website. But this is not visible to the customer and store the identity details of the user and send to the hacker.

6. **Key loggers and Screen loggers:** These are the different types of malware attack in which input is tracked from the keyboard and transmit this crucial data to the hacker. And sometimes, they may enter themselves into the browser of the customer as a small utility function.
7. **Cross-Site Scripting:** It is the kind of vulnerability of computer privacy discovered in the application of the web that permits code by malicious web customers into the pages of the web seen by other people, for example, HTML codes and scripts of client side.
8. **Session Hijacking:** This kind of phishing attack monitors the activity of the customer or track the user actions such as bank details and sensitive data of the customer and behalf of that malicious software take action that is illegal, like transferring funds without customer knowledge.
9. **Denial of service (DoS) Attack:** In this, the hacker floods the system with so much traffic to steal the crucial data of the customer by misdirecting them. The main purpose of this attack is to restrict the services of the authentic user by so much traffic.
10. **Clone Phishing:** Phisher makes a cloned mail via getting data or addresses of the recipient from the authentic mail that was transferred earlier, then the attacker transfers the similar email with the malicious connection. Phisher utilized a previously sent legitimate email to tackle the customers to misdirect into giving them confidential data.
11. **Content-Injection Phishing:** In this, then, the hacker inserts the malicious code into the authentic website, and this code redirects the customer to another site or installs malware on the system of the user. This phishing attack replaces the content of the authentic site with false data to misdirect the customer into providing their sensitive data or account details.
12. **Man-in-The-Middle Phishing:** This is a kind of phishing attack that is introduced by phishers by inserting themselves between the website and users to record the data of the customer without knowing the customer. It is complicated to identify compared to other forms of attack. In this, the phisher intercepts the connection of the user or website, sits in the middle, and stores data that is entered by the user but does not show the effect on the transaction of the customer.

C. The Phishing Existence Cycle

The different periods of existence of phishing site are depicted in Fig. 3 [1] and are explained below:

Period 1: A fake webpage is created by a phisher that is visually similar to a genuine webpage.

Period 2: The fake webpage is sent to the user via email.

Period 3: The fake webpage is opened by the client, and personal information of the client is collected.

Period 4: The client's personal information is gathered by the phisher and is misused by him.

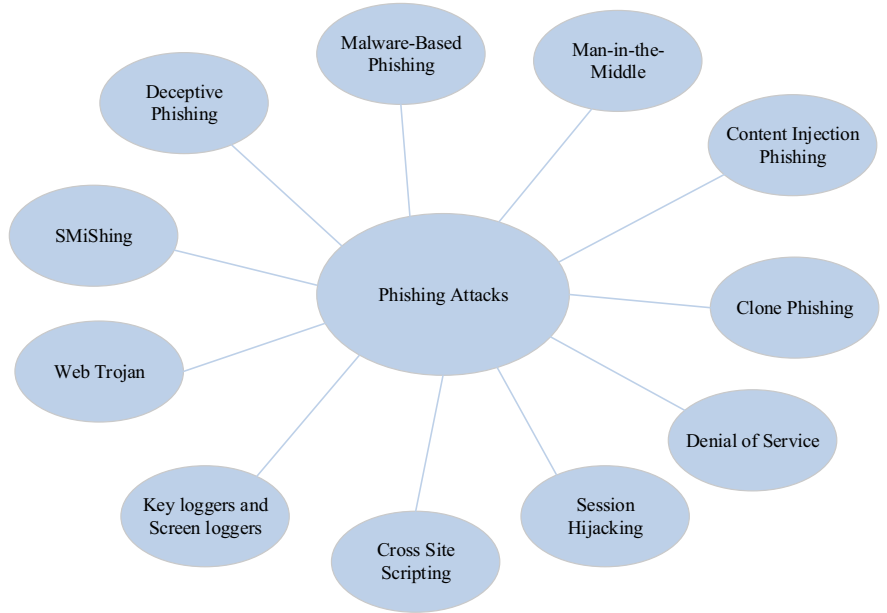
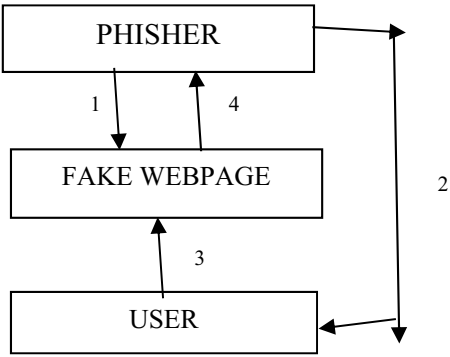


Fig. 2 Phishing attack

Fig. 3 Phishing existence cycle (1 Phisher creates a fake webpage. 2 Phisher sends the fake webpage to the user. 3 User clicks the link to the phishing webpage and enters sensitive information into it. 4 Phisher gets the personal information of the user and uses it to perform fraud)



The clients are defenseless to phishing assault because of the accompanying reasons:

1. A few people may need basic information existing on the web dangers.
2. Only a few clients may have a decent comprehension of what does PC infections, programmers, and extortion mean and how to shield themselves from these dangers; they may not be well-known of what does phishing implies. Subsequently, they cannot sum up what they knew to new dangers.

3. Albeit a few clients are careful about being victims of phishing attacks; they do not have an idea about phishing countermeasures.
4. Customers may focus on their essential endeavors while concentrating on security snippets of data is seen as a helper task.
5. A few clients may disregard some basic security pieces of information in the uniform resource locator (URL) of the webpage, for example, the presence of security protocol **h**ypertext **t**ransfer **p**rotocol **s**ecure (HTTPS).
6. Customers do not have any idea of protocols used for security purpose (e.g., SSL: secure socket layer).
7. A couple of customers may ignore warnings.

3 Anti-phishing Techniques

Anti-phishing has been utilized to recognize the attack of the hacker. It protects the customer from illegal access.

Many authors introduced several techniques of anti-phishing to distinguish the phishing attack.

The anti-phishing method may also have an inbuilt feature to identified illegal access from the unauthorized party, such as one-time password, captcha, hypertext transfer protocol secure.

The major approaches used for preventing users from phishing scam are described below [5, 6, 3]:

A. Blacklist

Blacklist holds URLs that allude to destinations that are viewed as malevolent [1]. At whatever point a program loads page, it questions blacklist to decide if right now visited URL is on this rundown. Assuming this is the case, proper countermeasures can be taken. Something else, the page is viewed as real.

The blacklist can be put away locally at the customer or facilitated at the focal server. Clearly, a critical factor for the viability of the blacklist is its inclusion. The inclusion demonstrates how many phishing pages on the Internet are incorporated into the rundown. Another factor is the nature of the rundown. The quality shows how many non-phishing locales are inaccurately included in the rundown. For each off-base section, the client encounters a bogus cautioning when she visits a genuine site, undermining her trust in the convenience and accuracy of the arrangement.

At long last, the last factor that decides the adequacy of blacklist-based arrangement is the time which it takes until a phishing site is incorporated. This is on the grounds that numerous phishing pages are brief, and a large portion of the harm is done in the time length between going on the web and evaporating. Notwithstanding when a blacklist contains numerous passages, it is not viable when it takes excessively long until new data is incorporated or achieves the customers.

B. Whitelist

A white list is a list containing all genuine URLs. White list is used to classify URLs as legitimate or phishing. If a given URL is available in the white list, then declare the URL as legitimate, else the URL is declared phishing. The drawback of using the whitelist approach is that the updation process of the white list is time-consuming. One solution is automated individual-white list [7].

C. Heuristics

Ordinarily, phishing countermeasures depend on URL blacklists or on methods for separating the basic highlights (attributes) from a site [8, 9]. As opposed to blacklist approaches, which principally rely upon the client's encounters, the highlights-based methodologies are moderately progressively advanced and requires profound examinations. Highlight-based systems right off the bat gather a lot of discriminative highlights that can isolate phishing sites from real ones, at that point, train an AI model to anticipate phishing endeavors dependent on these highlights, lastly utilize the model to perceive phishing sites in reality [10]. Selecting an appropriate set of attributes or features (feature set) is of primary concern (Fig. 4).

D. Visual Similarity

This approach is freethinker to the essential development that provides the visualization to the customers' eyes [11]. Phishing sites give a similar look-and-feel as given by legitimate sites. For instance, phishing sites may use similar images as used in legitimate sites [12]. GooglePay, Amazon, Flipkart, banks, and other financial institutions are the main target websites that are attacked by phishers. Users should visit these sites only after assuring security.

E. Machine Learning

Like heuristic tests, machine learning-based strategies can direct phishing strikes, which makes them beneficial when they appeared differently in relation to blacklists. Inquisitively, machine learning frameworks are in like manner prepared for structure their very own gathering models by examining far-reaching courses of action of information [1, 3]. ML methods have the accompanying preferences when compared with the heuristic approach:

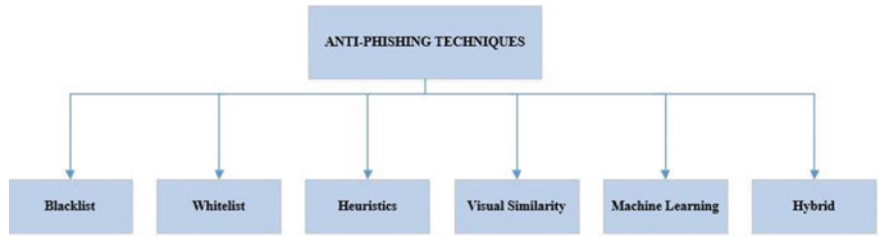


Fig. 4 Anti-phishing techniques

- It is conceivable to build viable characterization models when vast informational collection tests are accessible, without the requirement of physically dissecting information for finding complicated connections.
- As phishing endeavors create, machine learning classifiers can thus progress through learning. On the other hand, it is likewise conceivable to intermittently develop more up to date arrangement models by basically retraining the student with refreshed example informational collections. The examination of various phishing discovery strategies is presented in Table II.

F. **Hybrid**

The hybrid approach utilizes a blend of previously described anti-phishing approaches (list-based approaches, heuristics, visual similarity, and machine learning).

4 **Evaluation Metrics**

A. **Stability**

The steadiness estimates how stable every calculation performs as far as recognition precision. Standard deviation (SD) is used to evaluate security. A vast SD esteem infers the vacillation in discovery exactness and precariousness of the execution.

B. **Speedup**

The speedup is defined as the ratio of the runtime of a sequential algorithm for solving a problem to the time taken by the parallel algorithm to solve the same problem on multiple processors.

C. **Performance Measures**

Here, PP is a number of correctly identified phishing occurrences. LP is a number of incorrectly identified legitimate occurrences. PL is a number of incorrectly identified phishing occurrences. LL is a number of correctly identified legitimate occurrences. Table 1 shows the confusion matrix. Table 2 shows different performance measures [3]. The anti-phishing algorithms are compared in Tables 3, 4, 5, and 6.

Table 1 Confusion matrix

Predicted	Phishing	Legitimate
True		
Phishing	PP	PL
Legitimate	LP	LL

Table 2 Performance measures used in anti-phishing techniques

S. no.	Measure	Definition	Formula
1	False-positive rate (<i>FPR</i>)	Quantifies the incorrectly identified legitimate instances relative to the total number of legitimate instances	$FPR = LP/(LL + LP)$
2	True-positive rate (<i>TPR</i>)	Quantifies the correctly identified phishing instances relative to the total number of phishing instances	$TPR = PP/(PP + PL)$
3	False-negative rate (<i>FNR</i>)	Quantifies the incorrectly identified phishing instances relative to the total number of phishing instances	$FNR = PL/(PP + PL)$
4	True-negative rate (<i>TNR</i>)	Quantifies the correctly identified legitimate instances relative to the total number of legitimate instances	$TNR = LL/(LL + LP)$
5	Accuracy (<i>ACC</i>)	Quantifies the correctly classified instances relative to the total number of instances	$ACC = (LL + PP)/(LL + LP + PL + PP)$
6	Precision (<i>P</i>)	Quantifies the correctly identified phishing instances relative to the number of instances that are identified as phishing	$P = PP/(LP + PP)$
7	Recall (<i>R</i>)	It is same as true positive rate	$R = TP$
8	<i>f1</i> score	It is equal to the <i>H.M. (harmonic mean)</i> between <i>precision</i> and <i>recall</i>	$F1 = (2 * P * R)/(P + R)$

Table 3 Comparison of different anti-phishing algorithms

Detection technique	Advantages	Disadvantages	Remarks
Auto-updated white list [7]	It can detect a zero-hour phishing attack	Only hyperlink features are considered for classification	More highlights can be included alongside the hyperlinks, yet it will build the run-time multifaceted nature of the framework
Collaborative approach [13]	Classification accuracy is high	Complex and time-consuming	Not efficient
Security protocols [14]	Prevents users from phishing	Many users are unaware of security protocols	Effective from the users who have an idea of security protocols. User education can improve the efficiency of this method
Routine activity theory [15]	It helps to increase the chances of cyber-crime detection	Attackers cannot be caught easily. They are smart	It focuses on the methods to prevent cyber-crime

(continued)

Table 3 (continued)

Detection technique	Advantages	Disadvantages	Remarks
User education [16]	Simple technique	Cannot prevent all phishing attacks	Simple phishing attacks can be easily
URL-based phishing detection [2]	Simple and easy to implement	Classification accuracy is low, a large number of rules are needed to achieve high accuracy, but it will increase the run-time complexity	URL features are explored to prevent phishing
LinkGuard algorithm [4]	A robust algorithm, fewer false positives	Time-consuming	In this algorithm, the actual and visual links are compared. If the DNS names of both the links are the same, then the links are declared as legitimate
Features-based Approach [17]	Efficient	The feature set can be improved	Twenty-eight features are used as critical indicators of phishing. More features can be added to improve efficiency
Machine learning (SVM learning algorithm)-based phishing detection using features extractable from URLs [18]	Efficient (high detection rate, fewer false positives)	The feature set can be improved	Eighteen features are used as critical indicators of phishing. More features can be added to improve efficiency
Visual similarity assessment [11]	High accuracy	Time consuming	It highlights the main features of the webpages and calculates the similarity of the current website with the genuine webpage on the basis of design and style

Table 4 Comparison of different anti-phishing algorithms

Detection technique	Advantages	Disadvantages	Remarks
CANTINA [8]	Simple and easy to implement	High false positives	It is a content-based way that helps distinguishing phishing sites from genuine ones by using TF-IDF (term frequency-inverse document frequency) algorithm. It is a tedious methodology
CANTINA+ [9]	Low FP rate, good run-time speed	Cannot deal with image data	Feature set can be improved for better results
Intelligent phishing URL detection using association rule mining [10]	High detection rate	The feature set can be improved for better results	Spotlights on perceiving the huge highlights that separate among real and fake URLs. The main highlights are extracted. The standards acquired are deciphered to underscore the highlights that are increasingly predominant in phishing URLs
A secure and practical authentication scheme using personal devices [19]	High detection rate	High run-time complexity	Enables clients to dispose of numerous issues, for example, retaining usernames and passwords for various sites and frameworks. Lightweight cryptographic procedures or visual unscrambling and mark check can improve this plan
Effective defense schemes for phishing attacks on mobile computing platforms [20]	It does not depend upon HTML code	Less run-time speed	Utilizes OCR, which can precisely remove content from the screen capture of the login interface with the goal that the guaranteed personality can be confirmed
New rule-based phishing detection method [21]	High accuracy	Feature sets are totally relying upon the website page content	Cannot deal with phishing that is done through images

(continued)

Table 4 (continued)

Detection technique	Advantages	Disadvantages	Remarks
A new fast associative classification algorithm for detecting phishing websites [22]	High classification accuracy	Classification accuracy depends upon the feature selection method	The associative classification was used as a powerful administered learning approach to anticipate inconspicuous occurrences
Phishing threat avoidance behavior: An empirical investigation [23]	Designed a game for URL classification	More areas, identifying fake content, should be included to teach users	The main motive was to train users how to identify phishing URLs, which is one of many ways of identifying a phishing attack

Table 5 Comparison of different anti-phishing algorithms

Detection technique	Advantages	Disadvantages	Remarks
Statistical Twitter spam detection demystified: performance, stability, and scalability [24]	>90% of accuracy was achieved using C5.0 and random forest algorithms	Training dataset can be updated by adding more tweets	Random forest performed was found to be the most stable among all algorithms
A survey of phishing email filtering techniques [25]	This overview improves the comprehension of phishing messages issue, current arrangement space, and future phishing email recognition procedures	Discusses the detection techniques proposed till 2013	Discusses advantages and limitations of phishing email detection techniques proposed till 2013
Email classification research trends: review and open issues [26]	Analyzed email classification area, data sets, feature space, techniques used for classifying emails, and the significance of performance measures	Feature selection and email classification tools were not examined	Reviewed articles on the classification of e mails
Phishing susceptibility: An investigation into the processing of a targeted spear phishing email [27]	Provides a research model for email processing	Sample data is that of university students. The sample should be more representative	This is the first study that presents an empirical model for phishing and concludes the importance of two factors: visceral triggers and deception indicators

(continued)

Table 5 (continued)

Detection technique	Advantages	Disadvantages	Remarks
You are probably not the weakest link [28]	An automated model to predict user susceptibility	“Selection of features” can have some limitations. For example, security training is a high-level feature, the content of training should also be considered	Automates the prediction of user susceptibility to phishing attacks. Uses machine learning algorithms (random forest and logistic regression) for implementation
PhishStorm: detecting phishing with streaming analytics [29]	Classifies URL as fake or genuine	This technique cannot be applied to all types of URLs	Uses an approach based on intra-URL relatedness to classify URLs as phishing or legitimate. This technique is implemented using machine learning algorithms. The performance of the random forest algorithm comes out to be the best

Table 6 Comparison of different anti-phishing algorithms

Detection technique	Advantages	Disadvantages	Remarks
Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks [30]	Concludes that device affordances (uses of mobiles) enhance habituation	The number of design elements can be increased	Describes that device affordances stimulate heuristic processing and that uses of mobiles enhance habituation
PhiDMA: A phishing detection model with multi-filter approach [31]	Visually challenged people can utilize this model	This paper focuses only on phishing detection capabilities. Research should be done on phishing detection usabilities as well	Uses a hybrid approach to solve the phishing problem. It makes use of whitelist approach; heuristics approach, content-based approach, and string matching algorithm

(continued)

Table 6 (continued)

Detection technique	Advantages	Disadvantages	Remarks
Phishing websites features classification based on extreme learning machine [32]	Extreme learning machine came out to be the most accurate method when compared with traditional machine learning methods	Feature set should be improved	This study used 30 features and an extreme machine learning approach for classifying websites
Inside a phisher's Mind: Understanding the anti-phishing ecosystem through phishing kit analysis [33]	Analyzes main components of the anti-phishing ecosystem	The database used by APWG is partial for its partners	Pointed an image of an anti-phishing ecosystem from the viewpoint of culprits
Performance comparison of classifiers on reduced phishing website dataset [34]	Feature selection is used so as to reduce the dataset	Feature set should be improved to get better results	This study compared different anti-phishing algorithms on the basis of their performance on a reduced data set
Using URL shorteners to compare phishing and malware attacks [35]	Analyzed that phishing attacks have a shorter timespan than malware attacks	Flagged URLs no longer record new clicks	URL shortener click analytics is used to compare the lifecycle of phishing and malware attacks

5 Conclusion

This study explored various countermeasures of phishing programming procedures. A portion of the essential angles in estimating phishing countermeasures is as follows: The most recent phishing attack, which is termed as “zero-hour phishing attack,” is not caught by all countermeasures; a framework with a high false-positive rate may cause more damage than anything else. There are a number of approaches used as anti-phishing methods such as blacklist, whitelist, heuristics, content-based approach, visual similarity method, and machine learning algorithms. The machine learning method shows the best performance among all methods.

References

1. Mohammad, R.M., Thabtah, F., McCluskey, L.: Tutorial and Critical Analysis of Phishing Websites Methods, pp. 1–24. Elsevier (2015)
2. Waziri Jr., I.: Website forgery: understanding phishing attacks & nontechnical countermeasures. In: IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015
3. Khonji, M., Iraqi, Y., Jones, A.: Phishing detection: a literature survey. *IEEE Commun. Surv. Tutorials* **15**(4) (2013)
4. Shekokar, N.M., Shah, C., Mahajan, M., Rachh, S.: An ideal approach for detection and prevention of phishing attacks. *Proc. Comput. Sci.* 82–91 (2015) (Elsevier)
5. Nazreen Banu, M., Munawara Banu, S.: A comprehensive study of phishing attacks. *Int. J. Comput. Sci. Inf. Technol.* **4**(6), 783–786 (2013)
6. Gupta, S., Singhal, A., Kapoor, A.: A literature survey on social engineering attacks: phishing attack. In: International Conference on Computing, Communication and Automation, 2016
7. Jain, A.K., Gupta, B.B.: A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP J. Inf. Secur.* 1–11 (2016)
8. Zhang, Y., Hong, J., Cranor, L.: CANTINA: a content-based approach to detecting phishing web sites. In: ACM Proceedings of 16th International Conference on World Wide Web, pp. 639–648, May 2007
9. Xiang, G., Hong, J., Rose, C.P., Cranor, L.: CANTINA+: a feature-rich machine learning framework for detecting phishing web sites. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **14**(2), 1–32 (2011)
10. Carolin Jeeva, S., Rajsingh, E.B.: Intelligent phishing url detection using association rule mining. *SpringerOpen Hum. Centric Comput. Inf. Sci.* 1–19 (2016)
11. Liu, W., Deng, X., Huang, G., Fu, A.Y.: An antiphishing strategy based on visual similarity assessment. *IEEE Comput. Soc.* 58–65 (2006)
12. Chen, K.-T., Huang, C.-R., Chen, C.-S.: Fighting phishing with discriminative keypoint features. *IEEE Comput. Soc.* 56–63 (2009)
13. Nirmal, K., Janet, B., Kumar, R.: Phishing—the threat that still exists. In: IEEE International Conference on Computing and Communications Technologies, 2015
14. Iuga, C., Nurse, J.R.C., Erola, A.: Baiting the hook: factors impacting susceptibility to phishing attacks. *Hum. Cent. Comput. Inf. Sci.*, SpringerOpen (2016)
15. Choo, K.K.R.: The cyber threat landscape: challenges and future research directions. *Comput. Secur.* **30**, 719–731 (2011) (Elsevier)
16. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., Jerram, C.: The design of phishing studies: challenges for researchers. *Comput. Secur.* **52**, 194–206 (2015) (Elsevier)
17. Montazer, G.A., Yarmohammadi, S.A.: Identifying the critical indicators for phishing detection in iranian e-banking system. In: IEEE 5th Conference on Information and Knowledge Technology, 2013
18. Chu, W., Zhu, B.B., Xue, F., Guan, X., Cai, Z.: Protect sensitive sites from phishing attacks using features extractable from inaccessible phishing URLs. In: IEEE Communication and Information Systems Security Symposium, 2013
19. Althothaily, A., Chunquiang, Hu., Alwaris, A., Song, T., Cheng, X., Chen, D.: A secure and practical authentication scheme using personal devices. *IEEE Access* **5**, 11677–11687 (2017)
20. Wu, L., Du, X., Wu, J.: Effective defense schemes for phishing attacks on mobile computing platforms. *IEEE Trans. Veh. Technol.* (2015) (Accepted for publication)
21. Moghimi, M., Varjan, A.Y.: New rule-based phishing detection method. *Expert Syst. Appl.* (2016) (Accepted for publication)
22. Hadi, W., Aburub, F., Alhawari, S.: A new fast associative classification algorithm for detecting phishing websites. *Appl. Soft Comput.* **48**, 729–734 (2016) (Elsevier)
23. Arachchilage, N.A.G., Love, S., Beznosov, K.: Phishing threat avoidance behaviour: an empirical investigation. *Comput. Hum. Behav.* **60**, 185–197 (2016)

24. Lin, G., Sun, N., Nepal, S., Zhang, J., Xiang, Y., Hassan, H.: Statistical twitter spam detection demystified: performance, stability and scalability. *IEEE Access, Special Section on Big Data Analytics in Internet of Things and Cyber-physical Systems* **5**, 11142–11154 (2017)
25. Almomani, A., Gupta, B.B., Atawneh, S., Meulenberg, A., Almomani, E.: A survey of phishing email filtering techniques. *IEEE Commun. Surv. Tutorials* **15**(4) (2013)
26. Mujtaba, G., Shuib, L., Raj, R.G., Majeed, N., Al-Garadi, M.A.: Email classification research trends: review and open issues. *IEEE Access* **5**, 9044–9064 (2017)
27. Wang, J., Herath, T., Chen, R., Vishwanath, A., Raghav Rao H.: Phishing susceptibility: an investigation into the processing of a targeted spear phishing email. *IEEE Trans. Prof. Commun.* **55**(4), 345–362 (2012)
28. Heartfield, R., Loukas, G., Gan, D.: You are probably not the weakest link: towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access* **4**, 6910–6928 (2016)
29. Marchal, S., François, J., State, R., Engel, T.: PhishStorm: detecting phishing with streaming analytics. *IEEE Trans. Netw. Serv. Manage.* **11**(4) (2014)
30. Vishwanath, A.: Mobile device affordance: explicating how smartphones influence the outcome of phishing attacks. *Comput. Hum. Behav.* **63**, 198–207 (2016)
31. Sonowal, G., Kuppusamy, K.S.: PhiDMA—a phishing detection model with multi-filter approach. *J. King Saud Univ. Comput. Inf. Sci.* 1–14 (2017)
32. Sönmez, Y., Tuncer, T., Gökal, H., Avcr, E.: Phishing web sites features classification based on extreme learning machine. In: 6th International Symposium on Digital Forensic and Security, pp. 1–5, 2018
33. Oest, A., Safei, Y., Doupé, A., Ahn, G.-J., Wardman, B., Warner, G.: Inside a phisher's mind: understanding the anti-phishing ecosystem through phishing kit analysis. In: APWG Symposium on Electronic Crime Research, pp. 1–12, 2018
34. Karabatak, M., Mustafa, T.: Performance comparison of classifiers on reduced phishing website dataset. In: IEEE, pp. 1–5, 2018
35. Le Page, S., Jourdan, G.-V., Bochmann, G.v., Flood, J., Onut, I.-V.: Using URL shorteners to compare phishing and malware attacks. In: IEEE, pp. 1–13, 2018

Assessment of Open Source Tools and Techniques for Network Security



U. Guru Prasad, R. Girija , R. Vedhapriyavadhana ,
and S. L. Jayalakshmi 

Abstract Providing network security with an open source has been a huge concern today. Data transmitted over the network shall not be assumed to be stable. There are numerous attacks such as phishing, spoofing, and sniffing. This paper provides a summary of the tools available to fight against these network attacks and threats. There are several resources in the open source that are built to use to handle these threats. Resources including OpenSSH, OpenSSL, NMap, digital certificate, and IP tables were discussed in this article.

Keywords OpenSSH · OpenSSL · NMap · Digital certificate · IP tables

1 Introduction

Networks are easily vulnerable to multiple threats due to the exponential growth of the Internet and e-commerce [1]. Undoubtedly, the Internet has created a big infrastructure in the world that makes and supports both personal and technical statements around the world. Wide use of the Internet work by consumers has opened the door to a number of threats. The effects of the attacks are rising rapidly. There are a lot of data breaches going on in the Internet world. Network security consists of measures implemented to avoid and track the denial of entry to the computer network, permitted entry, manipulation, and misuse of the computer. It is the method of utilizing applications and physical prevention. Measures are to

U. Guru Prasad (✉) · R. Girija · R. Vedhapriyavadhana · S. L. Jayalakshmi
Vellore Institute of Technology, Chennai Campus, Chennai, India
e-mail: guru.prasad2018@vitstudent.ac.in

R. Girija
e-mail: girija.r@vit.ac.in

R. Vedhapriyavadhana
e-mail: vedhapriyavadhana.r@vit.ac.in

S. L. Jayalakshmi
e-mail: jayalakshmi.sl@vit.ac.in

safeguard the underlying networking system against unwanted entry, misuse, degradation, change, loss, or inappropriate disclosure, providing a safe computing interface.

The purpose of network protection is to have permission to access data on a network. Network protection begins with verification and is supported with a username and password. Another means of delivering protection uses a firewall. Firewall enforces access rules such as which resources should be reached by the network administrator. Thus, security of the computer is vulnerable (weakness in the network) and leads to misuse of the network by the hackers [2]. To prevent the network from various attacks such as phishing, spoofing, and sniffing, various security tools are used. There are several security tools in the open source that are built to use to handle these threats and attacks. This review gives an overview of a few security tools which are highly used by network professionals. Some tools used include OpenSSH, OpenSSL, NMap, digital certificate, and IP tables [3].

2 Network Security Tools: Overview

2.1 *OpenSSH*

OpenSSH (popularly known as OpenBSD Secure Shell) is a package of secure networking utilities based on the secure shell protocol [4]. It is commonly used to provide a secure channel, for multiple parties, over an unsecured network using client–server architecture. Unlike most GUI based tools, OpenSSH is not a single computer program, but a bundle of programs that serve as a better alternative to the various unencrypted connectivity protocols like Telnet and FTP. OpenSSH is built-in into several operating systems, mostly macOS and almost all Linux operating systems by default. As it is a terminal-based tool, this is expected. OpenSSH or SSH, as it is generally referred to, has a variety of operations available. We can execute shell commands in the same way as we would if we were physically operating the remote computer.

SSH utilizes various encryption algorithms like—Symmetric Encryption, Asymmetric Encryption, and Hashing. It can easily transfer files using the associated SSH protocols such as SSH file transfer protocol (SFTP) or secure copy protocol (SCP). SSH works by trying a client–server model to allow for authentication of two remote systems and thus encryption of the data that will pass between them. SSH operates on TCP port 22 by default (however, this can be changed if needed, as demonstrated in the presentation). The host (server) listens on port 22 for any inbound connections. It starts the secure connection by first authenticating the client and only then opening the correct shell environment if the verification is successful. Now, there are two major stages in establishing a connection: First, both the systems must agree upon an encryption standard, so that the unknown client can be added to the known clients' list for future reference. Second, the user must authenticate themselves [5].

2.1.1 Output

Become root user in the client system: Command: `sudo -i`, (Option: `-i` login).

By becoming a root user, the user can accomplish any task on the remote system as the root user group has all permissions and access rights enabled. The root user can also add other users to the group. It can also allow for other client systems to connect to the server system.

Debug Mode ON: SSH-ing to the server system through client system to get a detailed explanation of how the systems are reacting to form the SSH connection, Command: `ssh -v fv@127.0.0.1 -p 2222`

Options: `-v`—Verbose-list out all background details, `fv`—Server System Name, `127.0.0.1`—Server IP address, `-p`—To set custom port number , `2222`—Custom Post Number (Fig. 1).

```
debug1: key_load_public: No such file or directory
debug1: identity file /home/sagarika/.ssh/id_ed25519 type -1
debug1: identity file /home/sagarika/.ssh/id_ed25519-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
debug1: Remote protocol version 2.0, remote software version OpenSSH_8.0
debug1: match: OpenSSH_8.0p1 Ubuntu-6ubuntu0.1 pat OpenSSH* compat 0x040
debug1: Authenticating to 127.0.0.1:2222 as 'fv'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ecdsa-sha2-nistp256 SHA256:+ZFYP0k+sH1pDVF+jrnR
debug1: Host '[127.0.0.1]:2222' is known and matches the ECDSA host key.
debug1: Found key in /home/sagarika/.ssh/known_hosts:4
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<ssh-ed25519,ssh-rsa,rsa-sha
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Trying private key: /home/sagarika/.ssh/id_rsa
debug1: Trying private key: /home/sagarika/.ssh/id_dsa
debug1: Trying private key: /home/sagarika/.ssh/id_ecdsa
debug1: Trying private key: /home/sagarika/.ssh/id_ed25519
debug1: Next authentication method: password
fv@127.0.0.1's password:
debug1: Authentication succeeded (password).
Authenticated to 127.0.0.1 ([127.0.0.1]:2222).
debug1: channel 0: new [client-session]
```

Fig. 1. Displays the output of SSH

SSH Custom Key Generation: Command: `ssh-keygen`

Option: `-keygen`—To generate custom key, Passphrase is optional.

Web sites such as GitHub and Heroku often ask for an SSH public key, so that we can push/deploy code without entering a password. This can be generated using the `ssh-keygen` command. The RSA key pair is stored in the home directory under `.ssh` directory (Fig. 2).

Service Command to check the status: Command: `service ssh status`.

The service command can be used to check the status of the service of your choice. Apart from status, it can also be used to start, stop and restart the said service through the terminal with the following syntax.

`service ssh stop`, `service ssh restart`, `service ssh stop`.

The status screen also shows the last interactions with the particular service that took place in the current login session. It gives a variety of information such as Process Name, Main Process ID, Tasks performed, Memory consumed, Doc files or associated Man pages to name a few.

SSH Secure Copy: Command: `scp filename username@hostname:destination_path`.

Alternatively, `scp filename from_destination to_destination`, can also be used.

```
fv@fv-VirtualBox:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/fv/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/fv/.ssh/id_rsa.
Your public key has been saved in /home/fv/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:M1ai7AaoUxfcrdQNgje3hH3GZAZHQz/a7Sc2CklyDxg fv@fv-VirtualBox
The key's randomart image is:
+---[RSA 3072]---+
|      ..oo*0      |
|    ...+++*+0     |
|   o.o+E+o o      |
|  . + o.= o o     |
| o o + S = . .    |
| o . o . * + .    |
|o   o o . = .     |
| .   .   . o +    |
|                   |
+---[SHA256]-----+
fv@fv-VirtualBox:~$
```

Fig. 2 Service command

2.2 Open SSL

OpenSSL might be termed as a strong, business-grade, and feature-rich tool-set used for the transport layer security (TLS) and secure sockets layer (SSL) protocols [6]. It is also a general-purpose cryptography library. OpenSSL may be a cryptography software library or tool set that creates connections between computer networks safely. This is a command-line based tool for using various cryptographic functions of OpenSSL's cryptolibrary from the shell. OpenSSL is a software library for applications that protect connections over computer networks against intrusion or need to recognize the party at the other end. It is extensively employed by Internet servers, including the bulk of HTTPS Web sites [7]. The core library, written within the C programming language, executes basic cryptographic functions and provides various utility functions.

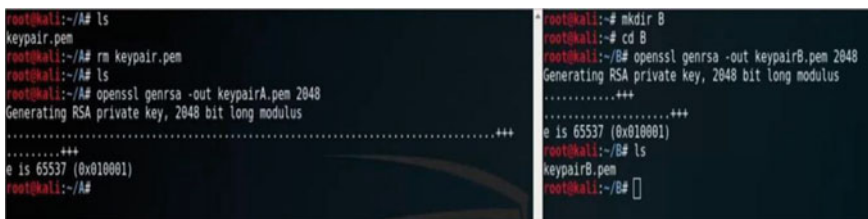
2.2.1 Output

Public key cryptography: In this type of cryptography, two keys are used—one key for encryption and the other key for decryption. It is used for authentication and confidentiality [8]. The first key is a public key that is available to everyone, and the second key is the private key which is kept as secret and known only to the owner who generated the key pair (Fig. 3).

Command for Creating Private Keys: openssl genrsa -out keypairA.pem 2048.

Command for Creating Public keys: openssl rsa -in keypairA.pem -pubout -out publicA.pem.

Command for Creating Public keys: openssl rsa -in keypairA.pem -pubout -out publicA.pem, openssl rsautl -decrypt -in received -out msg -inkey keypairB.pem (Figs. 4 and 5).



```

root@kali:~/# ls
keypair.pem
root@kali:~/# rm keypair.pem
root@kali:~/# ls
root@kali:~/# openssl genrsa -out keypairA.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 (0x010001)
root@kali:~/#

root@kali:~/# mkdir B
root@kali:~/# cd B
root@kali:~/B# openssl genrsa -out keypairB.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
root@kali:~/B# ls
keypairB.pem
root@kali:~/B#
  
```

Fig. 3 OpenSSL—key pair generation

2.3 *N-Map*

It is a network scanner used to find hosts and services on a network by sending packets and analyzing the response [9]. Network administrators use this to discover the devices running on their systems, identify hosts and the services, discovering open ports, and identifying security risks. It is used to look after single hosts and vast networks which in turn look after hundreds of thousands of devices and subnets. It is free and open source and extremely flexible, but deep down it is a port scanning tool. It used to gather information on whether the ports are opened or closed by sending raw packets to system ports as well as listens for responses. Likewise, it can also be called port discovery or enumeration [10].

2.3.1 Output

There are four types of output formats in N-Map in which the interactive output is saved to a file. N-Map output may be manipulated by text processing software, enabling the user to form customized reports [11].

Interactive: When a user runs N-Map from the terminal, it is updated in real-time. Various options are entered during the scan to facilitate monitoring.

XML: A format that will be further processed by XML tools. It will be converted into an HTML report using XSLT.

Grepable: Output that is tailored to line-oriented processing tools like grep, sed, or awk. **Normal:** The output as seen while running N-Map from the terminal, but saved to a file.

N-Map [9] present Scans: Intense scan - Command: `Nmap -T4 -A -v`, this scan is reasonably quick and is used to scan the most used TCP ports, which will help in determining the OS type and what services and their versions are running. Intense scan plus UDP - Command: `Nmap -sS -sU -T4 -A -v`, this command is similar to the regular intense scan, the difference is that it will also scan the UDP ports (-sU). Intense scan, all TCP ports—Command: `Nmap -p 1-65,535 -T4 -A -v`, this command checks all the TCP ports without leaving anything unchecked. Ping scan Command: `Nmap -sn`, This command is used to ping on the target network and does not do a port scan. Quick scan—Command: `Nmap -T4 -F`, this command is used to scan the TCP ports faster than the intense scan by constraining the number of TCP ports to be scanned to only the top 100 most used TCP ports. Quick traceroute—Command: `Nmap -sn -traceroute`, This option is used when you need to list hosts and routers in a network scan. It will traceroute and ping all hosts defined within the target. Regular scan—Command: `Nmap`, this command is used for TCP SYN scan for the most used 1000 TCP ports by using an ICMP echo request (ping) to detect the host. Slow comprehensive scan—This command is used to detect the host with an immense amount of effort without giving up even if the first ping request fails. TCP, UDP, and SCTP are the protocols used to detect the host. Quick scan plus—Command: `Nmap -sV -T4 -O -F`.

```

admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
admin@ip-172-26-0-73:~$

```

Fig. 6 N-Map

–Version-light+, this command is used to detect the operating system and the version (Fig. 6).

Port Scan—To scan a single port—use -p: Nmap -p 53 192.168.1.8,

To scan a single port when the port number is specified: Nmap -p T:7777, 973 192.164.0.1,

To scan a range of ports—separate it by a hyphen: Nmap -p 76–973 192.164.0.1

To scan the top port of a scan—use –top-ports flag: Nmap –top-ports 10 scanme.nmap.org (Fig. 7).

2.4 IPTables

It is a utility program that is used by the system administrator to set the IP packet filtering rules in the Linux kernel firewall, and it is also implemented as various Netfilter modules [12]. All these filters are arranged in different tables, which has the rules on how to filter network traffic packets. Various kernel modules and programs are used now for different protocols like IPv4 uses iptables, IPv6 uses ip6tables, ARP uses arp tables, and Ethernet frames uses the ebtables. They need high privileges to operate and should be executed by the root user, otherwise, it might fail to function. On most Linux kernel, iptables are installed in /usr/sbin/iptables and documented in man pages. These pages can be opened using iptables after installing. It can also be found in /sbin/iptables, because iptables is like a service rather than an “essential binary,” the preferred location remains /usr/sbin. iptables that allow the system administrator to define the tables which have the rules on how to treat the packets. Each table is linked with a different way of treating the packet which is processed by sequentially following the rules. A rule in a chain can cause a jump to another chain, and this can be repeated to any level depending on the desired nesting. (A jump is like a “call,” i.e., the point that was jumped from is remembered.) Every packet that is entering or leaving the device will traverse at least one chain. The source of the packet shows which chain it traverses in the

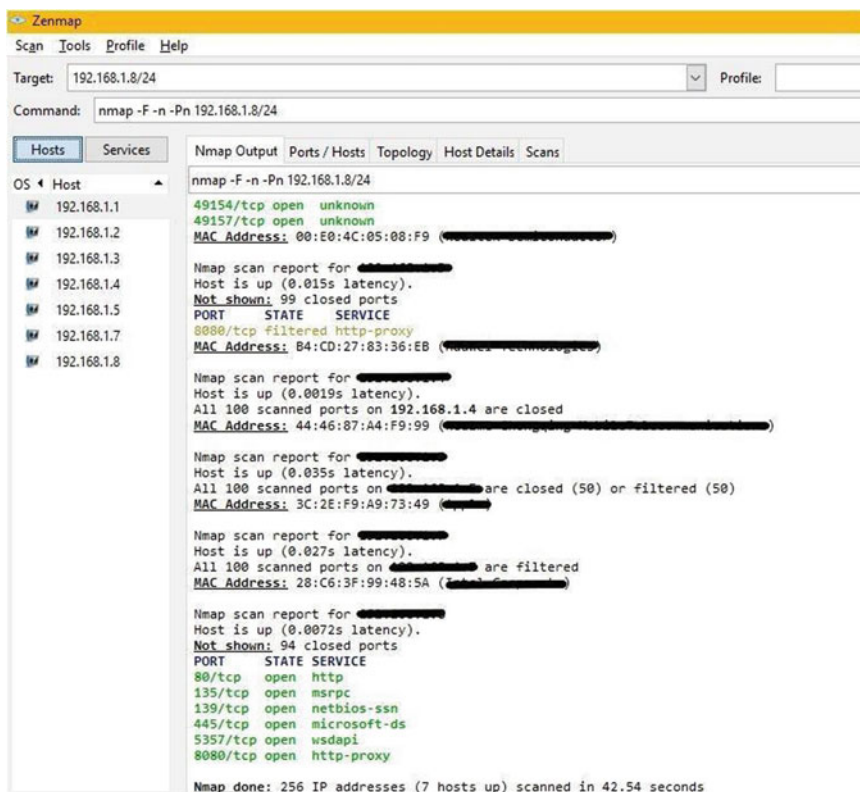


Fig. 7 Port scan—network map

beginning. There are five types of pre-defined chains which has a policy, like DROP, which is added to the packet when it reaches the end of the rule chain. The system administrator has the privilege to create as many chains as they want. These chains do not have a policy; if a packet reaches the end of the chain and then returns to the initial chain, this type of chain might be empty.

2.4.1 Features

It uses the concept of having a separate rule table for various types of packet processing functionality. The three types of primary modules are the rule filter table, the NAT table, and the packet-handling mangle table. Module extensions are dynamically loaded when it will be first referenced unless you have built them directly into the Linux kernel for each of these table modules. The filter table is the default table, and other tables are specified by a terminal option. The features in the filter table are chain-related operations on the built-in chains that are INPUT,

OUTPUT, and FORWARD and on user-defined chains that are help and target disposition (ACCEPT or DROP). The IP header field has similar operations for protocol, source, and destination address. The packet also contains input and output interfaces, and matches operations on the TCP, UDP, and ICMP header fields.

2.4.2 Output

Packet Processing In IP tables: IP tables are complex for beginners. There are three built-in tables for processing: (1) MANGLE: it is used to manipulate QoS bits in TCP header, (2) FILTER: it is used for packet filtering and has three built-in chains containing the firewall policy rules and (3) Forward chain: it is used to filter the packets that are sent to servers protected by a firewall, Input chain: Filters packets destined for the firewall- Input chain: Filters packets originating from the firewall, (4) NAT: network addresses translation has two built-in chains. Pre-routing: it is used when the destination address is needed to change in NAT packets, and Post-routing: it is used when the source address is needed to change in NAT packets (Figs. 8 and 9).

Processing For Packets Routed By The Firewall 1/2			
Queue Type	Queue Function	Packet transformation chain in Queue	Chain Function
Filter	Packet filtering	FORWARD	Filters packets to servers accessible by another NIC on the firewall.
		INPUT	Filters packets destined to the firewall.
		OUTPUT	Filters packets originating from the firewall
Nat	Network Address Translation	PREROUTING	Address translation occurs before routing. Facilitates the transformation of the destination IP address to be compatible with the firewall's routing table. Used with NAT of the destination IP address, also known as destination NAT or DNAT .

Fig. 8 IP config table

Processing For Packets Routed By The Firewall 2/2

		POSTROUTING	Address translation occurs after routing. This implies that there was no need to modify the destination IP address of the packet as in pre-routing. Used with NAT of the source IP address using either one-to-one or many-to-one NAT. This is known as source NAT , or SNAT .
		OUTPUT	Network address translation for packets generated by the firewall. (Rarely used in SOHO environments)
Mangle	TCP header modification	PREROUTING POSTROUTING OUTPUT INPUT FORWARD	Modification of the TCP packet quality of service bits before routing occurs (Rarely used in SOHO environments)

Fig. 9 IP config table (continued)

3 Conclusion

The reliability of the network is the biggest concern these days. While the open source is deemed stable, the data exchanged over the network is still not safe. This paper reviews some network security tools for handling various types of attacks and threats on the Internet. This paper discusses various tools with their features and their structure with respect to different types of network attacks.

References

1. Kumar, S.N.: Review on network security and cryptography. Int. Trans. Electr. Comput. Eng. Syst. **3**(1), 1–11 (2015)
2. Dowd, P.W., McHenry, J.T.: Network security: it’s time to take it seriously. Computer **31**(9), 24–28 (1998)
3. Kartalopoulos, S.V.: Differentiating data security and network. In: Conference on Differentiating Data Security and Network, pp.1469–1473, 19, 23 May 2008
4. Hofstede, R., Hendriks, L., Sperotto, A., Pras, A.: SSH compromise detection using NetFlow/IPFIX. ACM SIGCOMM Comput. Commun. Rev. **44**(5), 20–26 (2014)
5. Alsaadi, H.H., Aldwairi, M., Taei, M.A., Albuaainain, M.: Penetration and security of OpenSSH remote secure shell service on raspberry pi. In: International Conference on New Technologies, Mobility & Security (NTMS’18), February 2018
6. Viega, J., Messier, M., Chandra, P.: Network Security with OpenSSL: Cryptography for Secure Communications. O’Reilly Media, Inc. (2002)

7. Chordiya, A.R., Majumder, S., Javaid, A.Y.: Man-in-the-middle (MITM) attack based hijacking of HTTP traffic using open source tools. In: IEEE International Conference on Electro/Information Technology (EIT), 2018
8. Großschädl, J., Kizhvatov, I.: Performance and security aspects of client-side SSL/TLS processing on mobile devices. In: International Conference on Cryptology and Network Security, pp. 44–61, 2010
9. Calderon, P.: Nmap: Network Exploration and Security Auditing Cookbook. Packt Publishing Ltd. (2017)
10. Sarmiento, O.P., Guerrero, F.G., Argote, D.R.: Basic security measures for IEEE 802.11 wireless networks. *Revista Ingeniería E Investigación* **28**(2), 89–96 (2008)
11. Bagyalakshmi, G., Rajkumar, G., Arunkumar, N., Easwaran, M., Narasimhan, K., Elamaram, V., Ramirez-Gonzalez, G.: Network vulnerability analysis on brain signal/image databases using Nmap and Wireshark tools. *IEEE Access* **6**, 57144–57151 (2018)
12. AL-Musawi, B.Q.M.: Mitigating DoS/DDoS attacks using iptables. *Int. J. Eng. Technol* **12**(3), 101–111 (2012)

A Detailed Comparative Study and Performance Analysis of Standard Cryptographic Algorithms



Chetan Rathod and Atul Gonsai

Abstract Nowadays the most important issue we face during data transmission and exchanging of data is security of data. The cryptographic algorithms play very significant role to secure data. By using different algorithms, it improves security of data by making data unreadable, only the authenticate users can read data after decryption using keys. All algorithms perform same work, but consume different volume of computing properties such as time of CPU, memory utilization, throughput time, encryption and decryption time, simulation etc. Also different algorithms use various size of keys, size of block and cipher type. So we need to compare the cryptographic algorithms to choose the best one. In this paper, we have done the evaluation of both block cipher (AES, DES, 3DES, Blowfish) as well as stream cipher (SALSA20) cryptographic algorithms is shown by taking different size of audio files. This comparison of different algorithms has been conducted to evaluate parameters such as encryption/decryption time, throughput time, memory utilization, scalability and ratio. Simulation results are given to demonstrate the efficiency of each. This research contributes to identify state of the art cryptographic technique.

Keywords Encryption • Decryption • Cryptography • Cipher • AES • 3DES • Blowfish • SALSA20

1 Introduction

Encryption means coding and decryption means decoding, by this technique, we can protect our information through transmission so that only authorized user can read the data and data can be prevented from being misused. If data goes to the unauthorized user, there can be a chance to read and misuse it [1]. That is why we translate our data into unreadable form by encryption and in decryption it will be convert into readable form. In other word, we can say that by encryption, plain text

C. Rathod (✉) • A. Gonsai

Department of Computer Science, Saurashtra University, Rajkot, India

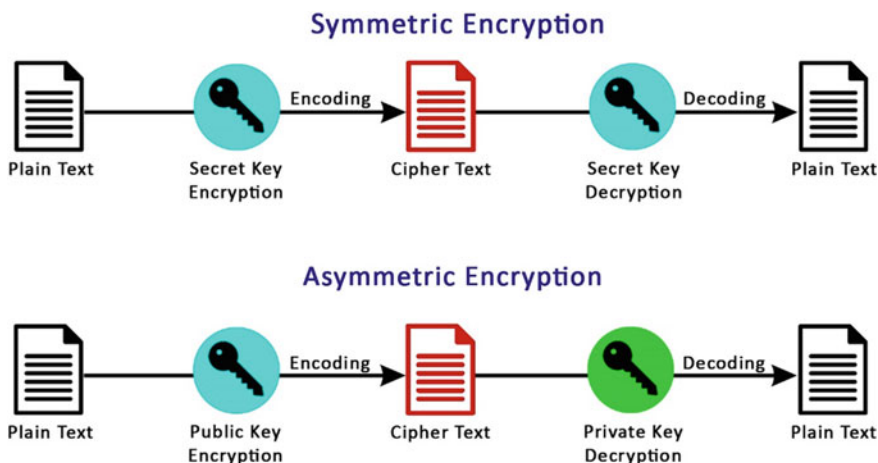


Fig. 1 Symmetric versus asymmetric encryption [2]

will be converted into cipher text and in decryption, cipher text will be converted into plain text. Only authorized user who has the key, they can read the message, e.g., original message is “ABCD” after encryption it will be “1234,” if someone got the message through transmission, they will get “1234,” not “ABCD” but if someone has the key then they can convert your encrypted message (“1234”) into original form (“ABCD”). This method is known as encryption/decryption or cryptography [2, 3].

Figure 1 shows that there are no. of algorithms available for encryption/decryption [4]. Two different techniques are available for cryptography: Symmetric and Asymmetric. In symmetric, only one key (private) is used and in asymmetric two keys (private and public) are used [5]. There are two types of cipher text: block cipher and stream cipher [6]. Apart from that different parameters like methods (structures), no. of rounds, different kind of P-Arrays and S-Boxes will be considered to select the best algorithm for encryption/decryption. Each has its own unique features and specialties like speed, memory utilization, security level, throughput time, encryption ratio etc. these parameters are also considered for selecting an algorithm.

2 Literature Review of Standard Algorithms

2.1 Aes: [3, 6–8]

AES means advanced encryption standard is a block cipher algorithm in symmetric category for encryption as well as decryption. In 1998, it was established by Daemen and Vincent Rijmen. It is a commonly used encryption algorithm. AES performs encryption on plain text and decryption on ciphertext of 128 bits with the same

key at both side. It is 128 bits block size algorithm which has variable length key size (128, 192, 256 bits). Key size decides the rounds for encryption and decryption.

- 128 bits = 10 cycles
- 192 bits = 12 cycles
- 256 bits = 14 cycles

2.2 *Blowfish: [3, 6–8]*

In 1993, Bruce Schneier designed Blowfish algorithm for encryption. It is a symmetric block cipher technique. It has key size 32–448 bits with same key at both side and 64 bits block size. Blowfish has feistel network of 16 rounds with XOR operation in each round. It has key expansion technique. This algorithm contains P-Array and S-Boxes. P-Array consists 18 sub keys each of 32 bits. S-Boxes contain 256 entries each of 32 bits. Blowfish is faster and secure algorithm.

2.3 *Des: [3, 6, 7]*

In March 1975, data encryption standard developed by IBM later adopted in 1977 by NIST. For encryption, DES is mostly used algorithm. DES is block cipher algorithm with 64 bits key size. It is symmetric algorithm for input it takes 64 bits plain text and gives 64 bits ciphertext as an output. DES contains 16 Round. Each block is divided into each of two 32 bits block L and R (Left and Right). This algorithm is not robust enough. Some attacks noted against DES algorithm.

2.4 *Triple DES: [7, 9]*

It is an advanced form of DES created by IBM in 1978. With long key size, it is created by using same rules of DES. Performance of triple DES is twice it means it has 48 rounds that is why it is slower than DES, but it is more secure than DES. 3DES is block cipher algorithm including key size of 192 bits and block size of 64 bits. In terms of power consumption, its performance is low compared to DES. It is symmetric block cipher algorithm. Several attacks also recorded against it.

Table 1 Comparison of algorithms with various parameters

Algorithms	Key size	Block size	Cipher type	Rounds	Structure	No of S-Boxes
AES	128–192–256 bits	128 bits	Block	10, 12, 14	Substitution-permutation network	1
DES	64 bits	64 bits	Block	16	Feistel	8
3DES	192 bits	64 bits	Block	48	Feistel	8
Blowfish	32–448 bits	64 bits	Block	16	Feistel	4
SALSA20	256 bits	N/A	Stream	20	ARX	0

2.5 Salsa20: [10, 11]

Salsa20 is come in stream cipher category’s algorithm developed by Daniel J. Bernstein for encryption submitted to eSTREAM. Salsa20 used the key of 256 bits, 64 bits nonce and a 64 bits position of stream to a 512 bits block of the keystream. It used pseudorandom function based on add rotate xor(ARX) operations 32 bits addition, bitwise addition (XOR) and rotation operations. The user can seek to any position in the keystream constant time. Some attacks noticed.

In this paper, we have compared various parameters like key size, block size, cipher type, no. of rounds, no. of S-boxes and structure of these algorithms. Following Table 1 shows details of this.

Nowadays in the era of multimedia security of data transmission is very annoying task in any format of data required more secure algorithm they may be in a form of text, image, audio or video. In this paper, we used different cryptographic algorithms for audio files.

3 Research Methodology

Here, we used five most common security algorithms in this program for encoding and decoding (Blowfish, AES, DES, Triple DES and SALSA20). A computer having Intel® Core™ i5-4210U CPU @1.70 GHz 2.40 GHz with 4 GB RAM and 64-bit operating system (Windows 10 Home). Python 3.7.2 (64 Bit) used to developed and run programs for the algorithms. Blowfish, AES, DES, Triple DES and SALSA20 cryptographic algorithms were implemented using Python programming language on the same programming environment. Program consists of three phases: (1). Key generation, (2). Encryption and (3). Decryption. It also checks encryption/decryption time, memory utilization during encryption/decryption, scalability of algorithms along with throughput and encryption ratio of all algorithms. The Python program took as individual inputs for five different size audio file, the sizes (463.77, 777.52 KB, 2.08, 11.2 and 24.03 MB) of mp3

format for each algorithm. The time of encryption and decryption, memory utilization, throughput scalability and ratio for each algorithm and for each size of audio files were recorded. We also compared various parameters (key size, block size, cipher type, no. of rounds, no. of S-boxes and structure of these algorithms.

3.1 Outcome of Research: A Comparative Study

Tables 2, 3, 4, 5 and 6 show the detailed comparative study of the audio encryption using different standard algorithms. As the tables showcases that there are mainly seven parameters and five standard algorithms using which we have carried out comparison. The results are as follows.

Table 2 Algorithms with various parameters for audio file of 463.77 KB

Algorithms	Enc. Time (s)	Dec time (s)	Memory utilization (Enc.)	Memory utilization (Dec.)	Loss	Throughput (MB/s)	Enc. ratio
AES	0.007943392	0.196688175	1,544,192	385,024	No	58.38400166	1
DES	0.036031008	0.039975405	1,011,712	221,184	No	12.87133024	1
3DES	0.040014982	0.079990149	466,944	294,912	No	11.58983396	1
Blowfish	0.0119977	0.020001411	274,432	135,168	No	38.65465966	1
SALSA20	0.004013062	0.053800344	626,688	487,424	No	115.5643883	1

Table 3 Algorithms with various parameters for audio file of 777.52 KB

Algorithms	Enc. time (s)	Dec time (s)	Memory utilization (Enc.)	Memory utilization (Dec)	Loss	Throughput (MB/s)	Enc. ratio
AES	0.011958599	0.087993145	487,424	294,912	No	65.01806726	1
DES	0.039977074	0.040005445	1,482,752	270,336	No	19.44927251	1
3DES	0.095997572	0.152122021	991,232	573,440	No	8.099423603	1
Blowfish	0.01997304	0.028001785	282,624	544,768	No	38.92872665	1
SALSA20	0.011981726	0.020003796	532,480	294,912	No	64.89257223	1

Table 4 Algorithms with various parameters for audio file of 2.08 MB

Algorithms	Enc. time (s)	Dec time (s)	Memory utilization (Enc.)	Memory utilization (Dec)	Loss	Throughput (MB/s)	Enc. ratio
AES	0.028020382	0.092093229	3,837,952	5,763,072	No	74.28521158	1
DES	0.083986282	0.088006973	3,551,232	2,228,224	No	24.78380923	1
3DES	0.192012787	0.196011305	2,424,832	2,269,184	No	10.84042388	1
Blowfish	0.060003757	0.132009983	1,019,904	1,990,656	No	34.68949425	1
SALSA20	0.040008545	0.043998003	3,416,064	2,375,680	No	52.02638596	1

Table 5 Algorithms with various parameters for audio file of 11.2 MB

Algorithms	Enc. time (s)	Dec time (s)	Memory utilization (Enc.)	Memory utilization (Dec)	Loss	Throughput (MB/s)	Enc. ratio
AES	0.144010544	0.196668625	16,207,872	11,038,720	No	77.78214499	1
DES	0.392023563	0.384027004	11,993,088	4,034,560	No	28.57340743	1
3DES	0.969902039	0.961265564	11,988,992	847,872	No	11.54905192	1
Blowfish	0.272023439	0.272011042	12,107,776	5,242,880	No	41.17824929	1
SALSA20	0.152007341	0.159998655	8,339,456	11,202,560	No	73.69018429	1

Table 6 Algorithms with various parameters for audio file of 24.03 MB

Algorithms	Enc. time (s)	Dec time (s)	Memory utilization (Enc.)	Memory utilization (Dec)	Loss	Throughput (MB/s)	Enc. ratio
AES	0.461263657	0.428479433	17,313,792	17,940,480	No	52.10560307	1
DES	1.001013756	0.976339817	4,653,056	8,269,824	No	24.01008064	1
3DES	2.445178032	2.23591423	2,805,760	5,480,448	No	9.82931332	1
Blowfish	0.768339396	0.742202282	5,570,560	18,096,128	No	31.28099527	1
SALSA20	0.464538336	0.504232883	7,483,392	17,801,216	No	51.73829402	1

4 Conclusion

According to the result of this program (Tables 2, 3, 4, 5 and 6), in encryption AES takes least time and then the less time consuming algorithm is Salsa20, but Salsa20 is stream cipher so according to cipher text Blowfish is second less time taking algorithm in block cipher. In decryption, Salsa20 takes least time, but according to cipher text Blowfish is the least time consuming algorithm and AES stands after blowfish in less time consuming algorithm in block cipher. In memory utilization, the best algorithm is Blowfish in both encryption and decryption and then after 3DES comes. According to throughput of above result the fastest algorithm is AES and then, followed by Salsa20, but when we consider according to block cipher, Blowfish will stand after AES in less time consuming algorithm.

References

1. Mota, A.V., Azam, S., Shanmugam, B., Yeo, C., Kannoorpatti, K.: Comparative analysis of different techniques of encryption for secured data transmission. In: IEEE International Conference on Power, Control Signals and Instrumentation Engineering, pp. 231–237, 2017
2. Dhanalaxmi, B.: Multimedia cryptography—a review. In: 2017 IEEE International Conference on Power, Control Signals and Instrumentation Engineering, pp. 764–766, 2017
3. Survey, R.C.A., Princy, P.: A comparison of symmetric key algorithms DES, AES, Blowfish. *Int. J. Comput. Sci. Eng. Technol.* **6**(5), 328–331 (2015)

4. Access, O.: International journal of computer sciences—comparative analysis on different parameters of encryption algorithms for information security. *JCSE. Eng.* **4**, 76–82 (2014)
5. Jeeva, A.L.: Comparative analysis of performance efficiency and security measures of some encryption algorithms. *IJERA* **2**(3), 3033–3037 (2012)
6. Thakur, J., Kumar, N.: DES, AES and Blowfish : symmetric key cryptography algorithms simulation based performance analysis. *IJETAE* **1**(2), 6–12 (2011)
7. Nadeem, A., Javed, M.Y.: Performance Comparison of Data. *IEEE*, Sept 2005
8. Mahamat, Y., Othman, S.H., Siraj, M., Nkama, H.: Comparative study Of AES, Blowfish, CAST-128 and DES encryption algorithm international organization of scientific research international organization of scientific research. *IOSR J. Eng.* **6**(6), 1–7 (2016)
9. Jun, Y., Na, L., Jun, D.: A design and implementation of high-speed 3DES algorithm system. *IEEE*, pp. 175–178 (2009). <https://doi.org/10.1109/FITME.2009.49>
10. Afdhila, M.D., Nasution, S.M., Azmi, F.: Implementation of stream cipher Salsa20 algorithm to secure voice on push to talk application. In: *IEEE Asia Pacific Conference on Wireless and Mobile Implement*, pp. 137–141, 2016
11. Panda, M., Nag, A.: Plain text encryption using AES, DES and SALSA20 by java based bouncy castle API on windows and linux. In: *Proceedings of 2015 2nd IEEE International Conference on Advance Computing and Communication Engineering, ICACCE 2015*, pp. 541–548, 2015. <https://doi.org/10.1109/ICACCE.2015.130>

Secured Communication Using Virtual Private Network (VPN)



Paul Joan Ezra, Sanjay Misra, Akshat Agrawal, Jonathan Oluranti, Rytis Maskeliunas, and Robertas Damasevicius

Abstract The evolution and era of the latest programs and services, collectively with the enlargement of encrypted communications, make it difficult for site visitors within a safety enterprise. Virtual private networks (VPNs) are an instance of encrypted communicate provider that is becoming famous, as a way for bypassing censorship in addition to gaining access to offerings which are geographically locked. This paper reviews the layout of an IP security, VPN. The Cisco Packet lines platform is used for the simulation, evaluation and verification. It uses a virtual connection to carry the records packets from a non-public network to remote places.

Keywords Virtual private network · Authentication · Security · Confidentiality

1 Introduction

Individuals who use the Internet are highly exposed to social media exploitation where they are victims of attacks. Due to the various attack and vulnerability that data are exposed to when been transmitted from a sender to a receiver, a protection mechanism ought to be provided to address several safety assaults on statistics transmission through the Internet. There are different attacks over the Internet, such

P. J. Ezra · S. Misra (✉) · J. Oluranti
Center of ICT/ICE Research, Covenant University, Ota, Nigeria
e-mail: Sanjay.misra@covenantuniversity.edu.ng

J. Oluranti
e-mail: jonathan.oluranti@covenantuniversity.edu.ng

A. Agrawal
Amity University, Gurgaon, Haryana, India

R. Maskeliunas · R. Damasevicius
Silesian University of Technology, Gliwice, Poland
e-mail: rytis.maskeliunas@polsl.pl

R. Damasevicius
e-mail: robertas.damasevicius@polsl.pl

as the denial-of-service attack which makes the network service unavailable by flooding network traffic to the target which exhausts the processing power of the target [1, 2]; information has been changed either accidentally or by malicious attack affects the integrity of the data or creates false information. Eavesdropping on data containing confidential information, such as the location, keys and even passwords of the node, can be redirected to another location. Many security mechanisms have been reviewed to protect data integrity, confidentiality, availability, authenticity and non-repudiation. Cell users want to get entry to assets from their company or domestic network in an efficient but relaxed manner which is done with the help virtual private network (VPN) connections. VPN is a virtual connection routed through the Internet on a public network, from the sender's private network to the receiver. VPN aims to initiate a secure communication path among different networks. It is usually created across the public network [3]. VPN tunnels are used to maintain the privacy of statistics shared over the physical network connection protecting packet-level encryption, consequently making it very hard to become aware of the programs strolling through these VPN services [4].

Authors in [5] showed that a current survey indicated that almost 50% of agencies would adopt the preceding idea by 2025. VPN provides privacy which prevents intermediated users from eavesdropping, altering or deleting the data, authentication which validates that the packet sent by the authorized sender, checks that the data is not altered and prevent intermediate users from copying and resending the information. A VPN tunnel is created for the information to be secured over the physical community connection, maintaining packet-stage encryption, making it very hard to discover the software passing through the VPN offerings. This paper focuses on secure communication using a VPN.

VPNs continue to develop with an increasing number of options that is frequently used in both big and small organization. They also have an advantage of flexibility, connectivity and security at cheap cost. Organizational gains from VPN are reduction in cost and increases in scalability and productivity without compromising the security [6]. This study covers the simulation, evaluation and verification with the help of a packet tracer simulator.

The main aim of the present work is to design a simple system that uses a VPN to secure wireless communication. The following are the main objectives of the presented work.

1. To show how to protect data from being attack over the Internet.
2. To enable communication to be kept private between only the receiver and sender.
3. To show how VPN is over other security mechanisms such as firewall defense.

A brief knowledge of the work is given in this section. Section 2 presented related works in the field of secured communication. Section 3 outlines the method that is used for design and implementation and results. Section 4 describes the conclusion and future work.

2 Related Works

We have reviewed the related works in several databases. The summary of all those important and selected studies is given in Table 1.

There are several other related works [8, 23, 24] available in the literature but due to limitation of work, we are not providing details.

3 Methodology and Results

CISCO packet tracer is used for the design and the simulation of the proposed network using VPN. Only the authorized user will be able to communicate with the other network. The routers will be configured with advance encryption standard to protect data and privacy, Hash-sha tool for IP security authentication, ISAKMP protocol to ensure that two hosts agree on how to build a security association.

3.1 Design and Implementation

Any device connected to the Internet has an IP address which is a sequence of number; a VPN will mask the IP address. An IP address identifies address and location, and a VPN erases IP address from been detected, encrypts your data and keeps your activities private but they do reduce the speed due to the extra security.

For a system to have a working VPN, the following must be configured.

1. Access-list to permit corresponding traffic that will go over the tunnel.
2. ISAKMP policy and ISAKMP key. It is used to set up key authentication and tunnel.
3. IP sec transform-set. It provides authentication and integrity.
4. Crypto map. The crypto map should be applied to the interface.

VPN tunnel must have a security license on the router. The encryption algorithm that was used is the advanced encryption standard (AES) with a key of 256, to protect data and ensure privacy. The IPsec message integrity used is the HMAC-SHA which defines the key size to support different encryption key size. The pre-shared authentication key was used to require VPN devices on each end to configure with the identical mystery key.

Figure 1 shows a conceptual diagram of the VPN network within an organization with all configured interfaces. If the interfaces are not connected to an IP address, there cannot be any form of communication, secured or not secured. This IP address is a unique identifier that indicates the location of a device and governs the way data is sent over the Internet. In the fig above, router 3 interface is

Table 1 Summary of the literature review

Summary of the literature review		
Authors	Work done	Result
Liyanage and Gurtov [7]	VPN architecture for LTE backhaul was addressed. The Internet key exchange model 2(IKEv2) and host identity protocol (HIP) were used as the safety key	Provided secured backhaul traffic during DoS, DDoS and TCP reset attacks
Deshmukh and Iyer [5]	A secure VPN for remote access was addressed. The advanced encryption standard (AES) algorithm was used for data security. The work was carried out on a packet tracer	The smart devices can securely get linked with users on the Internet as if they had been part of the equal non-public network
Busschbach [4]	Enhancing the QoS of a VPN by using an asynchronous transfer mode (ATM) and multiprotocol label switching is studied	An MPLS-based VPN using next-technology IP switches as the best method to enhance the QoS for VPNs
Jaha et al. [8]	A VPN formula that relies on remote access connections requirements and a site-to-site VPN formula that relies on site-to-site connections requirements	Provide a basis while creating business enterprise WAN which connects websites and customers using VPN technology
Azhar et al. [9]	A social media detection on SMS and camera by using application programming interface (API) and permissions was addressed	Identify measures for API and permission for SMS and camera and possible methods for API and permission SMS and API exploitation
Chze and Leong [10]	Proposed a secure multi-hop (SMRP) to merge the routing and authentication processes	Result suggests that the SMRP produces a secured multi-hop IoT communication network without performance degradation in comparison with the well-known optimized link nation routing protocol (OLSR)
Das and Islam [11]	A remarks-based dynamic computation version that could correctly come across unexpected strategic alteration in malicious behavior with the additional feature of balancing workload among service provider was addressed	Strategic behavior of a malicious agent was detected. They provided a mathematical definition of secured trust
Sarika et al. [12] Wu et al. [13] Dinesh et al. [14] Zhou and Hass [15]	Studied the vulnerabilities, attacks and security mechanisms for mobile ad hoc networks (MANETs)	Gives more understand on MANETs, their traits, uses, the criterion for the network security

(continued)

Table 1 (continued)

Summary of the literature review		
Authors	Work done	Result
Manvi and Tangade [16]	The authentication schemes in vehicular ad hoc networks (VANETs) were studied	Security was based on cryptography systems and digital signature. VANET became famous in transport because of the broadcast of safety messages between vehicles
Assadhan et al. [17]	Monitoring and analyzing of a botnet by the command and control (C2) communication traffic	The result achieved was by evaluating a periodogram of the packet and address count sequences
Lan et al. [18]	The hardware implementation of a lightweight Chaskey algorithm using different implementation scheme was studied	A hardware implementation of 3334.33 gate equivalent is achieved with an operating clock frequency of 1 MHz
Liu [19]	Hash-based message authentication codes (HMAC) was studied to achieve authenticity and integrity without the support of a digital signal	Prove that the HMAC is cheap and easy to implement, and it can be used on websites
Draper-gil et al. [3]	Two standard machine learning algorithms, C4.5 and KNN, were used as classification techniques for time-related features	The results prove that the proposed set of time-related features are good classifiers, reaching accuracy levels above 80%. C4.5 and KNN had a similar performance in all experiments; C4.5 has achieved better results
Padmavathi [20]	Zone routing protocol (ZRP) with wireless transport layer security (WTLS) models was addressed to provide security	The proposed work provided security in both routing and transport layer of MANET
Liang et al. [21] Kobayashi and Shitz [22] Nawej and Technologiae [6]	Secured communication over fading channel was addressed They evaluated the impact of VPN on network performance. The network performance covers the hypertext transfer protocol (HTTP), file transfer protocol (FTP) and constant bit rate (CBR)	They establish a capacity state of the parallel broadcast channel, parallel Gaussian broadcast channel and an optimal power location A simulation was done on NS2 for network on VPN and no VPN. network with VPN always delivers better results

having an IP address of 209.165.100.2 and 209.165.200.2, router 4 209.168.100.1 and 192.168.1.1 and router 5 209.165.100.2 and 192.168.3.1

Figure 2 shows that the router does not have a security license. Without this security license VPN encryption, secure collaborative encryption, dynamic multi-point VPN is impossible. The securityk9 can be checked by using the “show version” command in the privilege mode. The security license has been configured and shown in Figs. 3 and 4

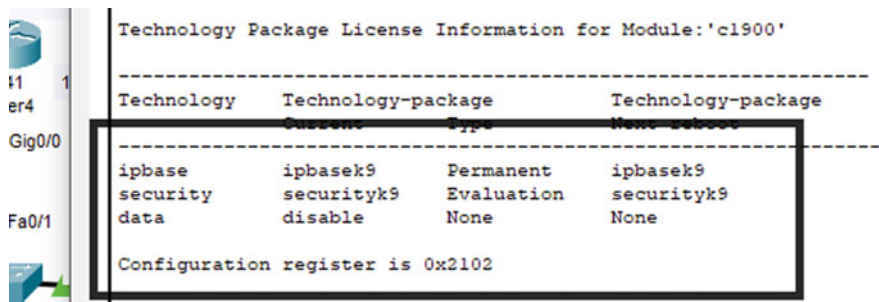


Fig. 4 Router with security license

Figure 5 shows the access-list configuration. The access-list grants permission to allow traffic from one network to the other through the tunnel. The access-list only allow listed IP addresses to communicate across the tunnel.

The policy and key enable the router to utilize IP security as showed in Fig. 6. Every ISAKMP coverage is assigned a unique precedence number among 1 and 10,000. The coverage with precedence number 1 is considered the highest priority policy.

Figure 7 shows the IP sec transform-set configuration, which verifies authentication and integrity. A transform set is a merger of an IP sec transforms designed to enact a particular protection coverage for data traffic

Figure 8, shows the crypto mapping configuration. A crypto map is a configuration entity that select data flow that needs security processing. A crypto map must be named. In the configuration above, the crypto map name is "IPSEC-MAP". Figure 9 shows interface of the crypto map.

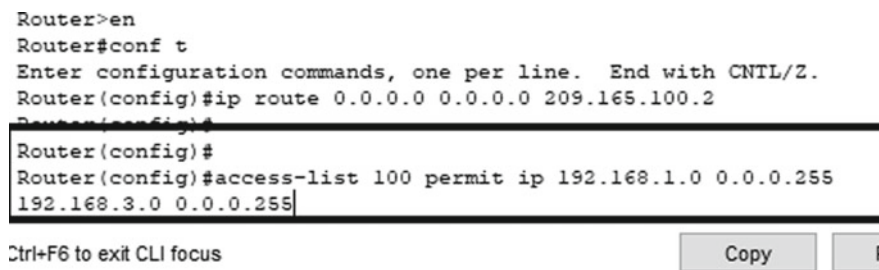


Fig. 5 Access-list

```

Router(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
Router(config)# cyo
Router(config)# crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fig. 6 ISAKM policy and ISAKM key

```

% Invalid input detected at '^' marker.

Router(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
Router(config)# cyo
Router(config)# crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#
Router(config-isakmp)#
Router(config)#crypto isakmp key tunnel address 209.165.100.1
Router(config)#crypto ipsec tran
Router(config)#crypto ipsec transform-set router3->router1 esp-aes
256 esp-sha-hmac
Router(config)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Fig. 7 IPsec transform-set

3.2 Result and Discussion

When using the real-time mode to check for the communication process, it is observed that laptop 2 could communicate with laptop 3 without router three been aware of the network; this process is seen using the simulation mode as shown in Fig. 10. Information about the VPN is checked from the inbound PDU details; it is



Fig. 8 Crypto map

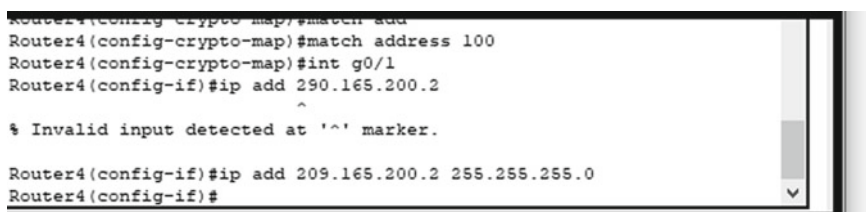


Fig. 9 The interfaces applied to the crypto map

noticed that router 3 had no idea about router 4 and router 5 but they are pinging across router 3 because of the VPN. From the simulation result below, only the source IP address 192.168.1.10 and the destination IP addresses 192.168.3.10 are seen, but the path through which the packet goes through is not recognized.

4 Conclusion and Future Work

This paper presented a VPN architecture within an organization that proposed solution to secure traffic through authentication, authorization, payload encryption and privacy protection. Simulation result on cisco packet tracer verifies that they provide secured traffic communication. This paper proposed a simple VPN solution that can be used in an organization. They also have the advantage of flexibility, connectivity and security at cheap cost. Organizational gains from VPN are increased in the scalability and productivity. Future work can be carried out by

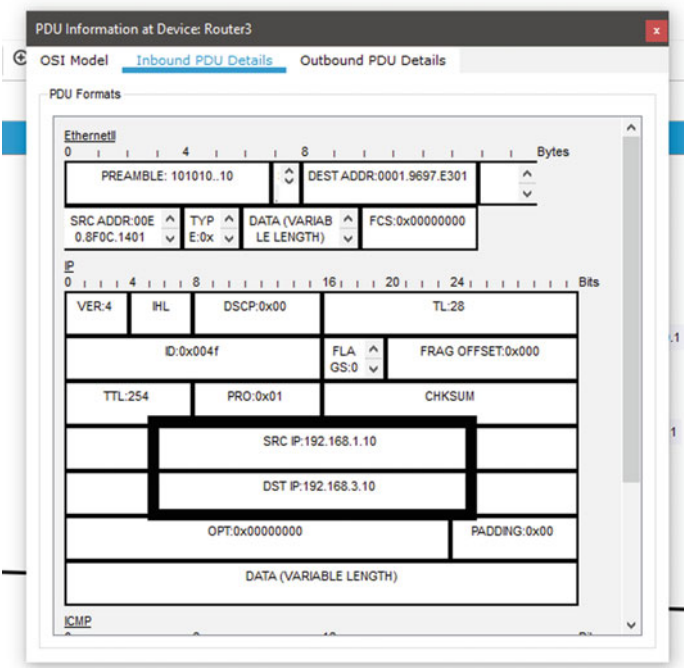


Fig. 10 Simulation result

using other simulation packages order than cisco packet tracer for a simple VPN connection within an organization, and also, the model can also be expanded by using VPN connections across multiple countries.

Acknowledgements The authors appreciate the sponsorship from Covenant University through its Center for Research, Innovation and Discovery, Covenant University, Ota Nigeria.

References

1. Oduami, M., Misra, S., Adetiba, E., Abayomi-Alli, O., Damasevicius, R., Ahuja, R.: An improved model for alleviating layer seven distributed denial of service intrusion on webserver. *J. Phys.: Conf. Ser.* **1235**(1), 012020 (2019)

2. Oduami, M., Misra, S., Abayomi-Alli, O., Abayomi-Alli, A., Fernandez-Sanz, L.: A survey and meta-analysis of application-layer distributed denial-of-service attack. *Int. J. Commun. Syst.* **33**(18), e4603 (2020)

3. Draper-gil, G., Lashkari, A.H., Saiful, M., Mamun, I., Ghorbani, A.A.: Characterization of encrypted and VPN traffic using time-related features. In: *Proceedings of the 2nd International Conference on Information Systems Security And Privacy (ICISSP)*, pp. 407–414, 2016

4. Busschbach, P.B.: ♦ Toward QoS-capable virtual private networks. *Bell Labs Tech. J.* **3**(4), 161–175 (1998)

5. Deshmukh, D., Iyer, B.: Design of IPSec virtual private network for remote access. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 716–719. IEEE, 2017
6. Nawej, M.C., Technologiae, M.: Evaluation of virtual private network impact on network performance (2016)
7. Liyanage, M., Gurtov, A.: Secured VPN models for LTE backhaul networks. In: 2012 IEEE Vehicular Technology Conference (VTC Fall), Sept 2015, pp. 1–5. IEEE
8. Jaha, A.A., Ben Shatwan, F., Ashibani, M.: Proper virtual private network (VPN) solution. In: Proceedings of 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies, NGMAST 2008, pp. 309–314, 2008
9. Azhar, M.A., Saudi, M.M., Ahmad, A., Bakar, A.A.: Detection of social media exploitation via SMS and Camera. *IJIM* **13**(4), 61–78 (2019). Last accessed 01 Mar 21. https://www.learntechlib.org/p/208525/paper_208525.pdf
10. Chze, P.L.R., Leong, K.S.: A secure multi-hop routing for IoT communication. In: 2014 IEEE World Forum on Internet of Things, WF-IoT 2014
11. Das, A., Islam, M.M.: SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems. **9**(2), (2012)
12. Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.: Security issues in mobile ad hoc networks. *Proc. Comput. Sci.* **3**(5), 1022–1024 (2014)
13. Wu, B., Chen, J., Wu, J., Cardei, M.: COUNTERMEASURES IN
14. Dinesh, D., Kumar, A., Singh, J.: Security attacks in mobile adhoc networks (MANET): a literature survey. *Int. J. Comput. Appl.* **122**(20), 31–35 (2015)
15. Zhou, L., Haas, Z.J.: Securing ad hoc networks. *IEEE Netw.* **13**(6), 24–30 (1999)
16. Manvi, S.S., Tangade, S.: A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* (2017)
17. Assadhan, B., Moura, J.M.F., Lapsley, D., Jones, C., Strayer, W.T.: Detecting botnets using command and control traffic, 4, 156–162 (2009)
18. Lan, J., Zhou, J., Liu, X.: An area-efficient implementation of a message authentication code (MAC) algorithm for cryptographic systems. In: IEEE Reg. 10 Annual International Conference Proceedings/TENCON, pp. 1977–1979, 2017
19. Liu, Z., Lallie, H.S., Liu, L., Zhan, Y., Wu, K.: A hash-based secure interface on plain connection, 1236–1239 (2011)
20. Padmavathi, G., Subashini, P., Aruna, M.D.D.: ZRP with WTLS key management technique to secure transport and network layers in mobile adhoc networks. *Int. J. Wirel. Mob. Netw.* **4**(1), 129–138 (2012)
21. Liang, Y., Poor, H.V., Shamai, S.: Secure communication over fading channels. *IEEE Trans. Inf. Theory* **54**(6), 2470–2492 (2008)
22. Kobayashi, M., Shitz, S.S.: Secured communication over frequency-selective fading channels : a practical vandermonde precoding, 2009 (2009)
23. Azeez, N.A., Salaudeen, B.B., Misra, S., Damaševičius, R., Maskeliūnas, R.: Identifying phishing attacks in communication networks using URL consistency features. *Int. J. Electron. Secur. Digit. Forensics* **12**(2), 200–213 (2020)
24. Osho, O., Musa, F.A., Misra, S., Uduimoh, A.A., Adewunmi, A., Ahuja, R.: AbsoluteSecure: a tri-layered data security system. *Commun. Comput. Inf. Sci.* **1078**, 243–255

Survey for Detection and Analysis of Android Malware(s) Through Artificial Intelligence Techniques



Sandeep Sharma, Kavita Khanna, and Prachi Ahlawat

Abstract Artificial intelligence techniques have been intensively used for android malware detection and analysis in the last past few years. The proposed methodologies do not suffice the requirement while characteristics of malwares are changing so rapidly and evolving new complex malwares. Therefore, it is a very complex task to classify and identify these malwares. This paper presents an organized and comprehensive survey for the detection techniques of android malware(s) in chronological order. These detection and analysis techniques are elaborated in two core categories: statics and dynamic analysis and hybrid analysis with machine learning or artificial intelligence. The core contributions of this paper are: (1) explaining a methodical, chronicle and organized summary of the existing techniques of android malware detection, (2) exploring the major elements and challenges in the detection methods and (3) explaining the importance of artificial intelligence for android malware detection. The detection approaches are explained in a manner that new approaches are compared with the old ones based on their features. The advantages and disadvantages of each approach are discussed. This study facilitates researchers and academics to have a wide-ranging conception of the field of android malware detection and provides a platform to enhance the fundamental knowledge to implement the new idea and subsequent improvement further in existing techniques.

Keywords Android • Malware detection • Static • Dynamic • Hybrid • Artificial intelligence

S. Sharma (✉) · K. Khanna · P. Ahlawat
The Northcap University, Gurugram, Haryana, India
e-mail: kavitakhanna@ncuindia.edu

P. Ahlawat
e-mail: prachi@ncuindia.edu

1 Introduction

The smart mobile phones are attracting all due to their tremendous features and have provided online banking, online marketing, online study, etc., in addition to fundamental telephony services. These mobile terminals are outfitted with huge processing power and ample storage that holds a variety of sensitive and critical data like contacts, pictures, passwords, cookies, credit card details, location information, etc. As per statista's report, the global figure of subscribers of smart mobile phone has reached 4.01 billion in 2020 and is expected to reach 4.7 billion in 2022 [1]. However, this popularity of smartphones has attracted the attention of hackers who may steal the data stored in smartphones and further may deduce the code to unlock the mobile to compromise the device or manipulate popular services. The various Android Operating Systems (OS) is the most accepted operating systems for the existing smartphones (82.8%) [2]. On one hand, the Android OS is an open-source software system to provide a wide range of accessibility to users and on the other hand, Android OS is more susceptible to cyber-attacks. The malicious apps or malwares are developing so rapidly worldwide that was never observed in the past. Normally, android apps and games are downloaded and installed from the Play store verified by play protect developed by Google. However, android apps and games can also be installed from other non-authenticated and not verified stores where apps and games are integrated with malicious codes that contaminate the android phones and exfiltrate the critical data to hackers. The protected Play store is also not secured from the hackers even after their continuous effort to monitor and remove infected applications. Moreover, several variants of Android Operating System are available in multiple manufacturer's devices and all variants are needed patches and updates regularly from the respective developer immediately. There are some major aspects like diverse ARM processors, limited RAM, and power battery restriction, etc. that create the complexity in detection of malicious codes. TrendMicro declared in the first quarter of 2020 that, mobile cyber espionage operations have increased by 1400%, distributed among multiple firmware(s) and operating systems from 2015 to 2019 [3].

Several anti-malware techniques, frameworks and solutions have been developed to protect android phones. These analysis frameworks are divided into static and dynamic features analysis. The static features analysis is based on the reverse engineering of apk file of apps. Applications are scanned for malicious code instead of executing them. This is helpful for detecting the malicious codes that only run in explicit circumstances like rebooting; however, the same techniques are not able to identify the encrypted and dynamically loaded malicious codes of android. In the dynamic feature analysis, runtime activities of apps are analyzed and encrypted and dynamically loaded malicious codes of android are identified. Since, all execution paths cannot be examined, which limits overall and complete analysis of the code/apk. The Hybrid techniques combine the advantage of static and dynamic features analysis; however, these techniques have several limitations that force the researchers to develop new hybrid analysis technique based on artificial or machine

learning to achieve high detection rates. All analysis techniques have some advantages and weaknesses for the detection of android malwares. It is also observed that there are several deficiencies in the surveyed presented in the research paper. A quantity of papers has not considered the latest articles in the comparison and analysis. On the other hand, some surveys have not classified the detection techniques systematically for their research work. To overcome these flaws, this paper presents an organized literature survey on the latest android malware detection and analysis frameworks. The main contributions of this paper and study are:

- (a) resenting a systematic, chronically and categorized study of the current approaches to android malware detection.
- (b) Exploring the architecture and elements of noteworthy android malware detection methods and challenges in these methods.
- (c) Demonstrating the importance of deep learning and artificial intelligence for android malware detection and analysis techniques.

The paper is organized as follows. “Review of Android Malware Analysis Techniques” presents a systematic assessment of the existing techniques for detection and analysis of android malwares. In “Discussion,” a brief tabulated comparison of malware detection techniques is presented for ready reference. A comparison chart for the efficiency of major android malware detection methods is presented which can work as a benchmark level for new research works. At last, “Conclusion” exhibits the crux of the same study.

2 Review of Android Malware Analysis Techniques

The existing android malware detection and analysis framework are elaborated based on their basic architecture, feature extraction module, test data set, efficiency and advantages and disadvantages. The technique is divided into two parts. The first basic techniques including static and dynamic analysis that are base for any artificial intelligence technique are discussed in chronological order. Then, the latest artificial intelligent techniques for the analysis of android malware are analyzed in detailed.

2.1 Integrated Static and Dynamic Malware Analysis Techniques

There are several android malware analysis techniques that implement the combination of static and dynamic analysis to improve the accuracy of detection of malware. The general architecture of an integrated static and dynamic analysis framework is shown in Fig. 1. Blaising [4] demonstrated an android application (AA) sandbox in 2010 that detects the malicious activities in android apps through

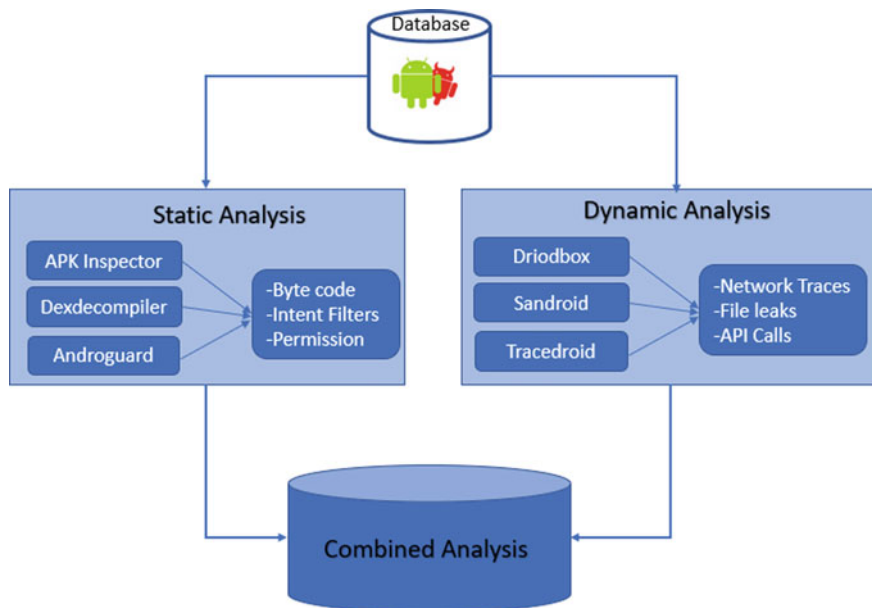


Fig. 1 Statics and dynamic combined malware analysis

analysis both statically and dynamically. In the section of static analysis, android api/code is decompiled by the Baks mali module. Then, the decompiled smali files are scanned and static features are extracted. In the section of dynamic analysis, the apk/code is run through the emulator devices. The Monkey module is also integrated to activate the apps with testing parameters like gestures and clicks. This framework is loaded in the kernel under a fully controlled environment for execution of the apk/code that generates the logs files by capturing the system calls. Vectors are defined based on the log of static and dynamic behavior analysis and these same vectors are inserted into a framework for monitoring of malicious activities of apps and further detection. The main constraint of AASandbox was that it could not be implemented in a large volume of android devices as the root privilege is required for capturing system calls. Authors did not calculate the accuracy of the proposed framework.

Zhou et al. [5] developed a new framework DroidRanger in 2012 for detection of unknown and known malwares. In first section, DroidRanger examines and detects the essential permissions which are used by the malwares to execute the malicious actions that segregate the malicious apps for further analysis in second stage. This data is then collaborated with the defined behavioral rules to distinguish, filter and analysis of identified malwares. However, detection of unknown malwares is achieved in two segments: In the first segment, the filter is defined based on heuristic algorithms. Researcher has implemented two heuristics algorithms in this technique. In the first heuristic technique, the code from the remote server is loaded

dynamically. In the other heuristic technique, the native code is loaded dynamically and the behavior of app is monitored. If app is not stored in default directory, then this behavior is noticeable. Heuristic technique facilitates the framework to determine the malwares which exploit the OS kernel and get root access and provides a capability to detect the DroidDreamLight [6]. Dynamic executions are performed to monitor the runtime behavior of applications. A data set of 204040 android applications was collected in which 75% and 25% were taken from the official and other alternative android markets, respectively. The limitation of this framework is that it developed for only official android markets (Google Playstore) and alternative android markets (eoe market, gfan, alcatelclubm mmoovv, etc.), not for android devices.

Talha et al. [7] developed a new framework for android malware analysis, i.e., APK Auditor in 2015, that uses permissions features for detection of malware behavior. This framework comprises of following segments: (1) database for signatures: store signatures of all the apps; (2) android client: offers the facility of malware analysis to clients; (3) server for processing, which offers a connection between android client and database and processing. The server executes the analysis without installing the apps on the device and optimizes the available assets. APK Auditor monitors all the permissions as called by the apps and determines the value of permission malware score (PMS). Thereafter, this tool classifies the apps as malware if the value of PMS apps scores higher than the threshold value. The outcome demonstrated that APK Auditor accomplished 92.5% accuracy but cannot identify the malicious payloads which installed dynamically.

Abraham et al. [8] developed a 2-Hybrid malware detection framework in 2016 which executes the detection and analysis of android malwares on the server installed at a distant location. The extractor module of framework extracts and accumulates the parameters of the apps and classifies the apps as malware or benign. This framework does not conclude the categorization of apps only based on host analysis but also sent to the server installed at a distant location for exhaustive analysis. If malicious activities are observed in app then server forwards the same data to local device for future detection. As a test set, 39 malicious samples were collected and 69 permissions were monitored from these samples. The results were satisfactory; however, authors did not compare the efficiency of this framework with other frameworks.

Sun et al. [9], developed a new framework MONET in 2017, that detects the malicious codes of an already acknowledged malware family. This framework extracts the static parameters, disassemble the codes, and monitors the dynamic activities of apps for uncovering of malwares. MONET uses client-end applications that run on the user device for analysis of application and design its specific signature. The sets of signatures are stored in the server and a signature matching algorithm is applied. A test set of 3723 and 500 malwares and legitimate apps, respectively, were used for experiments. MONET demonstrated 99% accuracy of detection of malware but shown lacks of resource efficient.

2.2 Hybrid Malware Analysis with Artificial Intelligence

The general architecture of the hybrid malware analysis technique with artificial intelligence is shown in Fig. 2. Wang et al. [10] developed a hybrid malicious code analysis framework in 2015 which performs both static and dynamic analysis and implement machine learning for training the framework. It implements signature-based detection to detect the malwares. In first stage, the manifest file is used for static features extraction and android packaging tools are used for disassembling the dex files [11]. In second stage, Cuckoo Droid [12] and Robotium [13] are used for dynamic features extraction. These static and dynamic features are converted into vectors and mapped into vector space. Different feature extraction and selection methods are implemented in this method to increase the accuracy and susceptibility for misuse and anomaly detection. In misuse detection, SelectKBest method is applied where k highest scoring features are selected and Chi2 is used as a scoring function. After feature selection, SVC [14] and SVM classifier [15] are applied for the classification of known and unknown malware, respectively. Based on the probability of signature matching, apps are categorized as malwares and training database is updated accordingly. In case, if there is any uncertainty, then only anomaly detection is applied and if any abnormal behavior is detected, then app is classified as unknown malware and training database is updated accordingly. A test set of 12000 and 5560 for benign and malware apps are collected,

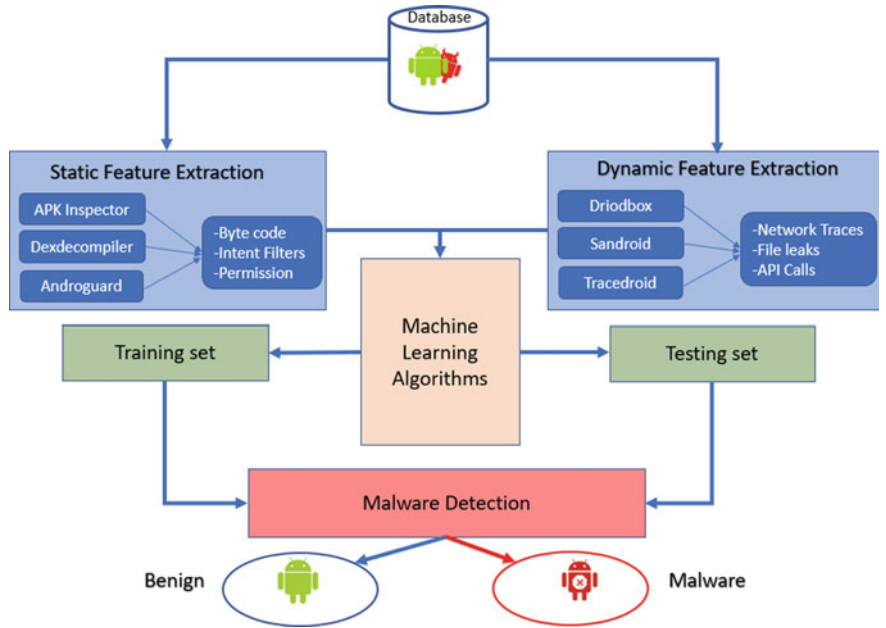


Fig. 2 Hybrid malware analysis using artificial intelligence

respectively, from various App stores. The Outcome demonstrated that the framework can detect the malwares with an accuracy of 98.79% from the used test set.

Sahijo et al. [16], developed an integrated framework for malware detection and analysis based on machine learning in 2015. This framework assimilates the static analysis and dynamic analysis for detection and analysis with training of modules of machine learning. Framework extracts printable strings information as static feature from app and then sorted as per the rate of incidence in each file. After extraction, feature selection is performed such that PSI features with the rate of incidence above benchmark are selected. Selected features are then enlisted into global list named feature list. This feature list is used for creating static feature vector. In next stage, Cuckoo platform is implemented and API call logs are extracted for dynamic feature extraction of apps. API call grams are generated for all codes and sorted as per the rate of incidents. The vectors for static and dynamic features are designed and inserted into two separate machine learning modules SVM [17, 18] and random forest [19] for classification. This framework demonstrated 98.7% accuracy on a test set of 997 malicious and 490 benign apps; however, huge storage and high processing power are required for the same framework.

Yuan et al. [20] developed an online framework DroidDetector in 2016 to detect malwares online. In this framework, both the static and dynamic features extraction tools are implemented in the servers hosted remotely and then machine learning modules are integrated for discriminating between malwares and benign apps. Major permissions and sensitive API are monitored to determine the static features. DroidBox is applied for a specific period of time to monitor the dynamic activities of apps. The static and dynamic features are mapped into vectors and these features are inserted into the machine learning module for learning of detection of malicious apps. A test set of 20,000 apps of a combination of both legitimate and malware apps is used to evaluate the framework of DroidDetector. Experimental results demonstrated the achievement of 96.7% accuracy for the detection of malwares. The key flaw of this framework is that the various malicious apps can be escaped from the detection of framework if malicious behavior of apps is not observed during the observation time-period.

Yu et al. [21] developed a hybrid automatic static-dynamic switch framework in 2016 to counter the transformation technique adopted by the malwares. This framework can distinguish the malicious codes of apps by either static or dynamic detection and analysis technique. In first section, apps are decompiled through Apktool [22] and accordingly manifest and Smali files are created and static malware analysis is applied. The extracted static features are mapped into the vectors and these vectors are inserted into machine learning modules for detection of the apps as malware. However, if apps are not properly decompiled due to transformation techniques, then automatic dynamic malware analysis is executed on the apps. In the same way, dynamic malware analysis is performed on apps and extracted dynamic features are mapped with vectors. These vectors are also inserted into machine learning modules like kNN and Naive Bayes, etc., for training of framework for detection. Framework demonstrated the 99% accuracy for static

detection and 90% accuracy for dynamic detection. However, the main flaw of this framework is that only static malware analysis process is executed if the app is decompiled properly. Framework does not have capability of detection of dynamically loaded codes in the app. Therefore, app that is not able to execute accurately cannot be analyzed properly and accordingly cannot be classified as malware or benign app.

Saracino et al. [23], developed a host-based novel framework MADAM in 2016 which suspicious the apps based on their misbehavior and malicious activities. The framework segregates the malware into a number of behavioral modules and each module execute specific misbehavior that is tagged with the same malware. Framework extracted and correlated features at four stages: package, application, user, and kernel. MADAM structural design consists of four main pillars that are App Risk Assessment, Global Monitor, App Monitor, and User Interface and Prevention. MADAM executes App Risk Assessment process and generates a list of suspicious apps. Framework applies the static and dynamic analysis to determine the risk of app. The Global monitor process monitors the system call, user activity, message and activity logger and generates feature vectors. These vectors are inserted in a machine learning module like kNN and are used to train the framework for legitimate and malicious behaviors. App monitor process decompiled the malicious codes by analyzing the behavior of malwares at API and kernel level. App Monitor continuously monitors the (a) Background apps with administrator privileges, (b) Automatic SMS send-receive apps, and (c) Foreground apps. Lastly, the user interface warns about the malicious apps and assistance for blocking and removing these apps. The proposed framework is tested on a test set collected from virus share and demonstrated 96.9% detection rate. However, MADAM framework has one flaw that a root privilege is required on the device to execute the detection and this cannot be executed in the mass market.

Hou et al. [24] developed a heterogeneous information network, i.e., Hindroid for android malware analysis in 2017. This framework created higher-level semantics in place of application programming interface (API) calls. HinDroid framework created a heterogeneous information network (HIN) of android applications and a meta-path to provide connection to these applications. All meta-path is required to calculate a similarity measure over android applications and automatically weighted by the learning algorithm to make predictions. The authors claimed that HinDroid shows better performance than other android malware detection systems; however, accuracy and efficiency were not provided.

Karbab et al. [25] developed an automatic framework MalDozer using deep learning in 2018 for android malware analysis. MalDozer automatically extracts the features and learns the new patterns from the actual samples to detect the malwares. MalDozer can be deployed not only on remote servers but also on android mobile agents. MalDozer offered many advance features like automatic features extraction in the training phase and minimal preprocessing power. A test sets of 33,000 malwares and 38,000 benign apps are used to evaluate the performance of framework. MalDozer demonstrated that malware can be correctly detected with an F1-Score of 96–99%.

Li et al. [26] introduced a new framework in 2018 for malware analysis system based on Significant Permission IDentification (SigPID). This framework is designed in three systematic stages of pruning approach with machine learning techniques to identify the most significant permissions so that framework can be utilized effectively. SigPID demonstrated that only 22 permissions out of 132 permissions are significant and improve the runtime performance by 85.6%. This framework also demonstrated that 90% of precision can be achieved by the support vector machine (SVM). A test set of 1,000 malwares was applied for testing and SigPID technique demonstrated 93.62% and 91.4% efficiency in detection of known malware and unknown/new malware samples, respectively.

Feng et al. [27] proposed an innovative ensemble learning-based EnDroid in 2019 for android malware detection. This framework integrated multiple types of dynamic features and analysis techniques and achieved very precise malware detection accuracy. These analysis techniques include the monitoring of malicious behavior of system and application level like stealing of critical data, uploading on a remote server, and update of firmware with malicious codes. Two datasets were taken for experiments and result demonstrated that stacking accomplished the best detection performance and exhibits 96.56% efficiency in android malware detection.

Zhou et al. [28] presented a new framework incorporating the control flow graph with machine learning algorithms in 2019 for android malware analysis. In this framework, the applications are decompiled and a control flow graph is constructed to obtain the API information. Three types of system API uses data sets, (1) API calls, (2) API frequency, and (3) API sequence based on control flow graphs are constructed to develop three detection models. The accuracy of all three models is compared using Precision, Recall and F-score metrics. The Framework demonstrated 98.98% detection precision on a test set of 10,683 malicious and 10,010 benign applications.

Mehtab et al. [29] proposed an innovative approach, AdDroid in 2019 to detect android malwares based on a variety of permutations of artifacts. The rules/artifacts designate the activities of codes of android device like establishing a connection to the ISP through the internet, secretly uploading personal data to the pre-defined server, updating malicious package/patches of firmware, etc. AdDroid uses ensemble-based machine learning algorithms, i.e. Adaboost to train the model for static analysis of android apps. AdDroid is able to extraction and selection of statics feature and then able to recognizing malicious applications based on the most unique rules. This machine learning framework is trained and developed by applying a test set comprising 1,420 apps including 910 malicious and 510 benign android apps. The framework demonstrated an accuracy of 99.11% on a similar test set. The Authors did not include dynamic features for machine learning.

Ma et al. [30] proposed the deep learning-based framework Droidetec in 2020, for android malware detection and exact localization of malicious codes in the apps. This framework implemented an innovative feature extraction method to monitor behavior sequences from malicious apps. Extracted behavior sequences are represented as a vector that automatically scrutinizes the semantics of sequence of

fragment and determines the malicious code. A test set of 9,616 malicious and 11,982 benign programs is used to evaluate the capability of Droidetec framework and the result demonstrated a precision of 97.22% for detection.

Mohammed et al. [31] proposed a deep learning framework, i.e., DL-Droid in 2020 to detect the malicious apps through dynamic features and generation of stateful input. DL-Droid framework is implemented with 30,000 benign and malware apps on real android terminals. Result demonstrates that the performance of detection of this framework with deep learning module is better than existing traditional methods. DL-Droid achieved accuracy of 97.8% for detection with dynamic features only and accuracy of 99.6% for detection with dynamic and static features. However, self-adaptation for intrusion detection systems is not available to improve the performance of model for malware detection.

Su et al. [32] proposed DroidPortrait in 2020, an approach of construction of multi-dimensional and vertical behavioral representation for detection of android malwares. In the analysis, the behavior of android malware is monitored and static and dynamic behavior as dataset are extracted. In the next phase of analysis, different kinds of behaviors are segregated based on android malware and a specific and unique behavioral tag is attached with its signature. Machine learning (ML) algorithms are implemented to correlate these behavioral tags with specific malwares automatically. A high performance machine learning algorithm, i.e., random forest algorithm is very suitable and easily integrates with the basic framework to detect the android malware. The result demonstrated that DroidPortrait framework can illustrate the behavior appearances of android malware with high accuracy. The efficiency level was 90% which is lower and can be increased further.

Mahindru et al. [33] proposed MLDroid in 2020, the web-based model to analyze the android apps as malware and benign. Authors implemented feature selection techniques and trained the framework by these techniques. These selected features developed an innovative model by implementing different machine learning algorithms. A test set of 500,000 plus android apps are used for the experiment and the four distinct machine learning algorithms (1) deep learning, (2) first and farthest clustering, (3) YMLP, and (4) nonlinear ensemble decision tree forest is applied in parallel. Experiment results exhibit that framework developed by considering all the algorithms can achieve an accuracy rate of upto 98.8% for detection of malware from android apps.

Zhang et al. [34] proposed an automatic framework TC-Droid in 2020, for android applications analysis based on text classification technique. In this framework, the text sequences of APPs are analyzed by AndroPyTool and generated analysis reports are feed in deep learning algorithms. A machine learning algorithm, i.e., convolutional neural network (CNN) is used to extract considerable information instead of manual feature engineering from the same analysis report. A variety of well-known samples were collected for evaluation, and it is demonstrated that the performance of TC-Droid is better than other classic algorithms, i.e., NB, LR, KNN, RF, etc. However, actual data for accuracy and efficiency were not provided for comparison.

Thongsuwan et al. [35] demonstrated a hierarchical approach in 2021 using extraction of authorization-sensitive feature and implementing deep learning algorithms to design an android malware detection framework. This framework extracts four sensitive features: basic blocks, permissions, api, and key functions used for authorization. An innovative machine learning model, i.e., convolution neural network and eXtreme Gradient Boosting (CNNXGB) are implemented for training, learning and detection of malware. This framework sequences the key functions as per the timing of API calls and collects a similar section that confines the global semantics of malware family. Permissions and API calls were extracted from 1,330 android test samples to drill the model by XGBoost. The result demonstrated that efficiency increased upto 98% by the CNNXGB model. However, as the input data for analysis is increased, the number of the convolution layers and complexity increases.

McDonald et al. [36] developed a framework based on manifest permission and machine learning for android malware detection in 2021. In this framework, four different machine learning algorithms (1) random forest, (2) support vector machine, (3) Gaussian Naïve Bayes and (4) K-Means are applied in conjunction with features selected from android manifest file permissions to distinguish the apps as malicious or benign. A test set of 5,243 samples are used to test the framework and it was demonstrated that random forest ML algorithm performed the best with 82.5% precision and 81.5% accuracy.

Above mentioned techniques are briefly explained and tabulated in Table 1 for ready reference for researchers.

Table 1 Overview of the existing framework and research gaps

S.no	Reference	Year	Methodology/ contribution	Research gap
<i>Integrated static and dynamic malware analysis techniques</i>				
	Android application (AA) sandbox [4]	2010	Uses static and dynamics analysis	Root privilege is needed to capture the system calls
	DroidRanger [5]	2012	Uses static and dynamic analysis	Developed for official android and alternative android markets only
	APK Auditor [7]	2015	Uses static analysis with permission-based malware detection	Framework is installed at central server, and therefore, internet connection is required for android terminal for the malware analysis at server

(continued)

Table 1 (continued)

S.no	Reference	Year	Methodology/ contribution	Research gap
	Novel hybrid android malware detection [8]	2016	Static and dynamic features of the applications, are extracted at the server configured at distant. If app is distinguished as risk, database is updated for this risk signature	Efficiency and accuracy of framework were not determined and compared with another existing framework
	MONET [9]	2017	The specific signatures for respective malware are generated and forwarded to server for matching and detection	This framework works only with android DVM; however, latest android supports only ART
<i>Hybrid malware analysis with artificial intelligence</i>				
	A novel anomaly and misuse hybrid mobile malware detection system [10]	2015	Static features from manifest file and dynamic features through CuckooDroid are used with SVC classifier in misuse detection	Comparison table for detection with other frameworks are not computed
	Detection and mitigation of android malware through deep learning [16]	2015	Static features from printable strings information (PSI) and dynamic features from Cuckoo are extracted. These features are inserted in machine learning modules for classification	Power and storage consumption are intense
	DroidDetector [20]	2016	The extracted static and dynamic features through different tools are applied in deep learning algorithm for classification as malware	Malwares are escaped from the detection system during the dynamic monitoring time-interval
	A hybrid automatic static-dynamic switch framework [21]	2016	Analysis is conditional-based. If properly decompiled the app, extracted static vectors are inserted into deep learning algorithms like SVM, kNN and Naïve Bayes. However, in case, app is not decompiled properly then only dynamic are inserted into machine learning for classification	Only performs one analysis, i.e., static or dynamic. Framework will not be able to detect the malicious codes if app is decompiled properly

(continued)

Table 1 (continued)

S.no	Reference	Year	Methodology/ contribution	Research gap
	MADAM [23]	2016	Features are extracted at four stages: (1) package, (2) application, (3) user and (4) kernel. These features are mapped with vectors and inserted as input in machine learning kNN classifier for training	It runs only on rooted device, therefore, not supported in the large users. Moreover, pre-loaded apps/games cannot be analyzed by this framework
	Hindroid [24]	2017	Created heterogeneous information network (HIN) of android applications is used with machine learning algorithms	Accuracy and efficiency were not provided
	MalDozer [25]	2018	Automatically extracts the features and learns the new patterns from the actual samples through machine learning algorithms	Less effective in malware family attribution
	Significant permission IDentification (SigPID) [26]	2018	Instead of all android permissions, only most significant permissions SigPID are extracted and utilized for machine learning models	The analysis can be performed only on the rooted devices
	EnDroid [27]	2019	Dynamic features with system-based behavior trace and common apps-based malicious behaviors are used for deep learning	Power consumption is very high
	A control flow Graph-based android malware detection including machine learning [28]	2019	An ensemble of three detection models is created based on control flow graph of three data sets for android malware detection and analysis	Capability to establish the malware family is not presented
	AdDroid [29]	2019	Only static features are extracted and inserted into the ensemble-based machine learning model that is trained by the Adaboost	Artifacts called rules were defined for only static analysis. Dynamic analysis is not integrated with the model

(continued)

Table 1 (continued)

S.no	Reference	Year	Methodology/ contribution	Research gap
	DroidDetec [30]	2020	An innovative behavior sequences feature is extracted for analysis of syntax of linked segments and finding of malicious code	Not accurate framework for further classification into various malware families
	DL-Droid [31]	2020	Dynamic feature extraction with stateless approach is used with deep learning algorithms for analysis of malicious android apps	Self-adaptation for Intrusion detection systems is not available to improve the performance of model
	DroidPortrait [32]	2020	Extracted static and dynamic behavior and create an informative behavior dataset that includes specific behavior tag for specific android malware	The efficiency level was 90% which can be increased further
	MLDroid [33]	2020	Static and dynamic features are extracted and inserted into 04 different machine learning algorithms in parallel	This framework has capability for only detection the app as malware or benign. Detection rate is lower
	TC-Droid [34]	2020	Convolution neural network (CNN) algorithm is used for extraction of significant tags instead of manual features	Data for accuracy and efficiency were not provided
	ConvXGB [35]	2021	Authorization-sensitive features are extracted for machine learning algorithm of convolution neural network and eXtreme gradient boosting (CNNXGB)	Number of the convolution layers is increased, depending on the input data for analysis
	Manifest permission (MP) and machine learning (ML)-based framework [36]	2021	Static features are selected and inserted into four different machine learning algorithms for grading the apps as malicious or benign	Other remaining static features can also be explored further to form a greater feature set

3 Discussion

Based on the review of all frameworks, an overall comparative analysis among all malware detection frameworks based on static and dynamic features and hybrid features using artificial intelligence are analyzed. We discover that the hybrid method using artificial intelligence has the best accuracy in comparison with statics and dynamic malware analysis detection approaches. The accuracy efficiency of each framework is analyzed and it is observed that all frameworks have an accuracy efficiency higher than 80%. It is also examined that the DL-Droid malware analysis framework has maximum accuracy efficiency that is 99.6% [31], and machine learning-based android malware detection framework using manifest permissions has minimum accuracy efficiency that is 81% [36].

4 Conclusion

A methodical and chronically literature investigation of the detection and analysis frameworks and techniques for android malware are explained. The work done by researches were reviewed and investigated and existing android malware analysis frameworks were categorized into two categories: (1) static and dynamic malware analysis and (2) hybrid malware analysis using artificial intelligence. These malware analysis frameworks were compared and analyzed according to their specific features and technique. The advantage and disadvantage of each analysis framework were deliberated. It is essential to develop the frameworks which automatically learn without the intervention of human and detect the zero-day malwares. Therefore, artificial intelligence techniques surfaced as a potential solution to handle the different types of malwares. This state-of-the-art research survey is a fundamental instrument for further any research which can make a tremendous change in the development of a new framework.

References

1. Gartner says worldwide sales of smartphones grew in the first quarter of 2020 [Online]. Available: <http://www.gartner.com/newsroom/id/3609817> (2020)
2. Number of smartphone users in India in 2015 to 2020 with a forecast until 2025 [Online]. Available: <https://www.statista.com/statistics/467163/forecast-of-smartphone-users-in-india/> (2020)
3. Trend micro threat report | review, refocus and recalibrate, the 2019 mobile threat landscape [Online]. Available: <https://www.trendmicro.com/vinfo/hk-en/security/research-and-analysis/threat-reports/roundup/review-refocus-and-recalibrate-the-2019-mobile-threat-landscape> (2019). Accessed 25 Mar 2020

4. Bläsing, T., Batyuk, L., Schmidt, A.D., Camtepe, S.A., Albayrak, S.: An android application sandbox system for suspicious software detection. In: 2010 5th International Conference on Malicious and Unwanted Software, October 2020, pp. 55–62. IEEE
5. Zhou, Y., Wang, Z., Zhou, W., Jiang, X.: Hey, you, get off of my market: detecting malicious apps in official and alternative android markets. In: NDSS, February 2012, vol. 25, no. 4, pp. 50–52
6. Balanza, M., Abendan, O., Alintanahin, K., Dizon, J., Caraig, B.: Droiddreamlight lurks behind legitimate android apps. In: 2011 6th International Conference on Malicious and Unwanted Software, October 2011, pp. 73–78. IEEE (2011)
7. Talha, K.A., Alper, D.I., Aydin, C.: APK auditor: permission-based android malware detection system. *Digit. Investig.* **13**, 1–14 (2015)
8. Rodriguez-Mota, A., Escamilla-Ambrosio, P.J., Morales-Ortega, S., Salinas-Rosales, M., Aguirre-Anaya, E.: Towards a 2-hybrid Android malware detection test framework. In: 2016 International Conference on Electronics, Communications and Computers (CONIELECOMP), February 2016, pp. 54–61. IEEE (2016)
9. Sun, M., Li, X., Lui, J.C., Ma, R.T., Liang, Z.: Monet: a user-oriented behavior-based malware variants detection system for android. *IEEE Trans. Inf. Forensics Secur.* **12**(5), 1103–1112 (2016)
10. Wang, X., Yang, Y., Zeng, Y., Tang, C., Shi, J., Xu, K.: A novel hybrid mobile malware detection system integrating anomaly detection with misuse detection. In: Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services, September 2015, pp. 15–22
11. Android aapt—eLinux.org [Online]. Available: http://elinux.org/Android_aapt (2016). Accessed 13 Aug 2016
12. CuckooDROiD: Dalvik monitoring framework for CuckooDroid (2020)
13. Ghahrai, A.: 10+ open source mobile test automation tools. Retrieved September, 16, 2016 (2014)
14. Gunn, S.R.: Support vector machines for classification and regression. *ISIS Tech Rep* **14**(1), 5–16 (1998)
15. Li, K.L., Huang, H.K., Tian, S.F., Xu, W.: Improving one-class SVM for anomaly detection. In: Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 03EX693), November 2003, vol. 5, pp. 3077–3081. IEEE (2003)
16. Shijo, P.V., Salim, A.J.P.C.S.: Integrated static and dynamic analysis for malware detection. *Proc. Comput. Sci.* **46**, 804–811 (2015)
17. Andrew, A.M.: An introduction to support vector machines and other kernel-based learning methods. Nello Christianini and John Shawe-Taylor, Cambridge University Press, Cambridge, 2000, xiii+ 189 pp., ISBN 0-521-78019-5 (Hbk, £ 27.50). *Robotica* **18**(6), 687–689 (2000)
18. Andrew, A.M.: An introduction to support vector machines and other kernel-based learning methods. *Kybernetes* (2001)
19. Dittman, D., Khoshgoftaar, T.M., Wald, R., Napolitano, A.: Random forest: a reliable tool for patient response prediction. In: 2011 IEEE International Conference on Bioinformatics and Biomedicine Workshops (BIBMW), November 2011, pp. 289–296. IEEE (2011)
20. Yuan, Z., Lu, Y., Xue, Y.: Droiddetector: android malware characterization and detection using deep learning. *Tsinghua Sci Technol* **21**(1), 114–123 (2016)
21. Liu, Y., Zhang, Y., Li, H., Chen, X.: A hybrid malware detecting scheme for mobile android applications. In: 2016 IEEE International Conference on Consumer Electronics (ICCE), January 2016, pp. 155–156. IEEE (2016)
22. Winsniewski, R.: Apktool: a tool for reverse engineering android apk files. <https://ibotpeaches.github.io/Apktool/> (2012). Visited on 27 July 2016
23. Saracino, A., Sgandurra, D., Dini, G., Martinelli, F.: Madam: effective and efficient behavior-based android malware detection and prevention. *IEEE Trans. Dependable Secure Comput.* **15**(1), 83–97 (2016)

24. Hou, S., Ye, Y., Song, Y., Abdulhayoglu, M.: Hindroid: an intelligent android malware detection system based on structured heterogeneous information network. In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1507–1515. ACM (2017)
25. Billah, K.E.M., Mourad, D., Abdelouahid, D., Djedjiga, M.: MalDozer: automatic framework for android malware detection using deep learning. *Digit Investig* **24**, S48–S59 (2018)
26. Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., Ye, H.: Significant permission identification for machine-learning-based android malware detection. *IEEE Trans. Industr. Inf.* **14**(7), 3216–3225 (2018)
27. Feng, P., Ma, J., Sun, C., Xu, X., Ma, Y.: A novel dynamic android malware detection system with ensemble learning. *IEEE Access* **6**, 30996–31011 (2018)
28. Ma, Z., Ge, H., Liu, Y., Zhao, M., Ma, J.: A combination method for android malware detection based on control flow graphs and machine learning algorithms. *IEEE Access* **7**, 21235–21245 (2019)
29. Mehtab, A., Shahid, W.B., Yaqoob, T., Amjad, M.F., Abbas, H., Afzal, H., Saqib, M.N.: AdDroid: rule-based machine learning framework for android malware analysis. *Mobile Netw. Appl.* **25**(1), 180–192 (2020)
30. Ma, Z., Ge, H., Wang, Z., Liu, Y., Liu, X.: Droidetec: Android malware detection and malicious code localization through deep learning. *arXiv preprint [arXiv:2002.03594](https://arxiv.org/abs/2002.03594)* (2020)
31. Alzaylaee, M.K., Yerima, S.Y., Sezer, S.: DL-Droid: deep learning based android malware detection using real devices. *Comput. Secur.* **89**, 101663 (2020)
32. Su, X., Xiao, L., Li, W., Liu, X., Li, K.C., Liang, W.: DroidPortrait: android malware portrait construction based on multidimensional behavior analysis. *Appl. Sci.* **10**(11), 3978 (2020)
33. Mahindru, A., Sangal, A.L.: MLDroid—framework for android malware detection using machine learning techniques. *Neural Comput. Appl.* 1–58 (2020)
34. Zhang, N., Tan, Y.A., Yang, C., Li, Y.: Deep learning feature exploration for android malware detection. *Appl. Soft Comput.* **102**, 107069 (2021)
35. Thongsuwan, S., Jaiyen, S., Padcharoen, A., Agarwal, P.: ConvXGB: a new deep learning model for classification problems based on CNN and XGBoost. *Nucl. Eng. Technol.* **53**(2), 522–531 (2021)
36. Mcdonald, J., Herron, N., Glisson, W., Benton, R.: Machine learning-based android malware detection using manifest permissions. In: Proceedings of the 54th Hawaii International Conference on System Sciences, January 2021, p. 6976

Section–B

A Blockchain-Based Secure Car Hiring System



Sonakshi and Seema Verma

Abstract Currently, the blockchain technology is a boom in creating a secure and distributed environment for many real-life applications. Here, the focus is to introduce a car hiring system so that the car owners will get the fare without any significant loss and consumers can hire the car with variety of preferences. The proposed system is designed with blockchain technology; anyone can join the system by entering user's information and is added to the specified block, computing hash for that required block by applying proof of work and storing hash of previous block in it. Thus, the system works on the complexity of blockchain with proof of work. The proposed model is implemented in Python and aims at removal of organizational role from car hiring system using blockchain technology.

Keywords Blockchain · Hash · Nonce · Timestamp · Proof of work

1 Introduction

All the car hiring system these days run under an organization where all a user can do is hire a car and use it for some period of time. As an example, in zoom cars, there is an organizational hold on all the cars and profit from the car, you just have to register yourself on their portal, hire a car, pay and go on. As a conclusion, all the profit goes into the pocket of the organization. After going through the existing systems like decentralized e-Voting portal using blockchain [1], A blockchain-based shopping cart [2], blockchain technology in farmer's portal [3] and securing e-FIR data through blockchain [4], our proposed system provides a distributed system to manage the renting of cars. To conquer this, we are planning to design something which will remove the role of organization between the car and customer. The user for this application can either be a car owner or the renter. For the sake of making this system more secure, we will be using blockchain technology, in which details of each car (owner details and list of customers who have hired the

Sonakshi (✉) · S. Verma

Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India

car) would be assigned a unique hash and stored in a block. Each block would be identified on the basis of that hash value. We are not using any pre-deployed blockchain like Ethereum or hyperledger but developing our own blockchain in Python. This gives us advantage of adding features to the block as per our own requirements [5]. The architecture, working, framework and implementation of basic blockchain using Python are discussed in this paper.

The structure of the paper follows as—blockchain technology is described with its architecture, applications and challenges in next section. The proposed system of car hiring is presented in Sect. 3 followed by the implementation results and analysis.

2 Blockchain

Basically, blockchain [6] provides resistance to change of data stored in it. As the name suggests, it is a chain of blocks. It is also known as distributed ledger technology (DLT), and it is a time-stamped record of unchangeable data. It is an infrastructure behind cryptocurrency. The most common example of blockchain is Bitcoin [5]. Dejan Vujičić, Dijana Jagodić, Siniša Randić in their work “blockchain technology, Bitcoin and Ethereum: A Brief Overview” [7] helped in increasing understanding about blockchain and basic terms related to it. Blockchain consists of different kind of data like in Bitcoin the data field which contains information regarding the receiver, sender and number of Bitcoin to be transferred. Nowadays, blockchain is highly used in IOT field to make smart decisions [8, 9].

2.1 *Blockchain Architecture and Working*

Blockchain architecture consists of nodes, i.e., a computer or user that has a complete copy of block chain ledger, a block, i.e., the data structure that will be storing the data [10]. Block is the smallest building block of blockchain system. A block mainly consists of index, data, block's hash, previous block's hash, nonce and timestamp.

Hash: Hash is encrypted string of data. If the data changes, hash also changes. Each block of a blockchain is assigned a unique hash. If someone tries to change the data of the block, its hash changes and the blockchain comes to know that something is corrupt as somewhere in between the “block's hash” will no more match “previous block's hash” of the next block; hence, any malicious activity gets highlighted.

Previous Hash: Previous hash of a block contains hash of block preceding the current block. It allows us to traverse through the blockchain. And also any malicious activity or attempt to corrupt the blockchain can be encountered with the use of previous hash (Fig. 1).

```

class block:
    def __init__(self, index, timestamp, data, previous_hash, nonce):
        self.index=index
        self.timestamp=timestamp
        self.data=data
        self.previous_hash=previous_hash
        self.nonce=0
        self.hash=self.proof of work()

```

Fig. 1 Data of a single block

```

def proof_of_work(self):
    found=False
    self.nonce=0
    while found==False:
        block_hash=str(self.hash_block())
        if block_hash.startswith('0000'):
            found=True
            self.nonce+=1
        block_hash=str(self.hash_block())
    return block_hash

```

Fig. 2 Procedure and working of proof of work

Data: Data is different for every blockchain. It may be text, audio, video, image or even smaller blockchain. Hash value of a blockchain depends upon the value of data (Fig. 2).

Proof of Work: In this general architecture of blockchain, anyone can corrupt the data of block and calculate the hash for preceding blocks within a few seconds as calculating hash is just a matter of 1–2 s, solution to this is something called proof of work [11, 12]. Working of proof of work can be explained as finding a hash which starts from a specified number of 0's, finding the hash which matches our requirement and takes computational time as the hash is computed again and again until a hash which starts with required number of zeros are found. So with proof of work, if someone tries to corrupt a block, it will take much more time as compared to a general blockchain. A Bitcoin blockchain takes about 8–10 min to add a new block [5].

3 Proposed System (Car Hiring System Using Blockchain)

When we think of hiring a car, all the organizations providing car rental facility are run by organizations that own all the cars. We are providing a connected network of car owners and renters where any car owner can lend their car to someone who is in

need and earn profit from their idle car. In this paper, we are focusing on implementation of such a network of cars. The role of blockchain in this network comes into play when we talk about non changeable or corruptible form of data, transaction or user history. Whenever the user will get involved in the transaction his caroins (used as cryptocurrency in this work later), all other necessary information would be encrypted in the form of hash using proof of work and will be added to the blockchain.

3.1 Framework

The framework of the system which would be working on blockchain follows the algorithm of a simple blockchain. The only difference is that the data field consists of car owner and renter’s name and car number. Other than this, everything is very much same such as the nonce, timestamp, hash and previous block hash. Whenever a new block is created, it goes through the assignment of hash to the block. The block gets its data through the user input which is depicted in the flowchart below. Each block is stored in a secure way using the proof of work mechanism on the localhost server.

In Fig. 3, initially, nonce = 0. As explained in the earlier part of paper. Proof of work increases the computing time by calculating hash again and again until a requirement is met. Hence, it makes the task of interfering with the blocks difficult and time consuming for any fraudulent activity. As depicted by the flowchart as per

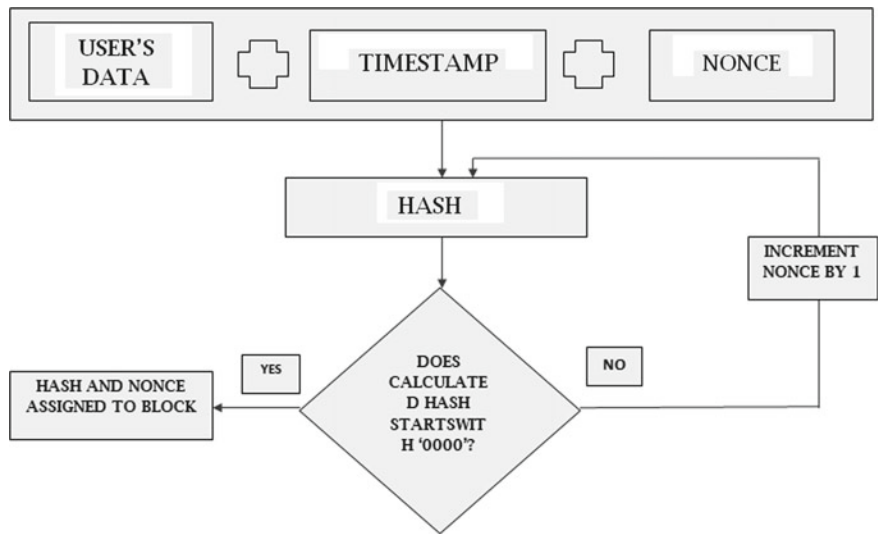


Fig. 3 Framework of hash calculation using proof of work

the difficulty of the developer, the time increases as finding a hash value which starts with some specified number of zeros and is not an easy task. In our paper, we are using a constant difficulty of 4, i.e., only those hashes would be taken which starts with 4 numbers of zeros. From the above flowchart, hash is calculated and assigned to the block. The user is asked to give his/his information and that is stored in the block.

Figure 4 depicts all the relevant information stored in the blockchain for the proposed system. Based on the type of user, the data to be stored in blockchain varies which is shown in the flowchart below. If the user is a car owner, car’s detail and user’s name are stored in the block. Likewise, if the user is a customer, details of car the customer are renting, customer’s name, amount based on user’s decision for hiring with or without fuel is stored in the blockchain.

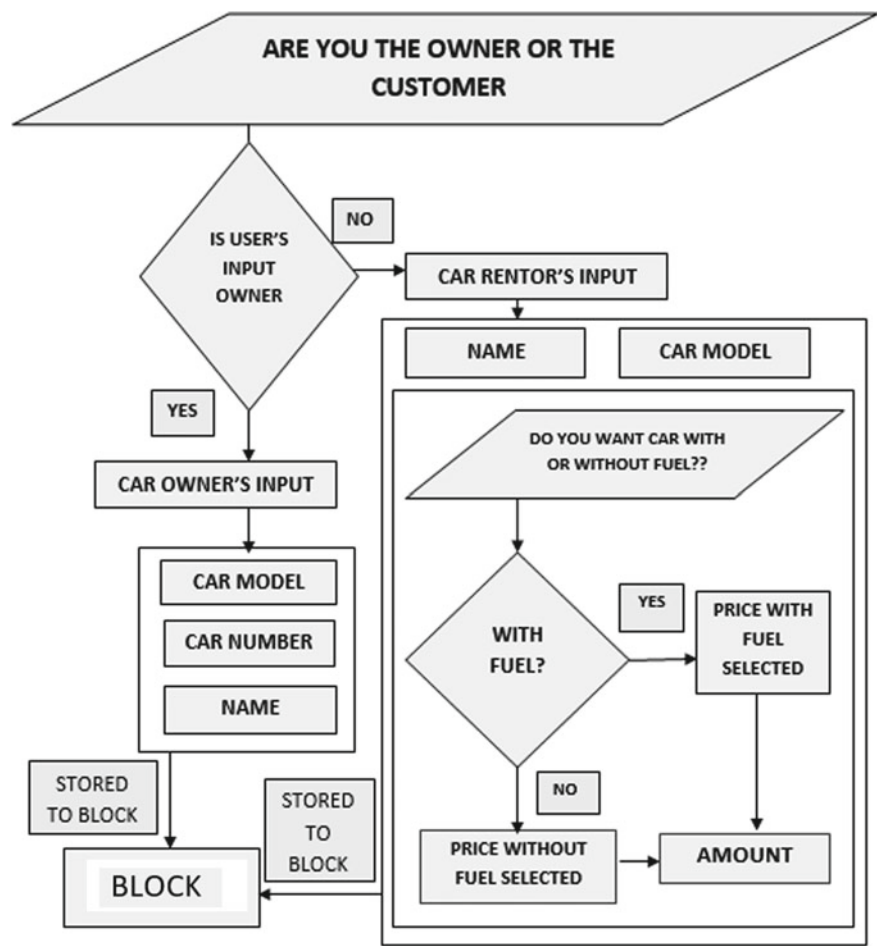


Fig. 4 Structure of block in our framework

3.2 Implementation and Result

Proposed car hiring system is implemented using Python 3.x. Firstly, the user will be identified as renter or owner based on the identification they would be asked to give his/her information which would be used in calculation of hash, and the user will get added in the blockchain running on the localhost server.

Python libraries used in its implementation are as follows:

1. Flask: This library is used for running web applications using Python. It is easy to use and have many applications.
2. sqlite3: It is used to run the database for keeping the records of various cars with its prices and availability.
3. hashlib: It is used for generating hash values for the blocks of blockchain. We here used SHA256 although there are many algorithms for the same including SHA1, SHA224 and SHA384, etc.
4. datetime: This library can be used in multiple ways for providing various timestamps. We used this to capture the time and date of a transaction made to hire a car.

Figure 5 depicts the blockchain running on localhost server as a flask application on the localhost server. This blockchain can be made available externally by running it on localhost:0.0.0.0 server, by default it is running on localhost:5000.

Case 1: The user is an owner.

Figure 6 depicts the interface for user depending upon their needs. If the user is a car owner, all the relevant information of that user is asked with the car details and availability.

Case 2: If the user is a customer.

If the user is a customer and wants to rent a car, the user is asked the information as shown in Fig. 7.

3.3 Analysis

The existing rental system like Yolo bikes and Zoom cars provide their vehicle to the renters for riding purpose for specific period of time at some pre-defined rates

```
===== RESTART: C:\Users\aa\Desktop\blockchain\block.py =====
* Serving Flask app "block" (lazy loading)
* Environment: production
WARNING: This is a development server. Do not use it in a production deployme
nt.
Use a production WSGI server instead.
* Debug mode: on
* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
```

Fig. 5 Starting the blockchain server

```

===== RESTART: C:\sqlite3\car_interface.py =====
Do You Want To Earn From Your Idle Car??? (y/n) y
Enter your namesonakshi
(car_ID, car_name)
(1, 'Hyundai Creta AT')
(2, 'TATA Tiago')
(3, 'Maruti Swift')
(4, 'Mahindra Scorpio')
(5, 'Hyundai Creta')
(6, 'Mahindra Marazzo')
(7, 'nano')
Choose Car ID corresponding to your Car Model if not available enter N5
('Hyundai Creta',) registered
Enter Your Car NumberDLDE325
Enter Your Citydelhi
Enter Your Mobile Number1234567890
Enter Your Email Idsona@gmail.com
Enter The Week's day when your car is availablewednesday
Enter the duration (Eg:2:00PM-7:00PM)1:00-4:00PM

```

Fig. 6 User interface for case 1

```

===== RESTART: C:\sqlite3\car_interface.py =====
Do You Want To Earn From Your Idle Car??? (y/n) n
enter your namehimani
If you want to rent a car these are the available cars with their price
('car_id','car_name','price without fuel','price with fuel')
(1, 'Hyundai Creta AT', 5163, 8580)
(2, 'TATA Tiago', 4623, 2782)
(3, 'Maruti Swift', 5700, 3400)
(4, 'Mahindra Scorpio', 6533, 3900)
(5, 'Hyundai Creta', 6500, 3940)
(6, 'Mahindra Marazzo', 7400, 4500)
(7, 'nano', 4500, 4500)
(8, 'WagonR', 5500, 5500)
Enter the car's ID in which you are interested
5
(5, 'Hyundai Creta', 6500, 3940)
Hyundai Creta selected
enter 1 for car with fuel and 2 for car without fuel
you have to pay 6500
enter your license numberSJDFIJE3432
enter your adhaar numberA45WEJ3
enter your phone number2545965
enter email IDhimani@gmail.com

```

Fig. 7 User interface for case 2

and fine (in case of any damage or exceeding the deadline for returning of their vehicle). In such system, all the vehicles are under one organization that has a centralized hold on the vehicles and profit made out of them. Taking an instance of OLA or Uber Cabs, if a person needs to go to airport, suppose he books a cab from his home to the airport, but after that, he has to pay for another cab from airport to hotel on the other side. Additionally, if someone's car returns with a scratch or dent, or if the owner finds that the car has violated any traffic rule and "challan" has been filed in his name the customer shall be liable to pay it and should be blocked to hire

Table 1 Comparative analysis between the existing and proposed system

Parameters	Existing system	Proposed system
Decentralized	No	Yes
Profitable	To organization	To general people
Secure	No	Yes
Employability opportunity	None	To car owners
User verification	Centralized	Distributed

any other car in future. Here, anyone who own a car can earn from their car by giving it on rent for a specific period of time, and any other person who is in need to get a car for approximately the same period of time can come and rent the car. So from the customer point of view, their problem of renting a car from home to airport and airport to hotel is gone, and from the owner point of view, the centralized hold on cars is gone.

For increasing the security, consensus and proof of work algorithm are applied to the blocks [5]. The proof of work increases the computational time of the hash and hence makes the task of changing data of blockchain a big challenge. To change the blockchain’s data after the application of proof of work needs a group of miner that can control 50% of the network mining rates, this is known as 51 attack and is not easy to implement it on a well-developed blockchain. The proposed approach starts with gathering user’s information and adding it to the specified block, computing hash for that required block by applying proof of work and storing hash of previous block in it (Table 1).

4 Conclusion

Current car hiring system is completely dependent on a single organization, centralized system. In case of zoom car or instance of yolo cycles all work on same framework and business model. Here, a completely different model is proposed for car hiring system. The proposed system with blockchain technology has provided security and hence has acted as a helping hand in gaining customer trust. The proposed model aims to remove organizational hold on car hiring system, and this system would not only benefit car renters but also will provide employment opportunity to many. Its user interface could be further enhanced by associating a web application or website with it.

References

1. Patidar, K., Jain, S.: Decentralized E-voting portal using blockchain. In: 10th ICCCNT 2019, 6–8 July 2019, IIT-Kanpur, Kanpur, India (2019)
2. Shrestha, A.K., Joshi, S., Vassileva, J.: Customer data sharing platform: a blockchainbased shopping cart. In: IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (2020)
3. Talreja, R., Chouksey, R., Verma, S.: A study of blockchain technology in farmer's portal. In: Second International Conference on Inventive Research in Computing Applications (ICIRCA-2020). IEEE Xplore (2020)
4. Khan, N.D., Chrysostomou, C., Nazir, B.: Smart FIR: securing e-FIR data through blockchain within smart cities. In: IEEE 91st Vehicular Technology Conference (VTC2020-Spring) (2020)
5. Jain, R., Dogra, A.: Solar energy distribution using blockchain and IoT integration. In: IECC'19, Okinawa, Japan (2019)
6. Memon, M., Hussain, S.S., Bajwa, U.A., Ikhlas, A.: Blockchain beyond bitcoin: blockchain technology challenges and real-world applications. In: 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (2018)
7. Vujičić, D., Jagodić, D., Randić, S.: Blockchain technology, bitcoin, and ethereum: a brief overview. Ministry of Education, Science, and Technological Development of the Republic of Serbia (2018)
8. Zorzo, A.F., Nunes, H.C., Lunardi, R.C., Michelin, R.A., Kanhere, S.S.: Dependable iot using blockchain-based technology. In: Eighth Latin-American Symposium on Dependable Computing (LADC) (2018)
9. Choi, S.S., Burm, J.W., Sung, W., Jang, J.W., Heo, Y.J.: A blockchain-based secure iot control scheme. In: 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE-2018) Paris, France (2018)
10. Syed, T.A., Alzahrani, A., Jan, S., Siddiqui, M.S., Nadeem, A., Alghamdi, T.: A comparative analysis of blockchain architecture and its applications: problems and recommendations. Deanship of Research, Islamic University of Madinah, KSA (2019)
11. Gemeliarana, I.G.A.K., Sari, R.F.: Evaluation of proof of work (pow) blockchains security network on selfish mining. In: International Seminar on Research of Information Technology and Intelligent systems (ISRITI) (2018)
12. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains (2016)

A Correlation Blockchain Matrix Factorization to Enhance the Disease Prediction Accuracy and Security in IoT Medical Data



P. Renuka and B. Booba

Abstract An IoT software product's reliability is the probability of the product working "correctly" under or over a given time. New opportunities are the result of expansion in the fast-paced Internet of Things (IoT) space. IoT technologies on the collected datasets improve disease progression technology, disease prediction, patient self-management and clinical intervention. To propose, the IoT with cipher block chaining in the traditional cryptographic operation mode will be used for cryptographic processing. Developing models for the supervised learning classification and security of imbalanced datasets is challenging, especially in the medical field. However, most real-time IoT datasets present most traditional machine learning algorithms challenging unbalanced datasets. Proposed a new framework for the Correlation Blockchain Matrix Factorization Classifier (CBMFC) related to comprehensive medical records. CBMFC uses a multiple class label machine learning that represents an independent population model based on disease meta functions such as profile age, group, or cognitive function keys. The Pairwise Coupling Multi-Class Classifier (PCMC) is used to prove the model's correctness. This produces more comprehensive data in various machine learning environments, such as predictive classification, similar to real data performance. For the results of security analysis confirmation, the proposed IoT application model's effectiveness can withstand various attacks, such as selected cryptographic attacks. In this proposed CBMFC system, classification accuracy, precision, recall, execution time and security matrix are used to evaluate performance.

Keywords Internet of Things • Correlation Blockchain Matrix • Pairwise Coupling Multi-Class Classifier • Cryptography

P. Renuka (✉) · B. Booba
VISTAS, Vels University, Chennai, India

1 Introduction

The use of the Internet of Things (IoT) in healthcare is sharply increased among a variety of specific Internet-use cases. The Medical Internet of Things takes more effort to improve care itself, with remote monitoring as the broader primary application of remote medicine. The synergies between medicine and technology have taken great strides around the world. For example, the Internet of Things (IoT) data analytics is gaining popularity, providing the next generation of electronic healthcare and mobile healthcare services. They are transforming traditional institutions based on the management of large data with a blockchain solution. The chain's evolution is in favor and permitted by technical means to maintain the support of strategic applications needed for its potential growth. In the cloud-enabled network blockchain, there are trading and mining nodes both in the cloud and on-premises. According to embodiments, the node may be an enterprise-level server. The final level of overall collaboration on evolution is based on cloud and blockchain applications as the basis for distributed chains' operation. The devices configured to use public blockchain services and private blockchain nodes clouds to communicate securely via APIs. The IoT devices combining blockchain technology as a security framework IoT system using secure distributed key management techniques make it possible to discover each other and transaction encryption machine-to-machine.

In this, Fig. 1 represents the cloud blockchain network communication. Machine learning techniques have been widely used in the medical field. Most of the medical data resources can use to transfer valuable knowledge to assistive scientific decision making. It is stored in each hospital or other medical institution separately, which poses a major issue to the medical data applied to the constructed prediction model, its quality and efficiency. For medical professionals, researchers, there are several machine learning techniques to be used throughout disease research. Medical data keeps a history of patient records and will be unused in the future. This can be analyzed and considered for future research. This huge database is analyzed to identify machine learning techniques used by healthcare staff to predict patient risk.

The most commonly used machine learning technology, which may be registered in the category. Occupies a set of pre-classified patterns to create a demographic model classification. Learning and classification are involved in a process called data classification. The training data is being learned and analyzed by a classification algorithm. The test data is used for classification to approximate the classification rules. The rules can apply to the new data tuple with acceptable accuracy. The pre-classification example has been used in the classifier training algorithm to verify the group that requires the appropriate identification parameters. This section discusses the process of classification of disease analysis using IoT clinical data and machine learning methods.

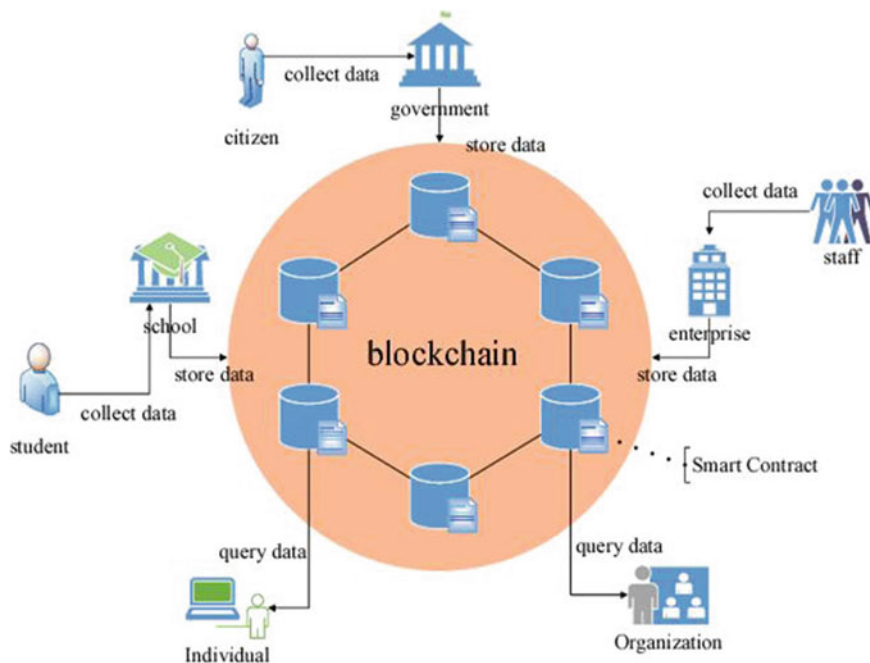


Fig. 1 Cloud blockchain network model

2 Related Work

The literature survey for various IoT blockchain security methods and disease classification strategies used to predict the result is discussed below.

Co-clustering is used simultaneously to group clinical features and patients to characterize block-wise data loss patterns [1] (A) group-based feature selection and data imputation for specific patient subgroups. (B) Miss the predictive model to consider data availability. The machine learning (ML) method of decision making and the medical field's data has proven highly predictive and supportive. ML technology's latest developments in the Internet of Things (IoT) [2] are being used. The task of breath estimation task [3] compares the performance of different machine learning techniques. Problems can be divided into two categories: high and low breathing work based on information extracted from pressure, volume and flow through signals recorded by mechanical ventilation.

Select the feature to solve the problem, and the proposed method is novel, rapid provision of mutual information to select the feature [4]. The feature selection algorithm improves the classification accuracy and is used to select the function to reduce the classification system's execution time. The neural network modification uses structured data and unstructured data and recommends a conventional neural network (CNN) basic peak disease risk prediction algorithm [5]. To the best of our

knowledge, existing work focuses on these two types of medical big data analytics. Machine learning technology has been used for [6] vegetation parameter estimation and disease detection; the effects of the disease symptoms on their performance have been small. Prevention to predict the actual occurrence of the pre epilepsy can help through therapeutic intervention [7]. Studies had found that abnormal activity in the brain begins minutes before the onset of a seizure, called a predictable condition.

Proposed DualFog-IoT is compared to the IoT-based architecture of the existing centralized data center. Having a genetic characteristic of blockchain, the proposed model system decreases rates and furthers existing IoT ecosystems unload minimum upper grayscale and [8, 9] to reduce the cloud data center. Blockchain technology's complexity is maintained for most developers or teams to build, usually expensive and difficult to monitor the support blockchain network in their application. This algorithm thereby forces the redesign of blockchain that uses cryptosystems to resist quantum attacks, creating quantum-fixed or quantum-resistant cryptosystems, called quantum proofs, called post-quantum [10]. Threatens public key cryptographic hash functions. If all copies of the opponent store segments [11], the opponent can leave the system, causing a permanent loss of segments due to the blockchain system's malfunction.

The unique geometry of [12] high-dimensional data using a manifold learning and support vector machine (SVM) proposed PVC detection and data visualization method. [13, 14] has proposed some of the blockchain-based storage systems in recent years. In most cases, the blockchain acts as a "witness of the agreement" with publishers. This method is, so far, because it is not managed to reduce the size of the blockchain itself, and it will not be able to avoid the storage model of Bitcoin. Maintaining this also a complete record of blockchain implementation in the IoT environment helps to insufficient storage capacity on edge devices. At the same time, the system does not require any significant transactions per second [15]. Even segment blockchain is used to improve blockchain sharing by separating transaction storage from transaction validation.

Our main contribution is to link the probability of failure as a group to each epoch by using the probability limit as the sum of the upper limit hypergeometric [16] and the two types of distribution. It is a reliable data management scheme based on blockchain in edge computing (BlockTDM called) [17] that has been proposed to solve the above problems. The flexible configuration of blockchain architecture, mutual authentication protocol, flexible consensus, smart contract management module and transaction data and blockchain node management and deployment are among them. Algorithms included artificial neural networks (ANN) [18], support vector machine (SVM), naïve Bayesian classifier (NBC), boosted decision trees (BDT) and multivariable logistic regression (MLR).

However, one of the important problems of fog computing and blockchain [19] integration is scalability. The group chain has proposed a new type of scalable public blockchain for the double-stranded structure of IoT services computing fog of computing. Despite its potential, there are some urgent problems to be solved to make the IoT services are widely used. Various loosely coupled distributed

intelligence [20] to adjust the connection operation requires an IoT device for managing the system. Developers' point of view analyzed blockchain from [21] blockchain, a larger software system, highlighting data storage and combination key concepts and considerations.

Two methods are currently introduced based on the heterogeneous network, protein interactions, genotype—is built using the phenotype correlations and phenotypic similarity. In HeteSim_MultiPath (HSMP) [22], HeteSim scores different routes contributing to the longer path and the damping constant. Therefore, a non-invasive diagnostic system based on machine learning (ML) has been developed to solve these problems. The decision-making system of experts based on the application of machine learning classifiers and artificial fuzzy logic is an effective diagnostic result; the mortality rate has decreased [23]. Therefore, no clear requirements should be treated as a technique to identify the most appropriate parameters during predictive analysis.

Instead, the feature extraction time-series EEG is converted to a time-frequency distribution (TFD) [24]. Gradient boosters use a set of programs aside to train the entire TFD directly. This paper proposes a machine learning method for predicting particulate matter concentrations from wind and precipitation levels, based on [25] two-year weather and air pollution data.

This paper [26] has been used to record valid composite minorities oversampling to generate new composites. Baldwinian learning and PSO (BLPSO) [27] are based on a novel hybrid algorithm to increase particle diversity and prevent premature convergence of PSO. Ability to compare calculated heart rate variability (HRV) baselines before the start of daytime antibiotics (LOS group) or during a randomly selected period (control group) during the calibration period [28].

In the future, Moderate Resolution Imaging Spectrum radix statistical model for predicting fire activity for 1–5 days to use satellite fire counts and meteorological data from temporary reanalysis [29] to develop. The component contains an apnea event [30], which automatically proposes the first use of EIT boundary voltage data from infants to obtain the main function of research apnea detection using machine learning. Factorial switching in linear dynamic systems is a common framework for addressing this issue [31].

This analysis of the previous method has a low classification accuracy and less security performance to introduce a new method in the next section.

3 Implementation of the Proposed Method

This IoT application model's main motivation is to provide a computationally secure key generation for protected data through encryption with blockchain technology. A master key is a secret key that is accepted between communicating parties before a communication protocol begins. The essential characteristic of machine learning is the design of heterogeneous data applications with different dimensionalities. Various IoT application consists of different information collected

by recording the data for producing diverse data representations. The collection of data is carried out by distributed and decentralized control with autonomous data sources.

Correlation Blockchain Matrix Factorization Classifier (CBMFC) algorithm is used to classify the given data into several columns and provide security in medical data information. Blockchain HMAC encryption is the enforcement of access control mechanisms, digital signatures, routing controls, notarization, etc., to provide data security services against attacks and prevention. The digest is calculated for ciphertext messages using the HMAC encryption algorithm. HMAC stands for the Hash-based Message Authentication Code. This authentication uses a key to implement the hash function product along with the content of the message. From Fig. 2, first, preprocess the data using Co-relational Matrix Data Preprocessing to remove the noise. The model is mainly executed in the preprocessing task. It presents a preprocessing task to remove noise and inconsistent data obtained from various sources. Interval-based measures are the discretization factors from large data applications, and the measured values reach the closest values. Data preprocessing is usually done to see if there is redundant information in the dataset. All attributes are initially considered separate subsets, with the final combination of attributes and features is marked as the highest subset of features. The hash value is stored on each block; if any new record enters the storage, it will update into the previous block. This proposed framework reduces the clustering task; a grouping of the same attributes occurs by using our framework for predicting the disease using a given disease dataset.

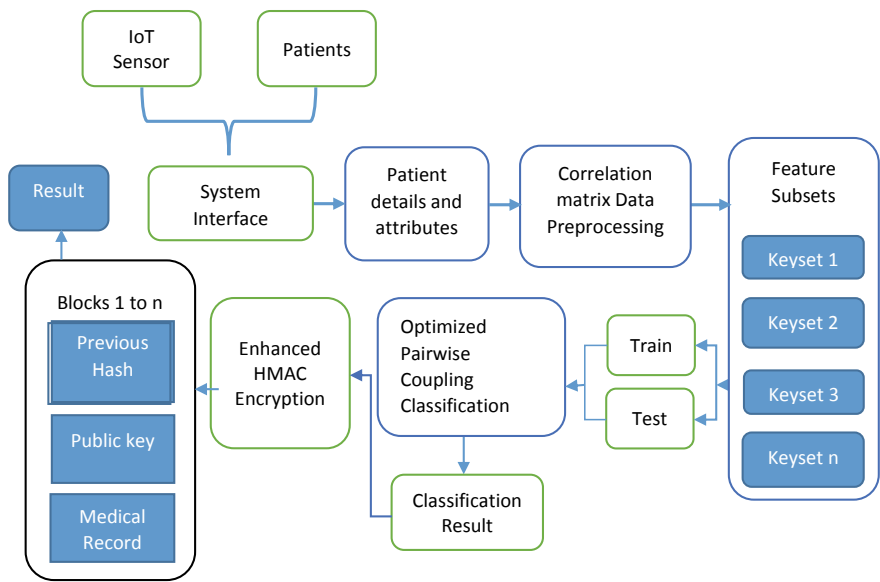


Fig. 2 Proposed Method CBMFC block diagram

3.1 Correlation Matrix Data Preprocessing

The initial stage in Correlation Matrix Data Preprocessing is finding the unrelated data and normalized datasets. While processing the data, it is essential to calculate the univariate stats like the mean value, standard error, and rate of recurrences to inspect the volume of missing data. In complete information, maximum likelihood the population criteria have approximated that would probably generate the estimate values from the sample set which is analyzed. The classification accuracy depends upon the accuracy of data, so data should be non-ambiguous, correct and complete. Data collection methods are loosely controlled, resulting in inappropriate values like out-of-range missing values. Correlation matrices are useful for showing the correlation coefficient (or degree of relevance) between variables. The correlation matrix is symmetric, just as the correlation between $V1$ and $V2$ is the same as the correlation between $V2$ and $V1$.

Let the data matrix V composed to n -dimensional observation dataset, and individual variable values (V) size of $[R \times n]$. To assume the row of R has centered, observe all the row values i to n . The correlational $\sum$ of each row V data.

$$\sum = \text{cor}(V) = E[V^T] \quad (1)$$

To estimate the correlation data matrix.

$$E[V^T] \approx \frac{V^T}{n} \quad (2)$$

Form the Eq. (2), matrices as the product of two simpler matrices E and L , using a procedure known as Eigenvalue Decomposition.

$$\sum = EL^{-1} \quad (3)$$

The data matrix E is resized $[R \times C]$ matrix, where each column to apply the eigenvector.

From Eqs. (2, 3), derivation of the correlation matrix is as follows,

$$\rho(R, C) = \text{corr}(R, C) = \frac{\text{cov}((R, C)V)}{\sigma_R \sigma_C} = \frac{E[\text{cov}(((R - \mu_R)(C - \mu_C))V)]^{-1}}{\sigma_R \sigma_C} \quad (4)$$

All such data discrepancies can lead to wrong research results; thus, data is processed before applying an algorithmic technique for better and improved results. Data needs to be preprocessed to ease the entire data process to improve machine techniques' efficiency. The main steps used for preprocessing the data include data cleaning, data integration, data conversion and data reduction. In this, fill attribute

values with the correlation value for unknown instances and convert all disease databases in a single file format.

3.2 Medical Feature Selection

A feature is that a subset selection which is a preprocessing step used in machine learning. It aims to increase learning accuracy to reduce and eliminate invaluable and irrelevant data dimensions. It indicates specific problems and their functions and the type of prediction that will be useful.

The input dataset is fed into the feature selection method block, where the feature selection is made according to the given dataset. It will take this way to reduce the number of attributes selected for a given number of dependent attributes.

The medical algorithm feature selected by randomly sampling instances from the training data and the selection process is shown in Fig. 3. It has been found that the nearest value class (adjacent value) of the same class is opposite each time to select the best models. The characteristic weight is based on its value to distinguish the example for detecting the model or has been updated from the latest hit and latest features.

$$\text{Weight } (W_m) = \sum_{i,j=0}^w f_m - \frac{(U, V, S)^2(i)}{N} \quad (5)$$

$$\text{Gain } (G_m) = \sum_{i=0}^n S_i \log_2 \quad (6)$$

where f_m , the weight for attributes U, V , which are randomly sampled instances, S is the latest hit and N is the number of randomly sampled instances. The function diff calculates the difference between two instances of a given attribute.

f_m is an attribute of U, V , if they are an approximate model example, S is the recent success and N is the approximate number of sample events. The functional differences are calculated as the difference between the two events of a given

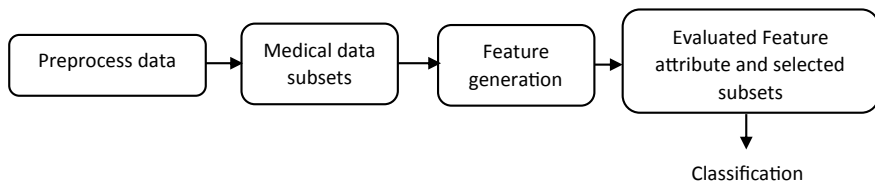


Fig. 3 Best feature selection process

attribute. The difference between the continuous attribute is the actual difference normalized to the interval $[0, 1]$.

Algorithm steps

Input: training data D and feature subsets f_{n-1}

Input: training data D and feature subsets f_{n-1}

Step 1: Initialize the Attribute $S = S_1$

Step 2: Calculate the feature weight and gain using above eqs. (5) and (6)

Step 3: $\alpha_f = \max(S_i, G, W)$ to evaluate the best feature (α_f)

Step 4: For each current iteration $\leq N$

If $\alpha_f > th$, then // where th is represented a threshold value.

$$f'(D) = S \cup \left(\frac{G(n)+W(n)}{\alpha_f} \right) \quad (7)$$

Feature $\oplus f'$;

End

If available in the presence and corresponding class distribution of the feature, feature selection measures the amount of information about the class prediction bit.

3.3 Optimized Pairwise Coupling Classification (OPCC)

It also serves as a classification mark supervised learning method and a statistical method of classification. It considers a basic natural model and assigns it to us by determining the probability of imprisonment with uncertainty in the moral model. This feature is characterized by information gain, and then, the best ranking features are selected as the best attributes to use in the classification.

Algorithm steps:

Step 1: Read data $Ds = \{ \{P_i, Q_i\} / i=1, 2, 3 \dots n \}$ be the set of training data.

Step 2: Initialize the random weight support values, $W(0)$.

Step 4: For each training data $(P_i, Q_i) \in Ds$.

To analysis the predicted output $Y_i^{\wedge}(k)$

For each weight, we do.

Update the weight $(k+1) = W_j(k) + (y_i - y_i^{\wedge}(k)) x_{ij}$.

End for.

End for.

Step 5: Until disease predicts the output.

The attributes are determined for each attribute's information to gain to classify a set of data segments. Then the information gain must be selected maximized attributes. After the classification result was stored in the database using HMAC encryption with blockchain.

3.4 HMAC Encryption and Blockchain Security Model

The Hash-based Message Authentication Code (HMAC) algorithm is implemented using binary operations and hash functions. HMAC is calculated with any cryptographic hash function; the resulting MAC algorithm is called HMAC-MD5. The security strength provided by the HMAC algorithm depends on the HMAC key, the most basic hash algorithm and the security features of the MAC Tag length. MAC is calculated using the data on the HMAC function, and the following operation is performed:

$$\text{HMAC}(k_1, k_2, \text{data}) = \text{hash}((k_1, \text{inner}) || (k_2, \text{outer})) \text{ t} \quad (8)$$

where t = time, k_1 and k_2 = a pair of keys (encryption and authentication).

Algorithm steps

Input: document, MK- master key, HMAC encryption key (k1, k2).

Step 1: To initialize the MK, $k1, k2$.

Step 2: compute the HMAC tag for authentication to create a block.

Step 3: To encrypt the document using the XOR function

Step 4: read the data hash function to generate the MK, $k1, k2$

XOR generate 64{MK, $k1, k2$ }

Step 5: If the tag T equal, then

to connect the blockchain network and authenticate the user.

Else

return

Step 6: Store the document SD

Step 7: mapping the authentication key to the array and remove the special characters, spaces from SD.

Step 8: for n to string

$K_{SD} = H_{k1}(A_i)$ // where, $H_{k1(x)}$ is hash key 1 and A_i authentication key

Convert to K_{SD} to integer list and remaining truncate bits

End

Step 9: Decryption process and verification key

for n to the number of character

If (SD is an integer), then.

$P(C_i - K_{SD(i)}) \bmod 10$ // where p is integer array and C_i ,

character array.

Else

$$P(C_i - K_{SD(i)}) \bmod 26$$

Return

End

End

Step 10: Mapping and validate the p array data to x .

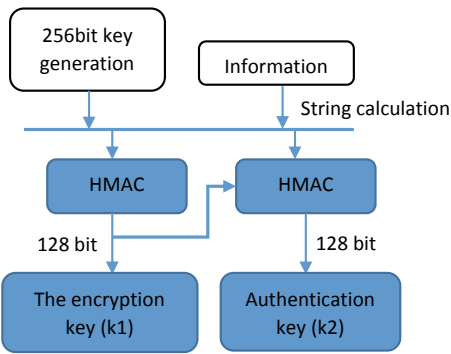
It is considered an easy way to compute the MAC value $h(x)$ for a given k and an arbitrary input x (Fig. 4).

$H_{k1(x)}$ is mapped to a message x of arbitrary length value having n number of fixed bits.

It is considered impossible to calculate the MAC value $hk(m)$ of a new message m if the key k is unknown, though we get MAC values of other messages.

Protecting HMAC is used to demonstrate the correct data relationship between the designer’s embedded strength and the HMAC hash function. In terms of an embedded hash function, the HMAC function’s strength for basic hash function encryption within security depends in a certain way. HMAC function is usually a safe and predetermined number of successes based on the probability of fraud. Created based on the time spent using the same key to create a MAC message.

Fig. 4 Process of Key Generation



3.5 *Blockchain Network Construction Algorithm:*

Step 1: To initialize the index of the variable (IN), Timestamp (Ts), Node Information List (NI), Previous Hash (PH), Data Identity (DI).

Step 2: Create a new block.

IN = Chain.Count // in this chain count is the total number of the node to enter the network

TS = DateTime.UtcNow

NI = {user request, request ID, ssLocation}.to list

PH = Get hash (Chain.Last)

DI = current data-id

Chain.add(IN, TS, NI, PH, DI)

Step 3: To create a user transaction data-id (DI)

DI =0

While (Is not valid (last DI, Current DI, PH))

DI++

Return DI

Step 4: To register the users in blocks.

For each user in users

$URL_{node} = \$ "http// \{user\ id\} "$

Register user (URL_{user})

Insert (user.count()) //new user is added.

End

Step 5: Check the user information and database block

If (block is empty == 0)

Go to step 2

Else

Verify the block attacker or not

Record = data size

IN = block.IN, TS = block.TS, NI = block.NI, PH = block.PH

For the user in u // u=users

PH (k) = HMAC [k] // k is keys

To evaluate the user (Li) using.

$$U(i) = IN_{n(i)}.getvalue + TS_{n(i)}.getvalue + NI_{n(i)}.getvalue + PH_{n(i)}.getvalue$$

End for

End if

From the above algorithm step to form the network group, the user can upload their document to a centralized server with encrypted format help of HMAC encryption. The HMAC authenticates the user using the master key for help to encrypt and decrypt the documents. This blockchain network incorporates patient medical data to diagnose and predict disease, and the resultant data is stored securely.

4 Result and Discussion

Statistics provide a strong basic background for quantifying and assessing results. However, it needs to be modified and tweaked for statistics-based algorithms before being applied to the IoT blockchain method. This section presents the results of a work that proposed a technique for predicting disease using machine learning.

Table 1 Simulation parameters

Parameters	Values
Language	C#
Dataset name	UCI Machine learning repository
Diseases	Cardiology
Total number of data	1500
Train data	1000
Test data	500

Section analysis to take cardiology disease data and some parameters (Temperature, heart rate and blood pressure) are considered to predict the disease level. Table 1 represents the simulation parameter of the proposed method to use.

The number of correctly classified files with patient data according to the total number of files is defined as classification accuracy. This proposed method evaluates the following Eqs. (9, 10, 11, 12) for classification accuracy, precision, recall, F1 score, security and authentication time analysis. The Correlation Blockchain Matrix Factorization Classifier (CBMFC) method prediction accuracy is compared to the random forest, Bayesian classifier and SVM methods. Similarly, the proposed method’s security analysis, Enhanced HMAC Blockchain (EHMACB) security, compares to existing method Blowfish, MD5 and MidChain methods (Fig. 5).

Different bytes of data are taken to estimate the method proposed in this execution time analysis. In this proposed method, EHMAC is compared to existing methods Blowfish, MD5 and MidChain. The proposed method is to authenticate users and store the data to the network within 270 ms less execution time than the HMAC blockchain method.

Figure 6 represents the comparison of the proposed and existing method graph. In this analysis of security result, the proposed method EHMACB provides a 93.5% security compare to existing methods MidChain has 91.3%, MD5 has 85.6% and blowfish has 83.4% security in the medical blockchain network. The machine

Fig. 5 Execution Time Analysis

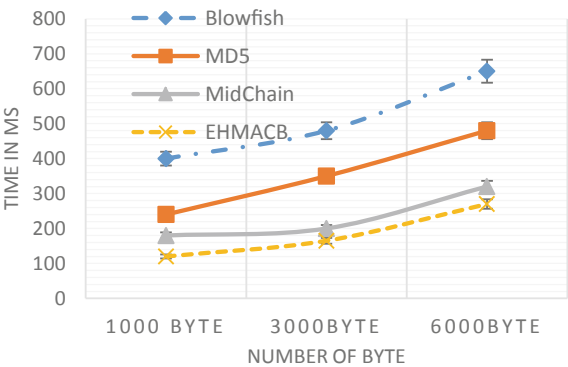
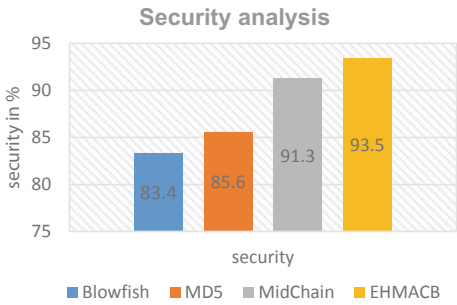


Fig. 6 Comparison of Security Analysis



learning performance of the clinical dataset classification after the analysis is evaluated using the equation below.

$$CA = \frac{\text{Number of classified files}}{\text{number of files}} * 100 \tag{9}$$

$$\text{Precision} = \frac{\text{true positive}}{\text{true positive} + \text{false positive}} * 100 \tag{10}$$

$$\text{Recall} = \frac{\text{true positive}}{\text{true positive} + \text{false negative}} * 100 \tag{11}$$

$$F1 = \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \tag{12}$$

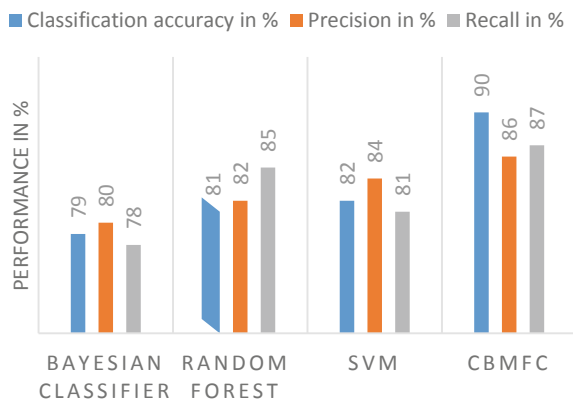
Table 2 shows a comparison of the existing and proposed method disease prediction performance. Table 2 shows the classification accuracy, precision, recall, proposed method CBMFC, existing methods SVM, random forest and Bayesian classifier (Fig. 7).

Using a pairwise coupling method to evaluate a two-pair feature matrix improves classification and prediction accuracy. The proposed machine learning method results provide higher performance than SVM, random forest and Bayesian classifier.

Table 2 Analysis of proposed method prediction performance

Methods	Classification accuracy in %	Precision in %	Recall in %
Bayesian classifier	79	80	78
Random forest	81	82	85
SVM	82	84	81
CBMFC	90	86	87

Fig. 7 Proposed method performance of prediction analysis



5 Conclusion

A given patient's cardiology disease needs to be diagnosed accurately and in time. The proposed Correlation Blockchain Matrix Factorization Classifier (CBMFC) analysis the IoT data disease prediction. First, to apply the co-relational matrix for preprocessing to remove the noise from the IoT dataset. Finally, a Correlation Blockchain Matrix Factorization Classifier (CBMFC) method uses the train data and predicts it. The Blockchain Enhanced Hash-based Message Authentication Code (EHMAC) Encryption is used to provide security, it encrypts the user request, and records are stored on blocks. This analysis of the proposed method simulation result has a 90% of classification accuracy, 86% of precision, 87% of recall values and 93.5% of security with 270 ms execution time more efficiently compared to the existing method. This proposed method to implement into hospitals for analysis disease and secure the data form unknown person.

References

1. Wang, H., Huang, Z., Zhang, D., Arief, J., Lyu, T., Tian, J.: Integrating co-clustering and interpretable machine learning for the prediction of intravenous immunoglobulin resistance in kawasaki disease. *IEEE Access* **8**, 97064–97071 (2020)
2. Mohan, S., Thirumalai, C., Srivastava, G.: Effective heart disease prediction using hybrid machine learning techniques. *IEEE Access*, 1–1 (2019)
3. Castro, L.F.B., Santacruz, L.F.E., Sánchez, M.B.S.: Work of breathing estimation during spontaneous breathing test using machine learning techniques. In: 2020 IEEE Colombian Conference on Applications of Computational Intelligence (IEEE CoCACI 2020), Cali, Colombia, pp. 1–6 (2020). <https://doi.org/10.1109/ColCACI50549.2020.9247855>

4. Li, J.P., Haq, A.U., Din, S.U., Khan, J., Khan, A., Saboor, A.: Heart disease identification method using machine learning classification in E-healthcare. *IEEE Access* **8**, 107562–107582 (2020)
5. Chen, M., Hao, Y., Hwang, K., Wang, L., Wang, L.: Disease prediction by machine learning over big data from healthcare communities. *IEEE Access* **5**, 8869–8879 (2017)
6. Ashourloo, D., Aghighi, H., Matkan, A.A., Mobasheri, M.R., Rad, A.M.: An investigation into machine learning regression techniques for the leaf rust disease detection using hyperspectral measurement. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **9**(9), 4344–4351 (2016)
7. Muhammad Usman, S., Khalid, S., Aslam, M.H.: Epileptic seizures prediction using deep learning techniques. *IEEE Access* **8**, 39998–40007 (2020)
8. Memon, R., Li, J., Nazeer, I., Khan, A., Ahmed, J.: DualFog-IoT: additional fog layer for solving blockchain integration problem in the internet of things. *IEEE Access* **7**, 169073–169093 (2019). <https://doi.org/10.1109/ACCESS.2019.2952472>
9. Zhang, W., Zheng, Z., Chen, X., Dai, K., Li, P., Chen, R.: NutBaaS: a blockchain-as-a-service platform. *Comput. Sci. IEEE Access* **7**, 134422–134433 (2019)
10. Fernandez-Carames, T.M., Fraga-Lamas, P.: Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, 1–1 (2020)
11. Xu, Y., Huang, Y.: Segment blockchain: a size reduced storage mechanism for blockchain. *IEEE Access*, 1–1 (2020)
12. Ribeiro, B.R., Henriques, J.H., Marques, A.M., Antunes, M.A.: Manifold learning for premature ventricular contraction detection. In: 2008 Computers in Cardiology, Bologna, Italy, pp. 917–920 (2008). <https://doi.org/10.1109/CIC.2008.4749192>
13. Xu, Y.: Section-blockchain: a storage reduced blockchain protocol, the foundation of autotrophic decentralized storage architecture. In: 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS), pp. 115–125. IEEE (2018)
14. Xu, Q., Aung, K.M.M., Zhu, Y., Yong, K.L.: A blockchain-based storage system for data analytics in the internet of things. In: New Advances in the Internet of Things, pp. 119–138. Springer (2018)
15. Ren, Y.J., Leng, Y., Cheng, Y.P., Wang, J.: Secure data storage based on blockchain and coding in edge computing. *Math. Biosci. Eng.* **16**, 1874–1892 (2019)
16. Hafid, A., Hafid, A.S., Samih, M.: New mathematical model to analyze security of sharding-based blockchain protocols. *IEEE Access* **7**, 185447–185457 (2019)
17. Zhaofeng, M., Xiaochang, W., Jain, D.K., Khan, H., Hongmin, G., Zhen, W.: A blockchain-based trusted data management scheme in edge computing. *IEEE Trans. Ind. Inf.* 1–1 (2019)
18. Mueller, M., Wagner, C.C., Stanislaus, R., Almeida, J.S.: Machine learning to predict extubation outcome in premature infants. In: The 2013 International Joint Conference on Neural Networks (IJCNN), Dallas, TX, USA, pp. 1–6 (2013). <https://doi.org/10.1109/IJCNN.2013.6707058>
19. Lei, K., Du, M., Huang, J., Jin, T.: Group chain: towards a scalable public blockchain in fog computing of IoT services computing. *IEEE Trans. Serv. Comput.* **13**(2), 252–262 (2020)
20. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y.: Consortium blockchain for secure energy trading in the industrial Internet of Things. *IEEE Trans. Ind. Informat.* **14**(8), 3690–3700 (2018)
21. Paik, H.-Y., Xu, X., Bandara, H.M.N.D., Lee, S.U., Lo, S.K.: Analysis of data management in blockchain-based systems: from architecture to governance. *IEEE Access* **7**, 186091–186107 (2019)
22. Zeng, X., Liao, Y., Liu, Y., Zou, Q.: Prediction and validation of disease genes using HeteSim scores. *IEEE/ACM Trans. Comput. Biol. Bioinf.* **14**(3), 687–695 (2017)
23. Ansarullah, S.I., Kumar, P.: A systematic literature review on cardiovascular disorder identification using knowledge mining and machine learning method. *Int. J. Recent Technol. Eng.* **7**(6S), 1009–1015 (2019)

24. Murphy, B.M., Goulding, R.M., O'Toole, J.M.: Detection of transient bursts in the EEG of preterm infants using time–frequency distributions and machine learning. In: 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Montreal, QC, Canada, pp. 1023–1026 (2020). <https://doi.org/10.1109/EMBC44109.2020.9175154>
25. Mbarak, A., Yetis, Y., Jamshidi, M.: Data—based pollution forecasting via machine learning: case of Northwest Texas. In: 2018 World Automation Congress (WAC), Stevenson, WA, USA, pp. 1–6 (2018). <https://doi.org/10.23919/WAC.2018.8430438>
26. Davagdorj, K., Lee, J.S., Park, K.H., Ryu, K.H.: A machine-learning approach for predicting success in smoking cessation intervention. In: 2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST), Morioka, Japan, pp. 1–6 (2019). <https://doi.org/10.1109/ICAWSST.2019.8923252>
27. Leon, C., Carrault, G., Pladys, P., Beuchee, A.: Early detection of late onset sepsis in premature infants using visibility graph analysis of heart rate variability. *IEEE J. Biomed. Health Inform.* <https://doi.org/10.1109/JBHI.2020.3021662>
28. Wang, W., Chen, L., Jie, J., Wang, H., Xu, X.: A novel hybrid algorithm based on baldwinian learning and PSO. In: 2010 International Conference on Computational Aspects of Social Networks, Taiyuan, China, pp. 299–302 (2010). <https://doi.org/10.1109/CASoN.2010.73>
29. Graff, C.A., Coffield, S.R., Chen, Y., Fofoula-Georgiou, E., Randerson, J.T., Smyth, P.: Forecasting daily wildfire activity using poisson regression. *IEEE Trans. Geosci. Remote Sens.* **58**(7), 4837–4851 (2020). <https://doi.org/10.1109/TGRS.2020.2968029>
30. Vahabi, N., Yerworth, R., Miedema, M., van Kaam, A., Bayford, R., Demosthenous, A.: Deep analysis of EIT dataset to classify apnea and non-apnea cases in neonatal patients. *IEEE Access* **9**, 25131–25139 (2021). <https://doi.org/10.1109/ACCESS.2021.3056558>
31. Quinn, J.A., Williams, C.K.I., McIntosh, N.: Factorial switching linear dynamical systems applied to physiological condition monitoring. *IEEE Trans. Pattern Anal. Mach. Intell.* **31**(9), 1537–1551 (2009). <https://doi.org/10.1109/TPAMI.2008.191>

A Self-Sovereign Identity Management System Using Blockchain



Tripti Rathee and Parvinder Singh

Abstract Blockchain is emerging as a functional technology for remodeling current technologies and also for creating new applications which in practical was not possible earlier. In this paper, we are building a self-sovereign identity management system using blockchain (*BSelSovID*). The application will serve as an interface to all the entities involved, viz. user, authority, and verifier. The use of blockchain is to dodge the centralized identity manager. The user gets digital identity after getting authority's verifiable claim and the identity is stored on interplanetary file system (IPFS) and the content address of these is stored on the blockchain. This makes it easy for the user to interact with different services without having identity for each one of them. The security of user data is ensured by encrypting the data and giving user the complete control over his data stored in the IPFS. The blockchain cannot extract the user's data but can only request the user to provide some data attribute or some verification as the verifier demands. Thus, the system provides security and privacy to users' data as well as user has control over his data.

Keywords Blockchain · Cryptography · Digital identity · Privacy · Security

1 Introduction

Blockchain technology gained its importance after the release of a white paper [1] in which Satoshi Nakamoto (which is an alias) introduced the trustless concept. If we utter the word blockchain to a group of people, most of them will relate it to bitcoin or cryptocurrency. But the application of blockchain is far wide than just

T. Rathee (✉)

Maharaja Surajmal Institute of Technology, New Delhi, India

T. Rathee · P. Singh

Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

371

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,

Lecture Notes on Data Engineering and Communications Technologies 73,

https://doi.org/10.1007/978-981-16-3961-6_31

cryptocurrency [2–6]. Since the world in which we are living is data-driven, therefore protecting the user’s data and identity is the need of hour. After the rise of Internet at global level, we are fighting the identity management (IM) challenges which include security and privacy. In real world, we have Aadhaar card, driver’s license and even passport to create personal identity. In digital world, there are systems to create digital identities; however, these systems seem to be imperfect. There is no system for online authentication of identities or the digital entity’s identity. Moreover, the users do not have control over their personal data. They do not face any national or international boundaries. Blockchain technology offers a solution to the above problem by delivering a system which can be used to create a digital identity on the blockchain. The system further can help the individual to manage and create their own digital identity, allowing them to have tremendous control over their personal data. Unfortunately, there is a possibility of Sybil attack if the whole system is distributed [7]. The inherent distributed principle of blockchain when combined with identity verification can be used to create a digital identity which can be used to perform any transaction over the Internet. It can encrypt and store the encrypted digital identity, so as to allow the users to share and manage their personal data on their own terms. The execution of smart contracts on blockchain can help everyone in the network to establish decentralized trust.

1.1 Our Contribution

In this paper, we propose *BSeISovID*; a blockchain-based self-sovereign identity management system that uses blockchain to eliminate the problems faced by centralized systems. The architecture deals with mainly three actors namely—user, verifier, and authority. A user uses the system to create and store identity, the authority checks users’ data from their database which allows the user to create their identity and verifier/third party uses our system to check/verify users’ identity. All the users’ information is stored on IPFS while blockchain only stores the content address of the users’ data and their public key which is a unique identifier of their information. All the verification is done by smart contracts that run on the blockchain. In this way, smart contracts can send a yes or no message to the verifier while verifying instead of revealing complete users’ information.

The rest of the paper is organized as follows: Sect. 2 describes the background of blockchain technology and needs the need for the new type of self-sovereign identity management system. Section 3 describes the proposed *BSeISovID*, Sect. 4 concludes this paper, and finally, Sect. 5 presents the limitations and future work.

2 Preliminaries

2.1 Blockchains

A blockchain is composed of some logical elements called as *nodes*, a distributed ledger consensus algorithms with cryptographic integrity [8]. Blockchain mainly consists of three layers, i.e., point-to-point network (P2P) [9] consisting of nodes, data storage, and asymmetric key cryptography [10]. The distributed P2P network allows the non-trusted members to interact with each other without the involvement of central authority [11]. It consists of transactions which are signed by the peers. The nodes in the network are responsible for grouping the transactions in the *blocks* and to determine the validity of the transactions. A valid transaction means, for example, User A receives one bitcoin from User B. However, User B may have tried to send the same bitcoin to user C. Therefore, it is now the responsibility of existing nodes to decide which transaction should be added into the blockchain so as to avoid any fraud entry in the blockchain [11, 12]. The *consensus* mechanism here plays a vital role in determining whether a transaction is valid or not. There are various consensus mechanisms available in the literature [13–16]. Asymmetric key cryptography is to ensure privacy and security of the data. The inherent property of blockchain provides immutability to the data stored in the blocks. Figure 1 describes the overall blockchain structure.

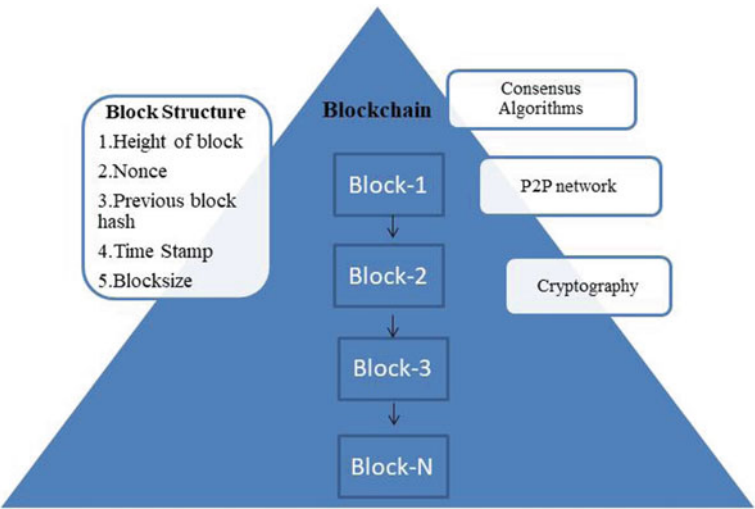


Fig. 1 Blockchain structure

2.2 Related Work Summary

The decentralized identity management systems are built using bitcoin blockchain in [17, 18] which provides a reliable and public identity. An identity system based on biometric is built in [19]. There has been a lot of research going on in the field of identity management [20–23]. But identity management using blockchain technology needs more attention. The privacy has been decentralized using blockchain technology in [24]. Blockchain has been used to access medical data records in [25]. The authors in [26] have proposed the utilization of auditable contacts using blockchain for fair data access. Similarly, the authors in [27] have proposed a framework to provide online rating based on user behavior. The authors in [28] have surveyed and analyzed three tools that use blockchain for identity management. The authors in [29] have produces a system for storing the identities of users on blockchain based on their credentials. The authors in [30] have concluded in their studies that in Canada, IdM system based on blockchain can enhance online services. The authors in [31] have proposed a framework for blockchain-based ID as service. The authors in [32] have proposed a framework for identity management based on blockchain in business to enable different parties to exchange identities. However, the above-mentioned models do not solve the identity management challenges defined by [33]. Therefore, it is a necessity to build strong IAM models.

3 Proposed Blockchain-Based Self-Sovereign Identity Management System

3.1 Overview

The proposed *BSelSovID* has been shown in Fig. 2. It is a system which is based on Ethereum blockchain and guarded by smart contracts. The design of *BSelSovID* mainly consists of authority, verifier, and end user.

The backend of *BSelSovID* is based on smart contracts which are deployed on Ethereum blockchain. These smart contracts are responsible for governing and managing the self-sovereign identity management modules as shown in Table 1.

The system consists of the following modules.

1. *Verification of data by Authority* deals with the whole verification policy and sending the verifiable claims back to the user.
2. *Validation* deals with validating the digital signature of authority and storing digital identifier (DID) on blockchain.
3. *Interaction with verifier* deals with the user interaction and verification did using third-party policy.

These modules and the smart contracts operation are discussed in the following sub-section

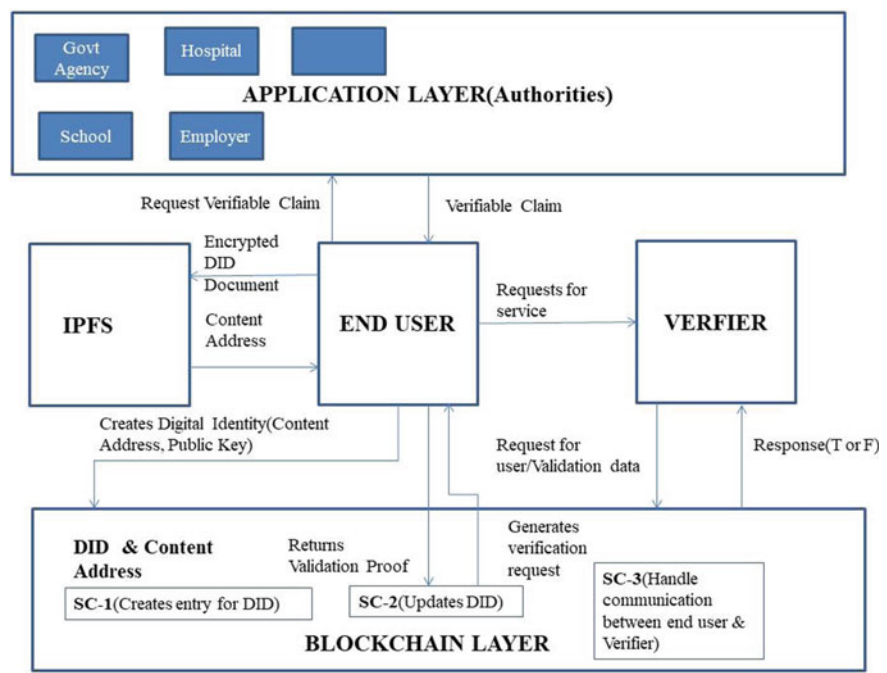


Fig. 2 Proposed self-sovereign identity management system

Table 1 Smart contract per module

Module	Smart contracts	Purpose
Verification of data by Authority	– createIdentity – getIdentity – editIdentity	• Creation of Digital Identity • Getting Digital Identity • Editing Digital Identity
Validation	– triggerDataRequest – triggerDataResponse	• Trigger Data Request • Trigger Data Response
Interaction with verifier	– triggerVerifyRequest – triggerVerifyResponse	• Trigger Verification Request • Trigger Verification Response

Application Layer:

The verification of data by authority is performed at application layer. The user is given a list of authorities to choose from. He chooses a particular authority to sign on a particular data attribute. This list of attributes along with their values and the specified authority whose sign is needed on that attribute by the user is sent on a backend API.

Every authority verifies the user's corresponding data attribute by matching the data present on its database depending on the implementation and checks for its correctness.

The verifiable claim that is sent by the authority back to the user is basically an object of signatures on all attributes. Each signature is made on an object of user which consists of attribute name, value, and user public key. This object is signed by the private key of the authority to make one attribute's claim.

Blockchain Layer:

The *Validation of the Digital Signature of Authority and Interaction with verifier* is done using blockchain layer. User validates the digital signature by decrypting it using the public key of the authority and then comparing the decrypted message to the users details which are sent back in response from authority. If these match, then it gets confirmed that authority has signed the message.

After validation from authority user stores their digital identifier (DID) and data on the IPFS in an encrypted. This data is only accessible to the user and cannot be accessed by the third party directly. Hence, this ensures data privacy. After successfully storing it on IPFS a content address is returned to the user.

The public key and IPFS content address are stored on blockchain after the smart contract checks if the data stored on IPFS is valid or not. If it finds it is valid, then the public key and content address are stored on the blockchain as DID otherwise it shows an error message.

User interacts with Verifier:

A user tries to login into a service provided by a third party; in order to prove their identity, the user provides their public key and data to the verifier. The verifier upon coming across the user public key and the data which needs to be true for the user in order to provide services emits an event through a blockchain smart contract which asks for the user to verify an attribute. Whenever the user reads an event asking for verification of data attribute, the user sends back a signed response. This is done by the user by emitting an event through a blockchain smart contract. This sign is verified at the smart contract to check whether the sign is made by a legitimate authority, and also whether the data on which sign is made matches with the value available with the authority. The verifier now constantly reads for the response event emitted by the user. It receives a true or false for the attribute, which depicts whether the attribute's value was successfully verified by the user through the smart contract event or not. This method ensures a complete safety to the user's data, as it verifies the data without actually disclosing the user details. This procedure ensures that the data provided by the user to the verifier is completely consensual and is provided by the user itself; hence, it ensures privacy to the user.

Table 2 Comparison of proposed system with existing systems

Laws of identity	uPort	Sovrin	ShoCard	BSelSovID
User control and consent	X	√	√	√
Minimal disclosure for a constrained use	√	√	X	√
Justifiable parties	√	√	X	√
Directed identity	√	√	√	√
Design for a pluralism of operators and technology	√	√	X	√
Human integration	X	X	X	X
Consistent experience across contexts	√	X	√	√

Source This table is inspired from [37]

3.2 Key Generation

The authenticity of each transaction should be verified using blockchain technology. The use of digital signature helps to guarantee the authenticity and non-repudiation of the data. RSA has been one of the very popular algorithms for key generation [34]. However, there is a continuous effort in improving the security of digital signatures. The algorithm used for key generation in our proposed system is elliptical key cryptography (ECC) [35].

3.3 System Implementation Details

The system is implemented on Intel(R) Core(TM) i5, 3.30 GHz CPU, 4 cores, and 8 GB RAM. Table 2 shows the comparison of proposed system with the existing identity management solution described in [28]. It has been observed that our system satisfies the laws of identity defined by [36] as compared to the other IdM solutions.

4 Conclusion

This paper has introduced the concept of *BSelSovID* which is based on the core concept of blockchain and self-sovereign identity. The architecture aims to replace the conventional centralized systems. It is a generic framework which can be applied to any use case. It makes use of smart contract to perform the verification process and hence speeds up the processing. The user’s data is encrypted before it is stored on IPFS, which adds more security to the data. Moreover, the data control is in the hands of the user which adds privacy. The system is feasible and easy to implement.

5 Limitations and Future Work

Although the system is easy to implement, it has certain limitations. Firstly, there is no provision to control the further distribution of user's data by the verifiers. Secondly, in case the smart contract fails, the system will lack reliability. As of now, we have implemented the system on local blockchain only. In the future work, a framework for public permissionless blockchain can be developed.

References

1. Nakamoto, S.: Bitcoin whitepaper. <https://bitcoin.org/bitcoin.pdf> (Дата обращения: 17.07. 2019) (2008)
2. Ali, M., Nelson, J., Shea, R., Freedman, M.J.: Blockstack: A global naming and storage system secured by blockchains. In: 2016 $\{\$USENIX\}$ annual technical conference ($\{\$USENIX\}\{\$ATC\}\$ 16$), pp. 181–194 (2016)
3. Fromknecht, C., Velicanu, D., Yakoubov, S.: A decentralized public key infrastructure with identity retention. *IACR Cryptol. ePrint Arch.* **2014**, 803 (2014)
4. Lee, J.-H., Pilkington, M.: How the blockchain revolution will reshape the consumer electronics industry [future directions]. *IEEE Consum. Electr. Mag.* **6**, 19–23 (2017)
5. Lee, B., Lee, J.-H.: Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *J. Supercomput.* **73**, 1152–1167 (2017)
6. Pilkington, M., Crudu, R., Grant, L.G.: Blockchain and bitcoin as a way to lift a country out of poverty-tourism 2.0 and e-governance in the Republic of Moldova. *Int. J. Internet Technol. Secur. Trans.* **7**, 115–143 (2017)
7. Douceur, J.R.: The sybil attack. In: International workshop on peer-to-peer systems, pp. 251–260 (2002)
8. Vitenberg, R.: Debunking blockchain myths. *NISK J.* **11** (2018)
9. Park, H., Ratzin, R.I., van der Schaar, M.: Peer-to-peer networks: Protocols, cooperation and competition. In: *Streaming Media Architectures, Techniques, and Applications: Recent Advances*, pp. 262–294. IGI Global (2011)
10. Thomsen, S.S., Knudsen, L.R.: Cryptographic hash functions (2005)
11. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. *IEEE Access.* **4**, 2292–2303 (2016)
12. Vukolić, M.: The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: International workshop on open problems in network security, pp. 112–125 (2015)
13. Antonopoulos, A.M.: *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc. (2014)
14. Dannen, C.: *Introducing Ethereum and solidity*. Springer (2017)
15. Pilkington, M.: Blockchain technology: principles and applications. In: *Research handbook on digital transformations*. Edward Elgar Publishing (2016)
16. Castro, M., Liskov, B.: Practical Byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst. (TOCS)* **20**, 398–461 (2002)
17. Augot, D., Chabanne, H., Clémot, O., George, W.: Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), pp. 25–2509 (2017)
18. Augot, D., Chabanne, H., Chenevier, T., George, W., Lambert, L.: A user-centric system for verified identities on the bitcoin blockchain. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pp. 390–407. Springer International Publishing, Cham (2017)

19. Othman, A., Callahan, J.: The Horcrux protocol: a method for decentralized biometric-based self-sovereign identity. In: 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1–7 (2018)
20. Halperin, R., Backhouse, J.: A roadmap for research on identity in the information society. *Identity Inf. Soc.* **1**, 71–87 (2008)
21. Pfitzmann, A., Hansen, M.: A terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (2010)
22. Jensen, J.: Federated identity management challenges. In: 2012 Seventh International Conference on Availability, Reliability and Security, pp. 230–235 (2012)
23. Jensen, J., Jaatun, M.G.: Federated identity management-we built it; why won't they come? *IEEE Secur. Priv.* **11**, 34–41 (2012)
24. Zyskind, G., Nathan, O., others: Decentralizing privacy: Using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pp. 180–184 (2015)
25. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30 (2016)
26. Kaaniche, N., Laurent, M.: A blockchain-based data usage auditing architecture with enhanced privacy and availability. In: 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), pp. 1–5 (2017)
27. Yasin, A., Liu, L.: An online identity and smart contract management system. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), pp. 192–198 (2016)
28. Dunphy, P., Petitcolas, F.A.P.: A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **16**, 20–29 (2018)
29. FAIDELLA, D.C., Schukai, R.J., Manuel, S.R., Pierleoni, M., Thomas, J.A.: Methods and systems for identity creation, verification and management (2020)
30. Wolfond, G.: A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. *Technol. Innov. Manag. Rev.* **7** (2017)
31. Lee, J., Member, S.: BIDaaS: Blockchain based ID as a service. *IEEE Access.* **6**, 2274–2278 (2018). <https://doi.org/10.1109/ACCESS.2017.2782733>
32. Ebrahimi, A.: Identity management service using a blockchain providing certifying transactions between devices (2017)
33. Torres, J., Nogueira, M., Pujolle, G.: A survey on identity management for the future network. *IEEE Commun. Surv. Tutor.* **15**, 787–802 (2012)
34. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978)
35. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **1**, 36–63 (2001)
36. Cameron, K.: The laws of identity. *Microsoft Corp.* **12**, 8–11 (2005)
37. El Haddouti, S., El Kettani, M.D.E.-C.: Analysis of identity management systems using blockchain technology. In: *CommNet*, pp. 1–7 (2019)

Blockchain and IoT for Auto Leak Unearthing



Pooja Sapra, Vaishali Kalra, and Simran Sejwal

Abstract Blockchain and Internet of Things (IoT) are important constituents of Internet-enabled era of information technology. Both technologies are distributed, autonomous, and decentralized systems. IoT devices require the strengthening of its security features, and security is an intrinsic aspect of blockchain due to cryptographic mechanisms. On the other hand, blockchain needs contribution from the distributed nodes and IoT includes within its architecture. So, blockchain can aid in the settlement of major security requirements in IoT. Blockchain features such as decentralization, immutability and transparency (DIT), auditability, and data encryption help to solve various IoT architectural problems. The main goal of water supply sector is to provide a solution to get shielded, authentic, and cost-effective water supply through well-regulated arrangements. It is very hard to achieve these goals. This paper introduces an algorithm for implementing a smart water management system that identifies and quantifies the water requirement by an individual consumer within a given locus and also identifies leaks (if any) in the plumbing system. The system proposed monitors both water quality and water scarcity aspects within the supplied vicinity. The smart water management system is collateral to a decentralized system implemented using smart tanks that uses the Internet of Things (IoT) for implementation and blockchain technology for providing a more rooted mechanism.

Keywords Blockchain · Internet of Things · Water management · Security

P. Sapra (✉) · V. Kalra
The NorthCap University, Gurugram, India
e-mail: poojasapra@ncuindia.edu

V. Kalra
e-mail: arya.vaishali17@gmail.com

S. Sejwal
Netaji Subhas University of Technology, Dwarka, India
e-mail: simran.cs19@nsut.ac.in

1 Introduction

The significance of the Internet of things has progressed on account of the mix of different advancements, real-time analytics, AI, wear sensors, and embedded systems. Internet of Things has been a blessing across each domain of modus and numerous business ventures, and some of the emerging fields in which IoT is largely used includes client engagement platforms, optimization of technology, waste reduction, enabling smart homes, elderly care, transportation, buildings and home automation, infrastructure application, health care, and many more. A major drawback of IoT in terms of water management is dispensing a sense of security within the system that has been lacking in the traditional methods for the same. This void can be replenished using the advantages of blockchain technology.

In a perfect world, water resource management planning has regard to all the contending requests for water and tries to designate water on an impartial premise to fulfill all uses and requests [1]. Probably the greatest worry for our water-based assets later on is the manageability of the current and future water asset allocation. As water turns out to be rarer, the significance of how it is overseen develops vastly. Finding a harmony between what is required by people and what is required in the earth is a significant advance in the maintainability of water assets. Non-revenue water (NRW) real losses include leaks and bursts from the underground pipeline network. About 20% of the water produced is simply wasted because of underground water leakage which goes undetected, and some old or worn-out pipes might end up wasting 50% of water in supply [2]. Most leaks remain unidentified being underground. Water leakage detection program identifies and reports leakage problem and reduce previously undetected leaks.

The system is required because leakage in pipes lead to:

- Health issues of people due to contaminated groundwater.
- Ineffective supply management.
- Ineffective demand management.
- Weakening of the physical infrastructure.
- Customer dissatisfaction due to unreliable service of poor quality.

This system is explicit, anchored, ensures to an extent that the condition of water scarcity does not arise and also encourages individuals to conserve water along with earning some reward. Also, the proposed system utilizes sophisticated methodologies of the buzzing technology—Internet of Things (IoT) [3, 4], blockchain, and smart contracts for implementing such systems [5].

Blockchain Technology: A chain of blocks, having information about each transaction, is called blockchain. Each block has the address of its previous block that makes data provenance easy and difficult to tamper. Further, if data received from IoT sensors is placed in blockchain, it would reduce the possible attacks of leakage.

Smart Contracts: Smart contracts are the logical piece of codes, recorded in the blockchain and are triggered when an event takes place. Ethereum virtual machine

(EVM) is deployed to avoid the hacking of the smart contracts. There are many languages and IDEs available to develop the smart contracts like serpent, solidity, Go, etc. In this paper, we have considered solidity language to develop the smart contracts on Remix IDE. Smart contracts are deployed using Ganache tool.

2 Literature Survey

Various methods have been considered and implemented toward providing a secure management plan, and in this section, we would discuss the related work toward a secure water management plan.

Author in [6] proposed a system that takes into account the acoustic emission techniques to identify leak in the pipeline. This method uses acoustic (sound) sensors which work on the phenomena of sound propagation and uses sound waves to detect leakage. Sound waves would travel back and forth in a pipe with a certain wavelength, and the wavelength noted on a leakage would differ from the original ones, and hence, the leakage is detected.

The proposed system has a few drawbacks associates to it which includes: (i) Relying on the concept of sound propagation might not be accurate enough to detect the exact location of the leak. (ii) Acoustic sensors do not yield accurate results which might cause errors or failure in detection.

Authors in [7–9] incorporated methods that uses global system for mobile communication (GSM) to monitor leaks. Once the leak is identified, GSM technology is used to deliver an alerting message to the users designated mobile. Major disadvantage of this method is that GSM technology only allows producing an alerting system and does not cater to provide the exact location of the leak within the plumbing system. Some other orthodox methods for management and for detection of leakage are using water sensors. This mechanism is very feeble and of low precision as (i) Water sensor would fail to identify leakage in underground pipes, (ii) Water sensor would detect minor leakages or underground water, (iii) The degree of accuracy decreases drastically. Such methods would be beneficial at small scale such as home automation or finding minor faults in the water supply.

Author in [4] caters to the issue in a sophisticated format using GSM technology for altering system on leakage, liquid crystal display (LCD) to remotely monitor inflow and outflow rate of water and flow sensors to determine the mass flow rate of inflow and outflow of water used in the pipelines. The system lacks a sense of security that could be provided taking into account the advancements in blockchain and cloud computing as blockchain has been seen as a cut above the traditional ways to secure our IoT devices.

The software-based solution for water management is provided in [1], wherein the author installed the smart water meters, and based on the data collected from the meter, the predictions are made using AI forecasting techniques. Based on the obtained predicted data, the meta-heuristics algorithms have been applied for smart management of non-renewable resource water. This one technique would also help

in reducing the pumping activity. In order to save the water usage, the author [10] brings an android-based solution for small to medium size garden that measure the soil moisture level, air condition, and humidity level using sensors and schedule the watering of the plants. The proposed framework is built on fuzzy rules and introduced block chains to provide access to trusted devices only. In 2018, IBM [11] also proposed a blockchain model with IoT integration to establish clarity in the use of water in the asymmetry industry and to illustrate its importance in sustainable water management. This blockchain solution also help in providing the transparent trading of water contracts which further saved our resources [12]. This blockchain with IoT implementation is also proposed for creating the future smart cities [13, 14].

3 Proposed System

Water being a non-renewable resource is critical for human sustainability, and proper methods are to be incorporated to ensure more longevity and better management for future needs; hence, a fool proof method is required for water management, and detection of underground leaks to eradicate the issues that are associated with it. In our proposed system, we have tried to eradicate some of the issues related to the same, which includes the following:

- Hydrostatic pressure sensors as they are more accurate sensors as compared to existing models
- Using GPS technology allows fetching the exact geographical location of the leak
- Introducing blockchain to secure the system
- Chances of error or failure decrease drastically
- Higher accuracy and exact location detection
- The proposed system can function underground as well.

The work flow of the proposed model given in Fig. 1:

- Connection and Establishment of Smart Tanks:** For identification of leaks, the proposed model will include implementation of a smart tank, using hydrostatic pressure sensor and pH level indicator for water quantity and



Fig. 1 Workflow diagram for creating an IoT-based Blockchain solution for water leakage management

quality management and lastly identifying leaks in underground pipeline. The devices required are:

- **Arduino board:** The monitoring of the sensors would be done by a concept of Internet of Things (IoT) circuit Arduino. Arduino is an open-source platform which relies on easy and convenient manner hardware and software programs. The hardware reads potential input, input from any connected sensor, a click on a button, or messages (via the internet platforms such as Twitter) and converts it into the required output. The user can send a set of instructions to the micro-controller on the board. The Arduino programming language which is used for writing syntax is the Arduino Software (IDE).
- **Pressure sensor:** The system would require an industry-based pressure sensor. A pressure sensor is a device used for measuring pressure value for gases and liquid. Example for applications for pressure sensor would be in the measuring of combustion pressure measured inside an engine cylinder or in a gas turbine. Pressure sensors are commonly manufactured from piezoelectric materials like as quartz.
- **GPS sensor:** Global positioning systems that can help detect leakage in underwater pipelines without any signal disparity. The global positioning system (GPS) is a satellite-based radio navigation sensor. GPS is a global navigation satellite sensor that gives geolocation and time information to a GPS receiver which provides output anywhere on or near the Earth surface where there is an unobstructed object or line which is in sight to four or more GPS satellite system. Obstructions such as mountains and buildings block the weak GPS signals.
- **pH Level sensor:** To determine the quality of water supplied, we would require a pH level indicator. A pH sensor is categorized as one of the most essential tools that is currently used for water quality measurements. This sort of sensor can gauge the measure of alkalinity and acidity in water and different solutions. The standard pH scale is from 0 to 14. When the pH value is seven, it is considered to be neutral. If pH value is above seven, it represents alkaline substances and substances with pH value less than seven are more acidic.

For determining the quality and quantity factor of the water supplied within the vicinity, the idea is to equip every water consuming unit (a house) within the decentralized network (a colony or sector) with a smart tank which automatically detects the water level in the tank using hydrostatic pressure level sensors and water quality using the pH sensor. If the water level in the smart tank is below a certain threshold, it fetches water from the main source and thereby checking it quality set by the administrator, and if the water stored in the tank is more than the average requirement, it can be shared within the network among another consuming unit.

- ii. **Formation of Decentralized Network:** Here, the entire process is decentralized to make it peer-to-peer and eliminates the need for a middle man. A transparent ledger is then generated to document the specifics of water use and delivery. Wherever the consumer drinks or distributes water, the entry for the same is registered in the decentralized ledger of the network.
- iii. **Correlating the Blockchain and IoT:** A pool of water token is distributed to each water consuming unit, and water token are deducted if water is consumed, while water token is earned if water is distributed by the unit.
- iv. **Monitoring and Analyzing the System:** The spent and unspent water token details help in data analysis and monitoring the water requirements.

Step by Step Procedure:

The step by step process can be seen in Fig. 2, where the pressure sensor first notes the difference in pressure between the two points and plots the same graph showing the peak value, the precise longitude, and latitude details of the leakage (if any) obtained after identification of the peak pressure value, and the GPS can include the geographical position of the leakage by which we can identify the location of the leakage. A decentralized ledger/record is created where the data (water tokens) of each water consumption unit are stored and can be used for review in a crisis situation; the water level indicator in each tank will assist with the data interpretation of each unit offering a deeper view into the locality's water requirements (Fig. 3 and 4).

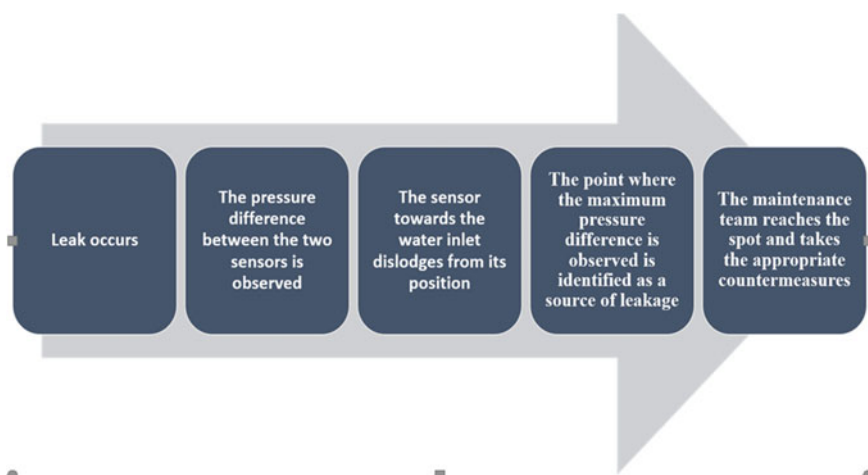


Fig. 2 Identification of the leaks

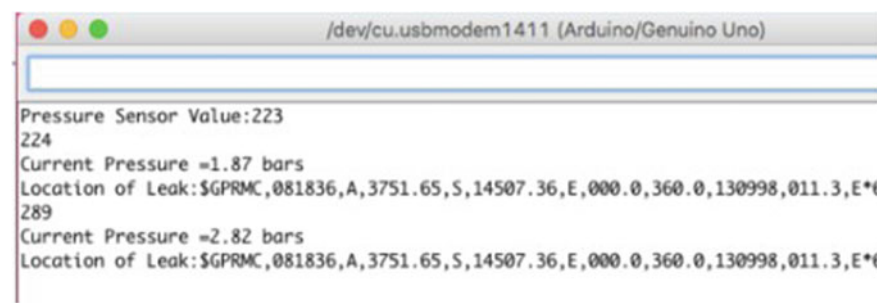


Fig. 3 GPS location and pressure value

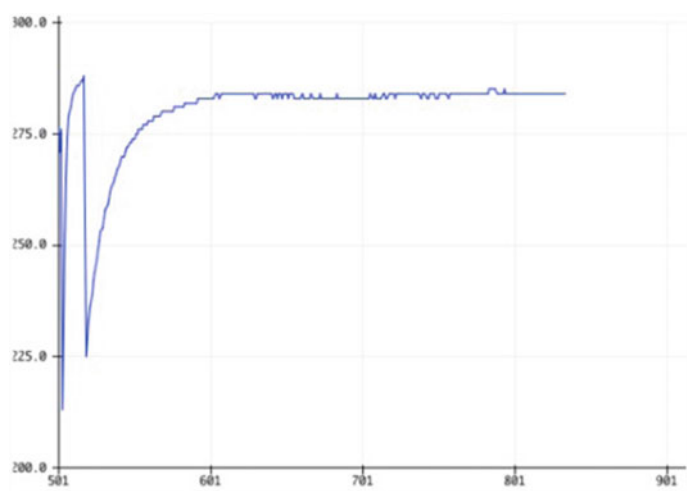


Fig. 4 Pressure sensor graph

4 Implementation and Results

For implementing the smart water management system, a blockchain is created. By creation of blockchain, we ensure:

- Water requirement for each unit (house) can be recorded and monitored
- Addition and deduction of water tokens
- To provide a valid and secure blockchain mechanism

In Figs. 5 and 6, we showed that how the block chain is created, and the chain of blocks is formed to make the data provenance easy and difficult to tamper, and in Fig. 7, the transactions are shown. Each transaction is hash code encrypted which is not easy to temper.

```

Block's Hash: 99999eeae168b0aef3cb1ee98540246957b78be27937607f089aef8430b86a40
Block added
Simran has 20 water_tokens on her account
The Chain is valid and secure

```

Fig. 5 Creating blockchain

```

Simran started minning
Previous Block's Hash: 999997e5ac38b6ae5b720cd4e325d9ef583502428b8becfe27e1e57f98e896de
[{'\n'
  '    "fromWallet": "Zining",\n'
  '    "toWallet": "Alex",\n'
  '    "amount": 0.01\n'
  '},\n'
  {'\n'
  '    "fromWallet": "Tom",\n'
  '    "toWallet": "Ankit",\n'
  '    "amount": 100\n'
  '},\n'
  {'\n'
  '    "fromWallet": "Raymond",\n'
  '    "toWallet": "Ankit",\n'
  '    "amount": 1e-07\n'
  '}]
Block's Hash: 99999ea8e9f36c128622bb966115613a7a66aa0802b2d975cf8e3a91e358d84b
Block added
Simran has 20 water_tokens on her account
The Chain is valid and secure

```

Fig. 6 Creating blocks

```

Simran started minning
Previous Block's Hash: 83247c122a3e29320a4e93412c3f76f11d9d3373a471fd183c8cfd61b84fa894
[{'\n'
  '    "fromWallet": "Ankit",\n'
  '    "toWallet": "Alex",\n'
  '    "amount": 3.2\n'
  '},\n'
  {'\n'
  '    "fromWallet": "Ankit",\n'
  '    "toWallet": "Raymond",\n'
  '    "amount": 1\n'
  '},\n'
  {'\n'
  '    "fromWallet": "Alex",\n'
  '    "toWallet": "Raymond",\n'
  '    "amount": 5.12\n'
  '}]
Block's Hash: 999997e5ac38b6ae5b720cd4e325d9ef583502428b8becfe27e1e57f98e896de
Block added

```

Fig. 7 Transaction

5 Challenges

- The following issues can be encountered during the system implementation and run and the following countermeasures or suggestions can be carried out for better accuracy in the system.
- The longevity of the sensors might vary for every smart tank installed.
- Longevity of the sensors depends on various external factors and quality of the sensor (average sensor life is between 3 to 4 years)
- The working of sensors can be affected due to various factors (water, pressure of water current)
- Need to monitor pressure and other factors on regular basis.
- Installation and retrieval of the system can be tedious.
- It would require a team of 5–6 members for the same and can use additional features of an in-built camera for better surveillance.
- Data collection and analysis of raw data.
- Blockchain technology and its advantages can be well utilized.
- External factors that may vary data.
- Need regular monitoring regarding external factors such as corrosion, pipe structure, and tanks.

6 Conclusions

This proposed paper contemplates a highly accurate and full proof method toward management of water. It assists ways to check quality and quantify water requirements within a sector. The system also identifies leakage in underground pipes along with furnishing the exact geographical location of the leak which helps in taking the required measures appropriately and within the least possible time frame to avoid unnecessary wastage of water. Key features the system showcases are—The pressure difference can be classified into categories to report the severity of the leak. The electronic mechanism shall be enclosed in an air-tight ball-like structure, To reduce response time in sealing, leaks shall provide a lot of direct and indirect benefits. The sensors shall be mounted on the inner walls of the pipes with an electronically controlled switch to dislodge. To identify potential leak sites, the recorded measurements can be timely sent to a central server. A similar device can be used for oil and gas pipeline. Blockchain helps in providing a decentralized ledger and security measures blockchain technology and Internet of Things (IoT) aids the proposed system to function in a coherent manner and provide it with the required contrivance and tools.

References

1. Grigoras, G., Bizon, N., Enescu, F.M., Guede, J.M. L., Salado, G.F., Brennan, R., Alalm, M.G.: ICT based smart management solution to realize water and energy savings through energy efficiency measures in water distribution systems. In: 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–4. IEEE (2018)
2. Maouriyani, N., Krishna, A.A.: Aquachain-water supply-chain management using distributed ledger technology. In: 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), (pp. 204–207). IEEE (2019)
3. Robles, T., Alcarria, R., de Andrés, D.M., de la Cruz, M.N., Calero, R., Iglesias, S., Lopez, M.: An IoT based reference architecture for smart water management processes. *JoWUA* **6**(1), 4–23 (2015)
4. Ntuli, N., Abu-Mahfouz, A.: A simple security architecture for smart water management system. *Proc. Comput. Sci.* **83**, 1164–1169 (2016)
5. Dogo, E.M., Salami, A.F., Nwulu, N.I., Aigbavboa, C.O.: Blockchain and internet of things-based technologies for intelligent water management system. In: *Artificial Intelligence in IoT*, pp. 129–150. Springer, Cham (2019)
6. Nicola, M., Nicola, C., Vintilă, A., Hurezeanu, I., Duță, M.: Pipeline leakage detection by means of acoustic emission technique using cross-correlation function. *J. Mech. Eng. Auto* **8**, 59–67 (2018)
7. Lee, S.W., Sarp, S., Jeon, D.J., Kim, J.H.: Smart water grid: the future water management platform. *Desalin. Water Treat.* **55**(2), 339–346 (2015)
8. Zhang, D., Gersberg, R.M., Wilhelm, C., Voigt, M.: Decentralized water management: rainwater harvesting and greywater reuse in an urban area of Beijing, China. *Urban Water J.* **6** (5), 375–385 (2009)
9. Bordel, B., Martín, D., Alcarria, R., Robles, T.: A blockchain-based water control system for the automatic management of irrigation communities. In: 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–2. IEEE (2019)
10. Munir, M.S., Bajwa, I.S., Cheema, S.M.: An intelligent and secure smart watering system using fuzzy logic and blockchain. *Comput. Electr. Eng.* **77**, 109–119 (2019)
11. Chohan, U.W.: Blockchain and environmental sustainability: case of IBM's blockchain water management. *Notes on the 21st Century (CBRI)* (2019)
12. Pee, S.J., Nans, J.H., Jans, J.W.: A Simple blockchainbased peer-to-peer water trading system leveraging smart contracts. In: *Proceedings on the International Conference on Internet Computing (ICOMP)*, pp. 63–68. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2018)
13. Lazaroiu, C., Roscia, M.: Smart district through Iot and blockchain. In: 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), pp. 454–461. IEEE (2017)
14. Ye, Z., Yin, M., Tang, L., Jiang, H.: Cup-of-Water theory: a review on the interaction of BIM, IoT and blockchain during the whole building lifecycle SSS. In: *Proceedings of the International Symposium on Automation and Robotics in Construction*, vol. 35, pp. 1–9. ISARC Publications (2018)

Coin Drop—A Decentralised Exchange Platform



Vanita Jain, Akanshu Raj, Abhishek Tanwar, Mridul Khurana,
and Achin Jain

Abstract In today's world, cryptocurrency has seen a boom in users' number, and the numbers are increasing day by day. There are multiple cryptocurrencies, so there must be a platform to provide an exchange of cryptocurrencies. These days, many platforms provide users with the service, but they lack speed and are limited to some cryptocurrencies. Thus, we have proposed and developed a system that will increase the transactions rate by performing it off-chain to increase the transactions' speed and perform exchange between any cryptocurrencies. The proposed system combines the best practices of both the decentralised and centralised exchange platforms.

Keywords Cryptocurrency · Centralised cryptoexchanges · Decentralised exchange · Blockchain · Ethereum · Smart contract

1 Introduction

A cryptocurrency [1] is a form of currency available only virtually and is protected using various cryptography techniques. Researchers and developers proposed it in the early 1980's giving hints of the systems having digital money. Cryptocurrency is a term that refers to a digital asset of a network that does all the money-related work using that cryptocurrency, and the network is distributed across a large number of computers. Thus, the network is considered to have a decentralised structure with no single authority having all the power.

We can also consider cryptocurrencies as the systems that allow users to make online payments securely [2]. These payments are denominated in terms of virtual

V. Jain (✉) · A. Raj · A. Tanwar · M. Khurana · A. Jain
Bharati Vidyapeeth's College of Engineering, New Delhi, India
e-mail: vanita.jain@bharativedyapeeth.edu

“tokens”, which are represented by ledger entries internal to the system. “Crypto” refers to the various encryption algorithms and cryptographic techniques that safeguard these entries, such as elliptical curve encryption, public–private key pairs and hashing functions [3].

In today’s world, there are thousands of cryptocurrencies with various functions and specifications. Some of these cryptocurrencies are clones or forks of popular cryptocurrencies like bitcoin and Ethereum, and also, some new currencies are built from scratch. Some popular cryptocurrencies apart from bitcoin [4] and Ether [5] include Litecoin [6], Peercoin, Namecoin [7] and Cardano [8]. The total estimated value of the cryptocurrencies in existence can be around \$214 billion [9].

However, there are several risks involved while using cryptocurrencies. The actual value as currency is effective \$0, so the only store of value is in other utility for a distributed trustless public append-only ledger [10]. Since the government does not monitor cryptocurrency, this creates a massive security risk as the criminals could use unmonitored money [11]. The private key protects the cryptocurrencies wallet, and once someone gets hold of the private key of the user, he can move the money from one account to another, and since the cryptocurrency is not monitored by the government or any central authority (in the case of decentralised exchange platforms), the owner cannot even file a report [12].

We already know that there are multiple cryptocurrencies globally, then there must be a system to allow trading between these currencies; this leads to the introduction of decentralised exchange platforms. Decentralised exchange (DEX) platforms provide the users of cryptocurrencies with a platform to perform cryptocurrency exchange. It allows users to have direct peer-to-peer cryptocurrency transactions online securely and without the need for any intermediary authority. Some of the famous DEX platforms are AirSwap, Atomex, Bancor and dex. blue [13].

However, these systems have some drawbacks in terms of speed, and they are also limited to the number of cryptocurrencies they can take into consideration in their respective platforms; these issues are discussed later in this paper, and a solution to overcome all those shortcomings is proposed.

The proposed system (coin drop) is comparatively much faster than the already present decentralised systems and can work with almost all kinds of cryptocurrencies available. In Section II of this paper, we have discussed cryptographic networks, their working, and the different types of wallets. In Section III, we have discussed the cryptocurrencies exchange platforms. Section IV discusses the working and architecture of “coin drop”. Section V holds the results obtained by comparing various cryptographic exchange platforms against the proposed system. In Section VI, we have concluded the paper.

2 Cryptonetworks and Wallets in Today's World

2.1 *Cryptographic Networks*

To create a network that uses cryptocurrency for online payments, we need to work with blockchain [14]. This technology can be used to keep track of all the transactions that have taken place ever been in a ledger. Blockchain provides the developers with a way to create a structure of the ledger that is to be stored. It is made sure that the structure is secure. This structure is then shared with the entire network, individual nodes or computer maintaining a ledger copy. When a majority of nodes in the network are in favour of the structure, then only the structure is established in the network. A set of transactions is forged into a new block verified by each node of the network. If the nodes confirm the block, then only the block is added to the chain. Thus, this process makes it almost impossible for the mishappenings of the transaction histories. The main goals of such a network are to allow members of the network to synchronise their view of the system state and then to disseminate peer information to allow peers to reenter the system after a disconnection [15].

One such network is the bitcoin network [16]. Bitcoin is a cryptocurrency created in January 2009 after the housing market crash. Bitcoin follows the ideas that are set out in a whitepaper by the mysterious and pseudonymous Satoshi Nakamoto. Bitcoin uses the blockchain network that keeps balances and maintains a public ledger that everyone has transparent access to; all bitcoin transactions are verified by a massive amount of computing power [17].

2.2 *Hot and Cold Wallets*

These cryptocurrencies are stored in digital wallets. There are two types of digital wallets: hot wallet and cold wallet [18].

A wallet that is connected to the network is referred to as hot wallet. They are generally easy to set up, access and be given more tokens. Hot wallets can hold any cryptocurrencies. These wallets are mainly for everyday cryptocurrency users. Nevertheless, they are open to hackers and other technical vulnerabilities because they are connected to the Internet. Some examples of hot wallets are Coinbase and Blockchain.info.

Any wallet which is not connected to the cryptographic network is termed as cold wallet. They are more secure than hot wallets, but they do not accept as many cryptocurrencies when compared to hot wallets. Cold wallets are mainly designed devices that are designated physical cryptocurrency storage. One of the main advantages these wallets provide is that we can have our cryptos beside us. They are expensive to buy, while hot wallets are free of cost and easy to access. Some examples of cold storage devices are Trezor and Ledger [19, 20].

3 Cryptocurrency Exchange Platforms

3.1 *Centralised Cryptoexchanges*

They are trading platforms like the stock market, where a company or a third party has total control over all the transactions made by both parties. In centralised cryptoexchanges [21], the user has to trust the third party because they do not have access to the private keys of exchange account wallets. Trust is the main factor in centralised exchange platforms. All the transactions are controlled by third parties, which could lead to hacks in these platforms or malicious activities by the service providers. Centralised exchange platforms have their system's off-chain. The transactions are not handled by the blockchain, due to which it is prone to security breaches and other attacks on the systems. Today most of the platforms are centralised, which run on high regulatory risk. Some famous CCEs are Binance, Bittrex, Bitfinex, Coinbase and Kraken.

None of the centralised cryptoplatforms is immune to hacks. More than 30 cryptocurrency exchange hacks have occurred in the last nine years, for example, MTGox, BitGrail, and Coincheck. Some government bodies have also banned CCEs in recent years. China, South Korea and Russia are among them. Using CCEs often comes with a large amount of risk, the user has to provide sensitive information about themselves, including bank details, address and govt. issued ID as well [22].

3.2 *Decentralised Cryptocurrency Exchanges*

Decentralised cryptocurrency exchanges overcome many disadvantages of the centralised structure as it operates on a peer-to-peer marketplace directly on the blockchain. Using this way, the traders do not have to reveal their sensitive information to a third party. Since it works on blockchain, it is less immune to security attacks, unlike centralised cryptoexchanges. Still, most of the platforms have a centralised structure because building decentralised exchange platforms is complicated and too costly. Currently, most of the platforms do not have the liquidity to compete with centralised cryptoexchanges.

Decentralised cryptocurrency exchanges operate on a peer-to-peer network because their nodes are distributed; they experience a lower risk of attacks compared to centralised cryptoexchanges [13]. There is no involvement of a third party in DEX which will have control over all the transactions. They are less prone to security attacks and malicious activities by service providers. In DEX, all the payments use cryptocurrencies. DEX enables users to remain in control of their funds by operating essential functions over the blockchain. It overcomes the centralised structure's main limitation since there is no point of failure in this exchange, making blockchain a powerful technology. There are many through backs and

inefficiencies in a centralised structure, due to which there is an introduction of many semi-decentralised exchanges which are coming into action. These are models that operate between the centralised and decentralised marketplace, which are highly efficient than centralised ones. CCEs lack security, transparency and efficiency, due to which demand for decentralised exchanges has increased. DEX promises two significant advantages: security control and the global marketplace. EtherDelta is one of the oldest projects in this field. It has a simple user interface and basic trading features. It has already gained sufficient attraction in the market. Some of the popular DEX are Wavesdex, Bancor protocol, Kyber Network, EtherDelta and Airswap.

4 Proposed System and Working

We have proposed a system that provides decentralised cryptocurrency exchange facilities using blockchain, which is merged with an interactive, user-friendly interface created using ReactJS. The proposed system is much faster than the traditional methods used and combines the best features from both the centralised and the decentralised exchange platforms. The working of the whole system is explained in great detail. Figure 1 shows the workflow of the system.

The trader interacts with the interface (web app in the diagram). The smart contract that we have to build is deployed on Ethereum blockchain and connected with the front end. For testing purpose, we have deployed a contract on the Rinkeby network and used injected web3 environment.

First of all, the user deposits the quote currency in the wallet provided in the exchange and any other token listed on the exchange. Figure 2 shows the wallet that a user will use.

Coin drop has two types of orders: one is market orders and the other one is limit orders. Market orders are filled immediately, irrespective of the price of the token.

To create a market order, there is a function in the smart contract called `createMarketOrder` that takes the ticker, amount of the token, and the side of the order book. For selling tokens, we can identify if the seller has enough tokens, but while buying market order, we cannot determine the price at which the market order will be fulfilled because one order can have several trades under it, i.e. market orders can be fulfilled partially as per availability in the order book. It is also checked whether the token for which the order is being created exists or not.

In the case of limit orders, there is a function called `createLimitOrder` that is used to create a new order in the order book. It takes ticker, amount, price of the token and side to place the order. It is checked that the token exists for which the order is being placed, and the token is not quoted currency. The cost to buy/sell one token is specified and is only filled if matching order is found in the counter order book, i.e. if a user wants to sell tokens using limit order, the order can only be filled if there is a matching order to buy.

Fig. 1 Flow chart of the system

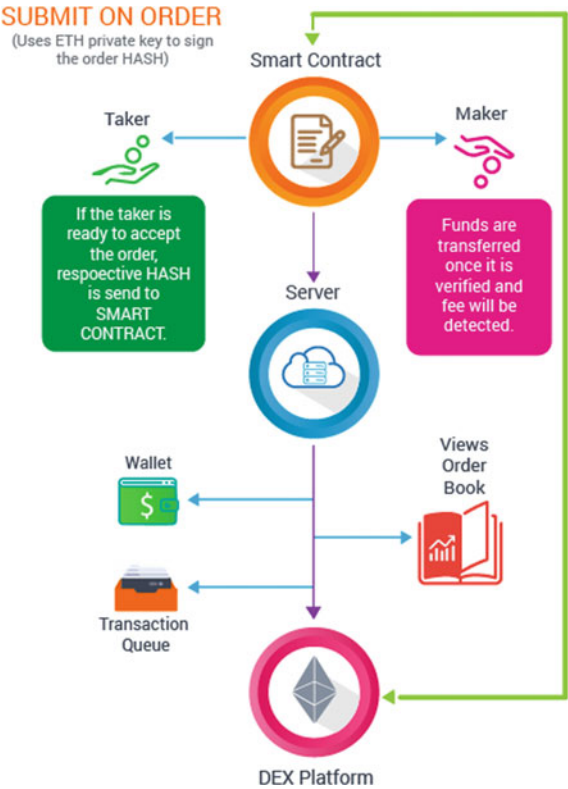
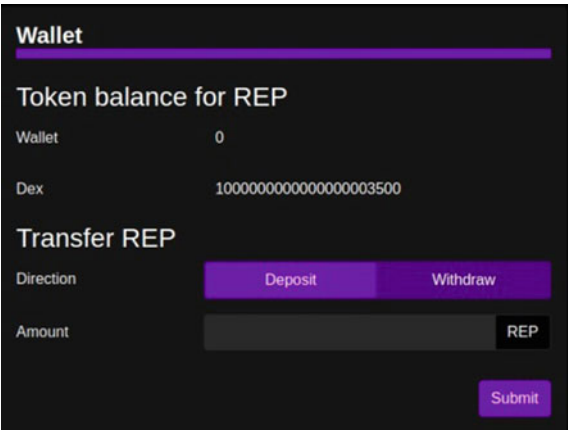


Fig. 2 User wallet in the coin drop



The `getOrders` function in the smart contract is used to list all the current orders from both sides of the order book, i.e. from the sell-side and buy-side. A `getTokens` function is used to list all the tokens purchased or sold on the exchange. It returns an array of tokens. The `addToken` process in the smart contract is used to record a

New Order

Type

Limit

Market

Side

Buy

Sell

Amount

Price

Submit

Fig. 3 New order function

All orders

BUY

amount	price	date
200	8	a minute ago
500	6	10 minutes ago
2000	5	10 minutes ago
3000	4	10 minutes ago

SELL

amount	price	date
31	4	a minute ago
800	8	10 minutes ago
2000	9	10 minutes ago
4000	10	10 minutes ago

My orders

BUY

amount/filled	price	date
800/600	8	a minute ago
2000/0	5	10 minutes ago
3000/0	4	10 minutes ago

SELL

amount/filled	price	date
31/0	4	a minute ago

Fig. 4 Orders placed on the coin drop platform

new token on the exchange. It takes token address and ticker (symbol) as an argument. The admin of exchange can only call this function. The Deposit function is used to deposit tokens into the exchange, and the Withdraw function is used to withdraw the tokens from the exchange into external wallets.

DAI token is used as quote currency using which any listed token can be purchased or sold for DAI. DAI is used because it is a stable coin and its value always remains close to \$1.

Figure 3 shows the function where a user can place new orders.

Figure 4 shows all the orders placed on the platform by the users worldwide and the orders that a particular user places on the coin drop platform in my orders' section.

Characteristics	Centralized Exchange Platforms	Decentralized Exchange Platforms	Coin Drop (Proposed System)
Control	platform has the most control	User has the most control	User has the most control
Security	Risk of Hackers	No chance of hacking	No chance of hacking
Transaction Fees	Charges fees for using the platform	Charges zero or very minimal fees	Charges zero fees
Type of Transactions	On-Chain	On-chain	Off-chain
Number of Currencies	2-5	2-5	Almost all
Liquidity	High Liquidity	Low Liquidity	High Liquidity
Speed	Executes orders in milliseconds	Can take up to an hour to execute orders	Executes orders in milliseconds

Fig. 5 Comparison of centralised exchange [13–15], decentralised exchange [13, 14, 22] and coin drop

5 Result

From the proposed system stated in the paper, we found that the decentralised platform that is proposed and created has the control in the hands of users and is less prone to attack by the malicious users as compared to the centralised exchanges as the amounts in the personal wallets are comparatively less when compared to the centralised banks. The proposed system aims to take no amount to create or validate a transaction, and the transactions are performed off-chain, which increases the speed of transactions. The proposed system can handle any cryptocurrencies using DAI token, a stable currency form, as an intermediary currency when exchanging between two currencies. Thus, all these points were taken into consideration, and a comparison of current centralised and decentralised exchange platforms with the system proposed in the paper is shown in Fig. 5.

6 Conclusion

The cryptocurrency users have increased, and so the worth of cryptocurrencies. Many platforms provide cryptoexchanges services, but they have certain limitations, and they work with a few cryptocurrencies. We have developed and proposed a system that increases the cryptographic transactions’ speed as they are done in the off-chain. The coin drop system can handle exchange between any cryptocurrencies. Thus, the developed system provides a better approach and takes the right parts of both the centralised and decentralised systems.

References

1. Farrell, R.: An analysis of the cryptocurrency industry (2015)
2. Peters, G., Panayi, E., Chapelle, A.: Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. *J. Financ. Perspect.* **3**(3) (2015)
3. Bucko, J., Pal'ova, D., Vejacka, M.: Security and trust in ' cryptocurrencies. In: Central European Conference in Finance and Economics, pp. 14–24 (2015)
4. Bohme, R., Christin, N., Edelman, B., Moore, T.: Bit- " coin: Economics, technology, and governance. *J. Econ. Perspect.* **29**(2), 213–238 (2015)
5. Bouoiyour, J., Selmi, R.: Ether: Bitcoin's competitor or ally? *arXiv preprint arXiv:1707.07977* (2017)
6. Reed, J.: Litecoin: an introduction to litecoin cryptocurrency and litecoin mining (2017)
7. Gkillas, K., Bekiros, S., Siriopoulos, C.: Extreme correlation in cryptocurrency markets. Available at SSRN 3180934 (2018)
8. Guides, T.S.: Why cardano ada deserves your attention—cardano cryptocurrency strategy (2018)
9. Wei, W.C.: Liquidity and market efficiency in cryptocurrencies. *Econ. Lett.* **168**, 21–24 (2018)
10. Liu, Y., Tsyvinski, A., Wu, X.: Common risk factors in cryptocurrency. National Bureau of Economic Research, Technical Report (2019)
11. Barone, R., Masciandaro, D.: Cryptocurrency or usury? Crime and alternative money laundering techniques. *Eur. J. Law Econ.* **47**(2), 233–254 (2019)
12. Twomey, D., Mann, A.: Fraud and manipulation within cryptocurrency markets. In: Alexander, C., Cumming, D. (eds.) *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation*, pp. 205–250 (2020)
13. Lin, L.X.: Deconstructing decentralised exchanges. *Stanf J Blockchain Law Policy*, **2** (2019)
14. Scott, B.: How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? UNRISD Working Paper, Technical Report (2016)
15. Bashir, I.: *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. Packt Publishing Ltd (2018)
16. Velde, F., et al.: *Bitcoin: A primer* (2013)
17. Nakamoto, S.: *Bitcoin whitepaper* (2008). <https://bitcoin.org/bitcoin.pdf> (17.07. 2019)
18. Khan, A.G., Zahid, A.H., Hussain, M., Riaz, U.: Security of cryptocurrency using hardware wallet and qr code. In: 2019 International Conference on Innovative Computing (ICIC). IEEE, pp. 1–10 (2019)
19. Das, P., Faust, S., Loss, J.: A formal treatment of deterministic wallets. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 651–668 (2019)
20. Jasem, F.M., Sagheer, A.M., Awad, A.M.: Enhancement of digital signature algorithm in bitcoin wallet. *Bull. Electr. Eng. Inf.* **10**(1), 449–457 (2021)
21. Bacon, J., Michels, J.D., Millard, C., Singh, J.: Blockchain demystified: a technical and legal introduction to distributed and centralised ledgers. *Rich. JL Tech.* **25**, 1 (2018)
22. Pop, C., Pop, C., Marcel, A., Vesa, A., Petrican, T., Cioara, T., Anghel, I., Salomie, I.: Decentralizing the stock exchange using blockchain an ethereum-based implementation of the bucharest stock exchange. In: *2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, pp. 459–466 (2018)

Smart Contracts and NFTs: Non-Fungible Tokens as a Core Component of Blockchain to Be Used as Collectibles



Akash Arora, Kanisk, and Shailender Kumar

Abstract Non-fungible tokens are one of the most important future application domains for smart contracts. Ethereum is the pioneer of a blockchain-based decentralized computing platform that has ultimately standardized these types of tokens into a well-defined interface, now known as ERC-721. Blockchain-based cryptocurrencies have received extensive attention recently. Massive data has been stored on permissionless blockchains. This paper aims to analyze blockchain and cryptocurrencies' technical underpinnings, specifically non-fungible tokens or "crypto-collectibles," with the help of a blockchain-based image matching game. While outlining the theoretical implications and use cases of NFTs, this paper also gives a glimpse into their possible use in the domain of human user verification to prevent misuse of public data by automated scripts. This demonstrates the interaction of the ERC-721 token with the Ethereum-based decentralized application. Further, we aim to reach a definitive conclusion on the benefits and challenges of NFTs and thus reach a solution that would be beneficial to both researchers and practitioners.

Keywords Blockchain · Dapp · Decentralized · Ethereum · NFT · ERC-721 · Smart contract · Truffle

A. Arora (✉) · Kanisk · S. Kumar

Department of Computer Science Engineering, Delhi Technological University,
Shahbad Daulatpur, Bawana, New Delhi, India
e-mail: akasharora_2k17se13@dtu.ac.in

Kanisk

e-mail: Kanisk_2k17se13@dtu.ac.in

S. Kumar

e-mail: shailenderkumar@dce.ac.in

1 Introduction

The concept of blockchain was initially envisaged as a decentralized network that could store records of transactions that happened on it and thus act as a source of trust. “The data stored on the blockchain is immutable and updated by the peer-to-peer network” [1]. By design, entities called “blocks” constitute a blockchain. These blocks have the capability by design to store transactions that have been broadcasted. Only such transactions are deemed to be valid that have been broadcasted and hence been verified. To put it quite simply in layman terms, a blockchain is a database [1]. To grasp this concept clearly, we have to understand what a database is. A database points to collecting stored information either electronically or otherwise on either a computer system or a ledger. In databases, information or data is typically structured in table format to allow for easier searching and filtering specific details. While a blockchain ultimately aims to serve a similar purpose as a database, it offers many advantages over the latter. The primary difference arises in the way that the data is stored in a blockchain. While in a database, data is often stored in a tabular format, a blockchain stores data in small chunks or blocks (and hence the name blockchain) that hold sets of information that are all connected together.

The entities which constitute a blockchain and are known as “Blocks” which are designed to have storage capacities. When the storage capacity of one such block is completely full, it is then attached to the previously filled block. In this manner, a chain of data known as the “blockchain” is created. New information is written after creating that freshly added block is added into a newly created block that will also be added to the chain once it is completely full (Fig. 1).

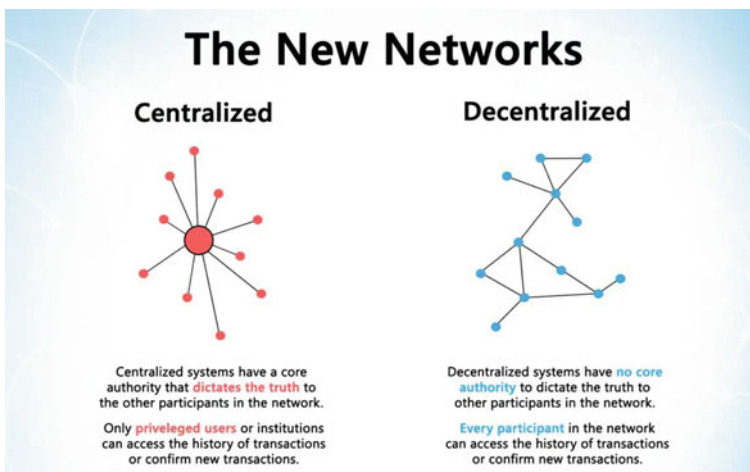


Fig. 1 Centralized versus decentralized system. Source <https://blockgeeks.com/blockchain-infographics/>

One of the central tenets of blockchain technology is “Decentralization” [2, 3]. The concept of decentralization can be best understood by contrasting it with a centralized network. The basic idea behind any centralized network is straightforward, “any centralized entity will anyways store all the data, and hence, an individual will always have to interact solely with this particular centralized entity to get whatever information or data that one requires” [2]. The traditional Client–Server network model is a perfect example of a centralized system. However, centralized systems have their drawbacks. The primary disadvantages include security vulnerabilities, lack of redundancy, and excessive dependency on the central node, which increases the chances of complete failure. These are the drawbacks that a decentralized system aims to address. By definition, in a decentralized system, “the information will not be stored by any one single entity. Everyone in the network owns the information” [2, 3].

Every node in a blockchain is designed to have a complete record of all the data that has been stored on the blockchain since its inception. The error in one node’s data can be corrected by referencing the correct data in thousands of other nodes. This way, the creators of blockchain have ensured by a design that a single malicious node cannot inject information on the entire chain. This also means that the transaction history present in each block that constitutes the Bitcoin blockchain cannot be altered or modified. Another advantage of this decentralized nature of blockchain is transparency. A user can independently verify any transaction transparently, either by a personal node or by using automated scripts that crawl through the blockchain. This would enable interested individuals to witness ongoing transactions. Moreover, every constituting node contains a private version of the blockchain that gets refreshed as new blocks are verified and included.

Non-fungible tokens are an integral part of this paper. Non-fungible tokens are dissimilar tokens that do not conform to the concept of fungibility. The idea of fungibility deals with the currency’s ability to maintain a standard value and uniform acceptance. Fungibility implies the immunity of the currency’s value from its precedents; this ensures that each piece of that currency is equal in value to every other piece [4]. This means that one ₹100 note in my pocket is equal in value, identical, and replaceable with any other ₹100 note in any other individual’s pocket. Hence, a ₹100 note is a fungible asset.

On the contrary, non-fungible tokens are blockchain assets that are designed not to be equal. Non-fungibility is the USP of such investments. This characteristic is of enormous importance when we are talking about rare and unique collectibles. The value of such items is derived from their non-fungibility (Fig. 2).

Another essential part of a blockchain network is smart contracts. Strictly speaking, a smart contract can be classified as a self-executing contract with the terms of the agreement between the buyer and seller being written from the get-go into the lines of code that make it up. The script and the contract contained within the smart contract are present across a distributed ledger and a decentralized network. The code controls the execution, and transactions are trackable and are hence irreversible.

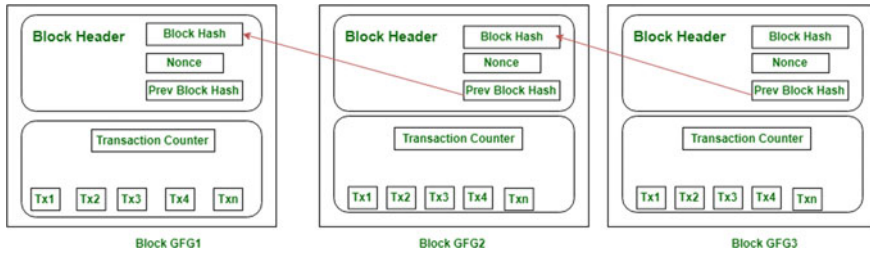


Fig. 2 Blockchain structure. Source <https://www.geeksforgeeks.org/proof-of-work-pow-consensus/>

“The biggest advantage of smart contracts is that they permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism” [5]. Smart contracts were originally proposed in the late twentieth century by Nick Szabo. Nick was a western computer scientist who had invented a virtual currency called “Bit Gold.” His original intention behind creating smart contracts was to scale up the capabilities of contemporary transaction methods, such as point of sale (POS) to the digital realm.

Having glossed through this paper’s fundamental building blocks, it would be prudent to revert to this paper’s intention. We intend to showcase the interaction of NFTs built on the ERC-721 standard with smart contracts on the Ethereum blockchain using an Ethereum Dapp. To achieve this, we will be mining NFTs using an image tile-matching game. In this game, we will be collecting tokens in the form of collectibles. Furthermore, this collection is driven by smart contracts, and hence, the interaction between smart contracts and NFTs is established on the Ethereum network.

2 Related Work

2.1 Blockchain

A blockchain can be referred to as a decentralized network that can keep transaction records and thus get the capability to act as a bank of reliability [6]. The electronic details cached on the blockchain are perceived to be unchangeable, and it is designed to be continually updated by the peer-to-peer network. These blocks have the capability by design to store transactions that have been broadcasted. Only such transactions are deemed to be valid that have been broadcasted and hence been verified.

Blockchain technology can be said to have evolved from the development of Bitcoin as a distributed, immutable ledger that is maintained and verified on a network of peers. Since then, several industries have sought to explore the

fundamental peer-to-peer technology and its myriad other applications, including creating extremely cost-effective and decentralized business network models or architecture.

Blockchain can also be a working specimen of a distributed computing system with high secure fault tolerance. Satoshi Nakamoto pioneered blockchain in 2008, who initially conceptualized it and then implemented it in the following year as a core component of the digital currency Bitcoin. Blockchain forms the public ledger for all transactions that are done using Bitcoin. Blockchain databases are designed to be managed without any human intervention, i.e., autonomously using a peer-to-peer network and a distributed timestamping server. Blockchain helped Bitcoin to attain the status of the first digital currency to solve the double-spending problem.

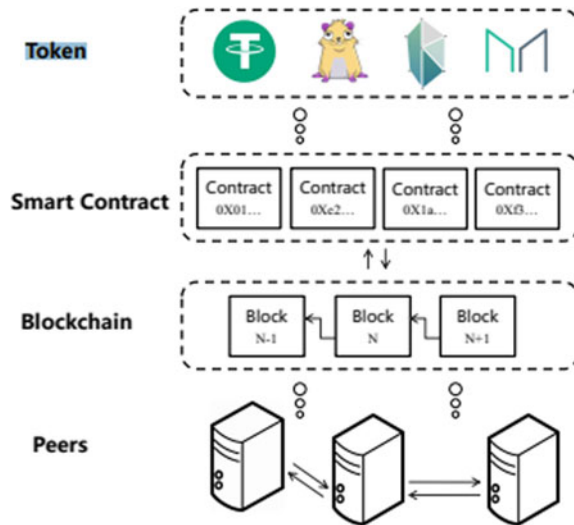
Blockchains, based on ownership and exclusivity, can be classified into private and public. The primary difference between the two is that anyone can join and contribute to a public blockchain. In contrast, one requires permission from a central authority to do so on a private blockchain. An advantage of public blockchains is that they are pseudo-anonymous by design as all transactions are public and hence hard to link them to identity.

2.2 *Ethereum*

Ethereum was initially conceptualized in 2013 by Vitalik Buterin, a 19-year-old Canadian developer. He sought to expand on the Nakamoto whitepaper and published a paper which was titled “A Next-Generation Smart Contract and Decentralized Application Platform.” Buterin worked on all the primary strengths of Bitcoin, which included an incentive scheme for miners, proof of work, and hashing, to name a few, and further capitalized it to create a new Blockchain known as Ethereum. A significant advantage possessed by Ethereum can be said to be the implementation of a turing-complete language. What that meant was that the Ethereum blockchain could handle complex code to exploit the immense computing power that was being harnessed (but ultimately wasted) by the incentive scheme, something which could not be done successfully or optimally by the Bitcoin blockchain due to inherent defects of designs. It can be said that while Bitcoin was envisaged to be an unhackable store of value with few capabilities other than this one objective. Ethereum was designed and intended from the start to expand and ultimately realize the full scope of capabilities that could potentially be offered by blockchain technology and hence, theoretically, create a decentralized computer that could operate on a global scale.

It would be worth noting that Ethereum is a blockchain designed to build on the abstractions introduced by Bitcoin. Hence, Ethereum does not have an overarching outfit to handle the transactions leading to all recorded events on a blockchain. A consensus algorithm called proof of work is used to secure this open and decentralized network. The general public has complete access to all events

Fig. 3 Overview of ethereum blockchain. *Source* Zheng et al. [7]



happening on the blockchain. Ethereum is supposed to tackle use cases related to Bitcoin, with error avalanche, underlining and dictating the creation of coins on the network and arriving at a network-wide consensus. A spinoff of this capability is that Ethereum has become one of the most popular platforms for developing new blockchain-based applications (Fig. 3).

2.3 Nodes

Nodes can be described as the participants in the blockchain. All the nodes are connected on a peer-to-peer network. Every node has complete access to the blockchain and can thus verify any incoming transactions. The operational requirement of a full node is a copy of the blockchain and ample storage space. The basic requirement for a user to become a miner is to run a full node. There is one other type of node, which is known as a lightweight node that stores only the hashes of the blocks. It occupies significantly less space as it receives additional information from full nodes.

2.4 Mining

Mining is the method through which new transactions are added to the blockchain. Hence, mining can be described as the process through which a block of transactions can be created and added to the Ethereum blockchain. Ethereum currently

uses a consensus mechanism known as proof of work (PoW) [8]. Mining is said to be the lifeblood of proof of work. Ethereum miners are generally computers running specific software which use time and high computation power to process transactions and produce blocks. Further, miners are greatly incentivized to compete with each other because finding a reward in the form of newly minted coins and transaction fees is guaranteed on finding the right solution. When compared to Bitcoin, Ethereum does not have a limit on the number of possible Ether that can be mined. Subsequent to the successful creation of the target block and its verification by the network, “miners start competing for the next block” [1].

2.5 Proof of Work

It is a type of consensus algorithm which is also used in Ethereum blockchain. Proof of work can be best described as the algorithm that has to be solved by miners so as to find an appropriate hash for the next block.

Hash rate denotes the rate of mining activity on the network. We can suitably adjust the difficulty of this algorithm if the hash rate increases. This algorithm is said to be innovative because not only does it allow unrestricted entry to anyone who is running a full node but it also accredits the network to frame a protocol that can be used to amend the blockchain. Furthermore, it has error avalanche handling capability, which means that it can positively handle setbacks and malicious users that disrupt the network (Fig. 4).

2.6 Addresses and Wallet

Asymmetric cryptography is a fundamental concept to blockchain. Any user can spawn a random digital signature in the form of a private key. This key can be used to spawn a public key. The user address can be spawned using the public key only. This is the address where the number of funds can be stored, and then, the user can use his private key to sign transactions from his address. The public key shall be used to check the origin of those transactions and get them verified by the network.

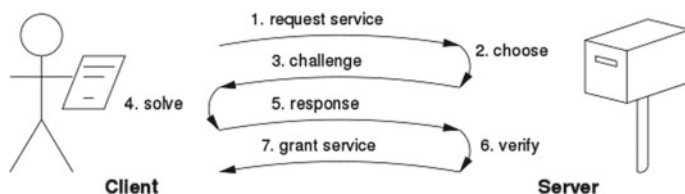


Fig. 4 PoW consensus. Source https://en.wikipedia.org/wiki/Proof_of_work

This means that access to funds would be lost if the private key is lost. Wallets help users to keep track of their financial assets and addresses. In the case of Ethereum, the wallet also can communicate internally with smart contracts and Dapp.

2.7 Transactions

“Messages that are signed by the address that has triggered them and can thus change the state of the network are known as transactions” [1, 9]. The fundamental concepts of the proprietary algorithm used are as follows:

Proof of authority: Unique signature of the owner of the private key.

Non-repudiation: The above is undeniable.

Unchangeability of transaction data: The transaction contents are unchangeable, and its integrity is not compromised.

The transaction structure on the Ethereum blockchain is the following.

Nonce: Numerical quantity of transactions that have been sent from an address.

Gas price: The financial cost to be levied on the initiator of the transaction for its execution.

Gas limit: The maximal gas permitted.

Recipient: The smart contract address or the payable address for the transaction.

Value: The financial weight in terms of Ether in the transaction.

Data: Quantity of binary input.

v , r , s : Worth of transaction signature.

2.8 Non-Fungible Tokens (NFTs)

Non-fungible tokens possess a specific digital signature that is contained within their smart contract. This identifying information is what makes each NFT different from another, and hence, an individual cannot swap them for another token. What this means is that they cannot be supplanted one for another, considering no two are undifferentiated. To put things in perspective, banknotes can be simply exchanged one for another if they possess the same value, and thus, it makes no difference to the holder. Non-fungible tokens are indivisible, in the same way as it is not possible to send someone part of a movie ticket. Part of a movie ticket is not redeemable and is not worth anything on its own. Crypto-kitties collectibles were the first famous non-fungible tokens. When referring to crypto-kitties collectibles, each cat is unique; i.e., if anyone sends someone a crypto-kitty and receives a crypto-kitty from someone else, the received kitty will be a unique and different crypto-kitty from the one you sent. Some noteworthy attributes are associated with non-fungible tokens. For instance, tokens are generally chained to a specific asset. Moreover, they can also prove the right of possession over items like vinyl's used in games and even the ownership of physical assets. Other tokens can be purported to possess

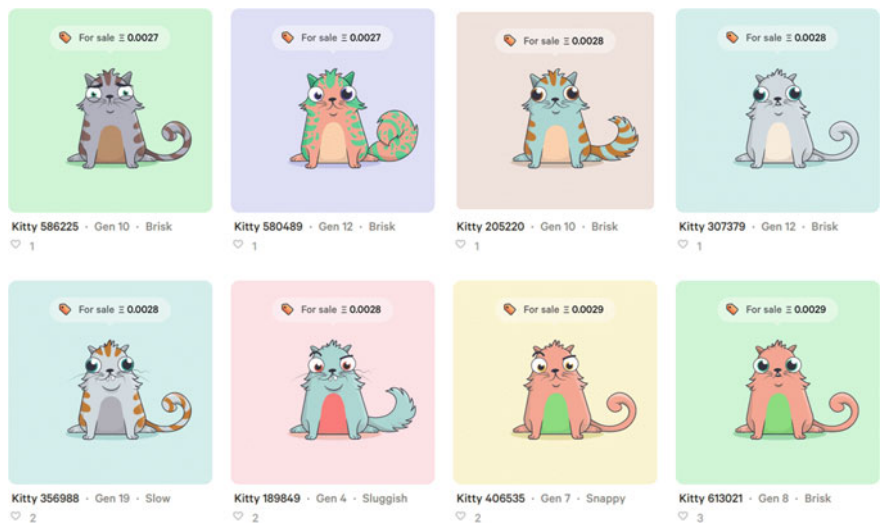


Fig. 5 Crypto-kitties collectibles. <https://www.investopedia.com/news/cryptokitties-are-still-things-heres-why>

the characteristic of fungibility in the same way as any fiat currency is said to be fungible. Fungible tokens are different from NFTs as they are identical, and thus, they have the same denomination when exchanged.

NFTs are as follows:

- (a) Rare (b) Unique (c) Indivisible (d) Transferable (Fig. 5).

2.9 Smart Contracts

For a layman, “smart contracts can be described as lines of code that are stored on a blockchain and are automatically executed when predetermined or predefined terms and conditions are met” [10]. Technically speaking, smart contracts were defined in 1994 by Nick Szabo as “a computerized transaction protocol which can be used to execute the terms of any contract.” As is evident from the description, business collaborations can demonstrate most of the smart contracts’ upsides. “Smart contracts can be used to enforce some agreement so that all participants can be certain of the outcome without an intermediary’s involvement in such business collaborations” [10]. Ethereum pioneered the use of smart contracts among blockchain, which led to the development of high-utility applications in various sectors, including the finance sector. “The code can only be deployed on the network after its high-level code is compiled to low-level code and is sent to a 0 × 0 address” [1]. Subsequently, “an address is allotted to it which can subsequently be used to utilize the contract’s functionalities by calling its functions. Although the high-level

Fig. 6 Representation of smart contracts. *Source* <https://www.edureka.co/blog/smart-contracts/>



language of choice for writing Ethereum code in solidity, there are various other high-level languages which can be used for writing Ethereum code” [1] (Fig. 6).

3 Literature Review

After assessing a substantial number of research papers on the subject matter at hand, we learned the following points. Our learnings can be categorized under the following sub-headings.

3.1 Decentralized Finance (DeFi)

The YoY growth of the market for NFTs is expected to be above 60% in this FY. Adopting an iterative research approach to the use-case about ownership of NFTs, a novel solution that proposes to increase market penetration of NFTs has been reached. This solution will provide a platform for developing increasingly complex financial instruments, enabling NFT users to leverage and lease their valuable assets linked/stored in tokens [1].

Some proposed use cases include:

1. Leasing tokens to generate income for passive users.
2. Lending/leveraging tokens generate quick liquidity, thereby eliminating the overhead costs associated with selling the asset.

3. Creating financial tools on the lines of futures will help to stabilize the market.
4. Creating a legal framework for the tokenization of real estate assets.

3.2 Blockchain Development Platforms

There are multiple platforms that users can utilize for the development and implementation of smart contracts based on the level of advancement attained by the user and the specific use cases that the user is targeting. Truffle suite is best suited for developers who are just starting and are nascent to this technology owing to the limited capacity of truffle suite to implement multi-layered smart contracts. Developers who are looking for a robust compiler and development environment would be better suited to utilizing remix. An ideal combination would be using truffle suite for testing while remix would be utilized for compiling the smart contracts, and the deployment would be handled by Mist and Geth [10].

3.3 Recent Advancements and Future Trends in Smart Contracts

Smart contracts are fundamental to the optimal exploitation of the immense potential offered by blockchain and associated technologies. Due to this, a large amount of research is going to be done on smart contracts in the academic field, and the resultant interest generated in the industry will be immense. The trump card of smart contracts is their immutable and irreversible characteristic. These characteristics facilitate the exchange of money and other assets in a way which avoids the involvement of a third party. Smart contracts face certain challenges which include reentrancy vulnerability, transaction ordering dependence, time-stamp dependence, untrustworthy data feed, and privacy issues. The future of society is a transition into a cyber physical social system (CPSS). Blockchain and smart contracts will play an instrumental role in aiding this transition [5].

3.4 Trends on Crypto-Collectibles

The meteoric rise of crypto-collectibles on the blockchain network can be best understood by taking a glance at crypto-kitties. Crypto-kitties can be said to be the pioneer among collectibles in terms of raising financial interest. An initial amount of \$12 million followed by another \$15 million was successfully raised by VC method. Thus, it can be argued that crypto-games, just like crypto-Kitties, are financially viable. These games would serve to amplify the movement toward blockchain-based gaming. Coming back to crypto-kitties, the game works on the

principle of ownership of tokens, which are very valuable due to a limited supply by algorithmic design, being proven by blockchain. This lends to value addition of collectibles. Moreover, cryptocurrencies also reflect a kind of “digital materiality” due to this design [9].

Hence, it can be concluded that the major factors which would determine the worth of crypto-game tokens can be refined to three most influential ones. The first factor can be said to be the limited technical infrastructure which impedes the capabilities of the network. Limited technical infrastructure can refer to the lack of scalability of the blockchain itself or the steep learning curve involved in learning how to operate crypto-wallet. The second limiting factor is the unequal playing field for blockchain users. By an unequal playing field, we are referring to the gas fees required to be paid by the users to cryptocurrency miners for the purpose of infrastructure maintenance which gives an unfair advantage to users with greater financial resources. Finally, the third limiting factor is the unclear or unvalidated legal ownership of tokens due to the anonymity accorded to the users by design on a blockchain. Any attempt to validate or prove legal ownership of tokens can only be done after the user de-anonymizes himself which would then defeat the purpose of cryptocurrencies based on a blockchain network.

3.5 Blockchain Digital Art

One of the major use cases of blockchain technology lies in the creative industry. The creative industry relies heavily on the revenue generated by the trio of rights management, licensing, and data management of digitized/digitizable products. Blockchain technology could be leveraged to manage the aforementioned in a manner which is automated and decentralized. Block technology will increase the power in the hands of the original content creators by offering a shared data layer on the application level rather than on the data level which is offered by existing Internet-based solutions. A business model which is based on token issuance and management by the creator can be built on the framework provided by blockchain technology [6].

4 Research Background and Methodology

4.1 Decentralized Applications (DApps)

Dapps were created to operate as applications compatible with smart contracts enabled, which had the capacity to work on distributed ledgers. Users have the capability to interact with a wide range of Dapps on Ethereum.

4.2 How Do You Make a Token?

The definition of tokens is contained within smart contracts. A token smart contract, once deployed, keeps track of the number of tokens owned by any address. Addresses also have the capability to transfer tokens attributed to them to other addresses. The smart contract keeps track of the number of tokens owned by each individual and not the underlying blockchain itself in contrast to ETH [11]. Hence, we would need to query the smart contract in order to find out how many tokens an address has. This is a distinction that everyone must recognize. When one is querying how many ETH an address has, one is querying the blockchain. When user query the amount of ETH (Ethereum currency) linked to an address, blockchain is queried. In contrast, when user query the amount (number) of tokens linked to an address, smart contract is queried. Hence, to know how many ETH and tokens a wallet has, an individual needs to know all the addresses of where the token smart contracts are deployed on the blockchain [1].

4.3 ERC-721

ERC-721 has been established as the basest standard that a smart contract will have to adhere to so that it is allowed to own and trade unique tokens. ERC-721 has not decreed a caliber for token metadata and neither does it restrict adding supplemental functions. Thus, ERC-721 can be described as a protocol that is subject to free peer assessment, which advises how to build NFTs on the Ethereum decentralized network of nodes. A whole lot of tokens are fungible (fungibility implies that every token is exactly the same to and changeable with any other token), ERC-721 tokens have to be all one of a kind. ERC-721 tokens are non-fungible in nature. “Their lack of fungibility connotes that each token has a set of characteristics and standards associated with it which are exclusionary to it” [1]. The “uniqueness of such tokens makes ownership more desirable especially in the case of collectibles and other such highly sought-after tokens” [1].

4.4 Open Zeppelin

Open Zeppelin is a library that was created for the purpose of safe contract development. It is built on a solid foundation of community-vetted code. It enables the implementation of standards like ERC20 and ERC721. It boasts of a flexible role-based permissioning scheme. Further, components of solidity, which are used to build custom contracts and complex decentralized systems, are reusable, which enhances its utility. Moreover, top-grade interoperability with the gas station network for systems with no gas fees also contributes to its varying uses. It has been audited by leading security firms and is, thus, perfectly safe.

4.5 *Truffle Suite*

“Truffle is a development environment, testing framework, and asset pipeline for Ethereum, which aims to make the life of an Ethereum developer much easier” [12]. Truffle offers the following advantages to an Ethereum developer:

- Deployment and binary management linked using built-in smart contract compilation.

- Computer robotized testing of contract.

- Custom build processes supported by configurable build pipeline.

- Scriptable deployment and migrations framework.

- Public and private networks deployed using network management.

- Scripts executed within a truffle environment by an external script runner.

4.6 *Web3.js*

Web3.js enables an Ethereum developer to fulfill his/her second responsibility, i.e., creating modules that communicate with the Ethereum decentralized network. Web3.js is basically an amalgamation of non-volatile computer code that permits the developer to perform actions like the transfer of Ether and modify smart contracts. The diagram demonstrates how a client does tête-à-tête with Ethereum.

Web3.js talks to the Ethereum blockchain using a JSON RPC, which stands for the “Remote Procedure Call” protocol. As Ethereum is based on a peer-to-peer network of nodes that needs to save an additional version of important information on the blockchain, Web3.js allows a developer or a user to make requests to an individual Ethereum node with JSON RPC in order to modify or access the data in the network. An appropriate would be the cohesion of jQuery with a JSON API to modify a web server.

4.7 *Metamask*

“MetaMask is a browser plugin that also serves as an Ethereum wallet and is installed like any regular plugin. It allows users to store Ether and other ERC-20 tokens and thus enables them to consummate transactions with any Ethereum address” [13].

4.8 Ganache

Ganache is used for setting up an individual Ethereum decentralized network of nodes for validating solidity contracts. Moreover, it provides more functionalities when compared to other similar software.

5 Design and Implementation Setup

See Figs. 7, 8.

A. Installing the Following Dependencies:

```
{
  ``name``: ``blockchain-game``,
  ``version``: ``0.1.0``,
  ``description``: ``token collection game``,
  ``author``: ``akash and kanisk``,
  ``dependencies``: {
    ``@openzeppelin/contracts``: ``^2.3.0``,
    ``babel-polyfill``: ``6.26.0``,
    ``babel-preset-env``: ``1.7.0``,
    ``babel-preset-es2015``: ``6.24.1``,
```

Fig. 7 Design workflow: <https://medium.com/free-code-camp/how-to-design-a-secure-backend-for-your-decentralized-application-9541b5d8bddb>

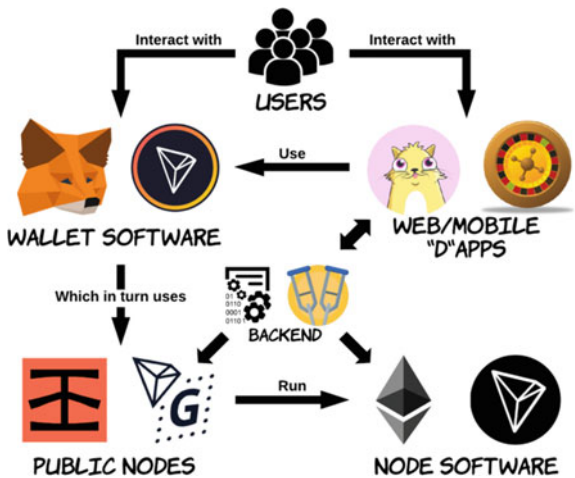


Fig. 8 Setting up environment

```
npm install --g truffle@5.1.39
```

```

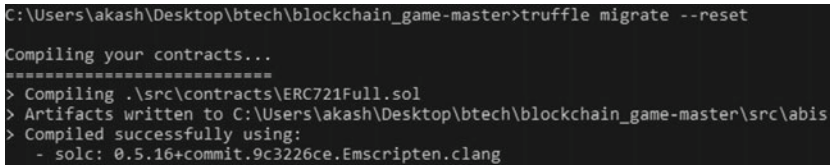
``babel-preset-stage-2``: ``6.24.1``,
``babel-preset-stage-3``: ``6.24.1``,
``babel-register``: ``6.26.0``,
``bootstrap``: ``4.3.1``,
``chai``: ``4.2.0``,
``chai-as-promised``: ``7.1.1``,
``chai-bignumber``: ``3.0.0``,
``react``: ``16.8.4``,
``react-bootstrap``: ``1.0.0-beta.5``,
``react-dom``: ``16.8.4``,
``react-particles-js``: ``^3.4.1``,
``react-scripts``: ``2.1.3``,
``truffle``: ``5.0.5``,
``truffle-flattener``: ``^1.4.2``,
``web3``: ``1.0.0-beta.55``
n}

```

See Figs. 9, 10.

6 Application. Conclusions

See Figs. 11, 12, 13, 14, 15, 16, 17.



```

C:\Users\akash\Desktop\btech\blockchain_game-master>truffle migrate --reset
Compiling your contracts...
=====
> Compiling .\src\contracts\ERC721Full.sol
> Artifacts written to C:\Users\akash\Desktop\btech\blockchain_game-master\src\abis
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang

```

Fig. 9 Compilation of smart contract

```

Starting migrations...
=====
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)

1_initial_migration.js
=====

Replacing 'Migrations'
-----
> transaction hash: 0xcabda9f9cd0af580fbd415ca42290620d536c8a450f0f4e9ade3ea01a6b28816f
> Blocks: 0        Seconds: 0
> contract address: 0x02C116f2d00Fe641C77af4cd4548e8718a90dE9c
> block number:    7
> block timestamp: 1606671479
> account:         0xbB82F68A0eE8942b4552159D83C2dBAF1230EC0E
> balance:         99.93599252
> gas used:        225237 (0x36fd5)
> gas price:       20 gwei
> value sent:      0 ETH
> total cost:      0.00450474 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost:      0.00450474 ETH

2_deploy_contracts.js
=====

Replacing 'MemoryToken'
-----
> transaction hash: 0x22cfaea207211e9d38fd66c6d405c5813f6348c49fe29ef1d66d751f5314cf4a
> Blocks: 0        Seconds: 0
> contract address: 0xc2E7000ae8210dAA2C508316a60DE30c882b264d
> block number:    9
> block timestamp: 1606671480
> account:         0xbB82F68A0eE8942b4552159D83C2dBAF1230EC0E
> balance:         99.89009146
> gas used:        2252690 (0x225f92)
> gas price:       20 gwei
> value sent:      0 ETH
> total cost:      0.0450538 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost:      0.0450538 ETH

Summary
=====
> Total deployments: 2
> Final cost:       0.04955854 ETH

```

Fig. 10 Deploying the smart contract

```

> contract address: 0xc2E7000ae8210dAA2C508316a60DE30c882b264d

```

Fig. 11 Smart contract address

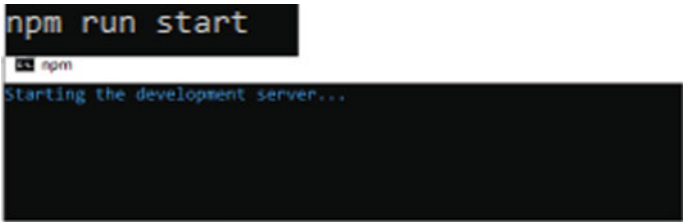


Fig. 12 For starting the server



Fig. 13 Application home page

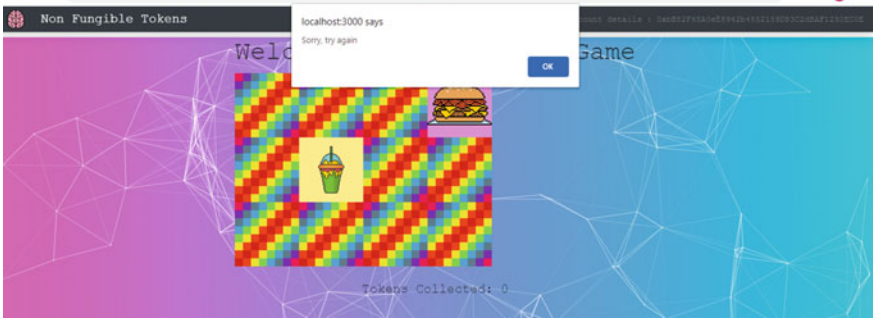


Fig. 14 Flow 1: tiles did not match (unsuccessful attempt)

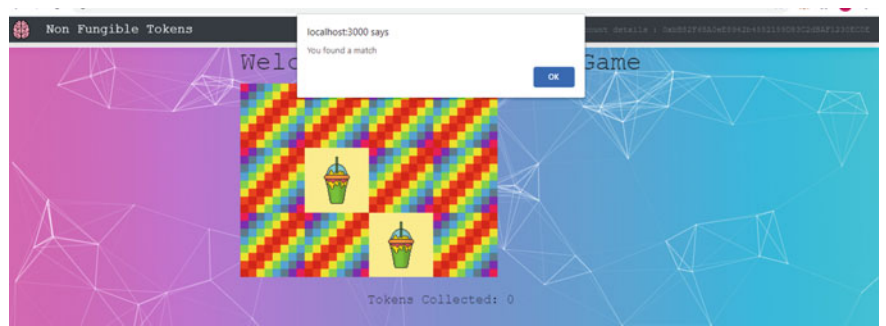


Fig. 15 Flow 2: tiles match (successful attempt)

Fig. 16 Transaction notification by MetaMask on successful matching and collection of tokens initiated

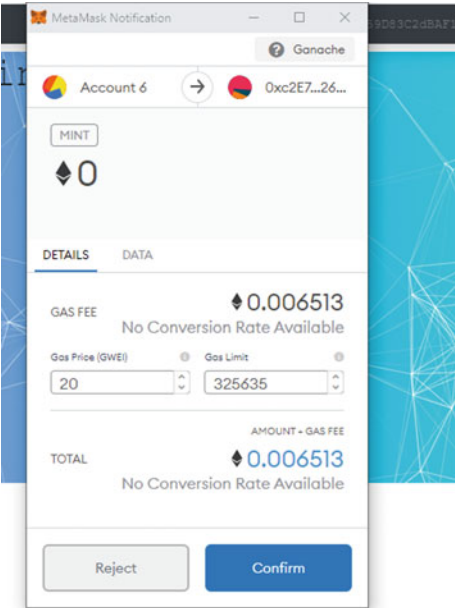


Fig. 17 Token collected



7 Results

The application environment is initially set up by installing the required dependencies. Consequent to the successful installation of the required dependencies, we then proceed to initiate the Ethereum node on the blockchain network using Ganache. Pursuant to the successful initiation of the Ethereum node, we then move on to smart contracts. The custom-tailored smart contract, written in solidity, has to be compiled by using truffle suite. Upon the successful compilation of the smart contract, we then deploy the smart contract. Once the smart contract is successfully deployed, a unique address is provided to the smart contract using which all further transactions can be accounted for and tracked [14]. This completes the back-end setup of our Ethereum decentralized application (Dapp).

The front-end part of the application is initiated by starting the application server, which is based on a React.js framework. It should be noted that a prerequisite for the successful initiation of the application server is that the plugin for MetaMask is installed in the web browser. The absence of which will lead to an unsuccessful connection attempt with the back-end server. On the successful initiation of the application server, we will see an image tile-matching game hosted successfully on localhost.

There are two flows of events that may take place henceforth. The first flow can be labeled as the unsuccessful match event. In this flow, as two similar-looking tiles are not matched by the user, no transaction is initiated by the smart contract as the token IDs do not match. The local host displays an unsuccessful attempt message and directs the user to make another attempt. The second flow can be labeled as a successful match event. In this flow, as two similar-looking tiles are correctly matched by the user, the smart contract initiates the transaction as the token IDs are matched correctly. The local host displays a successful attempt message to the user. A MetaMask window subsequently pops up to inform the user of the gas charge deducted to facilitate the transaction. The transaction details can be tracked using Ganache.

After the completion of the transaction, the token is collected and displayed on the application window. Hence, we have successfully gained a collectible NFT. By gaining this collectible NFT, the user can establish the provenance of the collectible as that collectible now possesses the uniqueness and rareness of the NFT it is linked to.

8 Conclusion and Future Scope

To conclude, we can state that the transaction of non-fungible tokens using deployable smart contracts has immense commercial and academic implications. The ERC-721 standards have given us immense power to accomplish next-generation advancements in fields as varied as art, culture, online gaming, rare collectibles, and more. This whole process hence confirms the non-fungibility of the

tokens created on the ERC-721 standard and their interaction with the smart contract as shown with the help of an Ethereum Dapp.

In the future, this work can be extended to the domains of authentication and human user verification so as to prevent misuse of cyber facilities and public data by automated scripts. These non-fungible tokens can also be used to validate the authenticity and pedigree of high value, rare, vintage collectibles, which could otherwise be faked so as to commit fraud. This will give the power of proof of originality/ownership to the owner or creator in the digital world. Hence, advanced applications can be made along similar lines of thoughts, which would give us a deeper insight into this domain and hence help us in verifying the antecedents of the product or any other item of value.

References

1. Musan, D.I.: NFT . finance leveraging non-fungible tokens. Imperial College London, Department of Computing (2020)
2. Kumar, A., Kumar, S.: A systematic review of the research on disruptive technology—blockchain. In: 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 900–905 (2020). <https://doi.org/10.1109/ICCES48766.2020.9138055>
3. Kumar, A., Kumar, S.: Implementation of decentralized electronic polling system using ethereum blockchain. *Int. J. Adv. Sci. Technol.* **29**(4), 10717–10728. (SCOPUS Indexed) ISSN: 2005–4238 (2020)
4. Uribe, D., Waters, G.A.: Privacy laws, genomic data and non-fungible tokens. *J. Br. Blockchain Assoc.* **3**(2) (2020) [Online]. Available: <https://jbba.scholasticahq.com/article/13164-privacy-laws-genomic-data-and-non-fungible-tokens>
5. Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., Wang, F.Y.: An overview of smart contract: architecture, applications, and future trends. *IEEE Intell. Veh. Symp. Proc.* 2018-June, no. Iv, pp. 108–113 (2018). <https://doi.org/10.1109/IVS.2018.8500488>
6. Chevet, S.: Blockchain technology and non-fungible tokens: reshaping value chains in creative industries. Sylvé CHEVET Under the supervision of Alain BUSSON, pp. 1–73 (2017)
7. Zheng, P., Zheng, Z., Wu, J., Dai, H.: XBlock-ETH: Extracting and exploring blockchain data from ethereum. *IEEE Open Journal of the Computer Society*, pp. 1–1 (2020). <https://doi.org/10.1109/OJCS.2020.2990458>
8. Buterin, V.: A next-generation smart contract and decentralized application platform. *Ethereum*, no. January, pp. 1–36 (2014) [Online]. Available: <http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf>
9. Bal, M., Ner, C. arXiv: NFTracer: A Non-Fungible Token Tracking Proof-of-Concept Using Hyperledger Fabric, pp. 1–9 (2019)
10. Chirtoaca, D., Ellul, J., Azzopardi, G.: A framework for creating deployable smart contracts for non-fungible tokens on the ethereum blockchain. In: 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, United Kingdom, pp. 100–105 (2020). <https://doi.org/10.1109/DAPPS49028.2020.00012>
11. Serada, A., Sihvonen, T., Harviainen, J.T.: CryptoKitties and the New Ludic Economy: How Blockchain Introduces Value, Ownership, and Scarcity in Digital Gaming. *Games Cult.* (2020). <https://doi.org/10.1177/1555412019898305>

12. Anilkumar, V., Joji, J.A., Afzal, A., Sheik, R.: Blockchain simulation and development platforms: survey, issues, and challenges. 2019 International Conference on Intelligent Computing and Control Systems ICCS 2019, no. Iciccs, pp. 935–939 (2019). <https://doi.org/10.1109/ICCS45141.2019.9065421>
13. Dagher, G.G., Marella, P.B., Milojkovic, M., Mohler, J.: Bron covote: secure voting system using ethereum's blockchain. ICISSP 2018—Proceedings of 4th International Conference on Information System Security and Privacy, vol. 2018-Janua, pp. 96–107 (2018). <https://doi.org/10.5220/0006609700960107>
14. Mofokeng, N.E.M., Matima, T.K.: Future tourism trends: Utilizing non-fungible tokens to aid wildlife conservation. *Afr. J. Hosp. Tour. Leis.* **7**(4) (2018)

Blockchain in Health Care: A Review



Sanya Bindlish, Sargam Chhabra, Kshitij Mehta, and Pooja Sapra

Abstract Blockchain is taken to be a system of ledger which handles data and manages their transactions with the help of their time stamps through cryptographic hashing and serves in a decentralized technique over the computer networks. Despite the fact that blockchain concept is used on a large scale for cryptocurrency, this paper explores some potential applications of the blockchain concept in the healthcare industry as well. It discusses the use of blockchain technology in the healthcare sector and how it can help in overcoming the present challenges like interoperability, security, and cost of maintenance in the traditional healthcare system. This paper highlights the applications of blockchain in detail and why it is hard to implement in the healthcare sector.

Keywords Blockchain · Internet of things · Security · Health care

1 Introduction

Blockchain [1] is a type of database that consists of information in the form of blocks connected to each other using cryptographic methods, with each block containing the hash of the previous block, the records, and their time stamps. These blocks are consistently growing in number with the present value at 672,425 (recorded at 05:00 PM February 27, 2021).

S. Bindlish (✉) · S. Chhabra · K. Mehta · P. Sapra
The NorthCap University, Gurugram, India
e-mail: sanyabindlish@gmail.com

S. Chhabra
e-mail: sargamchhabra15@gmail.com

K. Mehta
e-mail: kshitij.mehta28@gmail.com

P. Sapra
e-mail: poojasapra@ncuindia.edu

The features of blockchain are:

- 1.1 **Immutability:** Blockchain does not allow any modification or deletion of the data once it has been recorded. This is because each block contains the hash of the previous one and if we modify the data then the hash of every following block will have to be altered.
- 1.2 **Decentralization:** Blockchain does not have a central entity that manages or controls the system. Instead, it works on the concept of a distributed network in which data is shared with all the computers on the network. This is called a ledger. Each time a new block is added, all these computers display the addition as every connection has the same copy of the ledger.
- 1.3 **Transparency:** This feature of blockchain allows anyone to join the network and validate the transactions of their peers so they can be added to a block. A history of all the transactions is also available.
- 1.4 **Trust and Consensus:** The blockchain system is established on trust as data is secured with the help of cryptographic methods. Consensus is a way of validating transactions on a distributed ledger by establishing an agreement between the peers. It eliminates the need of a central authority.

In this paper, Sect. 2 discusses the literature available for the applications of blockchain in health care, and Sect. 3 focusses on challenges in the healthcare sector and various domains where blockchain can be implemented. Section 4 concludes the paper.

2 Literature Survey

In [2], authors have presented a structured literature survey of research on blockchain applications such in the healthcare area. This analysis includes 42 article write-ups presenting the most up-to-date knowledge on present-day implications and loopholes in the blockchain execution for improvement in the healthcare sector. The findings in the sheet show that blockchain is being utilized to build advanced and up-to-the-minute interventions to upgrade the universal standards of handling, processing, and sharing of medical information/data and health records of the patients. This technology is going through an evolution in the healthcare sector where it has added a positive impact through improved efficiency, technological advancements, access control, security of data handling, privacy protection, etc. The sheet also presents some discoveries that suggest that some limitations primarily prevail to model the performance as well as have some effect on the cost of execution.

This research paper [3] addresses the potential areas where the future researchers or experimenters could contribute some value in the areas like system architecture,

data security, etc. Concluding the research, the findings suggest that the researches in the future will contribute in the deployment of this technology on a larger scale and also in the critical issues related to legal consents, security measures, medical diagnostics, and improving patient care in some cases like remote monitoring or emergency situations.

In this research paper [4], the researchers have surveyed a lot of interesting implementations of blockchain technology. Apart from the financial sector, a lot of sectors have been implementing the blockchain concept where its beneficial features add innovations and solutions to some compromised areas. These sectors which are mentioned in this paper are—health care, electronic voting, etc. For each of these topics, they have given a detailed study including the problems and solutions given by the blockchain concept.

In this research paper [5], authors reviewed important use cases of blockchain in the healthcare industry: patient record management, research, and billing claims management alongside the related projects. The authors have also discussed the challenges in the implementation of blockchain technology in the healthcare industry. Most of the blockchain projects and concepts are still in the form of prototypes and white papers. However, the use of blockchain technology is expanding.

In this research paper [6], authors gave an overview about the application of blockchain in the healthcare sector and how it helps in automation of healthcare services. The authors have not only focussed on the different applications of the technology but also identified the limitations of existing research and surveys. The authors conclude with stating the need of research for better understanding and development of this technology.

This research paper [7] gives us knowledge of how blockchain is gaining popularity in the market due to its concept of digitally shared ledger and consensus algo removing all the risks and threats of the mediators and intercessors. It also shows that the usage of blockchain has now extended to all the major sectors of research including banking, governance, IoT, health care, education, etc. The study reviews the existing literature about this field so as to list the major issues in health care and inspect the features of blockchain that could rectify the identified issues. However, a few challenges and limitations of this technology still need more research.

In this research paper [8], authors gave an overview of benefits and drawbacks related to blockchain technology. This paper also discusses the existing challenges related to crypto-currencies. Authors have discussed the advantage of using blockchain in the healthcare industry. There are various potential challenges in implementing blockchain in the healthcare sector; authors have also provided solutions to some of the challenges. Blockchain can help in the advancement of the medical sector in various ways and authors expect many more applications of blockchain in the near future.

In [9], the authors proposed a medical data management system using blockchain technology, which is much more secure than the traditional model and also allows patients ownership over their records while granting hospitals a temporary

and easy access to the data. This patient-centered blockchain model is based on Ethereum and it stores the actual medical records on a decentralized cloud system, Ethereum Swarm. Each medical record having its unique swarm hash is combined with the decryption key to form the root chunk and only the authorized personnel have access to the content in the root chunk.

In this research paper [10], authors have presented a basic introduction of blockchain technology and its structure. The authors have discussed the implementation of blockchain in the healthcare sector. Blockchain is an emerging technology but has some major challenges including usability and authentication of patients. The paper also briefly mentions the impact of blockchain in the near future. Future of blockchain in the healthcare sector is promising and will authorize the patients to take control of their medical records so that they can keep track of their health condition.

This research paper [11] discusses the management of confidential medical information of patients, sharing of medical records, image sharing, and log management. The authors have also reviewed studies that intersect with other areas and have performed SWOT analysis on the basis of these to analyze their positive and negative aspects. The authors provide guidance to future researchers by assessing the benefits and limitations of the medical concepts of blockchain. The paper concludes by summarizing the techniques used in health care, their applications, and pros and cons.

3 Blockchain and Health care

With the concept of blockchain becoming increasingly popular, it is believed that this technology will also evolve the healthcare sector in the near future. It can grant a new framework for health information exchanges (HIE) by listing medical records of patients more systematically keeping privacy, security, and interoperability in check.

3.1 *Blockchain Versus Current Healthcare Challenges*

This section provides an insight on how blockchain technology can help in overcoming some of the existing challenges in the healthcare field. Some of these are:

- (i) **Interoperability:** It refers to the characteristic of health information systems to operate together with other such organizations to deliver quality healthcare services to people more efficiently. Blockchain overcomes this challenge by retrieving data with the help of APIs, which helps in achieving data format standardization.

- (ii) **Security and Integrity:** It refers to the set of guidelines and standards to protect the confidentiality and integrity of personal health information. Data tampering and breach is a matter of concern in the healthcare sector. Blockchain provides security as it is immutable and data is stored in encrypted form so it is not possible to modify information.
- (iii) **Access Rights:** Managing health records across the organization is a challenge where blockchain technology can come in use. It makes sure that records are updated and available at every node. Also, access rights can be defined using the concept of smart contracts.
- (iv) **Cost of Maintenance:** Maintenance of healthcare systems includes various actions such as backup and recovery mechanisms.

In the case of blockchain, there is an open-distributed network where data is shared with all the nodes in the network. Therefore, failure of one node does not affect the other nodes. This reduces the need of a backup mechanism.

3.2 Applications of Blockchain in Health care

In this section, several important use cases and applications of blockchain in health care are discussed below:

- (i) **Blockchain for Electronic Health Record (EHR):**

Ideally, it is required that EHR should maintain a lifetime medical record which is accessible to the entire medical staff. In the present application of EHR, patient information is stored in multiple organizations throughout his lifetime. The physician conducts the diagnosis, specifies the problem, medication, and this record remains with him even after the patient is treated. In the blockchain implementation of EHR, only the individual will have access to his medical record and doctors will be granted access through smart contracts when required.

At present, interoperability and data fragmentation is a huge challenge among different organizations as they are reluctant to share data with each other. Using blockchain, the owner can set viewership permissions on the data shared with another entity. This is supported by smart contracts which are self-executing conditional contracts in which the agreement is coded. New records can be updated regularly on the patient's profile and he can decide which entity has access to which content, hence providing authorization.

- (ii) **Blockchain in Clinical Research:**

This also centralizes around the issue that an individual's medical data is scattered across the databases and records of multiple organizations which causes hindrance in sharing of data. Not only does it leads to inefficient treatment of patients, but also causes a setback in the domain of clinical research.

Clinical trials require real-time medical information of patients to conduct a sound hypothesis and research which is backed up by a set of realistic data. Gathering all these records from the scratch can be a very hard, time consuming, and costly process. Surveys show that people are ready to share their medical records for research provided that their data is not compromised. Blockchain supports this due to its features of transparency and trust. The data is public and anyone can write to it but no one has the permission to store it because of encryption. Patients can manage their data and also have the rights to deny access to it anytime. This framework would be beneficial for research entities to get hold of secure and accurate data.

(iii) ***Blockchain in Drug Supply Chain Management:***

Transparency and security of the supply chain are major challenges in the pharmaceutical sector. These services of this sector directly impact the lives of their consumers which is why safety and efficiency of the product are necessary. The product reaches the consumer after passing multiple stages: manufacturing, transportation, handling, storage, redistribution, and retail. Anything can go wrong in these stages from a simple human error to a malicious fraud as in the traditional system, identifying the cause of the issue can be very difficult. This is because records are maintained on a personal level and can be tampered with very easily. Such an unorganized set of data is not available to the company itself, let alone the government and consumers.

Blockchain solves this problem by providing a distributed ledger shared among all concerned members in the supply chain. The records stored in the form of blocks are immutable, permanent, and transparent. This reduces the possibility of errors and frauds significantly and also provides organized data visible even to the consumers.

(iv) ***Blockchain in Claim and Billing Management:***

Fraudulent claims and billing is one of the issues in the healthcare sector that needs to be eliminated. Some of the challenges faced in the claim and billing process are overcharging, performing unnecessary medical tests, and claiming charge for non-performed services. There are a lot of third parties involved in resolving the claim process, to ensure faster processing of claims and cost reduction for suppliers and clients.

Blockchain technology can help in automation of claim processing with the help of a smart contract between the involved parties. Also, the challenges faced in this process can be reduced to a great extent because of the transparent and distributed network in blockchain.

(v) ***Blockchain Application in Health Information Exchanges (HIE):***

HIE's goal is to offer secure delivery of healthcare data beyond geographical boundaries. To achieve this goal, data privacy and security should be given priority.

Security: Securing patient data is important and blockchain can be useful in doing so. On a blockchain, data is in encrypted form and can be accessed by using

the shared public key of a patient. Use of private and public keys defines access rights and ensures data privacy.

Decentralization: Centralized network is a traditional setup for HIE in which data from patients is stored in a central storage system where failing of the central node will lead to loss of medical records. Blockchain is an open-distributed ledger where each node will have the updated records and patients can define the access rights of their medical records, thereby scaling the infrastructure to a decentralized network from a traditional centralized network.

Interoperability: It refers to the characteristic of health information systems to operate together with other such organizations to deliver quality healthcare services to people more efficiently.

Blockchain offers access to patient's data with regular updates across all healthcare organizations. Its distributed-ledger feature removes the chances of duplicity as the same copy of data is available to all the organizations.

3.3 *Blockchain Technology—Challenges in Health Care*

Applying blockchain in the domain of health care has numerous advantages but the practical implementation of this technology is not as easy as it seems. This portion of the paper will discuss the challenges which blockchain technology has yet to overcome.

- (i) Blockchain has already been widely accepted in the field of banking but the awareness regarding this technology in the healthcare sector is yet to come by. Organizations are not aware of this technology and even if they are, the crucial challenge is understanding how it works and the benefits of adopting this technology.
- (ii) Organizations are comfortable with working in a centralized environment and do not prefer to shift to a decentralized system as it incurs cost for ensuring speed and efficiency.
- (iii) Another reason why healthcare entities are resistant to change is that shifting from their current system would require a lot of time and effort.

4 Conclusion

Blockchain is an emerging technology and has the capability to change the traditional business model to a brand-new advanced framework. Some organizations have started to adopt this technology in the healthcare sector, and it is expected to take over at least 55% of the global healthcare system by the year 2025. Blockchain technology offers promising solutions to the healthcare industry, and at this rate, it will soon become an integral part of the data management and supply chain

systems. There are various advantages of this technology in the healthcare sector; however, there are some challenges related to the implementation of blockchain such as lack of awareness regarding the working and implementation of technology that have yet to be tackled. Another challenge in implementation of blockchain in the healthcare sector is the amount of time and effort that will be required in shifting from the current centralized system to the decentralized system. This paper presents a review of numerous studies that deals with the use of blockchain technology in the healthcare sector.

On the basis of all the studies reviewed, it is evident that blockchain technology has a lot of scope in the future to develop and take over most of the traditional healthcare models. With this advancement in the health care, patients will have the assurance that their private data will not fall in the wrong hands and be misused.

References

1. Swan, M.: Blockchain: "Blueprint for a New Economy"; O'Reilly Media, Inc., Sebastopol, CA, USA (2015)
2. Nakamoto, S.: Bitcoin: "A Peer-to-Peer Electronic Cash System" (2008). Available online: www.bitcoin.org (accessed on 12 March 2019)
3. Hölbl, M., Kompara, M., Kamišalić, A., Zlatolas, L.N.: A systematic review of the use of blockchain in healthcare. *Symmetry* **10**, 470 (2018)
4. Patel, V.: A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* (2018)
5. Katuwal, G.J., Pandey, S., Hennessey, M.: Bishal Lamichhane: Applications of Blockchain in Healthcare: Current Landscape & Challenges (2018)
6. Fekih, R.B., Lahami, M.: Application of blockchain technology in healthcare: a comprehensive study. In: *ICOST 2020: The Impact of Digital Technologies on Public Health in Developed and Developing Countries*, 23, June 2020 (2020)
7. Yaqoob, S., Khan, M.M., Talib, R., Butt, A.D., Saleem, S., Arif, F., Nadeem, A.: Use of blockchain in healthcare: a systematic literature review. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, **10**(5) (2019)
8. Kuo, T.-T., Kim, H.-E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **24**(6), November 2017 (2017)
9. Chen, H.S., Jarrell, J.T., Carpenter, K.A., Cohen, D.S., Huang, X.: Blockchain in healthcare: a patient-centered model. *Biomed. J. Sci. Tech. Res.* (2019)
10. Revanna, N.: Blockchain in healthcare. *Int. Res. J. Eng. Technol. (IRJET)* **07**(04) (2020)
11. De Aguiar, E.J., Faíçal, B.S., Krishnamachari, B., Ueyama, J.: A survey of blockchain-based strategies for healthcare. *ACM Comput. Surv.* **53**(2), Article 27 (2020)

Section–C

A Comparative Study of the Energy-Efficient Advanced LEACH (ADV-LEACH1) Clustering Protocols in Heterogeneous and Homogeneous Wireless Sensor Networks



Nitin Kumar, Vinod Kumar, and Pawan Kumar Verma

Abstract Wireless sensor network (WSN) is a promising technology for monitoring the physical world. The energy limitation of WSNs makes it an energy saver technology. A number of diverse routing protocols can be used to enhance the network lifetime of WSNs. There exist two types of clustering-based approaches, namely homogeneous and heterogeneous. In the former case, all nodes have the same technical characteristics (bandwidth, processor, initial energy, etc.). In contrast, in the latter case, nodes have different technical characteristics, i.e., some of the nodes have higher ability than others in terms of the parameters listed above. In this paper, we analyze the ADV-LEACH1 algorithm for the homogenous WSNs. The mathematical modeling and simulation results achieved by MATLAB-2017b show a comparative analysis of heterogeneous and homogeneous WSNs in terms of the energy consumption, alive/dead nodes, and network lifetime. The ADV-LEACH1 with heterogeneous network performs better than that with the homogenous network because of advanced node presence in the network with higher energy level.

Keywords Node deployment • Heterogeneous • Homogeneous • WSN

N. Kumar · V. Kumar (✉)

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ghaziabad, UP, India
e-mail: vkchaudhary.rs.ece@iitbhu.ac.in

P. K. Verma

Department of Electronics and Communication Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, PB, India
e-mail: vermapk@nitj.ac.in

1 Introduction

The productive enhancement of WSNs has grown into an evolving subject matter of concern in communication. WSNs have erratically dispersed sensors that convey the data to base station (BS) nodes over the network wherever information can be retrieved and analyzed, as shown in Fig. 1. A BS is essentially considered the same as an interface to interrelate among an operator and a system. Utilizing radio signals, a sensor node (SN) can interact with another node. Afterward, arranging nodes above, sensors generate an appropriate infrastructure with multihop as well as single-hop communication. It also consists of a shortage of power because of the slight handling speed and storage capacity. To confirm a long-lasting network lifetime, lengthy detachment communication must be remained separately [1, 2]. Wireless Sensor Networks are different from Ad-hoc networks such as Vehicular Ad-hoc Network (VANET) [3] and Mobile Ad-hoc Network (MANET) [4] based on the mobility models, node mobility, higher node density, power consumption and network lifetime.

A clustering method is organizing the sensor nodes so that advantageous energy effectiveness and productivity are attained. Nodes in a cluster can convey that information to the cluster-head (CH) intended for the BS as exhibited. CH assists in exchanging data amid BS and SN [5].

Clustering can be categorized as homogeneous as well as heterogeneous. The SNs in homogeneous WSNs have equal energy, memory space, handling ability, etc. On the other hand, SNs in heterogeneous WSNs are different in one or additional characteristics like initial energy, memory space, handling ability, etc. [6].

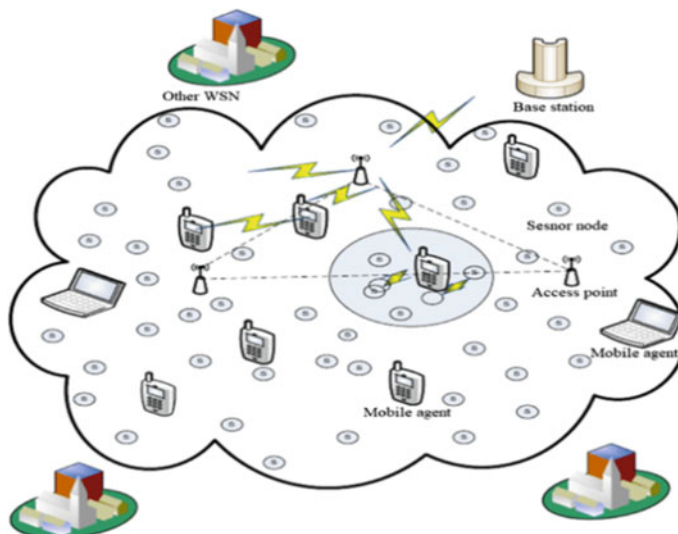


Fig. 1 A wireless sensor network

This paper proposes and analyzes the homogenous and two-tier heterogeneous network model as per the ADV-LEACH1 [7]. In this paper, we implement and analyze the clustering algorithm of ADV-LEACH1 [7]. This algorithm is a threshold-based cluster algorithm and is implemented on the heterogeneous wireless sensor networks (HWSNs). We propose the same clustering algorithm on homogenous wireless networks and analyze the model performance. Then, we evaluate the network performance as per ADV-LEACH1 for our proposed model by considering the homogeneous network model. Therefore, the homogenous ADV-LEACH1 (HOM-ADV-LEACH1) assumes all SNs in this model having the same amount of energy. As per ADV-LEACH1 [7], the protocol is present with two-tier heterogeneous WSNs.

The rest of the work is structured as follows. Section 1 presents the layout and basic information about WSNs. In Sect. 2, literature of clustering algorithm is mentioned. Section 3 gives the clustering algorithm parameter for heterogeneous and homogeneous WSNs model. Section 4 discusses the WSN model and radio energy dissipation model. The experimental results of the proposed layout are given in Sect. 5 and finally, conclusion in Sect. 6.

2 Literature Review

In general, the power supply of SNs in WSNs is provided by a battery that is not rechargeable or replaceable. Improving energy efficiency and optimizing the lifetime of WSNs are key challenges. In recent years, various protocols have been deliberately centered explicitly on energy use to prolong the network's existence. In this context, the low-energy adaptive clustering hierarchy (LEACH) approach reduces energy consumption to extend network lifetime [8]. It chooses few SNs as CH is dynamically determined based on the remaining energy by every round in the WSN. The CHs fetch data from the SNs within the clusters, collect it, and then forward the collected information to the BS LEACH-C [9], and enhancement through the LEACH protocol is managed by spreading CHs across the network to achieve better output. Stable election protocol (SEP) [10], an extension of LEACH, having bi-level heterogeneity in the heterogeneous WSNs provides a longer constant region due to efficient SNs generating extra energy; heterogeneity cannot be prolonged to multilevel heterogeneous WSNs. Distributed energy-efficient cluster (DEEC) [11] approach considers two-level and multilevel heterogeneity of energy.

HEED's primary objectives are to enhance the network's lifetime by absorbing energy supplies and the clustering run within the number of rounds [12, 13]. It minimizes overhead control and creates well-distributed CHs and compact clusters. HEED regularly selects CHs as a primary parameter, allowing two clustering constraints to be combined, namely the remaining energy of every SN and the cost of intracluster interaction as a method of adjacent closeness or cluster density as a secondary parameter. The initial parameter is utilized to elect the CH in a probabilistic manner. HEED shows the best load balancing in the network. HEED

clustering technique extends the network lifetime as compared to the LEACH approach. LEACH algorithms choose CHs randomly, which may reduce the network performance and make some nodes die more easily. In HEED, the final CHs chosen are well spread across the network, and connectivity costs are minimized. Another energy-efficient clustering approach [14] suggests the existence of a WSN extended by dividing the network into clusters. To reduce the cluster's size, the CHs are selected in every round based on the cluster's number of SNs.

3 Network Model

We consider two different types of the sensor networks, i.e., heterogeneous and homogeneous network (in Fig. 2) having N SNs, which are randomly distributed over the monitoring area. A radio energy model is used for energy dissipation. There are some assumptions that are considered about the network and its SNs:

- (1) The SNs are inside the communication range. The SNs communicate with each other. CH node directly communicates with the BS.
- (2) All nodes have heterogeneous and homogeneous sensing, communication capabilities, and cost computing.
- (3) SNs are randomly distributed in the monitoring area.
- (4) BS is positioned in the inside and outside of the area, and BS has a source with infinite energy.
- (5) All SNs in the homogeneous network have equal initial energy, and heterogeneous networks have different initial energy for both types of nodes as advanced node has higher energy than the intermediate node.

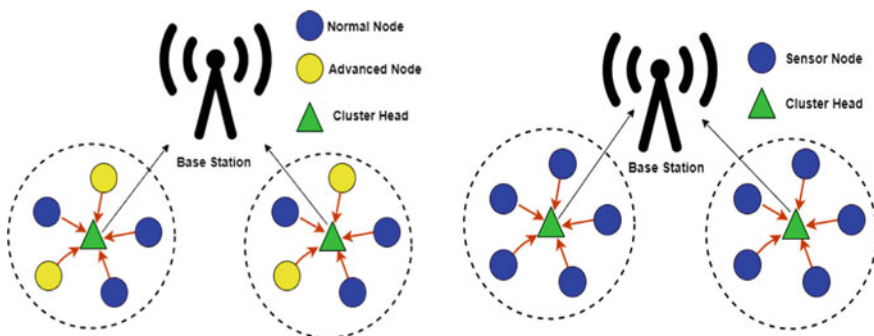


Fig. 2 Heterogeneous and homogeneous wireless sensor network

3.1 Energy Consumption Model

To dissipate communication energy, simplified model is used as presented in [9]. According to the distance among the sender and receiver, as shown in Fig. 3, free space (d^2) and the multipath fading (d^4) power loss channel systems are utilized. The 1-bit packet is used for the transmission over distance d . The energy model is:

$$E_{TX}(k, d) = E_{Tx-elec}(k) + E_{Tx-amp}(k, d) \\ = \begin{cases} E_{elec} * k + \epsilon_f * k * d^2, & d < d_o \\ E_{elec} * k + \epsilon_m * k * d^4, & d > d_o \end{cases} \quad (1)$$

$$E_{Rx}(k) = E_{elec} * k \quad (2)$$

where $d_o = \sqrt{\frac{\epsilon_f}{\epsilon_m}}$, E_{elec} denotes the energy depletion of radio dissipation, ϵ_f and ϵ_m denote the energy depletion for amplifying radio, which is used depending upon the communication distance.

The sensory information is believed to be highly correlated. In contrast, the degree of correlation of sensory data from various clusters is comparatively low. The CH can still aggregate the information collected from its cluster members (CM) into a only fixed-length packet, and the energy is absorbed as E_{DA} by the process of data aggregation.

4 Proposed Clustering Method

In our proposed model, four stages consist of cluster-based routing protocols: CH election, cluster creation, aggregation of data, and data communication. As shown in Fig. 4, the setup state begins with selecting the CH and continues with the

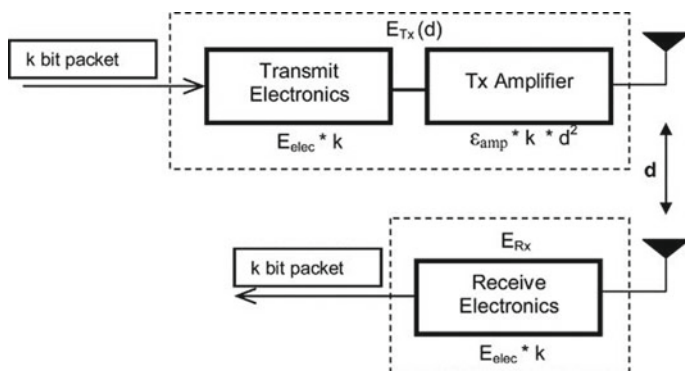


Fig. 3 Radio dissipation energy model

creation of clusters. The state of setup is monitored by the steady-state data communication that is partitioned into phases of data aggregation and transmission. Every round of running a cluster approach, which iterates over running the protocol or the network lifetime, forms the setup and steady data communication. SNs in clustering approach can be clustered into four categories, depending on the role:

Cluster head (CH): The key duties of a CH are the organization of a community of SNs located within the transmission range, the aggregation of sensed information by the cluster members (CM), and the transfer of aggregated information to the next hop.

Base station (BS): Because of the high computing capabilities and the infinite energy source, BS can be the network coordinator and the BS where entirely the aggregated information is processed based on the type of application and the end user's demands.

General node (GN): The common of network nodes that provide sensed data only based on the type of use.

The LEACH [9] is the first and the most common self-organizing clustering protocol for WSNs. Every node chooses whether to be a CH or not for the setup process in LEACH. CH's choice is based on a node decision with the choice of arbitrary numbers among 0 and 1. If the value is not greater than the default $T(n)$ threshold, then the SNs for the current round is considered to be CH. We may define $T(n)$ as the threshold as:

$$T(n) = \begin{cases} \frac{P_{CH}}{1 - P_{CH} * \left(r_c \bmod \left(\frac{1}{P_{CH}} \right) \right)}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Here, r_c is a random number lies among 0 and 1; probability P_{CH} . The proportion of SNs is selected as a CH while data transmission whereas G is the SNs group that was not CHs in current rounds.

The proposed algorithm is improved by the remaining energy stored in the SNs and distance (d) between the CH and SNs. The SNs are having high energy for advance SN and low energy for normal SNs. The remaining energy is considered along with the distance of the SNs for the election of the new CH. SNs are divided into normal and advanced SNs for the heterogeneous network [7, 10, 15]; α is a component that implies a higher energy as compared to normal SNs; m denotes the

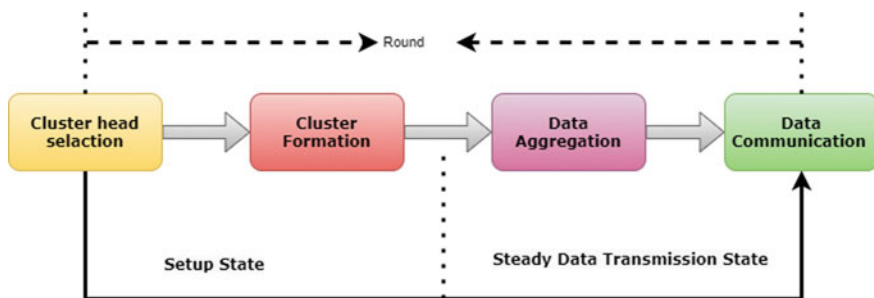


Fig. 4 Categories clustering algorithm model

ratio of advanced SNs. P_{ad} and P_{erm} stand for the probability of advanced as well as normal SNs nominated to be CH, respectively, in Eqs. (4 and 5).

$$P_{nrm} = \frac{P}{1 + \alpha * m} \quad (4)$$

$$P_{adv} = \frac{P * (1 + \alpha)}{1 + \alpha * m} \quad (5)$$

The combination of current energy ($E_{current}$) and initial energy factor ($E_{initial}$), as well as the distance of the current SN ($D_{current}$), is used to design a new probability formulation. The (D_{max}) is the highest value of SNs to BS distance that is utilized to design an enhanced formulation of $T(n)$ for CH election. The main purpose to design a new formulation is to decrease the CH SNs energy consumption. Equations (6)–(8) are taking to deploy the SNs of WSNs. The new formulation of $T(n)$ for normal and advanced nodes by [7].

For normal SNs (heterogeneous WSN) [7]:

$$T(n)_{nrm} = \begin{cases} \frac{P_{bnrm} * (u(\frac{E_{current}}{E_{start}}) + v(\frac{d_{current}}{d_{max}}))}{1 - P_{nrm} * (\text{rmod}(\frac{1}{P_{nrm}}))}, & n \in G \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

For advanced SNs (heterogeneous WSN) [7]

$$T(n)_{adv} = \begin{cases} \frac{P_{badv} * (u(\frac{E_{current}}{E_{start}}) + v(\frac{d_{current}}{d_{max}}))}{1 - P_{adv} * (\text{rmod}(\frac{1}{P_{adv}}))}, & n \in G \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

According to Eqs. (6), (7), $P_{bnrm} = b * P_{nrm}$, $P_{badv} = a * P_{adv}$ is the weight of P_{nrm} , P_{adv} , respectively. The value of b is a proportional constraint according to network size. u , v is the ratio coefficient, and having the value between 0 and 1 and $u + v = 1$.

For general SNs (homogeneous WSN):

$$T(n)_{GN} = \begin{cases} \frac{P_{CH} * (u(\frac{E_{current}}{E_{start}}) + v(\frac{d_{current}}{d_{max}}))}{1 - P_{CH} * (\text{rmod}(\frac{1}{P_{CH}}))}, & n \in G \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

5 Result and Simulation

The network terminology with their value is mentioned in Table 1. In the network 20% of advance and 80% of normal sensor node of the total nodes. The BS is located at (50, 50) and (50, 150). The initial parameters are mentioned in Table 1.

Both the algorithms are implemented using MATLAB (R2017b) on the Windows 10 platform. The line plot is also designed on MATLAB with the respective color code. The outcome shows that ADV-LEACH1 (HETRO) performs better based on these alive/dead node analysis metrics, throughput, network life time, residual energy, and optimized CH selection of network. ADV-LEACH1 (HETRO) further improves efficiency; however, ADV-LEACH1 (HETRO) performs best as compared to the ADV-LEACH1 (HOMO).

Figure 5 shows that after only 1600 rounds, the average energy of the ADV-LEACH1 (HOMO) approach comes to 0, wherein ADV-LEACH1 (HETRO) continues till ~ 2000 rounds. This becomes possible since energy has been saved for those SNs with higher energy in ADV-LEACH1 (HETRO); that node can choose CH for a few more. ADV-LEACH1 (HOMO) did not have any higher energy nodes; all nodes have equal energy, so as SNs get selected as CHs for a few rounds, then their energy gets depleted faster, and a SN becomes a dead node. As per Fig. 5 ADV-LEACH1 works better in the heterogeneous sensor network. ADV-LEACH1 (HETRO) works better than the ADV-LEACH1 (HOMO).

The proposed method for alive nodes up to 2000 rounds is shown in both Fig. 6. We notice that the number of alive nodes in ADV-LEACH1 (HOMO) drops significantly around 1600th round and continues to decrease as compared to other ADV-LEACH1 (HETRO) approaches. In contrast, the number of alive nodes in ADV-LEACH1 (HETRO) is much higher than ADV-LEACH1 (HOMO).

Figure 6 (left) compares the number of dead nodes in every round when both the ADV-LEACH1 (HETRO) and ADV-LEACH1 (HETRO) approaches are run on the network with similar parameters. The results demonstrate that the SN could not remain alive after 2000 rounds in the case of ADV-LEACH1 (HOMO). However, the last node died after 2000 rounds in ADV-LEACH1 (HOMO), but ADV-LEACH1 (HETRO) approach still has them alive nodes after 2500 round. The ADV-LEACH1 (HETRO) approach has better results in the dead/alive node analysis than the ADV-LEACH1 (HOMO) approach.

In addition to network lifetime, its performance is another metric to determine an approach's effectiveness. The efficiency of the proposed solution is verified by a CH having more data packets. In a sense, but not always, throughput relies on network life. Figure 7 clearly demonstrates the throughput of ADV-LEACH1 (HETRO) that

Table 1 Initial parameter

Parameters	Value
No. of round [®]	2500
P	0.2
E_{TX} or E_{RX}	50 nj/bit
ϵ_f	10 pj/bit/m ²
E_{elec}	5 nj/bit/message
ϵ_m	0.0013 pj/bit/4
No. of sensor (N)	200
Packet size	4000 bits

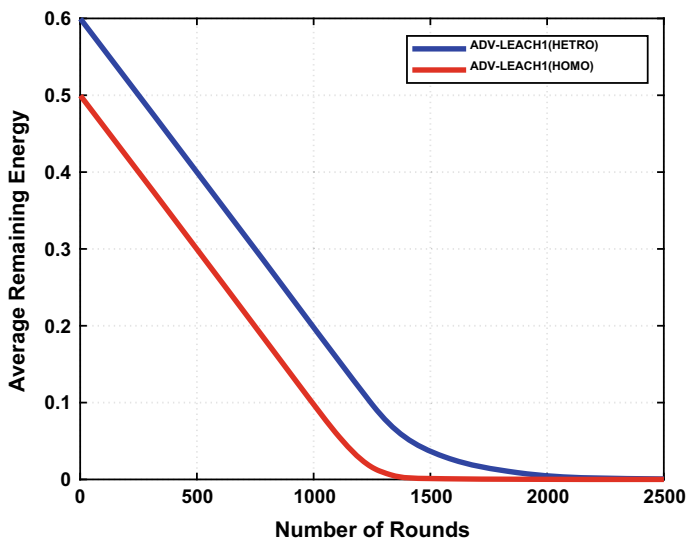


Fig. 5 Comparative analysis of average remaining energy for homogeneous and heterogeneous sensor network versus the number of nodes

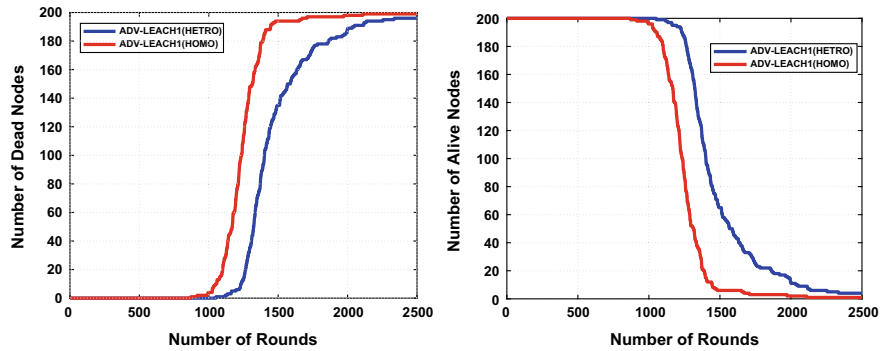


Fig. 6 Comparative analysis of number of dead (left) and alive nodes (right) for homogeneous and heterogeneous sensor network versus number of nodes

is quite similar to the approach of ADV-LEACH1 (HOMO). The performance increase is caused by limiting the amount of data transmission obtained on the CH side. In ADV-LEACH1 (HETRO), the number of packets received at CH is equivalent to 500 nodes.

The energy efficiency of WSNs is significantly influenced by a selection of CHs. Thus, these CHs are going to die sooner. Thus, the stability of the CH numbers around an optimum number is needed in successive rounds to obtain balanced energy consumption. The number of CHs in each round as opposed to

ADV-LEACH1 (HETRO) and ADV-LEACH1 (HOMO) is shown in Fig. 7 (right). The experiments show that in both cases, the optimal amount of CH is mismatched. In this case, better performance than others cannot be explained by the approach. This enhancement is based on the modified CH selection approach that also increases the number of rounds.

Considering network lifetime of ADV-LEACH1 (HETRO) and ADV-LEACH1 (HOMO) performance concerning differently positioned of the BS network lifetime is used in three metrics, the first node dead (FND), half nodes died (HND), and the last node dead (LND). As shown in Fig. 8, ADV-LEACH1 (HETRO) outperforms ADV-LEACH1 (HOMO) in the FND metrics, and it has stable performance based on number of rounds with changing the position of the base station (BS).

Figure 8 demonstrates the distribution of the dead nodes versus number of rounds for every approach. The number of dead nodes in ADV-LEACH1 (HETRO) changes over round more slowly overall than ADV-LEACH1 (HOMO). The comparative analysis between the ADV-LEACH1 (HETRO) and ADV-LEACH1

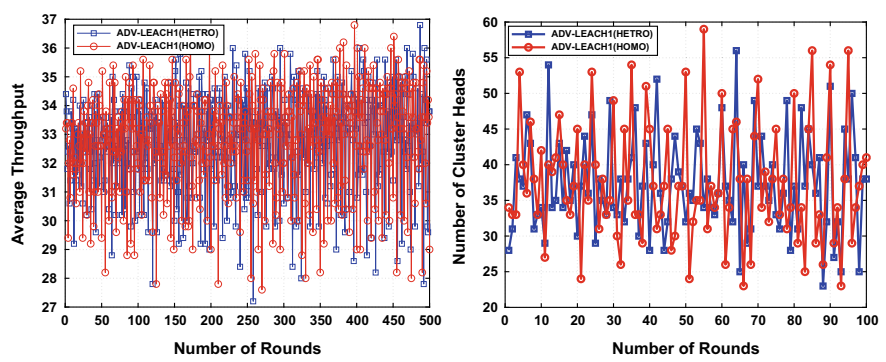


Fig. 7 Comparative analysis of average throughput (left) and the number of cluster heads (right) for homogeneous and heterogeneous sensor networks versus the number of nodes

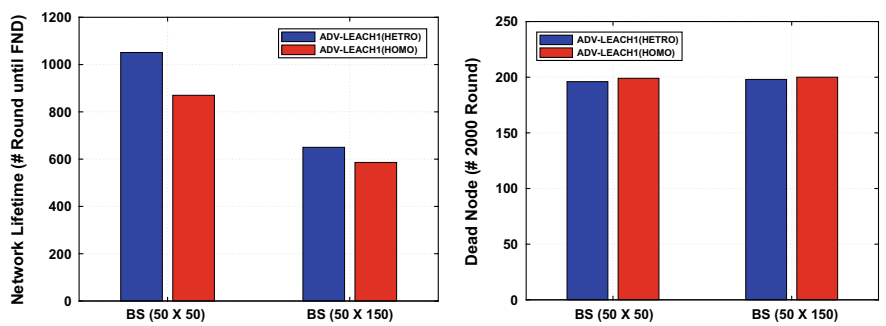


Fig. 8 Comparative analysis of network lifetime (left) and dead node (right) for homogeneous and heterogeneous sensor network based on the base station (BS) position

Table 2 Comparative analysis

Algorithms	BS Position (50 × 50)		BS Position (50 × 150)	
	Network LifeTime (#FND)	Dead node (# 2500 rounds)	Network LifeTime (#FND)	Dead node (# 2500 rounds)
ADV-LEACH1 (HETRO)	1051	196	650	198
ADV-LEACH1 (HOMO)	870	199	586	200

(HOMO) based on the network lifetime and dead nodes till 2000 nodes, as mentioned in Table 2.

6 Conclusion

In this paper, we have analyzed the ADV-LEACH1 for the heterogeneous and homogeneous networks based on the analysis of the latest clustering algorithm ADV-LEACH1 with two different types of network and different base station positions (BS). The SNs are randomly deployed in the square area and base station in the center of the area. Also, a solution is proposed in the form of ADV-LEACH1 (HETRO) and ADV-LEACH1 (HOMO) approaches that uses the modified threshold probability of clustering for the CH selection. The performance is evaluated based on the various performance parameters. The simulation results show that ADV-LEACH1 (HETRO) performed better in terms of residual energy and network life time compared to ADV-LEACH1 (HOMO).

References

1. Ngangbam, R., Hossain, A., Shukla, A.: Lifetime improvement for hierarchical routing with distance and energy based threshold. In: International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 77–83. Springer, Cham (2019)
2. Sara, G.S., Sridharan, D.: Routing in mobile wireless sensor network: a survey. Telecommun. Syst. **57**(1), 51–79 (2014)
3. Hussain, N., Rani, P.: Comparative studied based on attack resilient and efficient protocol with intrusion detection system based on deep neural network for vehicular system security. In: Distributed Artificial Intelligence, pp. 217–236. CRC Press (2020)
4. Jawandhiya, P.M., Ghonge, M.M., Ali, M.S., Deshpande, J.S.: A survey of mobile ad hoc network attacks. Int. J. Eng. Sci. Technol. **2**(9), 4063–4071 (2010)
5. Jan, B., Farman, H., Javed, H., Montrucchio, B., Khan, M., Ali, S.: Energy efficient hierarchical clustering approaches in wireless sensor networks: a survey. Wirel. Commun. Mob. Comput. (2017)

6. Singh, S.: Energy efficient multilevel network model for heterogeneous WSNs. *Eng. Sci. Technol. Int. J.* **20**(1), 105–115 (2017)
7. Kumar, N., Kumar, V., Ali, T., et al.: Prolong network lifetime in the wireless sensor networks: an improved approach. *Arab. J. Sci. Eng.* (2021). <https://doi.org/10.1007/s13369-020-05254-3>
8. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: *Proceedings of the 33rd annual Hawaii international conference on system sciences*, p. 10. IEEE (2000)
9. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **1**(4), 660–670 (2002)
10. Smaragdakis, G., Matta, I., Bestavros, A. SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. Boston University Computer Science Department (2004)
11. Qing, L., Zhu, Q., Wang, M.: Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. *Comput. Commun.* **29**(12), 2230–2237 (2006)
12. Younis, O., Fahmy, S.: Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach. In: *IEEE INFOCOM 2004*, vol. 1. IEEE (2004)
13. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Trans. Mob. Comput.* **3**(4), 366–379 (2004)
14. Singh, M.P., Gore, M.M.: A new energy-efficient clustering protocol for wireless sensor networks. In: *2005 International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 25–30. IEEE (2005)
15. Chen, X., Wang, Z., Wu, J.: The improved wireless sensor network routing algorithm based on LEACH. *Chin. J. Sens. Actuators* **1** (2013)

Cognition of Driver Drowsiness to Inculcate Predictive Analysis



Abra Shafiq Siddiqi, Md. Afshar Alam, Sherin Zafar, Samia Khan, and Nida Iftekhar

Abstract Life being the most valuable assets is lost myriads of time due to dreadful vehicular accidents. However, a real-time drowsiness detector used on a car can significantly obviate these accidents and save valuable lives worldwide. The main reason being inattention of driver mainly referred to as driver's drowsiness. The driver drowsiness monitoring system works with a high frequency detection system using an incoming video stream of a driver focusing on the natural visual changes in driver such as the steady closure of eyes and slow changing facial expression using artificial intelligence and scientific drowsiness detection measure. The proposed work focuses on the various monitoring systems used in the drowsiness detection as well as the process of the detection system. The driver drowsiness detector attached to crucial predictive analysis system is proposed to be utilized. This research paper focuses on the analysis of various drowsiness system so that better predictive analysis could be done. Machine learning is a very important paradigm for predictive analysis, so this paper focuses on the various machine learning techniques and their efficiency for detection of drowsiness in various systems.

Keywords Drowsiness detection • Driver drowsiness detector • Facial expression • Predictive analysis • Machine learning algorithms

1 Introduction

AI The available statistical data prescribes over 20% people die and 76,000 people suffering fatal injuries caused by road accidents [1]. The statistics further emphasize that majority of road accidents are caused by driver drowsiness. Driver when falls asleep during a journey ultimately there exists a loss of control over the driving vehicle that majority times causes a serious crash either with another running

A. S. Siddiqi · Md. A. Alam · S. Zafar · S. Khan · N. Iftekhar (✉)
Jamia Hamdard, New Delhi, India
e-mail: nida.iftekhara@jamiyahamdard.ac.in

vehicle or any standing objects. The term “drowsy” literally means an inclination to fall asleep. Drowsiness is synonymous to sleepy. Further the stages of sleep can be divided as awake (not sleepy), non-rapid eye movement sleep (NREM), and rapid eye movement sleep (REM). NREM can be further subdivided into the following given three stages below [2].

Stage I: change from awake to asleep (drowsy)

Stage II: light sleep

Stages III: deep sleep

In order to determine driver drowsiness, researchers mainly have evaluated Stage I (change from awake to asleep) that is the drowsiness stage. Various crashes mainly occurring due to drowsiness of driver have varied characteristics features [3].

- Occurs mainly at late night
- Driver is frequently alone
- Involving an individual vehicle running off the road
- Mainly occurs mainly on high-speed roadways
- Driver usually a young male
- Blood alcohol level that are actually below the legal driving limit
- Absolutely zero skid figures or braking signal in relation to these features.

However, the police databases use the following given indices to determine accidents caused due to drowsiness [4].

- if vehicle has any mechanical failure or defect
- no brakes applied
- weather conditions and clear visibility
- lack of sleep
- if vehicle ran off the appropriate road or onto the back of another moving or standing vehicle
- excluding “driving too close to the vehicle in front” and “speeding” as potential causes

The statistical data obtained using these methods cannot usually ascertain fully for road accidents that are caused by drowsiness in drivers because of the various number of complexities involved. Thus, the accidents recognized due to driver drowsiness could be more ugly, devastating, and fatal than these statistics data reveal. Hence, to obviate accidents, it becomes out most significant to effectively measures and detect driver drowsiness such that the drivers are left alert. The later parts of the research paper focus on the drowsiness detection process and the advancements in the field of the driver drowsiness detection systems and the future advancement scopes in this field.

In the research paper, further Sect. 2 defines literature review. Section 2 talks about the gaps in literature. Further, Sects. 3, 4, 5 discuss methodology, objective of study, the process of driver drowsiness detection, and conclusion, respectively.

The research paper lastly discusses the conclusion under Sect. 6. References and the resources utilized during the research paper construction are enlisted under title references.

2 Literature Review and Gaps

This literature reviewed the head movement-based change for detection of driver drowsiness [5]. The research paper emphasizes on general measures and methods utilized to determine the drowsiness in drivers and also provides a well distinguished analysis of different systems detection drowsiness utilized throughout the globe. In addition to this, a well distinguished system for determining the drowsiness fatigue caused in drivers is signified [6]. The research paper also focused on the works that used varied methods to obviate catastrophic road havocs and accidents caused by drowsiness [7]. However, a great number of literature have been gathered around the detection of drowsiness systems, this field actually draws an immense advancement, and this time demands great need for a review literature for machine learning techniques and approaches which can be applied to drowsiness detection. This research paper now basically attempts to address and evaluate various cardinal needs by ascertaining behavioral techniques specifically focusing on the machine learning technologies for distinguishing the various drowsiness stages.

The research paper has extensively undergone the evaluation and consultation of various works done on the drowsiness detection systems which are accepted worldwide and are turning into cardinal norms in detection and measuring of drowsiness in vehicles to obviate the fatal accidents and save precious lives. Various works and methodologies have been adopted to present and increase the efficiency of detection systems which are broadly discussed in the research paper. However, there also exists certain areas which definitely need to filled and worked upon further to overcome the gaps and improve the efficiency of the detection system which are roughly presented below:

- While using the subjective measures for detection, drowsiness levels are frequently measured every 5 min approximately. However, rapid changes cannot be determined or measured using these subjective measures
- An additional gap identified using various subjective ratings suggests that the self-introspection majorly alerts the driver, therefore dropping their levels of drowsiness. In addition to this, it is also very hard to evaluate feedbacks related to drowsiness from a driver in a real driving situation. Since, subjective ratings are very useful in detecting drowsiness in a replicated environment; therefore, the remaining measures and indices may be better obtained for the drowsiness detection in a real environment
- The vehicle-based method used can reliably function only at specific surrounding which are also dependent on varied geometric individuality as well as

the matrices of road but to lesser extent on the dynamic features of the vehicle which needs to be amended such that more focus is on the characteristic features of the vehicle

- Another limitation identified by this study is a vision-based approach that uses lighting since usual cameras cannot perform efficiently during night hours. Researches should use active and efficient illumination methods such as a light emitting diode (LED) of infrared nature. However, LEDs work fairly significant during night hours but less significant during day time.

Therefore, it is very essential to use a high frequency hybrid technology to overcome the above-mentioned gaps and increase the efficiency of the detection system through the predictive analysis techniques.

3 Objective of Study

Analysis the research paper mainly focuses on the driver drowsiness detection and identification of its various technologies used. Driver drowsiness detection system being a safety technology which helps saving the life of driver by obviating accidents, while the driver is drowsy. The main objective of the research paper is initially designing a system to detect the drowsiness by:

- continuously examining the eye retina
- The proposed system works despite the fact driver wears spectacles and also considers various lighting conditions
- Alerting the driver of drowsiness utilizing an buzzer or alarm system through analytics
- Reducing the speed of the vehicle after predictive analysis
- It can efficiently reduce accidents by maintaining the traffic management
- Fetching authenticated data of driver drowsiness and performing predictive analysis for getting best possible results through artificial intelligence/machine learning/ deep learning algorithms.

4 Methodology

The behavioral measurement techniques accurately monitor the levels of drowsiness by using high definition mounted cameras fixed in a car such that the change in facial expressions including yawning, eye state, blinking rate, slow eye closure, head movement, etc. The scientific approaches mostly practice specific procedure to process driver features of face recorded from the provided camera as depicted in Fig. 1. After gathering the above-mentioned features, the further work is counted in order to monitor drowsiness levels. This is specifically obtained by using

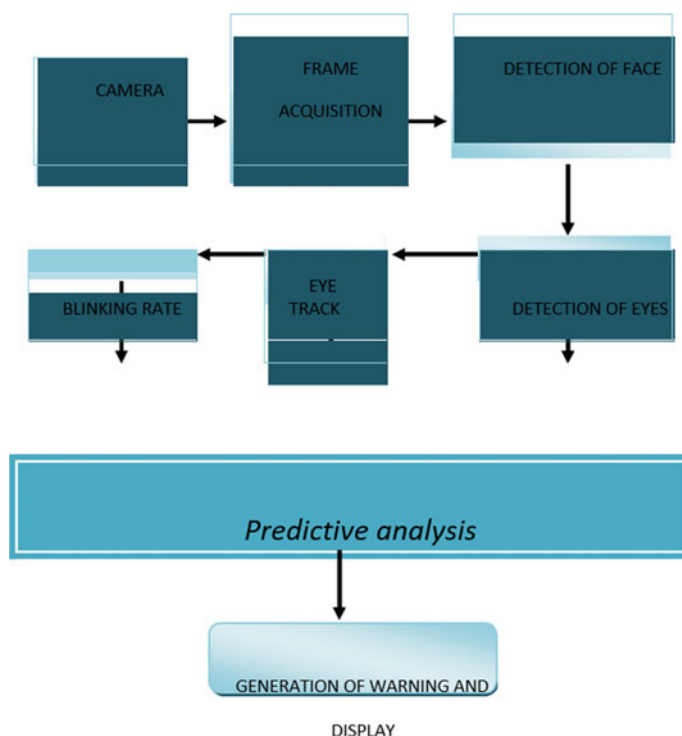


Fig. 1 Drowsiness detection process

technologies of machine learning which frequently include convolutional neural networks or hidden Markov models support vector machines (SVM) [8]. These procedures, however, are applied by specific characteristics as well as labeled data matrices in order to construct systems detecting drowsiness and obviate fatal hazards. However, the most challenging part in detection process is to find huge dataset that contains featured variations throughout different course of race as well as skin pigments. This being a significant concern because of myriad of security as well as discretionary issues that can surely arise during the whole process of publishing these datasets for academic as well as commercial purpose [9].

The following expressions mentioned below are marked from the facial features which are specifically gained from a face of driver:

1. *Changing facial expression analysis*: Here the technique combines more than one facial expression such that the driver drowsiness detected. This encompasses expressions such as wrinkles found specially on the forehead also the head poses that are sometimes extreme [10].
2. *Rate of eye blink*: This technique detects the rate of blinking by considering the frequency with which the eye-blinks such that the drowsiness is measured. Since

the normal blinking rate of a human eye is roughly 10 per [5], the drowsiness is detected if the blinking rate falls the given number.

3. *Eye closure analysis*: This being an important expression is frequently and specifically used to measure the drowsiness level in the driver. This includes techniques such as percentage of the eye closure (PERCLOS) [11] as well as eye aspect ratio (EAR). EAR is identified as the ratio of height and width of the eye. This technique was founded by Soukupova and Cech [12]. On the contrary, PERCLOS is calculated as the percentage eye closure over a certain period of time. However, the primary difference between PERCLOS and EAR is that the later distinguishes between the eye ratio, which descends while the former detects if the eye is open widely enough or the eye is closed.
4. *Analyzing Yawning*: Yawning is usually observed during tiredness or boredom. Its presence mainly in drivers defines the predication of their falling asleep during the journey. Methods used can measure the mouth widening. This can be traced using yawning features in the driver on observing shape of the mouth as well as lip corners position [13].

In order to obviate these catastrophic accidents, it becomes significantly cardinal to measure the drowsiness state of drivers. For this reason, various driver drowsiness monitoring methods are widely used some of them enlisted below:

- (a) *Physiological measures*—This defines relationship between physiological signals such as electromyogram (EMG), electroencephalogram (EEG) [2], electrocardiogram (ECG), and electrooculogram (EoG) with driver [5]. These measurements yield a highly efficient and accurate measurement data but are not globally prevalent mainly due to certain practical downfalls.
- (b) *Vehicle-based measures*—This includes various metrics such as pressure on the acceleration pedal, braking patterns, movement of the steering wheel, deviations from lane position, etc., which are constantly evaluated including any changes in these metrics that crosses a particular threshold. Thus, indicating an essential increased probability of driver drowsiness [14]. Among all the methods in vehicle-based measures, steering wheel yields the most accurate results. However, vehicle-based methodology being non-invasive, this may in the long run not be a reliable and efficient determining technique mainly as they are solely reliant on the road nature as well as driving skills of drivers.
- (c) *Behavioral or computer vision measures*—this method is much steadfast than the vehicle-based method as it focus mainly on the person itself than the monitoring system based on vehicle. This focuses on driver's natural responses gathering information using cameras for detecting minute change in facial features of the drivers which includes yawning of the person, closure of eye, blinking of eye, change in head pose, etc., is monitored through a camera, and the driver is alerted if any of these drowsiness symptoms are detected [15]. This method being non-invasive is gaining immense popularity in drowsiness detection determination. The rate of positive detection reduced to a significant amount when the experimental work when conducted in actual atmosphere.

Table 1 enlists the work of various authors referred during this work who had used behavioral measures for driver drowsiness detection.

There exist numerous procedures and techniques for detection of face as well as to draw and determine features collected from the video data. However, majority of these works conducted approach various databases which could follow the individual algorithms. This exists mainly because of insufficiently systematic datasets which could be mainly applied as a point of references in the study. Thus, it is

Table 1 Previous works list on driver drowsiness detection using behavioral measures

Sensor used	Drowsiness measure	Detection techniques	Feature extraction	Classification	Positive detection rate (%)
CCD camera	Yawning	Grey projection and gravity-center template	Gabor wavelets	LDA	91.97
Simple camera	Eye blinking	Algorithm diamond searching for tracing the face and cascaded classifiers algorithm to detects face	Frequency of continuous blinks, frequency of eye blink, duration of eyelid closure	Region mark algorithm	98
CCD micro camera with infrared illuminator	Pupil	AdaBoost	Red eye effect, detection method for texture	Eye-height, eye-width ratio	92
Camera	Multi-scale dynamic featuring	Gabor filter	LBP	AdaBoost	98.33
Digital video camera	Facial action	Gabor filter	Decomposing wavelet	SVM	96
IR camera	Eye state	Gabor filter	Condensation algorithm	SVM	93
Fire wire camera and webcam	Eye closure frequency and duration of eye closure	Hough transform	Transforming discrete wavelet	Neural classifier	95
IR Illuminator attached to camera	PERCLOS	Detecting face by Haar algorithm	Kalman filter algorithm unscented	SVM	99

difficult to distinguish methods by merely determining the reported data efficiencies. The techniques of machine learning studies are mainly used to determine the different stages of drowsiness that are now listed along with their discussions below. Also, including the analysis of various measures and methods that sufficiently form a drowsiness detection system for drivers.

(a) *Hidden Markov Model (HMM)*

This is basically a statistical data models and methods applied to predict and determine about the hidden states based on the actual perceived states which are defined by the probability methods. HMMs were extracted during late 1960s period and early 1970s period [1]. In this era, these methods have a global application in various technologies such as modeling sequence errors, DNA gene annotation, and face expression recognition. Table 2 shows the varied range of features as well as perspectives which are used by hidden Markov model-based driver drowsiness detectors. However, [10, 16] have excluded some of the cardinal information perspective for the formation of the differentiation which are not actually used for the meta-analysis step formation. The authors have beautifully enumerated various fresh facial characteristics using changing wrinkles that are differentiated by calculating the edge potencies from the driver's facial features by using a camera of infrared nature to exclude the variations in illumination such that it permits the proper functioning both in day and night conditions. Howbeit, the deeper and strong wrinkles formed on faces of the older people may provide the false results generated by this system. In contrast, the HMM techniques implied for the eye tracking movements which are based on the varied geometrical features and color of eyes. For eliminating the illumination, authors have used a 2-stage Lloyd-max quantization method which is calculated to be sufficient enough to eliminate changes in illumination. Unfortunately, the system suggested is drafted for the inside conditions which does not succeed to display the facial features when the driver is actually not forward facing. Table 2 enlists the HMM technique below used for driver drowsiness detection.

Table 2 Driver drowsiness detection based on HMM technique

Author list	Year	Metric	Classifiers	Frame per second (fps)	Accuracy %
Choi et al.	2016	State of eye and position of head	HMM	16–20	N/A ^a
Aboalayon et al.	2019	State of eye	HMM	N/A ^a	95.9
Deng et al.	2019	Blink of eye	SVM and HMM	61	90.99
LaRocco et al.	2020	Eye state	HMM	3	99.7
Tadesse et al.	2014	Closure of eye and other varied features	HMM and SVM	20	97
Muhammad et al.	2019	Blinking eye	HMM	25	95.7

^aDependent variable

(b) *Convolutional Neural Network (CNN)*

This technique is very similar to a neural network commonly used that is also compiled of the neurons which further consists of the learnable weights. CNNs use varied spatial convolutions layers that are convenient enough for drawing images used to display the strong spatial relations. The methods have shown success in certain areas of image recognition, classification, and video analysis [1]. First to describe CNNs for vision of computer, however, this was manifested in 2012 only, when fabulous results were found using in object recognition deep convolutional neural networks. Table 3 provides a brief CNN-based techniques used for the determination drowsiness in driver. Dwivedi et al. [17] provide an database algorithm for detection of drowsiness by using a demonstration of this learning. However, this stage witnessed algorithm by Jones, and for recognition of faces, Viola was used. The images were trimmed to the dimensions of (48 * 48 square) which were incorporated into the initial layer of the network that comprises basically of 20 filters. The overall network consists of 2-layer systems. CNN provided a data which preceded to one layer softmax for the purpose of classification. CNN system, however, could not contemplate the change in the head pose, thus, can result in a fail. Nevertheless, authors [14] have applied a featured 3D deep neural network for attaining more efficient results. In this system, the face feature followed by a combined filter predicts for correlation encompassed with a Kalman filter system to track face robustly. The regions of face are drawn out and passed directly to a 3D-CNN system further to a gradient boosting machine for classification in an optimum manner. The advantage added to this system is that it also works well with the change in head position.

(c) *Support Vector Machines (SVM)*

SVMs are specialized, supervised, and efficient learning techniques used as regression and classification system. The methods were initially utilized in [15]. These specialized methods focused to find a hyperplane to discontinue data of training into pre-defined classes. To analyze the varied states of the driver drowsiness obtained from the labeled data, SVMs are initially used. A significant

Table 3 Driver drowsiness detection using the CNN technique

Author	Year	Metric	Methods	Classifiers	Accuracy %
George and Routray	2016	Gaze of eye	Algorithm of Jones and Viola	CNN	98.32
Zhang et al.	2017	State of eye	PERCLOS, AdaBoost and LBF	CNN	95.18
Reddy et al.	2017	State of eye	Eye state and mouth	MTCNN and DDDN	91.6
Dwivedi et al.	2014	Visual features	Algorithm of Jones and Viola	Softmax layer CNN	78

Table 4 Detection of driver drowsiness using SVMS

Author	Year	Measure	Classifiers	Frame per second (fps)	Accuracy %
Pauly and Sankar	2015	State of eye	HOG and SVM	5	91.6
Manu	2016	Eye closure and Yawning	Binary SVM including linear kernel	15	94.58
ALAnizy et al.	2015	Closure of eye	Haar features with SVM	60	99.74
Ren et al.	2014	State of eye	SVM	25	98.4
Punitha et al.	2014	State of eye	SVM	15	93.5

work on SVM done to mark its capabilities for drowsiness detection. Innumerable measures and techniques have been put forward to determine a significant amount of drowsiness in driver's using SVMs. The contrast obtained in these techniques presented in Table 4 with their perspectives embraced are reported in the table [18] have submitted a total mechanized system with the capacity of driver drowsiness detection. The detection of face and extraction of eye measurements was calculated using Haar featured algorithm. In the work further, classification of SVM was demonstrated to signify open or closed eyes such that an alarm is activated. Similarly, the proposed approaches have provided a system to detect distractions caused by the driver drowsiness. Here also using Jones algorithm and Viola for face detection in addition to this also a color-based histograms including local binary pattern system (LBP), data was obtained for smooth tracking of face over the frames. This technique further attained a 100% accuracy for detection of face howbeit, and a potential downfall still exists in the approach that is the minute rate of mount attainable which possibly could end in insufficient and inappropriate expressions obtained from facial. Table 4 represents the list of authors who worked on driver drowsiness detection using SVMS technology including their measures and data.

(d) *META-ANALYSIS*

Even though a considerable amount of work has been amalgamated to gather the data, however, a notable room exists to make up more accurate and efficient drowsiness detection systems. The significant concern observed according to this system analysis is that varied datasets have been used to obtain the goals but are not actually contrasted. However, the datasets which are reviewed so that the bound orders are maintained within a guided surroundings which could easily conduct an authentic world scenario surveillance. For a reasonable differentiation, 25% of the data collected under this work has been mainly due to the use of meta-analysis [1]. These collections of papers formally use sorting accuracy and efficiency to aggregate the systems production. Approximated performance observed that more

accurate results were submitted by the CNNs that too when actually differentiated with HMMs and SVMs [19]. Skillings-Mack test actually non-parametric in nature was used that provided a 6.66 Chi-square estimate which was notable $p = 0.035709$ [20]. This stipulates an actual contrast between the procedures conducted in presentation. Further the tests were conducted acquiring exactness using Eye-Chimera, ZJU Eye blink Database ULg Multimodality Drowsiness Database (DROZY), and the NTHU-drowsy driver detection video dataset Yawn Detection Dataset (YawnDD).

However, all the literatures conducted showed significant majority classifiers used were SVMs than by HMMs and later followed by CNN. Therefore, it is also been observed that there is a significant increase in the use of CNN for driver drowsiness detection since 2012, including the growing increase in use of deep learning.

Further, the machine learning aspects like SVM, HMM, and CNN were also bought up into the consideration during this paper. However, it is significantly difficult to sum up these perspectives, due to their restricted number of datasets systematized that actually exist. Meta-analysis was executed in an attempt to obtain these results. This procedure enshrined CNNs performance which excelled other existing approaches, but it also observed a huge need for datasets with quality specification features for detection of drowsiness.

5 Conclusion and Future Scope

As described in the research paper, different technologies and methods do exist to detect and determine the driver drowsiness fatigue. The research paper tried to evaluate various evolving techniques such that the best possible approaches are designed to obviate fatality caused by drowsiness crashes. This research paper has reviewed and analyzed varied methodologies that are accessible to detect the state of driver drowsiness. However, no universally accepted definition for drowsiness exists but this research paper certainly enshrines various systems and ways in which drowsiness can be obtained in a simulated environment. The various methods used to detect drowsiness mainly consists of subjective, behavioral measures, and vehicle-based as well as physiological, which were also discussed in detail including their advantages and disadvantages. The accuracy and efficiency rate to detect drowsiness while using physiological measures is high being highly intrusive. Howbeit, these intrusive nature of physiological measures can be resolved utilizing contactless electrode placement. Thus, it would be worth developing hybrid system using vehicle-based measures as well as physiological measures such as ECG and behavioral measures such that an appropriate and efficient drowsiness detection system is developed. Also, it becomes very essential for maintaining and focusing on the driving environment to obtain optimal adequate results. Authors further purposed to find out dataset and apply better machine learning algorithms to get better results which are not considered in this research study and will be our

further work of implementation. Random forest and decision trees are the proposed algorithms that authors propose to an authenticated data set for building much accurate analytical models.

References

1. Deng, W., Wu, R.: Real-time driver-drowsiness detection system using facial features. *IEEE Access* **7**, 118727–118738 (2019). <https://doi.org/10.1109/ACCESS.2019.2936663>
2. LaRocco, J., Le, M.D., Paeng, D.G.: A systemic review of available low-cost eeg headsets used for drowsiness detection. *Front. Neuroinform.* **14**, 553352 (2020). <https://doi.org/10.3389/fninf.2020.553352>
3. Parkhi, O.M., Vedaldi, A., Zisserman, A.: Deep face recognition. *BMVC* **1**, 6 (2015)
4. Manu, N.: Facial features monitoring for real time drowsiness detection. In: *Proceedings of the 12th International Conference on Innovative and Information Technology*, IIT 2016, pp. 78–81 (2017)
5. Shakeel, M., Bajwa, N.A.: Detecting driver drowsiness in real time through deep learning based object detection. In: *Advances in Computational Intelligence*, pp. 283–296 (2019)
6. Nair, I.R., Ebrahimkuty, N., Priyanka, B., Sreeja, M., Gopu, D.: A survey on driver fatigue-drowsiness detection system. *Int. J. Eng. Comput. Sci.* **5**(11), 19237–19240 (2016)
7. Gill, Chisty: A Review : Driver Drowsiness Detection System, vol. 3, no. 4, pp. 243–252 (2015)
8. Reddy, B., Kim, Y., Yun, S., Seo, C., Jang, J.: Real-time driver drowsiness detection for embedded system using model compression of deep neural networks. *Comput. Vis. Pattern Recognit. Work.* (2017)
9. Han, W., Yang, Y., Bin Huang, G., Sourina, O., Klanner, F., Denk, C.: Driver drowsiness detection based on novel eye openness recognition method and unsupervised feature learning. In: *Proceedings of the IEEE International Conference on System Man, Cybernetics, SMC* 2015, pp. 1470–1475 (2016)
10. Choi, I.H., Jeong, C.H., Kim, Y.G.: Tracking a driver's face against extreme head poses and inference of drowsiness using a hidden Markov model. *Appl. Sci.* **6**(5) (2016)
11. Provisional Registrations or Sales of New Vehicles (2018) [online] Available: <http://www.oica.net/wp-content/uploads/>
12. Cech, J., Soukupova, T.: Real-time eye blink detection using facial landmarks. In: *21st Computer Vision Winter Working* (2016)
13. Bin Zainal, M.S., Khan, I., Abdullah, H.: Efficient drowsiness detection by facial features monitoring. *Res. J. Appl. Sci. Eng. Technol.* **7**(11), 2376–2380 (2014)
14. Huynh, P., Kim, Y.G.: Detection of Driver Drowsiness Using 3D Deep Neural Network and Semi-Supervised Gradient Boosting Machine, vol. 10116 (2017)
15. Ren, S., Cao, X., Wei, Y., Sun, J.: Face alignment at 3000 FPS via regressing local binary features. In: *Proceedings of the IEEE Conference on Computer Vision Pattern Recognition*, pp. 1685–1692 (2014)
16. Zhang, B., Wang, W., Cheng, B.: Driver eye state classification based on co-occurrence matrix of oriented gradients. *Adv. Mech. Eng.* **7**(2) (2015)
17. Dwivedi, K., Biswaranjan, K., Sethi, A.: “Drowsy driver detection using representation learning” *Souvenir* 2014. In: *IEEE International Advance Computer Conference IACC* 2014, pp. 995–999 (2014)
18. AL-Anizy, J., Nordin, M.J., Razooq, M.M.: Automatic driver drowsiness detection using Harr algorithm and support vector machine techniques. *Asian J. Appl. Sci.* (2015)
19. Nandy, G.T., Manna, N.: Real time eye detection and tracking method for driver assistance system. *Adv. Med. Electron.* (2015)

20. Ngxande, M., Tapamo, J., Burke, M.: Driver drowsiness detection using behavioral measures and machine learning techniques: a review of state-of-art techniques. In: 2017 Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech), Bloemfontein, pp. 156–161 (2017). <https://doi.org/10.1109/RoboMech.2017.8261140>

Correlation Between K-means Clustering and Topic Modeling Methods on Twitter Datasets



Poonam Vijay Tijare[✉] and Jhansi Rani Prathuri[✉]

Abstract Twitter is a popular platform for people to express their feelings on any subject or topic irrespective of place and time in the world. The view expressed by the Twitter community gives enormous information about them and the trend going on. To identify these trends and patterns, many data science techniques are used. However, using appropriate clustering technique always remains a challenge for researchers. The research concentrates on using hard clustering approaches like K-means and soft clustering approaches like Latent Dirichlet Allocation (LDA) and Latent Semantic Indexing (LSI). The proposed methodology uses K-means on numerical attributes, LDA, and LSI on textual attributes. The experiments are done using different Twitter datasets and tested on Sabarimala temple tweet dataset. The first time experimental study shows the promising correlation of the K-means cluster sentiments with topic sentiments. This helps in understanding the stance of the topics formed. The paper concludes by highlighting the relevance between the results of K-means clusters with the topics formed using LDA and LSI techniques.

Keywords LDA · LSI · Clustering · Sentiment · K-means · Twitter dataset

1 Introduction

Users around the world with diverse backgrounds express their opinion on any matter using various social media platforms. Social media platforms generate a lot of data. Diving into the world of huge data and drawing important inference out of that seems a most difficult task. This task is possible with the help of recent trends and techniques like clustering and classification.

P. V. Tijare (✉) · J. R. Prathuri

Department of Computer Science and Engineering (VTU RC), CMR Institute of Technology, Bengaluru, India

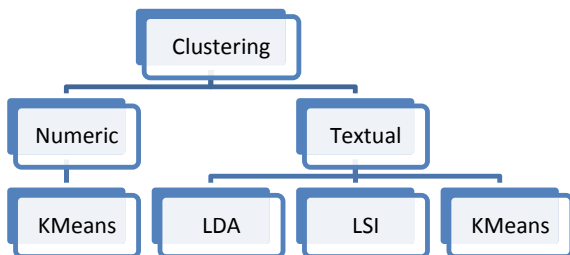
Twitter data analysis involves dealing with multiple Twitter data attributes including different formats like date, numeric fields such as latitude and longitude values, and textual data such as tweets. Though these attributes hold different data formats, nevertheless they are highly coherent and correlated in terms of analyzing subject dominance, a stance of the subject or its sentiments. For example, tweets holding the negative sentiment tweeted from the border region of India holds more sensitivity. Border region can be identified by latitude and longitude values.

As Twitter data have a broad spectrum of opinions and topics, finding their sentiments will help in understanding the emotions related to a particular subject. Tweets on behavioral analysis make the messages tweeted by user as one of the most important attributes compared to other attributes discussed above to perform such analysis and to draw out inferences. Sentiment analysis of the tweets is one of the important sources to capture the emotions or opinions of people who tweeted. Grouping the tweets based on sentiments will help to understand the sensitivity of that subject in public, and it can be further used for many applications [1].

This paper proposes a novel method to perform clustering analysis of Twitter datasets. The proposed method concludes the coupling between numerical attributes and textual attributes. Numerical attributes considered as sentiment score of the tweets and textual attribute as 'Tweet' which are tweets twitted by Twitter uses.

Numerical values are used to cluster the tweets based on their sentiment score. The textual attribute is processed further to identify important topics. The correlation between the above two factors is derived by calculating the common tweets in both approaches. This helps to analyze the important topics and sentiments associated with those topics. This work focuses on the application of the K-means algorithm to cluster the data on numerical fields and topic modeling algorithms such as LSI and LDA to find clusters based on textual data such as tweets. Figure 1 displays the clustering techniques applied based on the type of attributes [2].

Fig. 1 Choosing clustering technique based on type of data



2 Related Work

Clustering is an important task in data analysis. The approaches used for clustering depend on the data. In textual clustering, the methodology uses sentiments, rule-based methods, lexicons, etc. When the clustering is applied on short texts like Twitter, the traditional methodologies give unpredictable results. Singh et al. highlighted the textual similarity in words used by social media users. Strength matrix is created for each user based on words used. WorldNet, K-means, and spectral K-means are used. Authors found that spectral K-means gives good results on sparse data at the expense of computational cost [6]. Asif et al. used the lexicon dictionary with the word intensity weight created to detect multilingual sentiment and found that the repeated words in the lexicon reduce the accuracy [7]. Han et al. build the model with word embeddings to create lexicons to interpret personality [8].

The rule-based approach for sentiment analysis is also popular for short text analysis. Singh and Sachan present the system SentiVerb using rule-based classifiers. The dictionary on opinion is created. The novel concept of negative parameter threshold is introduced [9]. Vashishtha and Susan proposed the fuzzy rule-based approach for sentiment analysis. The nine rules are formulated to find the sentiment of each tweet. The approach is tested on online datasets using SentiWordNet, AFINN and VADER lexicons [10]. Researchers also presented work on the anomalies with textual analysis on social media along with sentiment diffusion and sentiment reversal techniques. It is observed that self-supervised learning algorithms give better accuracy than traditional supervised algorithms [11, 12].

Various clustering methods used for short text involve hybrid clustering. The approach involves clustering on different levels, such as first on location and then on the text. The author used DBSCAN and K-means algorithms to compare results [13–15]. Self-learning-based max-margin clustering, the Silhouette score, and Calinski–Harabasz score and Tf/Idf-based word embeddings with topic modeling algorithm are used to improve the precision of clustering [16, 17]. Gopal et al. proposed method by tagging keyword to perform topic modeling using LDA. This method gives better result at the expense of time taken to tagging [18].

Multiple methods and approaches were proposed by the research community, each having its pros and cons. The approach used in this paper is based on error value, sentiment score, and its correlation with the topics generated on the different dataset is presented in Sects. 4 and 5.

3 Datasets

As mentioned in Sect. 1, there are heterogeneous data fields available in Twitter data and choosing only one type of dataset would result in biased implementation. To overcome this issue, a variety of Twitter-based datasets are considered. The two benchmark datasets used are ‘Twitter US Airline sentiments’ and ‘Social media

disaster tweets’ [4, 5]. The third dataset is on Sabarimala temple tweets. The Twitter Airline sentiments are the tweets expressed on US Airlines in the month of February 2015. The dataset has 26 fields. Social media disaster tweets dataset is collected from ‘Data for everyone website.’ This dataset classifies the tweets into two categories that are relevant and irrelevant to disaster.

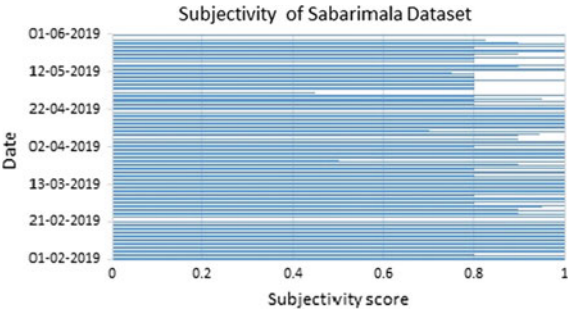
The third dataset is generated from Sabarimala temple tweets from January 2019 to May 2019. The dataset tries to collect data of patriarchy culture about Kerala temple, India. Earlier, the temple was open only for men to offer prayers inside the premises of the temple. When the Supreme Court of India decided that the temple will also be open for women, it created huge discussions and repulsions from its devotees and became the topic of discussion. This dataset contains the tweets based on this event. Some of the important fields are datetime, tweets, and then sentiment and subjectivity are calculated for implementation. Variety of Twitter datasets will give better understanding on clustering output using different techniques [3].

Sabarimala temple tweet datasets subjectivity score for each tweet computed. This will help to understand that the tweets in the dataset are related to the stated subject. Figure 2 shows the subjectivity score for each tweet. The *x*-axis is an individual tweet and the *y*-axis is the score of the tweet ranging from 0 to 1, where 0 indicates not relevant or objective sentence and 1 indicates highly relevant to the subject. Almost all of the tweets collected from Twitter on Sabarimala temple topic shows high subjectivity score which proves that the dataset is relevant to the subject Sabarimala temple.

4 Methodology

The Twitter datasets have various types of data such as text, numeric, and spatial. The approach used for the analysis also changes based on the characteristics of data attributes presenting the approach used for analysis of datasets in Fig. 3. The figure describes the different clustering techniques used based on the type of data. The results obtained are then compared and correlated.

Fig. 2 Subjectivity score on Sabarimala temple dataset



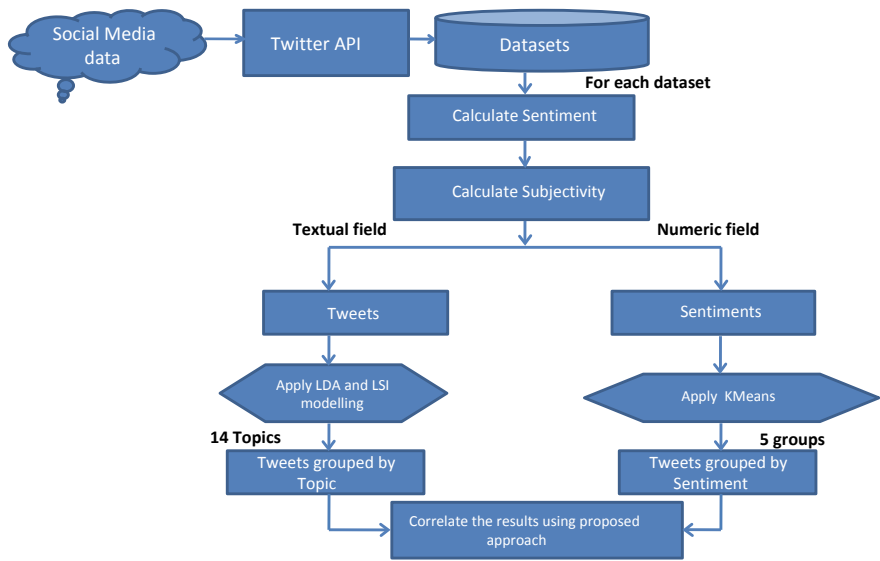


Fig. 3 Process to determine the correlation on Sabarimala temple verdict dataset

4.1 Proposed Algorithm

This section describes the algorithmic approach used for correlating clusters formed using techniques shown in Fig. 3. The parameters for correlation are sentiment score and topics formed using keywords in tweets. The sentiment score of the tweet is very important parameter which gives insight into emotions of the user. The proposed approach uses the density of the clusters formed using K-means based on sentiment scores and correlates with the results of topic modeling techniques applied.

Proposed algorithmic approach

for each dataset ds

step 1: initialize:
 numeric attribute
 textual attribute

step 2: for numeric attribute_dataset:
 apply K-means algorithm:
 calculate center and radius for each cluster
 identify tweets in each cluster based on sentiment score (say resultset R1)

step 3: for textual attribute_dataset:

A) apply LDA algorithm
 Find topics and their sentiment score
 identify tweets with keywords in each topic (say resultset R21)
B) apply LSI algorithm
 Find topics and their sentiment score
 identify tweets with keywords in each topic (say resultset R22)

step 4 : Novel method to compare the clustering results to identify overlapping between above results :

for each cluster in resultset R1: //K-means
 for each topic in resultset R21: //LDA
 if sentiment_cluster_center ~ sentiment_topic:
 find common tweets and
 consider that as “overlapping_factor”

for each topic in resultset R22: //LSI
 if sentiment_cluster_center ~ sentiment_topic:
 find common tweets and
 consider that as “overlapping_factor”

For each dataset mentioned in Sect. 3, apply the K-means method on sentiment scores of each tweet. Form clusters and find the centers of each cluster. Identify the tweets in each cluster density. The tweets identified are considered as a result set R1. This process is needed to be done for all the datasets considered as input. Apply LDA and LSI topic modeling techniques for textual attribute column Tweet in each dataset. This will give topics with 15 words in each topic forming that topic. These topics with top words are considered as result set R21 and R22. Find the topic sentiment. Topic sentiment is average sentiment of all the tweets containing the words in that topic. Compare the topic sentiment score with the cluster center.

If the values are almost close, then find common tweets and the overlapping tweets in topics formed in step 3 and clusters formed in step 2. Repeat this process for all topics formed using LDA and LSI method. The stated approach successfully shows the correlation between the clusters formed using numerical attribute and textual attribute.

4.2 Implementation and Results

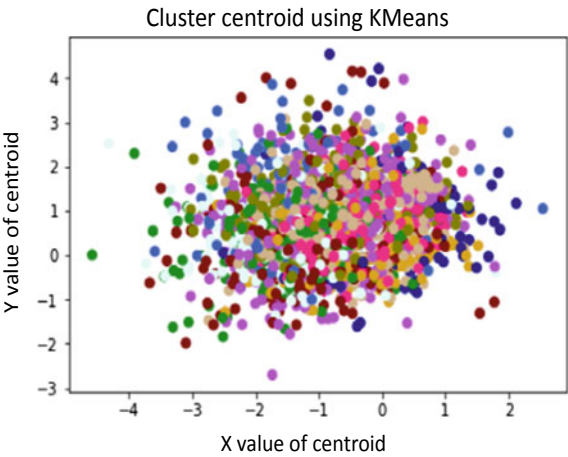
The algorithm described in Sect. 4.1 is applied to the datasets stated in Sect. 3. This section shows the implementation results on Twitter datasets.

4.2.1 Clustering Analysis Using K-means

As explained earlier about the dataset, the experiment is done by considering the text which involves the public tweets. After cleaning these tweets, the K-means algorithm applied on tweets of the datasets. Figure 4 shows the result of K-means applied on tweets of Sabarimala temple tweet dataset.

Figure 4 shows large number of clusters formed. These clusters are plotted using centroids. Majority of clusters are concentrated at the center of the graph. Clusters are not well separated. The clustering results on tweets were not worth considering, and the next analysis is done on sentiment scores. The sentiment and subjectivity scores found and added as an attribute.

Fig. 4 K-means labels on tweets



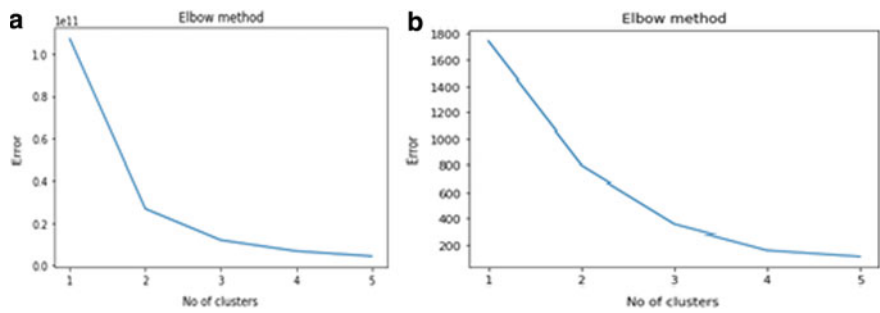


Fig. 5 K-means error rate **a** Benchmark datasets, **b** Sabarimala temple dataset

Usually, sentiments are grouped into three categories: positive, negative, and neutral. K-means is applied on sentiment with three clusters and five clusters. Analysis of cluster quality is done by plotting graphs with the error value. The curve in Fig. 5a, b shows the error curve formed using Elbow method with the K-means on benchmark and Sabarimala temple tweet datasets. The x -axis is number of clusters starting from 1 to 5, and y -axis is an error value for the number of clusters. Elbow method is used to find the appropriate number of clusters. This method is applied for clusters ranging from 1 to 5, and average error is calculated. The distortion is computed using mean squared error method between cluster centers and the point. It is seen from Fig. 5a, b that the error value is nearing to zero after crossing number of clusters as three, stabilizes to almost zero with cluster size 5. The results obtained on the Airline and social disaster dataset are verified on the Sabarimala temple dataset. Based on the above analysis, it is concluded to use the number of clusters as five.

The centers for each cluster using the K-means method with five clusters of sentiments is as shown in Table 1. The cluster centers for US Airline Sentiment dataset are -0.004226 , 0.6464205 , -0.89121 , 0.2706736 , -0.34945168 and for social disaster dataset 0.26843858 , -0.70356829 , 0.59311648 , 0.00351392 , -0.23977812 , ranging from -0.70356829 to 0.6464205 . The centers for Sabarimala temple dataset are -0.12742823 , 0.0358207 , 0.53544311 , 0.21365713 , -0.39216915 , ranging from -0.39216915 to 0.59311648 . The centers formed are well separated on all the datasets using the K-means method on sentiments. The K-means analysis is also done considering sentiment and subjectivity scores. In the analysis, it is found that subjectivity is not adding much value with the increased error rate during clustering. Hence, the results are not considered due to poor performance.

Table 1 Center of five clusters found using K-means

Dataset	Cluster center for 5 clusters				
	-0.00422636	0.6464205	-0.89121	0.2706736	-0.34945168
Airline dataset					
Social disaster dataset	0.26843858	-0.70356829	0.59311648	0.00351392	-0.23977812
Sabarimala temple dataset	-0.12742823	0.0358207	0.53544311	0.21365713	-0.39216915

4.2.2 Clustering Analysis of Text Data Using LDA and LSI

The result of K-means was not up to the mark on tweets (textual data). The topic modeling algorithms LDA and LSI are used to perform micro topic modeling on the Airline, social disaster dataset, and Sabarimala temple tweet dataset. These methods processes cleaned tweets and state the number of micro-topics. The decision on the number of micro-topics can be done by performing LDA GridSearchCV method with the number of topics as [5, 10, 15, 19, 20] and ‘learning_decay’ as [0.5, 0.7, 0.9]. This method takes combinations of both the parameters. The combination which gives best score is taken for optimal LDA model.

The log-likelihood score help in understanding the quality of fit. The perplexity is a measure used to decide the prediction ability of the probability model on a given sample. The log-likelihood score and perplexity help in deciding the ideal model. Higher log-likelihood score is always preferable. Table 2a shows the log-likelihood and perplexity scores of LDA. Table 2b shows the dominance of each topic and the number of tweets forming each topic. The ‘Topic’ in Table 2b indicates the clusters formed on tweets. Table 2b shows that topic 0 in US Airline sentiment dataset and topic 1 in the social disaster dataset is the most dominant topic formed using a maximum number of tweets compared to other topics.

Figures 6 and 7 show a log-likelihood curve for the three learning tests for choosing optimal LDA model for US Airline sentiment and social disaster dataset. The curve is formed using three learning rates as 0.5 (Blue), 0.7 (Orange), and 0.9 (Green). The best learning rate for dataset US Airline sentiment and social disaster dataset has come as 0.9 and the number of clusters as 5. The final LDA model is formed, and the resulting clusters are visualized using pyLDavis Python package.

Table 2 a Best scores on datasets. b Dominance of topics on tweets on datasets

(a)		
Dataset	Best log-likelihood score	Model perplexity
US Airline	−28,862.72	1183.2674
Social disaster	−24,552.78	887.6521
(b)		
Topic	Airline tweets	Social tweets
0	7400	1932
1	6496	2150
2	7233	1504
3	7297	1420
4	6063	1198

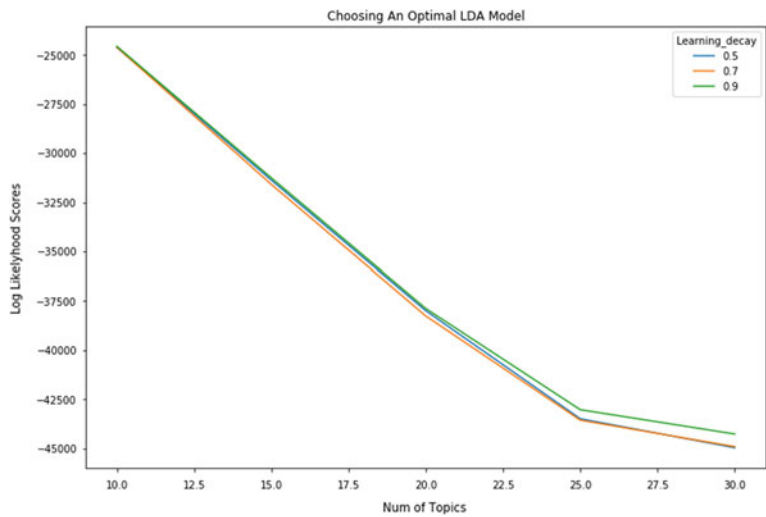


Fig. 6 Log-likelihood score to choose optimal LDA model

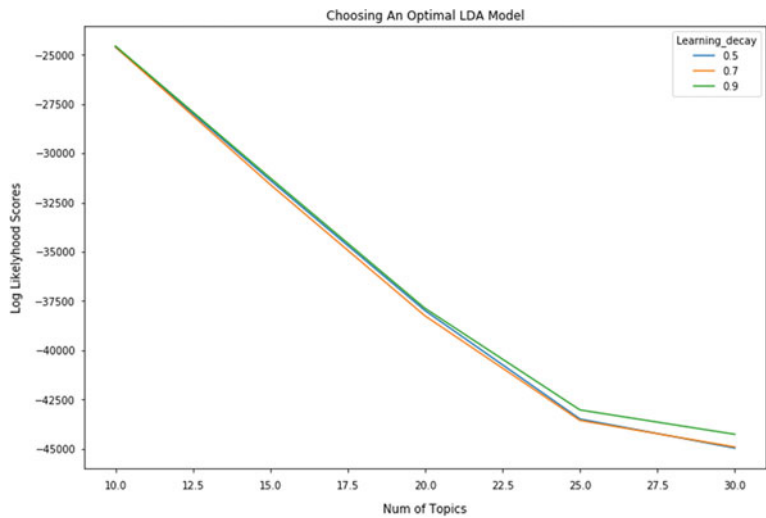


Fig. 7 Log-likelihood score to choose optimal LDA model

The topics are formed using the LSI method with the number of topics as 5 and log-likelihood score as in Table 2a. The topics formed using LDA and LSI models are further analyzed by finding their sentiment scores. This analysis will help in understanding the topic wise sentiment flow.

LDA and LSI are applied to the tweets field of the Sabarimala temple dataset. The ideal number of topics is found by applying GridSearchCV method, perplexity, and topic coherence methods. The perplexity scores are not enough to decide the number of topics; hence, the decision is made by looking at the coherence curve score. Figure 8a–c shows the log-likelihood scores, the coherence score, and the clusters formed using LDA. Figure 8a shows the curve formed using three learning rates. The orange color curve shows better log-likelihood scores compared to other two. It is concluded that the ideal learning rate for the model is 0.7. The coherence score curve in Fig. 8b reaches its peak when the topics are between 10 and 15; hence, the number of topics decided as 14 with learning rate of 0.7 for the topic modeling algorithms. Figure 8c gives the topic clusters on left hand side in circular shape and unigrams and bigrams forming topic clusters.

4.2.3 Proposed Method to Compare the Clustering Results

The results are compared and correlated using the algorithmic approach proposed in Sect. 4.1. This method is applied on the clusters generated by K-means and topic modeling methods. The clusters are compared by finding the percentage of overlap between the clusters formed by K-means and LDA and then K-means and LSI.

The results are shown using Tables 3 and 4 with the column names as follows: ‘Tno’ as ‘topic cluster number’ formed as clusters on tweets with number, ‘tweetsent’ refers to ‘topic tweet sentiment’ is an average sentiment of all the tweets comprising each topic, column ‘tsent’ is ‘topic sentiment’ is the sentiment of all the words forming the topic, ‘center’ is the center of each cluster formed using K-means, and ‘overlap %’ is a percentage of the total number of overlapping tweets.

Table 3a shows the relationship between each topic formed, its sentiment, and K-means cluster centers. The common tweets belonging to K-means cluster and LDA topic are found by calculating the density of each cluster and considering the tweets coming in the density of the cluster. Next, the total number of tweets belonging to that cluster is found out. Finally, the percentage of overlapping tweets is calculated. The same process is applied to LSI topics.

The results in Table 3a shows that the sentiment of topic 0 and K-means cluster center is almost the same. This shows the neutral polarity of that topic with more than 65% similarity. Topic 1 has sentiment -0.2 with K-means center as -0.2397 with 43% of overlapping tweets. Similarly, Table 3b shows the result of US Airline sentiment dataset using LSI and K-means. The ‘topic tweet sentiment’ for topic 0 is -0.5 and % of overlapping tweets more than 56% of rows 1, 3, and 4 of topic 0 in Table 3b. The remaining topics are also showing a high overlapping percentage.

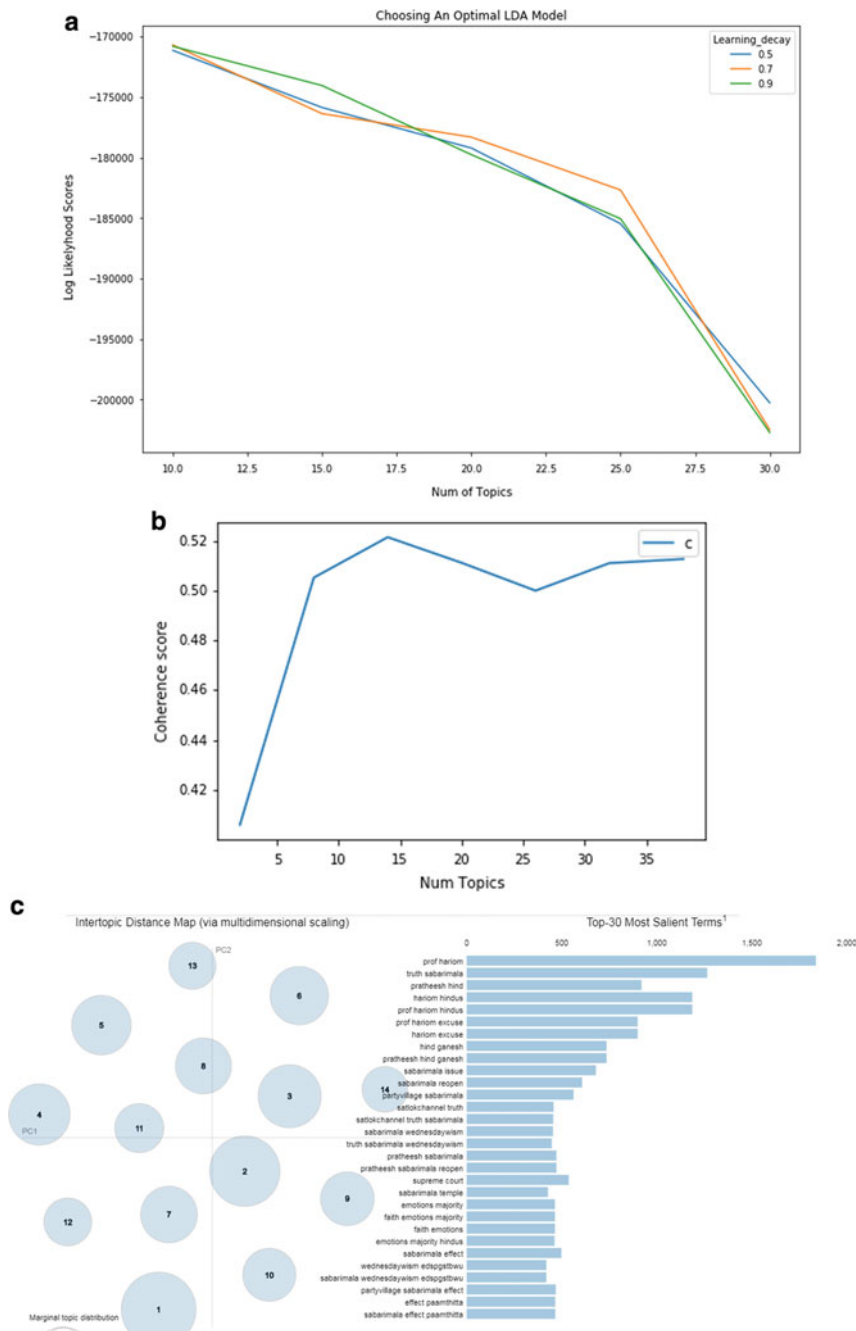


Fig. 8 **a** Log-likelihood curve, **b** coherence score on number of topics, **c** clusters using LDA on Sabarimala temple tweet dataset

Table 3 Relation between K-means clusters and topics formed on US Airline sentiment dataset using **a** LDA, **b** LSI

(a)					(b)				
Tno	tweetsent	tsent	center	Overlap %	Tno	tweetsent	tsent	center	Overlap %
0	0.0226	0	0.0035	67.7019	0	-0.0381	-0.5	-0.0042	57.7432
			-0.7036	23.2416				0.6464	46.5365
			0.5931	13.9773				-0.3495	57.1145
			-0.2398	15.8451				-0.8912	69.8864
			0.2684	17.2535				0.2707	49.4204
1	0.0253	-0.2	0.0035	22.9302	1	0.0382	0.1	-0.0042	49.6213
			-0.7036	23.8532				0.6464	35.5164
			0.5931	15.6818				-0.3495	51.7538
			-0.2398	43.5035				-0.8912	40.6250
			0.2684	22.1127				0.2707	53.8176
2	0.0600	0.1667	0.0035	63.5638	2	0.0415	0.2	-0.0042	47.8092
			-0.7036	11.9266				0.6464	51.0579
			0.5931	15.5682				-0.3495	46.3203
			-0.2398	12.3239				-0.8912	42.3295
			0.2684	16.3380				0.2707	58.4930
3	0.0182	-0.0633	0.0035	68.0282	3	0.0373	-0.3	-0.0042	46.5724
			-0.7036	10.7034				0.6464	40.9950
			0.5931	10.5682				-0.3495	58.5705
			-0.2398	16.5493				-0.8912	45.7386
			0.2684	9.7183				0.2707	38.4158
4	0.0321	-0.35	0.0035	23.2721	4	0.0224	-0.5333	-0.0042	57.3808
			-0.7036	16.8196				0.6464	34.6977
			0.5931	9.2045				-0.3495	52.8127
			-0.2398	60.3873				-0.8912	59.0909
			0.2684	15.5259				0.2707	39.6832

Table 4 Relation between K-means clusters and topics formed on social disaster dataset using a LDA, b LSI

(a)			(b)						
Tno	tweetsent	tsent	center	Overlap %	Tno	tweetsent	tsent	center	Overlap %
0	0.0226	0	0.0035	67.7019	0	0.0388	0	0.0035	63.8129
			-0.7036	23.2416				0.5931	24.5455
			0.5931	13.9773				-0.7036	22.9358
			-0.2398	15.8451				-0.2398	25.6162
			0.2684	17.2535				0.2684	23.3099
1	0.0253	-0.2	0.0035	22.9302	1	0.0476	0.1	0.0035	63.3317
			-0.7036	23.8532				0.5931	21.5909
			0.5931	15.6818				-0.7036	21.4067
			-0.2398	43.5035				-0.2398	18.3099
			0.2684	22.1127				0.2684	20.9859
2	0.0600	0.1667	0.0035	63.5638	2	0.0153	0	0.0035	68.2550
			-0.7036	11.9266				0.5931	9.2045
			0.5931	15.5682				-0.7036	13.4557
			-0.2398	12.3239				-0.2398	15.7570
			0.2684	16.3380				0.2684	13.3099
3	0.0182	-0.0633	0.0035	68.0282	3	0.0376	0	0.0035	70.8231
			-0.7036	10.7034				0.5931	10.2273
			0.5931	10.5682				-0.7036	6.1162
			-0.2398	16.5493				-0.2398	10.7394
			0.2684	9.7183				0.2684	10.2689
4	0.0321	-0.35	0.0035	23.2721	4	0.0324	0	0.0035	64.8714
			-0.7036	16.8196				0.5931	21.3636
			0.5931	9.2045				-0.7036	21.4067
			-0.2398	60.3873				-0.2398	26.6725
			0.2684	15.5259				0.2684	22.0423

Table 5 Relation between K-means clusters and topics formed on Sabarimala temple dataset using **a** LDA, **b** LSI

(a)			(b)								
Tno	K-means cluster center	Total tweets	K-means	Common tweets (3 and 4)	Topic sentiment	Tno	K-means cluster center	Total tweets	K-means	Common tweets (3 and 4)	Topic sentiment
1	0.0035	124	7111	80	-0.6	1	0.1940	124	65	57	0.3167
	0.5931		880	11			-0.1375		29		
	-0.7036		327	94			0.5354		6		
	-0.2398		1136	15			-0.3922		6		
	0.2684		1420	14			0.0205		40		
5	0.0035	10	7111	6	-0.125	5	0.1940	10	40	3	-0.05
	0.5931		880	1			-0.1375		29		
	-0.7036		327	0			0.5354		6		
	-0.2398		1136	2			-0.3922		6		
	0.2684		1420	1			0.0205		65		
6	0.0035	29	7111	3	0.2571	6	0.1940	29	40	8	0
	0.5931		880	2			-0.1375		29		
	-0.7036		327	1			0.5354		6		
	-0.2398		1136	3			-0.3922		6		
	0.2684		1420	20			0.0205		65		
10	0.0035	17	7111	10	0.3167	10	0.1940	17	40	3	0
	0.5931		880	2			-0.1375		29		
	-0.7036		327	0			0.5354		6		
	-0.2398		1136	1			-0.3922		6		
	0.2684		1420	13			0.0205		65		
11	0.0035	6	7111	1	0.33	11	0.1940	6	40	2	0
	0.5931		880	3			-0.1375		29		
	-0.7036		327	0			0.5354		6		
	-0.2398		1136	1			-0.3922		6		
	0.2684		1420	1			0.0205		65		

Table 4a shows the result of LDA compared with K-means cluster centers. The overall sentiment value for 'Topic 0' is 0, and K-means cluster center value is 0.0035. Topic 1 has -0.2 topic sentiment and K-means cluster center value for 4th cluster is -0.2398 . Similarly for other topics also values are very close. Table 4b shows the LSI topics of social disaster dataset. The topic sentiment for all the topics is the same as the first cluster center using K-means. The analysis is done on the results from the US Airline sentiment dataset, and the social disaster dataset shows that the topic sentiment matches with K-means cluster center, and the results show more than 60% overlapping tweets.

Table 5a, b shows the result for the Sabarimala temple tweet dataset using approach mentioned in Sect. 4.1. Topic 1 of Table 5a with cluster center -0.7036 has 94 tweets common with the average sentiment of -0.6 which is quite close to the cluster center value. Topic 5 has an average sentiment value of -0.125 , and cluster center at 0.0035 has 6 tweets in common. Topic 6 has K-means center of 0.2684 and topic sentiment as 0.2572. Topic 10 with the last cluster values as 0.2685 is close to the topic average sentiment value 0.3166. Similarly, the results in Table 5b also show a lot of closeness in sentiment and cluster center values with the topics formed using LSI.

Considering the results shown in Tables 3, 4, and 5, it is observed that the topics formed using topic modeling algorithm on tweets has more than 60% similarity with the clusters formed using sentiment.

5 Conclusion and Future Work

Twitter datasets on US Airline sentiment and social disaster are evaluated and tested on Sabarimala temple event dataset created with the help of LDA, LSI, and K-means clustering approach. The clustering is done on numerical values like the sentiment of each tweet and textual values as tweets tweeted by users. The analysis done using proposed approach shows significant correlation between the clusters formed using K-means and the topics formed using techniques LDA and LSI for each dataset. The average sentiment of each topic and the cluster centers is showing matching polarity at many places. It is observed that there is a maximum overlapping of tweets for the most relative centers and topics. Further, this work can be extended to find an improved correlation between each topic and its associated sentiment. Analysis on blog can be done after finding important topic using above work to find opinion and perform stance analysis. Results can be more precisely validated by comparing events from the blogs by performing analysis on blogs.

References

1. Kursuncu, U., Gaur, M., Lokala, U., Thirunarayan, K., Sheth, A., Arpinar, I.B.: Predictive analysis on Twitter: techniques and applications. In: *Emerging Research Challenges and Opportunities in Computational Social Network Analysis and Mining*, pp. 67–104. Springer, Cham (2019)
2. Crockett, K.A., Mclean, D., Latham, A., Alnajran, N.: Cluster analysis of Twitter data: a review of algorithms. In: *Proceedings of the 9th International Conference on Agents and Artificial Intelligence*, vol. 2, pp. 239–249. Science and Technology Publications (SCITEPRESS)/Springer Books (2017)
3. Chronology of events on entry of women into Sabarimala temple: New Delhi, November 14, 2019 IST 17:11 Updated: November 14, 18:29 IST. <https://www.thehindu.com/news/national/chronology-of-events-on-entry-of-women-into-sabarimala-temple/article29972784.ece> (2019)
4. Twitter US Airline Sentiment: Analyze how travelers in February 2015 expressed their feelings on Twitter. Updated: Wed October 16, 2019 IST 5:34:05. <https://www.kaggle.com/crowdflower/Twitter-airline-sentiment> (2015)
5. Disasters on social media: Which tweets are relevant news and which are just banter? Updated: Sun 15 April 2018 IST 12:34:59. <https://www.kaggle.com/jannesklaas/disasters-on-social-media> (2018)
6. Singh, K., Shakya, H.K., Biswas, B.: Clustering of people in social network based on textual similarity. *Perspect Sci.* **8**, 570–573. <https://doi.org/10.1016/j.pisc.2016.06.023> (2016)
7. Asif, M., Ishtiaq, A., Ahmad, H., Aljuaid, H., Shah, J.: Sentiment analysis of extremism in social media from textual information. *Telematics Inform.* **48**, 101345. <https://doi.org/10.1016/j.tele.2020.101345> (2020)
8. Han, S., Huang, H., Tang, Y.: Knowledge of words: an interpretable approach for personality recognition from social media. *Knowl. Based Syst.* 105550. <https://doi.org/10.1016/j.knosys.2020.105550> (2020)
9. Singh, S.K., Sachan, M.K.: SentiVerb system: classification of social media text using sentiment analysis. *Multimedia Tools Appl.* **78**(22):32109–32136. <https://doi.org/10.1007/s11042-019-07995-2> (2019)
10. Vashishtha, S., Susan, S.: Fuzzy rule based unsupervised sentiment analysis from social media posts. *Expert Syst. Appl.* **138**, 112834. <https://doi.org/10.1016/j.eswa.2019.112834> (2019)
11. Kokatnoor, S.A., Krishnan, B.: Self-Supervised Learning Based Anomaly Detection in Online Social Media. <https://doi.org/10.22266/ijies2020.0630.40>
12. Wang, L., Niu, J., Yu, S.: SentiDiff: combining textual information and sentiment diffusion patterns for Twitter sentiment analysis. In: *IEEE Transactions on Knowledge and Data Engineering*. <https://doi.org/10.1109/TKDE.2019.2913641> (2019)
13. Cresci, S.: Detecting malicious social bots: story of a never-ending clash. In: *Multidisciplinary International Symposium on Disinformation in Open Online Media*, pp. 77–88. Springer, Cham (2019)
14. Jiang, Y., Li, Z., Ye, X.: Understanding demographic and socioeconomic biases of geotagged Twitter users at the county level. *Cartogr. Geogr. Inf. Sci.* **46**(3), 228–242 (2019)
15. Bamakan, S.M., Nurgaliev, I., Qu, Q.: Opinion leader detection: a methodological review. *Expert Syst. Appl.* **115**, 200–222 (2019)
16. Gupta, S., Banerjee, B.: Unsupervised event detection using self-learning-based max-margin clustering: analysis on streaming tweets. *IETE J. Res.* 1–0 (2019)

17. Curiskis, S.A., Drake, B., Osborn, T.R. and Kennedy, P.J.: An evaluation of document clustering and topic modelling in two online social networks: Twitter and Reddit. *Inf. Process. Manag.* **57**(2), 102034 (2020)
18. Gopal, G.N., Kovoov, B.C. and Mini, U.: Keyword template based semi-supervised topic modelling in tweets. In: *International Conference on Innovative Computing and Communications*, pp. 659–666. Springer, Singapore (2021)

Design and Analysis of 2×4 Microstrip Patch Antenna Array with Defected Ground Structure for 5G Mobile Communication



Sameena Zafar, Vineeta Saxena, and R. K. Baghel

Abstract Wireless communication application is not possible without using the antenna. Nowadays, microstrip patch antenna (MPA) is using broadly due to its major advantages than others. Most of the electronics device is using MPA. There are various shapes, and pattern is proposed by antenna researchers. Microstrip patch antenna provides better performance in wireless communication applications. This paper proposed a novel design of microstrip patch antenna array for 5G Wi-Fi, wi-max applications. The CST microwave studio software is used to make a proposed antenna design and simulation. The resonant frequency of this antenna is 6.9 GHz. Overall bandwidth achieved by proposed antenna is 903 GHz. The large bandwidth is required for 5G communication applications.

Keywords Microstrip · Patch · Antenna · CST · FR4 · VSWR · Return loss

1 Introduction

It is generally utilized in versatile remote gadgets in light of the simplicity of creating it on printed circuit sheets. Numerous fix reception apparatuses on a similar substrate called microstrip radio wires can be utilized to make high pick-up cluster receiving wires and staged exhibits in which the shaft can be electronically directed. With the headway of distant correspondence propels, it has gotten continuously appealing for present day specific contraptions to facilitate diverse correspondence rules, for instance, 2G/3G/4G/5G. Consequently, radio wires with broadband execution are well known for multi-standard incorporation. To achieve broadband movement, various plans of microstrip gathering mechanical assemblies have been

S. Zafar (✉) · V. Saxena
UIT RGPV, Bhopal, India

R. K. Baghel
MANIT, Bhopal, India

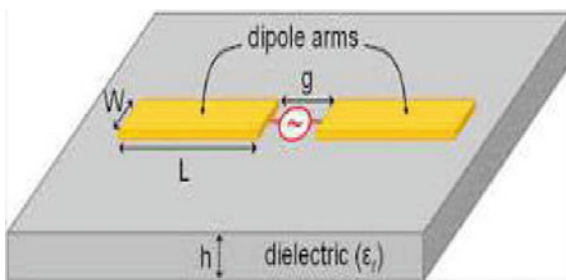
represented, for instance, adjusting the condition of the microstrip arms, improving dealing with methodologies, stacking parasitic radiators, and using magneto-electric complementary structures [1].

Besides, radiation execution is furthermore needed for some distant correspondence applications, for instance, indoor sign consideration, far off sections, and little scope base stations. Considering the multimode PFDA, a clear and incredible structure to achieve radiation execution is made by setting two of the proposed PFDA's successive. The ensuing gathering contraption shows extraordinary radiation plans in the even plane with level increment assortment of under 1.27 dB. The presented traditionalist broadband radio wire is a fair competitor for indoor sign incorporation. Three reverberating modes are gotten by using a changed planar imploded microstrip and its coupled dealing with structure. Combining the shorting pins and parasitic patches, various resonating modes in the reception apparatus are controlled, moved, and a while later joined to fabricate the impedance information transmission. Using this thought, a model of a multimode fell microstrip is arranged, made, and assessed [1]. Normal coupling between two microstrip reception apparatus with different estimations put at self-assured equivalent positions is bankrupt down using simultaneous key conditions with unequivocal parts and restricted opening feeds [2]. A story plan procedure for a wideband twofold delighted gathering device is presented by using shorted microstrips, consolidated baluns, and crossed feed lines. Reenactment and proportionate circuit examination of the reception apparatus are given.

To endorse the arrangement procedure, a receiving wire model is arranged, updated, produced, and assessed as depicted in Fig. 1 [3]. An epic super wide band immovably coupled microstrip reflects exhibit radio wire is presented in this work. This reflects cluster radio wire involves a wideband feed and a wideband reflecting surface. By joining the advantages of reflecting cluster gathering contraptions and those of solidly coupled show radio wires, the proposed TCDR reception apparatus achieves ultra-wide exchange speed with diminished capriciousness and creation cost [4].

Microstrip radio wire is especially notable considering the way that the information transmission of more modest scope strip microstrip receiving wire is high when appeared differently in relation to the scaled down scale strip fix gathering contraption. Little scope strip microstrip gathering mechanical assembly will be the

Fig. 1 Microstrip antenna



rule point of convergence of this work. A scaled down scale strip microstrip is a utilization of the standard microstrip radio wire on a dielectric piece, which can be easily made with existing PCB systems. Rather than standard little scope strip gathering device, that use one side of the piece as the ground plane, the more modest scope strip microstrip basically uses the dielectric segment as the host material. This radio wire is picked considering the way that it is direct, however, then has potential for future improvement. A traditionalist wideband twofold entranced reception apparatus with improved upper out-of-band camouflage is presented in this work. The proposed gathering mechanical assembly is a corresponding course of action of two electric microstrips and two appealing microstrips using the crossed shunt circles. The breaker of the electric and alluring microstrips enables the radio wire to achieve wide impedance bandwidth and a moderate radiator size. Likewise, four parasitic strips are inserted near the inside edge of the four circles to overhaul the radio wire upper out-of-band disguise at 3.5 GHz with improved impedance information move limit.

In the upcoming sections in this paper, authors will focus on background study of design and analysis of 4×4 microstrip patch antenna array with defected ground structure for 5G mobile communication in Sect. 2. Proposed design and results are presented in Sects. 3 and 4 that will highlight on the model building for predictive analysis, followed by conclusion and references.

2 Background

A. Singh et al. present a ten-part multi-gathering mechanical assembly terminal for huge different data diverse yield (MIMO) in the fifth-age (5G) sub-6 GHz with wide impedance bandwidth (IBW) is proposed. The most outrageous reproduced envelope relationship coefficient is viewed as 0.21 and remembering that the base receiving wire adequacy is 78.4%. Each element has a structure factor of $17.2 \times 3.8 \text{ mm}^2$ and engraved on a thick Rogers 4003 substrate. The proposed multi-antenna terminal is suitable for 5G sub-6 GHz (3.2–6.1 GHz) correspondence including long-term evolution bands 42, 43 and 46 [1].

Ojaroudi Parchin et al. present another various information/different yield (MIMO) gathering mechanical assembly setup is introduced for future PDAs. The proposed structure contains four arrangements of twofold dealt with round ring resonators arranged at different edges of the mobile phone printed circuit board (PCB) with a FR-4 substrate and a segment of $75 \times 150 \text{ mm}^2$. A respectable repeat information move limit ($S_{11} \leq -10 \text{ dB}$) of 3.3–3.9 GHz has been gotten for the mobile phone receiving wire group. Regardless, for $S_{11} \leq -6 \text{ dB}$, this value is 3.1–4.3 GHz. More than 3 dB recognized increment and 80% complete capability are refined for the single-segment radiator. The structure gives not simply satisfactory radiation consideration supporting different sides of the mainboard yet also the polarization grouped assortment [2].

Feng et al. present twofold straightforwardly charmed (LP) high-demand mode radio wire with high increment, and high separation is proposed for 5G millimeter-wave (mm-wave) applications. To get high increment and wide information move limit, a 2×2 space dealt with magneto-electric (ME)-group receiving wire segments are stimulated by a high-demand mode TM 430 cavity. Assessment results show that a covered repeat move speed of 14.6% (36.8–42.6 GHz) with a zenith increment of 25.8 dBi and a withdrawal of more significant than 45 dB for the 8×8 twofold LP gathering mechanical assembly bunch are refined, which guarantee strong fast data transmission and against impedance limit regarding 5G exchanges [3]. Hussain et al. present multiplication and assessment outcomes of a wideband planar organized bunch for 5G. The ideal wideband action is cultivated using an immovably coupled group display (TCDA). The group has a height of simply 0.144λ , and it shows high expands, high profitability >71% (greatest yield point), and extraordinary cross-polarization. The reenactments are endorsed by production and assessment of a display model, which shows agree to reproduced regards. The proposed twofold delighted radio wire bunch can be sent later on bar checking applications for 5G [4].

Serhsouh et al. present novel reconfigurable opened flawed wave gathering contraction (LWA) considering a substrate joined waveguide (SIW) with a fixed—repeat bar controlling capacity is presented in this paper. The pin diodes are tunable by changing the DC inclination voltage, which achieves column checking at a fixed repeat of around 27 GHz. In this manner, an electronically controlled steerable SIW radio wire has been organized and likely watched that the radiation edge shifts from -33° to $+33^\circ$ [5]. Pérez et al. present concerning the structure and masterminding of new radio interfaces for the fifth-age (5G) systems, and this paper presents a supportive obligation to the depiction of the wideband indoor radio redirect in the 3–4-GHz repeat band. An assessment campaign has been done in two unmistakable indoor circumstances to look at indisputably the main wideband limits of the expansion channel, including a cautious assessment of its direct to meet the new radio advancement challenges [6].

3 Proposed Antenna Design

Figure 2, showing top perspective on proposed microstrip antenna array, one side of a dielectric substrate goes about as an emanating microstrip and opposite side of substrate goes about as ground plane. As in Fig. 2 demonstrated as follows, top perspectives on a rectangular microstrip radio wire with coaxial feed have microstrip, and ground plane together makes bordering fields, and this field is answerable for making the radiation from the receiving wire. Microstrip reception apparatus is proposed because of little size and better reference. Resonant frequency of proposed reception apparatus is approx. 6.9 GHz that implies it work under 5G C-band. Thus, proposed radio wire ought to be valuable for all C-band application.

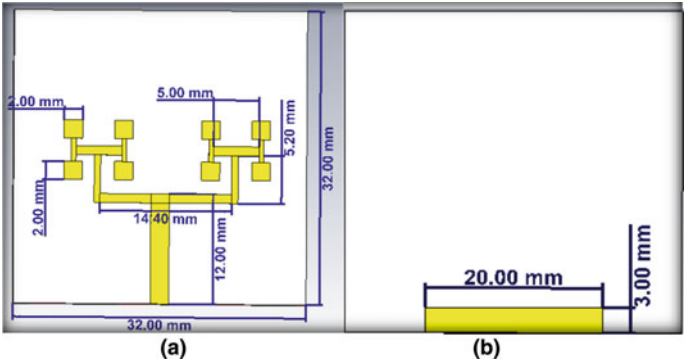


Fig. 2 a Top view, b defected ground structure of proposed microstrip antenna array

Above figure is indicating proposed microstrip antenna of plan. The top and ground layer is made by lossy copper material, and substrate is made by FR4 material which having 4.4 dielectric steady worth.

4 Result Analysis

The geometry of the proposed structure of microstrip for C-band applications is appeared in Fig. 2. The general size of the structure is 32 mm × 32 mm × 1.64 mm ($L \times W \times H$) and imprinted on fire resistant 4 (FR4), with an overall permittivity of 4.4, and a loss digression of 0.024. Table1 records the element of the proposed antenna. The antenna is taken care of by 50-Ω and 0.5 W coaxial link or straightforward. The antenna utilizes the microstrip structure with one opening for C-band applications.

Table 1 Design parameters for proposed antenna

S.No.	Parameter	Value
1	Lower frequency (f_L)	4 GHz
2	Higher frequency (f_H)	8 GHz
3	Dielectric constant (ϵ_r)	4.4/FR4
4	Ground ($L \times W$)	3 mm × 120 mm
5	Ground height	0.035 mm
6	Substrate ($L \times W$)	32 mm × 32 mm
7	Substrate height (h)	1.57 mm
8	Line impedance	50 Ω
9	Tangent loss	0.06
10	Input watt	0.5 W

CST microwave studio is used to recreate the proposed plan. Figure 3 is demonstrating reenacted electric and attractive field in round organize framework.

Figure 4 presents return loss of proposed structure. It is obvious to see this chart, and the return loss estimation of proposed antenna is -18.34 dB with 6.9 resonant frequency.

For broadband antennas, the bandwidth is communicated as a level of the recurrence contrast (upper less low) over the inside recurrence of the bandwidth as shown

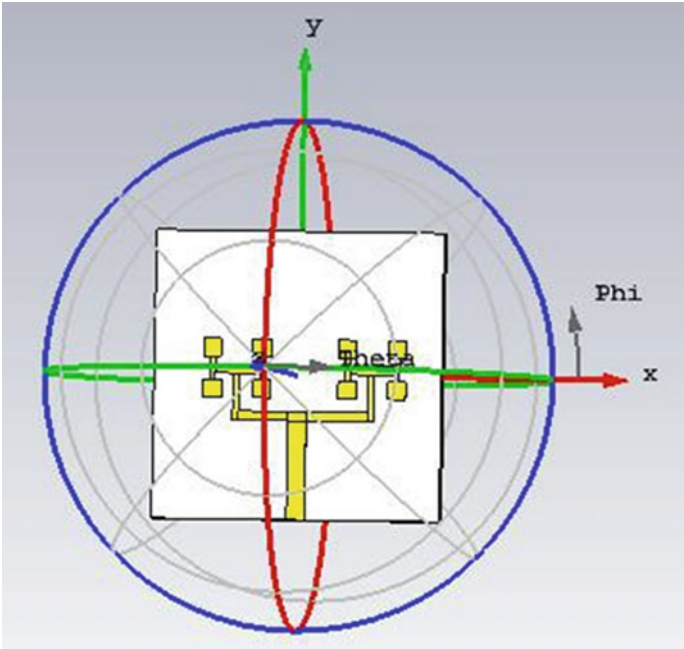


Fig. 3 Simulation and fields of proposed antenna

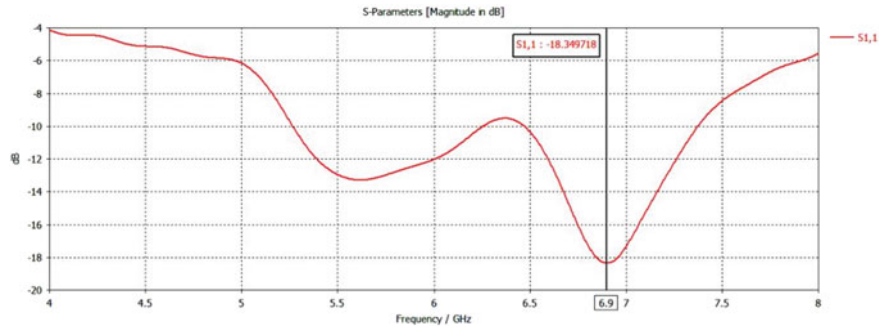


Fig. 4 Return loss

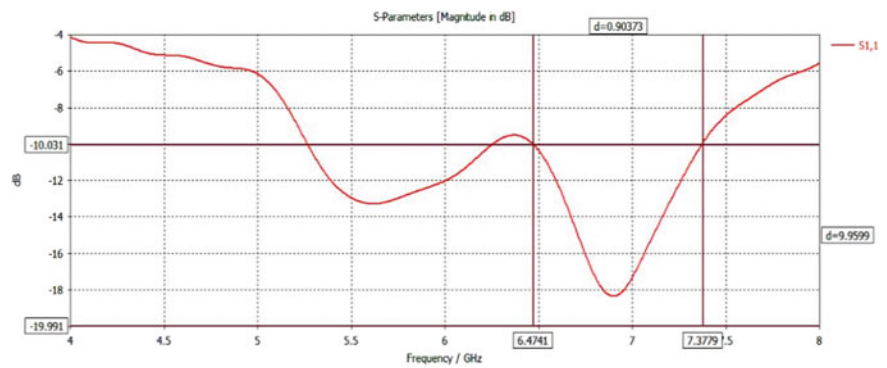


Fig. 5 Bandwidth

Table 2 Simulated results of proposed antenna

Sr. No.	Parameter	Value
1	Return loss or S11	−18.34 dB
2	Bandwidth	903.73 MHz
4	Resonant frequency	6.9 GHz

in Fig. 5. The bandwidth of proposed antenna is 903.73 MHz, (7.3779–6.4741 GHz), for optimized band. It is a variety of the force transmitted by an antenna as an element of the heading ceaselessly from the antenna.

Table2 shows about terms of every vital parameter like return loss, bandwidth, VSWR, and resounding recurrence. It is clear by observing reenacted values from Table 2, and proposed antenna accomplishes significant improved outcome.

5 Conclusion and Future Scope

A microstrip antenna array is planned and recreated utilizing CST reenactment programming. The reproduction results are introduced and examined. Structure of proposed antenna is basic and reduced in size of $32 \times 32 \times 1.6 \text{ mm}^3$. Reenacted results exhibit that the antenna bandwidth covers S-band and C-band, at full recurrence 6.9 GHz. The bandwidth is huge accomplished better than microstrip fix antenna structure. Microstrip antenna array configuration is recently exploring theme among specialists. The general bandwidth is 903.73 MHz. Subsequently, proposed antenna is reasonable and meets to current correspondence requests. In the future, above design can be implemented for higher number of elements thereby increasing the array size, and thus, better results can be expected using slots or fractal design.

References

1. Singh, A., Saavedra, C.E.: Wide-bandwidth inverted-F stub fed hybrid loop antenna for 5G sub-6 GHz massive MIMO enabled handsets. In: IET Microwaves, Antennas & Propagation, vol. 14, no. 7, pp. 677–683 (2020). <https://doi.org/10.1049/iet-map.2019.0980>
2. Ojaroudi Parchin, N., Al-Yasir, Y.I.A., Jahanbakhsh Basherlou, H., Abd-Alhameed, R.A., Noras, J.M.: Orthogonally dual-polarised MIMO antenna array with pattern diversity for use in 5G smartphones. In: IET Microwaves, Antennas & Propagation, vol. 14, no. 6, pp. 457–467 (2020). <https://doi.org/10.1049/iet-map.2019.0328>
3. Feng, B., Tu, Y., Chen, J., Yin, S., Chung, K.L.: Dual linearly-polarized antenna array with high gain and high isolation for 5G millimeter-wave applications. IEEE Access **8**, 82471–82480 (2020). <https://doi.org/10.1109/ACCESS.2020.2990494>
4. Hussain, S., Qu, S., Zhou, W., Zhang, P., Yang, S.: Design and fabrication of wideband dual-polarized array for 5G wireless systems. IEEE Access **8**, 65155–65163 (2020). <https://doi.org/10.1109/ACCESS.2020.2984613>
5. Serhsouh, I., Himdi, M., Lebbar, H., Vettikalladi, H.: Reconfigurable SIW antenna for fixed frequency beam scanning and 5G applications. IEEE Access **8**, 60084–60089 (2020). <https://doi.org/10.1109/ACCESS.2020.2983001>
6. Pérez, J.R., et al.: Empirical characterization of the indoor radio channel for array antenna systems in the 3 to 4 GHz frequency band. IEEE Access **7**, 94725–94736 (2019). <https://doi.org/10.1109/ACCESS.2019.2928421>
7. Shen, X., Liu, Y., Zhao, L., Huang, G., Shi, X., Huang, Q.: A miniaturized microstrip antenna array at 5G millimeter-wave band. IEEE Antennas Wirel. Propag. Lett. **18**(8), 1671–1675 (2019). <https://doi.org/10.1109/LAWP.2019.2927460>
8. Kim, Y., Kim, H., Yoon, I., Oh, J.: 4×8 Patch array-fed FR4-based transmit array antennas for affordable and reliable 5G beam steering. IEEE Access **7**, 88881–88893 (2019). <https://doi.org/10.1109/ACCESS.2019.2926379>
9. Chattha, H.T.: 4-Port 2-element MIMO antenna for 5G portable applications. IEEE Access **7**, 96516–96520 (2019). <https://doi.org/10.1109/ACCESS.2019.2925351>
10. Li, A., Luk, K., Li, Y.: A dual linearly polarized end-fire antenna array for the 5G applications. IEEE Access **6**, 78276–78285 (2018). <https://doi.org/10.1109/ACCESS.2018.2884946>
11. Khan, R., Al-Hadi, A.A., Soh, P.J., Kamarudin, M.R., Ali, M.T., Owais: User influence on mobile terminal antennas: a review of challenges and potential solution for 5G antennas. IEEE Access **6**, 77695–77715 (2018). <https://doi.org/10.1109/ACCESS.2018.2883788>
12. Mukhopadhyay, A.: J. C. Bose’s scientific inventions confirmed the truth of consciousness. IJOHNM **4**(6), 1–20 (2018). <https://doi.org/10.24113/ijohmn.v4i6.72>
13. Naqvi, S.H.R., Ho, P.H., Jabeen, S.: A novel distributed antenna access architecture for 5g indoor service provisioning. IEEE J. Sel. Areas Commun. **36**(11), 2518–2527 (2018). <https://doi.org/10.1109/JSAC.2018.2874144>
14. Bengtsson, E.L., Rusek, F., Malkowsky, S., Tufvesson, F., Karlsson, P.C., Edfors, O.: A simulation framework for multiple-antenna terminals in 5G massive MIMO systems. IEEE Access **5**, 26819–26831 (2017). <https://doi.org/10.1109/ACCESS.2017.2775210>
15. Li, M., Xu, Z., Ban, Y., Sim, C., Yu, Z.: Eight-port orthogonally dual-polarised MIMO antennas using loop structures for 5G smartphone. In: IET Microwaves, Antennas & Propagation, vol. 11, no. 12, pp. 1810–1816 (2017). <https://doi.org/10.1049/iet-map.2017.0230>
16. Neil, C.T., Shafi, M., Smith, P.J., Dmochowski, P.A., Zhang, J.: IEEE Transactions on Impact of Microwave and Wave Channel Models on 5G Systems Performance

Efficiency Analyzing on Vehicle Tracking Systems



L. Rahunathan, D. Harish, A. Antony Samson,
and D. Sivabalaselvamani

Abstract The vehicle tracking system is the fundamental part in our everyday life. Yet, the vehicle tracking system regularly utilized GSM/GPS procedure. Presently what the issue with is, we should need a web association with doing this kind of vehicle following, but a portion of the cases and in no organization regions this sort of vehicle following won't work. Along these lines, in this paper, we investigate the demonstration of GPS/GSM tracking system and the chance of LoRa-based vehicle tracking system. Results uncovered that all measurements measured with in re-enacted experiments were comparable to the results of a genuine examination; notwithstanding, we thought that by looking for a more realistic relationship with real inquiries, the model could be strengthened.

Keywords Arduino UNO · LoRa · GSM · GPS · Vehicle tracking system

1 Introduction

LoRa stands for “Low Power Wide Area Network” and requests decreased organization framework to cover an enormous region, with low force utilization. With regards to vehicle following, LoRa does have capacity to help with observing and appropriate path applications, whereby company can share small volumes of information non-concurrently. By and by, Lora's assessments are needed in setting up vehicle communications. LoRa (short for long reach) is a spread range adjustment strategy got from peep spread range (CSS) innovation. Utilizing of this gadget we can impart the GPS co-ordinates starting with one LoRa then onto the next. By sharing the co-ordinates, we can undoubtedly follow that LoRa area without utilizing web. Also, just as we would disk about the GSM/GPS vehicle global positioning framework for better comprehension about vehicle following.

L. Rahunathan (✉) · D. Harish · A. A. Samson · D. Sivabalaselvamani
Department of Computer Applications, Kongu Engineering College, Perundurai, Erode,
Tamilnadu, India

1.1 IoT

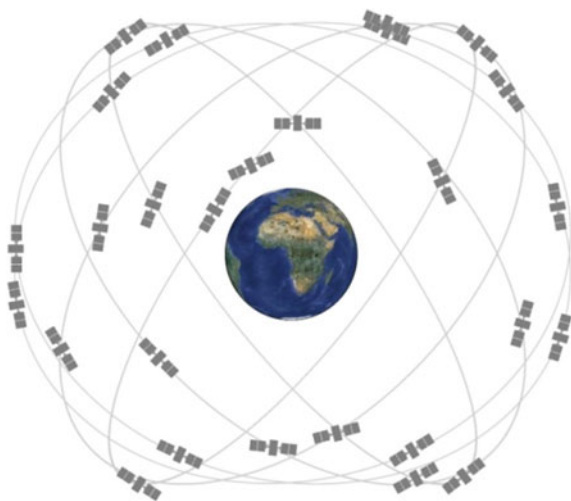
An IoT, or Internet of Things, helps billions of actual web-related devices across the globe to exchange and capture knowledge. It is imaginable to transform something, from anything as small as a pill for anything as large as a mountain to an IoT entity, because of its appearance of insanely the pervasiveness of remote organizations and central processors, Associating and attaching sensors to all these different articles brings a layer of specialized expertise to devices that would normally be idiotic, allowing them to relay continuous data without requiring a human. Through consolidating the advanced and real worlds, the Internet of Things renders the design of our general world more sensitive and more brilliant.

1.2 GPS

The GPS, or the Global Positioning System, world broad route satellite network that provides synchronization of location, time and speed. The Global Positioning System (GPS) is a free assistance that worked and claimed by the U.S. Government and is consistently accessible. GPS is all over. You can discover GPS frameworks in your vehicle, your cell phone and your watch (Fig. 1).

GPS causes you get where you are going, from point A to point B. What is GPS? Peruse this article to become familiar with how it functions, its set of experiences and future advancements. Firstly, At a given point, a sign of timing is transmitted from the GPS satellite. Thusly, a time distinction between the purpose of time clock and GPS time which a GPS beneficiary receives the time sign could be determined to generate the distinction to the satellite from the receiver. With three other open

Fig. 1 GPS satellites.
Copyright 2017 by NASA



satellites, a similar period will be completed. Determining the condition of the GPS receiver from a distance from the GPS collector is determined for three satellites. In any event, the location created by the methods for such a technique is not accurate, since there is an error in the distance calculated between the satellites and the GPS receiver, which is the result of a time error on the clock fused into the GPS collector. A nuclear clock is consolidated for a satellite to obtain data on the spot time, but the time generated by tickers entering GPS beneficiaries is not as precise as the time created on satellites by nuclear timekeepers. Hence, a fourth satellite assume its task and it is possible to use the isolation form of the satellite to a collector to work out the situation in relation to the location information generated by the distance between the 3 satellite and the receiver, thus reducing the space for the precision of give and take on the position.

1.3 Vehicle Tracking System

With its most straightforward definition, a vehicle global positioning framework is the framework that permits following and controlling of vehicles through an online PC, advanced mobile phone, tablet, and so forth on a day in and day out premise on account of GPS satellites. Vehicle global positioning frameworks make it conceivable to have a prompt and history following of vehicle speeds, the courses they followed, halting focuses, sitting occasions on guides furnishing a vault and checkpoint with over a wide span of time reports. Essentially, the vehicle global positioning frameworks work in a circle of GPS, GSM/GPRS, computerized guides and uncommon programming. Versatile information gadgets mounted on vehicles send two snippets of data they get from satellites—constant when the satellite data was sent and position of the satellite in circle at the hour of transmission and communicate telemetric data, for example, temperature to control and correspondence focuses by means of the GSM/GPRS network. Data got as such are then gathered gratitude to unique programming and recorded in a databank on workers. On the client side, vehicles can be followed on their prompt and history records through a PC or a cell phone/tablet by utilizing exceptional programming making it conceivable to picture all data from vehicles and to alter alerts and program statuses of vehicles. This structure shapes the reason for working of the vehicle global positioning frameworks.

2 Literature Review

The LoRa is a Semtech's physical layer (PHY) assurance [1], low power associations and planned for long reach. The development enables the accessibility of shrewd things at range of the solicitation for km, fundamental for Internet of Things networks, with low-energy use. To do the same, LoRa introduces a ludicrous

prohibitive way of distributing guidelines, which should be a variety of chirp spread range (CSS) [2], which changes repeat peep beats without altering the stage between touching images [3], encoded the data [1, 4].

Therefore, LoRa material obtained the resultant sign impenetrable to interference block or near-frequency signals. In addition, LoRa is represented by a decrease in the unpredictability of gear, a decrease in multifaceted existence header size in relation to hops and a propensity to participate in critical two-way correspondence using an unrelated low-energy method. LoRa physical layer switches, Repeat gatherings with unauthorized repetition of Industrial Research and Medical Band in sub GHz radio signals (ISM), To Brazil, a synchronized repeat band for Industrial Science and Medical band (ISM) is somewhere in the 928 and 915 MHz (AU 915 to 928 Megahertz) range, as per the National-Telecommunications-Agency (ANATEL) [5]. Also, a 433 MHz repeat could be executed for channel with very some devices [6]. A couple of limits for plan the LoRa PHY are according to the accompanying: Bandwidth, Spreading Factor, Code-Rate and Carrier repeat. For the transmitting band, the carrier repeat illustrates the middle repeat. It is defined by the area of action of the substance. Thus, as seen by the submission, this cap is usually not portable. The volume of the repeat distance used is defined by information transmission, with 3 programmable characteristics: 125, 250, and 500 kHz. To address a picture, SF chooses the quantity of peeps used [4, 7]. It thus determines the magnitude between the spot rate and also the twitter price. 6 extraordinary characteristics for SF limit are listed in the LoRa detail: Spread factor 7, 8, 9, 10, 11 and 12 [2], which enables even channel to be molded, so that there are no incidents between them along with different SFs. High SF raises the level of the social occasion by restricting the degree of sign power, by extending the relaxing time on air (ToA) and by reducing the association's transmitting movement [8].

Vangelista et al. [9] examine the various technologies of the less Power Large location Network (LoRa) and provide the detailed depiction of the success of LoRa. 2 studies are carried out: (i) The LoRa personal association is formed to monitor the humidity and temperature components of such a structure (19 stories) and (ii) an inspection is carried out in Italy, Padova, causing approximately 2 km length to be covered. A manufacture believes that LoRa-subject radio associations will interface equipment organized by several kilometers.

Gomez et al. [10] consider joining the creation of LoRa in a proposal for vehicular communication. They analyze two situations: I the topography of a vehicle-to-infrastructure and the geology of a vehicle-to-vehicle. The manufacturers research the RSSI levels for SF-7 and SF-12 in the critical circumstances, assuming that SF-12 had a highest level of RSSI, having a wider 10 km radius, higher than SF-7 (6 km). They survey the area covered by a left system inside of the vehicles for the resulting situations, submitting informed warnings. SF-12 appeared at a distance of 6 km, with much more distinct shadow areas and SF-7, which appeared at a distance of 2.5 km. The manufacturers believe that the refined presentations in terms of elimination are preferable to any other cell growth and that the findings of vehicle-to-vehicle limited the spectrum of integration by a stature of an access point collection unit in comparison to the vehicle-to-infrastructure situation.

Mikhaylov et al. [11] offer an examination of the application of the production with LoRa and examine its kindness toward the way of Doppler's. Roedig et al. [12] are using the SimPy system to create a discrete event diversion instrument called LoRa-Sim. This gadget makes a 2-dimensional space for dispensing N centers and M passages. In order to survey the most extraordinary requirements of the end devices in a LoRa interface, each center point is portrayed by transmitting limits unambiguous to LoRa growth.

Haxhibeqiri et al. [13] are operating an NS3 LoRa library that joins a slip-up model used to pick spectrum, analogous to the impedance between separate simultaneous transmissions. The device also enables bi-directional correspondence in addition. The manufacturers claim that it is important to coordinate implementation of the complex limit selection on endpoint contraptions. Similarly, they conclude that the restricted downlink movement amazingly debases the degree of bundle transport; the test could be alleviated by increasing the number of passages. In the LoRa physical layer executed [14] and [13], all SF and the all code values defined there in particular layer are retained.

3 Method

Simulations are done by the simulation model NS3 tool. In [14] that simulates a LoRa framework and physical layers, we add the LoRa publicly available libraries. In such, libraries are tailored for such a research to a specifications of the testing situations suggested. For all this, we reproduce a simulation model where the nodes interact in actual experiments at speeds and distances specified. In the NS3 simulation software, we choose a LoRa physical layer method to replicate a vehicular scenario, with such a prediction method for wide areas. A normal distribution variable is measured to evaluate faded loss of signal, an acceleration attribute of a different setting, in order to incorporate a probabilistic method.

4 GSM/GPS-Based Vehicle Tracking System

4.1 *Arduino Uno*

An Arduino is an open source, programming association and PC gear, attempt, produce microcontroller packs and customer bunch that plans for building modified gadgets and wise article that can identify and control inquiries in reality. The initiation of an Arduino Broadens began at the Institute of Interaction Design in Ivrea, Italy. A Creative Commons Attribution Share appropriates the hardware comparison plans. The device works from 1.8 to 5.5 V. The ATmega 328 is a solitary—microchip in the mega AVR family made by ATmega. The device

achieves bandwidth shifting toward one MIPS per each Megahertz. B. Force Supply AC connectors are utilized with electrical gadgets that require control yet don't contain inside parts to infer the necessary voltage and force from mains power. The inner hardware of an outer force supply is fundamentally the same as the plan that would be utilized for an inherent or interior stock. Outside force supplies are utilized both with hardware with no other wellspring of intensity and with battery-fueled gear, where the stockpile, when connected, can some of the time charge the battery notwithstanding driving the hardware. Utilization of an outside force supply permits transportability of gear fueled either by mains or battery without the additional heft of inner force parts and makes it pointless to deliver hardware for utilizing just with a predefined power source; a similar gadget can be controlled from 120 VAC or 230 VAC mains, vehicle or airplane battery by utilizing an alternate connector. Another bit of leeway of these plans can be expanded wellbeing; since the dangerous 120- or 240-V mains power is changed to a lower, more secure voltage at the divider source and the machine is dealt with by the client.

4.2 *GPS Module*

The GPS stands for Global Positioning System, is a global route satellite architecture focused on space that offers solid region and time data in all temperatures and continuously and everywhere on or near the Planet, when and when at least four GPS satellites are viewed unhindered.

4.3 *GSM Module*

As the world's most commonly used phone invention, GSM, this describes the Worldwide Framework for Phone Lines, regulations. By searching for PDA tower in the surrounding area, PDA uses a wireless assistance transporter GSM network. The GSM module is a SIM 900 Quad-band/SIM 900A Dual-band GPRS/GSM module breakout board and minimum arrangement. By way of AT instructions, it will speak with regulators (GSM 07.07 SIMCOM and 07.05 and improved at a Commands). This module maintains the on and resets power of programming. It has an 850/900/1800/1900 Megahertz quad-band and a 900/1900 Megahertz double band. It has power by way of AT instructions, an exceptionally poor 1.5 mA use of force (rest mode).

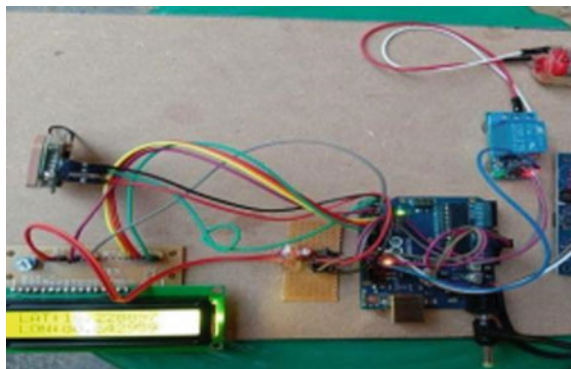
4.4 Relay

The Relay is an electronic switch that closes and opens heavily influenced by another electronic circuit. In the first structure, that switch is operated by an electromagnet to close or open one or several arrangements of contacts. The Relay can monitor a yield circuit of higher force than the information circuit; it very well may be viewed as, from a wide perspective, a type of an electric enhancer.

4.5 Working Principle

The principle expectation of this venture is to discover the specific area of the taken vehicle by burglaries and advise to the concerned authority through a SMS. This GSM-based vehicle burglary control framework recovers the specific area of a vehicle as far as its longitude and scope. This information is taken care of to the Arduino, that is interfaced to a GSM modem. The Arduino recovers the specific area subtleties from the GPS and sends a SMS to the concerned authority over GSM modem. An LCD show is associated with the Arduino for intersection the information got prior to being sent over GSM. This venture will be helpful to individuals to monitor their vehicles. Further, this venture can likewise have the option to stop the start of the vehicle by the proprietor distantly by sending a SMS in robbery circumstances. A bit of leeway of this undertaking is that the proprietor of the vehicle can likewise send back the SMS, which will deactivate the start of the vehicle (Fig. 2).

Fig. 2 Circuit setup from vehicle tracking system using GPS and GSM



5 LoRa-Based Tracking System

5.1 Lora

LoRa (short for long reach) is spreads arrive at rule procedure got from tremble spread reach (CSS) progression. Semtech's LoRa contraptions and removed radio recurrent headway is a long reach, low force distant stage that has become the recognized advancement for Internet of Things (IoT) networks all over. LoRa contraptions and the open LoRa show connect sharp IoT applications that settle no doubt the best inconveniences confronting earth: energy the board, brand name asset decay, contamination control, foundation productivity, disaster avoidance and the sky is the limit starting there. A few hundred recognized use cases for sharp metropolitan organizations, sharp homes and structures, mind-blowing growth, wise metering, impressive stock association and joint efforts have been amassed by Semtech's LoRa contraptions and the LoRa display, and the sky is the limit from there more than 167 million gadgets related with networks in 99 nations and making, LoRa gadgets are making a Smarter Planet, Which consolidated super low force utilization with a powerful long-range. Semtech's utilized on the intensity of the network through a consortium and changed the innovation into one of the critical drivers of the ebb and flow wave of computerized change being initiated by IoT. Utilizing LoRa innovation, gadgets can commonly convey over a scope of 13–20 km with the capacity to go similarly as 80 km in certain Line-of-sight arrangements, and to the extent a few 100 s of KM from space as shown by FOSSAT and Lacuna. This reach is accomplished at an extremely low force which makes LoRa more reasonable than other correspondence conventions, for distant, battery-controlled IoT gadgets that are relied upon to run for quite a long time (or years) on a solitary battery charge. Peer to Peer communication permits two gadgets with LoRa radios to converse with one another in a way like how two Bluetooth gadgets impart, with the significant distinction being the way that the reach increments enormously and less force is burned through (Table 1).

To identify a symbol length [16], which is really the time required to submit two SF chips at a chip value. It is distinguished by:

$$Ts = 2 \frac{SF}{BW}, \quad \text{with } SF \in \{7 - 12\}. \quad (1)$$

The length of a preamble is calculated by:

$$Tp = (np + 4.25) \times Ts. \quad (2)$$

Table 1 Comparison with related simulation versus experimental paper works

Reference papers	Analysis types		Scenarios	Metrics
	Experiment	Simulation		
[9]	Yes	No	Wide area	Coverage
[10]	Yes	No	Vehicular	To the end packet rate of loss
[15]	Yes	No	Vehicular indoor walking	To the end delay packet rate of rate
[12]	Yes	Yes	Large size	Package quality of receipt Level of extracting data
[11]	Yes	No	Vehicular boat analytical rotation analysis	Success ratio for the packet Coverage doppler impact of the RSSI standard
[14]	No	Yes	City sides	The ratio of packet distribution Limitation of service period Success of packet Likelihood Coverage
[13]	No	Yes	Fixed location	Analysis of scalability Ratio for packet distribution

The count of signs in the header and payload is calculated by:

$$\text{payloadSymbNb} = 8 + \max\left(\frac{8PL - 4SF + 28 + 16 - 20H}{4(SF - 2DE)}(CR + 4), 0\right). \quad (3)$$

The amount of payload signs multiplies by the time interval equals the payload length. It is distinguished by:

$$T_{\text{payload}} = \text{payloadSymbNb} \times T_s. \quad (4)$$

The packet length is calculated by:

$$T_{\text{packet}} = T_{\text{preamble}} + T_{\text{payload}}. \quad (5)$$

For a Band Width = 500 kHz and Coding Rate = 4/5, Table 2 displays the possible Time on air values of different SFs. These estimated results are being used to evaluate the receiving time period between successive packets, allowing the vehicle's situational perception and environment to be measured. In an attempt to create the conditions for programs that use LoRa and communications technology, we equate these factors to experimentally collected values.

Table 2 Theoretical data rate of Lora and time on air

Spread factor	Time on air (ms)
SpreadFactor 7	24.104
SpreadFactor 8	42.087
SpreadFactor 9	78.056
SpreadFactor 10	134.632
SpreadFactor 11	268.264
SpreadFactor 12	494.568

5.2 NS3 Simulator

The simulations were performed using version 3.28 of the NS3 simulator software. We use the LoRa open source libraries, which replicate the LoRa network and physical frameworks and can be found in [14]. This library has been updated to satisfy the needs of the theoretical conditions suggested in this report. To accomplish this, we created a simulation environment in which the modules interact at predetermined speeds and distances based on experimental findings. In order to explain the actions of the vehicular touch interaction in a virtual environment, it is critical to choose a transmission model that closely matches the real-world scenario. It shows how electromagnetic waves behave and travel from a transmitter to a receiver. Long-distance transmission is the transmission type that best suits the condition selected for research. This technique is commonly used in large situations and communications to sub-gigahertz radio frequency networks. Finally, Eq. (6) predicts signal attenuation that is equivalent to real-world results using signal strength and distance as variables.

$$PL(d) = PL(do) + 10n\text{Log}(ddo). \quad (6)$$

We used an irregular standard normal attribute to classify the damages suffered by the vanishing problem because Log Distance is a typical problem as a result, and Eq. (7) is used in the simulation analysis for going to compare simulated and real experimentation:

$$PL(d) = PL(do) + 10n\text{Log}(ddo) + X\sigma. \quad (7)$$

6 Experimentation Results

6.1 Efficiency Analyzing with Experimental Results

A RSSI amount is seen in Fig. 3. When the vehicle is moving, signal intensity with all spread factors is comparable with just an RSSI amount ranging from 120

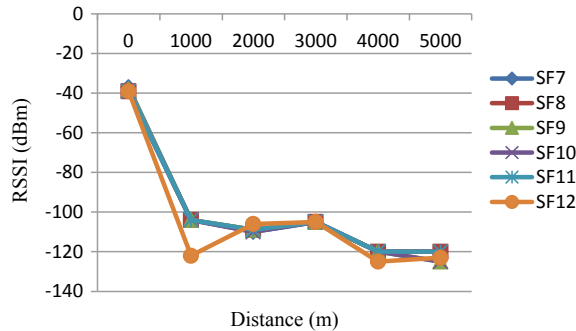


Fig. 3 The grade of RSSI acquired in the receiving unit using various SF for the highest communication range scenario

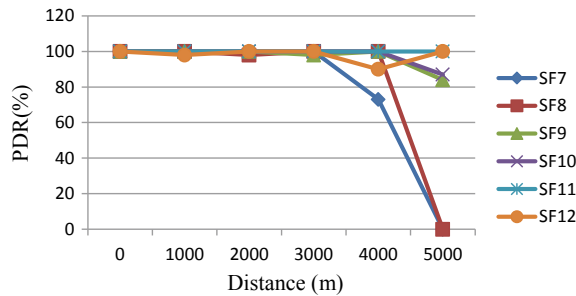


Fig. 4 The PDR acquired in the receiving unit using various SF for the highest communication range scenario

decibel-milliwatts for the actual demonstration to 110 decibel-milliwatts for the virtual demonstration at 5000 m.

A PIR period as in versatility case is depicted in Fig. 4. We described few minor time differences among frequencies that aren't important; however, this time reaction could be useful in defining contact connection outages.

A PDR measured at each stage recorded mostly by Geo location as in system impedance is shown in Fig. 5. This is clear to see that spread factor 7 to spread factor 12 have a similar behavior and after template, with such a PDR of more than 90% with both rates.

7 Conclusion

In general, cellular and Internet-based vehicle tracking is used. However, vehicle tracking allowed by the Internet and cellular does not fall into this category in off-limits areas. In this work, in these non-cellular and non-Internet environments,

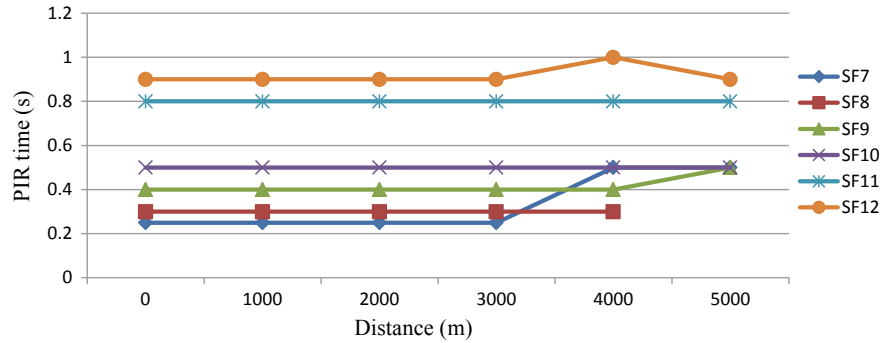


Fig. 5 The PIR time acquired in the receiving unit using various SF for the highest communication range scenario

we lead a demonstration evaluation analysis using LoRa innovation in vehicle tracking. The aim of the research is to see if LoRa can replicate a real-world environment and if it can copy a real-world vehicular correspondence. This experiment used a formulation that was suitable for wide regions, and then a regular odd variable was tested to look at transmission fading errors, which are typical in LoRa platforms. We investigate a situation to investigate the effects of range, speed rate and spread factor-(SF) on messaging, gathering information for the simulated studies to evaluate and differentiate RSSI scale, and PIR timing factors. Be that as it may, utilizing LoRa we can follow a vehicle in restricted distance itself. Finally, we conclude that in the future the distance will be increased with the assistance of forthcoming innovations.

8 Future Work

To make that product function as a real-world monitoring system, certain modifications must be made. According to interference from local structures such as homes, trees and hills, devices may not always accept the exact direction of a signal. The transmitter throughput determines its capacity to implement this concept. The performance is best when the throughput is high, and vice-versa. To perform simulation work, the LoRa physical model applied in NS3 emulator has been used. We prove that the LoRa-based vehicle monitoring system is effectively executed without the Internet with the restricted range region by the outcome of our analysis report. Although this is not appropriate for the condition and challenges that are coming up. We would try to expand the range of this approach with the use of future technologies in functionality.

References

1. LoRaalliance technology, LoRa Alliance: Available in online: <https://www.lora-alliance.org/technology>. Last accessed by November 2020 (2016)
2. Lora modulation basics by Semtech Corp.: Available in online: <https://www.semtech.com/uploads/documents>. Last accessed by November 2020 (2015)
3. Gorce, J.-M., Goursaud, C.: Dedicated networks for IoT: PHY/MAC state of the art and challenges. *EAI Endorsed Trans. Internet Things* (2015)
4. Roedig, U., Bor, M., Vidler, J.: LoRa for the internet of things. In: *International-Conference-on-Embedded-Wireless-Systems-and-Networks (EWSN)* (2016)
5. Radio-frequency-bands-usable by restricted-radiation-equipment in ANATEL: <http://www.anatel.gov.br/legislacao/resolucoes/2018>. Last accessed by November 2020 (2018)
6. Frequency-assignment, attribution and destination plan on Brazil by ANATEL: <http://www.anatel.gov.br/institucional/acervo-documental>. Last accessed by November 2020 (2016)
7. LoRa modem designer's guide by Semtech Corp.: Availability oninternet: <https://www.semtech.com/uploads/documents>. Last accessed by November 2020 (2013)
8. Sooriyabandara, M., Raza, U., Kulkarni, P.: Low power wide area networks: an overview. *IEEE Commun. Surv. Tutor.* **19**(2) (2017)
9. Vangelista, L., Centenaro, M., Zorzi, M., Zanella, A.: Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* (2016)
10. Gomez, J.S., Gomez-Skarmeta, A.F., Sanchez-Iborra, R., Santa, J., Fernandez, P.J.: Integrating LP WAN Communications Within the Vehicular Ecosystem (2017)
11. Mikhaylov, K., Petajajarvi, J., Pettissalo, M., Iinatti, J., Janhunen, J.: Performance of a low-power wide-area network based on LoRa technology. *Doppler Robustness, Scalability, and Coverage* (2017)
12. Roedig, U., Alonso, J.M., Bor, M.C., Voigt, T.: Do LoRa low-power wide-area networks scale? In: *Analysis and Simulation of Wireless and Mobile Systems of ACM International Conference on Modeling, (MSWiM)* (2016)
13. Haxhibeqiri, J., Van den Abeele, F., Hoebeke, J., Moerman, I.: Scalability analysis of large-scale LoRaWAN networks in NS-3. *IEEE Internet Things* (2017)
14. Centenaro, M., Magrin, D., Vangelista, L.: Performance evaluation of LoRa networks in a smart city scenario. *IEEE International Conference on Communications (ICC)* (2017)
15. Won, M., Patel, D.: Experimental study on low power wide area networks (LPWAN) for mobile internet of things. In: *IEEE 85th Vehicular-Technology-Conference* (2017)
16. Antoine-Santoni, T., Gualtieri, J.-S., Manicacci, F.-M., Aiello, A.: AMBLoRa: a wireless tracking and sensor system using long range communication to monitor animal behavior. In: *SMART: The Seventh International Conference on Smart Cities, Systems, Devices and Technologies* (2018)

Evaluation and Transformation Analysis of the Mithi River



Saumya Deshmukh, Shrishti Karkera, Prachi Rawale,
and Chhaya Narvekar

Abstract Excessive enrichment of nutrients can cause any water body to undergo eutrophication, thus damaging the water body and sometimes making it completely unusable and futile. Further, anthropogenic activities lead to cultural/accelerated eutrophication that becomes native to several species of algae including cyanobacteria and cyanotoxins causing algal blooms, organic pollution caused due to organic and inorganic waste, etc. Monitoring of the river and lakes for such phenomena using satellite images has become increasingly popular to understand the trends and patterns in order to further protect the environment. The Mithi River in Mumbai that travels 17.84 km from the Vihar Lake to the Mahim Bay has been studied in this paper using multispectral satellite images and remote sensing to understand the different processes that take place due to human and biological factors which degrade the river. Chlorophyll-a (vegetation index), chemical oxygen demand (COD) and biological oxygen demand (BOD) are the parameters that we have taken into consideration to measure the water quality index at eleven different predefined points (Table 1). Sentinel 2A multispectral images have been used to study the parameters along the stretch of the river by applying cloud masks to eliminate the cloud and the cloud shadow effects on the image collection.

Keywords Eutrophication · Biological oxygen demand · Chemical oxygen · Demand · Remote sensing · Sentinel 2 MSI

1 Introduction

Water is the necessity for all life on earth. Hence, not just water, but clean water should be available for all and it is our responsibility to keep such resources clean and safe. Mithi river situated on the island of Mumbai city is formed by the convergence of the tail water discharges from the Powai and Vihar lakes and is a

S. Deshmukh (✉) · S. Karkera · P. Rawale · C. Narvekar
Xavier Institute of Engineering, Mumbai, India
e-mail: chhaya.n@xavier.ac.in

seasonal river by nature which rises and overflows during monsoon [1]. It is a 17.84 kms stretch which is subjected to various illegal activities such as washing of cattle shed, vessels, oil/chemical drums, dumping of solid waste by the slums living along the stretches of the river, several drainage systems released into the river [2]. The pollution caused due to this is to a scale where the river can no longer be used which makes it futile. Many restoration projects are established to revive the river. The paper focuses on analyzing and studying the vegetation index (Chlorophyll a), the BOD and the COD index across the stretch using sentinel-2 satellite data.

2 Background

Remote sensing is the procurement of information about a geographical phenomenon or object without physically attending it or making any physical contact with it, remotely and thus, sensing it remotely by detecting and monitoring its physical characteristics by using satellites for measuring the reflected and emitted radiation from a distance [3, 4]. The image collection bands that are obtained by the remote sensing mechanism vary from satellite to satellite which depends on the sensor system (hyperspectral, multispectral, radar, etc.). These bands are used to obtain different perspectives of the same image and can be convoluted with the help of algorithms, formulas, expressions in order to analyze and study the area under observation. Sentinel 2 MSI image dataset which has a multispectral sensor system comprising of 13 bands is used for the purpose [5]. The different resolutions available are 10, 20 and 60 m according to the band. The river can be analyzed on various parameters like TSS, pH, etc. The parameters that are focused and analyzed in this paper are Chlorophyll-a (vegetation index), BOD and COD.

3 Data and Research Area

Since the river originates at an altitude of 246 m above sea level in the hills located in the east of the Sanjay Gandhi National Park, it gathers water from the streams and spillway discharges of the Tulsi, Vihar and Powai Lakes to the Mahim bay (Figs. 1 and 2).

Fig. 1 Mithi River flow across Mumbai



Fig. 2 Mithi River vicinity



The table demonstrates the division of the study area into eleven zones or regions [6] which helps in analyzing the stretch and study individual areas (Fig. 3 and Table 1).

Algal blooms are essential in photosynthesis; hence, it is directly related to Chl-a concentration [7]. Trophic state of the water body is predicted by Chl-a. Chl-a takes up most of its energy from wavelengths of violet-blue and orange-red light due to which the reflectance of Chlorophyll appears to be green. The spectrum absorption was then extended by the addition of Chl-b. Chl-a’s dispersion-absorption characteristics include heavy absorption between 450–475 nm (blue) and 670 nm (red) and reflectance peaks at 550 nm (green) and near 700 nm (NIR). A variety of algorithms

Fig. 3 Blue placemarks denote zones corresponding to the ones in Table 1



Table 1 Division of Mithi River into 11 zones

Zone	Description
1	Mithi River meeting the sea (Estuary)
2	Convergence of River Mithi with Vakola nalla
3	Slums and zopad
4	Small scale commercial units and few illegal residents
5	Airport area
6	Commercial area with industries and hotels
7	Resident area with few industries
8	Residential area with both structured and unstructured houses
9	Open area with natural vegetation
10	Slum area with few industries
11	Natural vegetation

to recover Chl-a in turbid waters were developed using the reflectance peak near 700 nm and its ratio to reflectance at 670 nm [8, 9].

The biological oxygen demand can be defined as the amount of oxygen consumed by micro-organisms like bacteria, to decompose the organic matter at a specific temperature under aerobic (rich in oxygen) conditions [10]. BOD is not an optically active component, and hence, an accurate and precise system is required to calculate BOD using satellite imagery [11, 12]. The paper [13] proposes a system which uses Landsat satellite images using National Sanitation Foundation Water Quality Index (NSFWQI) to analyze the pollution status of water body. The NSFWQI equation is

$$\text{NSFWQI} = \sum_{i=1}^P w_i I_i \quad (1)$$

wherein I_i is the sub-index for the i th water quality parameter, w_i is the weight associated with the i th water quality parameter p is the number of water quality parameters. The sub-index equations used for BOD are

$$I = 96.67 - 7 * \text{BOD} \quad (\text{for the range } 0\text{--}10) \quad (2)$$

$$I = 38.9 - 1.23 * \text{BOD} \quad (\text{for the range } 10\text{--}30) \quad (3)$$

The regression equations used for the prediction of NSFWQI, pH, DO, BOD and FC from radiance values from green, red, NIR and SWIR bands of satellite imagery were developed. For the regression model, radiance of satellite imagery is used as independent variables, and one of the above parameters is used as dependent variable. SPSS software is used to form different linear regression equations to find the most accurate one for each parameter. The best equation for BOD is the multiple regression equation formed by the radiance in red and SWIR bands. The equation is as follows

$$\text{BOD} = 32.465 - 11.923 * \text{Rr} + 3.799 * \text{Rm} \quad (4)$$

The conc. of BOD in mg/l, Rr—Radiance in red band, Rm—Radiance in MIR band.

The chemical oxygen demand (COD) index is used to understand the organic pollution of a water body. The measurement of COD can be done using CODCr (potassium dichromate oxidation) and CODMn (potassium permanganate index). CODCr is mainly for the wastewater from the industries and sewage monitoring which is a very time-consuming process. Hence, CODMn is used in order to measure the organic pollution of rivers, lakes, surface water, drinking water and reservoirs [14, 15]. Huang et al. [16] establish a method to measure the COD index with Landsat TM bands 1, 2, 3 and 4. Paper [17] uses the method in Wang and Ma [18] to estimate the CODMn index of Lake Dongting with Landsat TM bands 2 and 3 as shown below:

$$\text{CODMn} = e(0.3671 + 1.2454 * \ln(\text{TM2}/\text{TM3})) \quad (5)$$

where CODMn is the potassium permanganate index, TM2 and TM3 are the Landsat multispectral bands 2 and 3. The formula is further modified with respect to sentinel 2 bands and is used to estimate the COD index in the Mithi River.

4 Methodology

Chlorophyll-a is one of important components of the algae. Chlorophyll-a is an important parameter for reflecting the eutrophication degree. Due to this, it can determine spectral reflectance properties of water. If the concentration of Chlorophyll-a in an area is lower, it also has a lower value of trophic state index. If the concentration of Chlorophyll-a in an area is higher, it also has a higher value of trophic state index [19].

$$\text{Chlorophyll-a } \mu\text{g/L} = ((\text{B5} + \text{B6})/\text{B4}) \quad (6)$$

where B4, B5, B6 are bands in Sentinel-2A [20].

The BOD test involves the standard oxidation (or incubation) for a period of 5 days at 20 °C. At times where time isn't a constraint and highest accuracy is preferred, the test can go up to 20 days. BOD testing includes two stages—the first is carbonaceous stage where the oxygen demand is involved in the conversion of carbon-to-carbon dioxide and the second is nitrogenous stage where organic nitrogen, ammonia and nitrite are converted to nitrate [21]. BOD of water using remote sensing is calculated using the formula from [13] with suitable modifications, as shown below

$$\text{BOD} = (32.465 - 11.923 * \text{Rr} + 3.799 * \text{Rs})/100 \quad (7)$$

The bands selected Rr and Rs are the bands B4 (664.5 nm, 10 m) and B12 (2202.4 nm, 20 m), respectively, of sentinel 2. The original formula is derived for Landsat satellite. The required modification involves reflectance instead of spectral radiance and normalizing the data by 1000 to get the appropriate results.

The COD test involves potassium permanganate in this case since it is a strong chemical oxidizing agent. It is then used to oxidize the sample taken under the conditions of heat and strong acid. As mentioned above, the formula being used to determine the COD index is the same [17] with a slight variation since the equation should correspond to the Sentinel-2 bands:

$$\text{CODMn} = (e(0.3671 + 1.2454 * \ln(\text{B3}/\text{B4})) * 100) \quad (8)$$

where CODMn is the potassium permanganate index (Mg/L), B3 and B4 are the bands in Sentinel-2 MSI, i.e., green Band (560 nm-S2A) and the red Band (664.5 nm-S2A), respectively.

5 Results and Analysis

5.1 Preprocessing of Satellite Images

Function to mask clouds using sentinel-2A QA band: The image shows the GUI of earth engine code editor using cloud mask in order to eliminate the effects produced by the cloud [22, 23]. The filters applied are the area bound and time series. The image collection shows the 54 images that are valid as per the parameters (Figs. 4 and 5).

```
function maskS2clouds(image) {
  var qa = image.select('QA60');

  // Bits 10 and 11 are clouds and cirrus, respectively.
  var cloudBitMask = 1 << 10;
  var cirrusBitMask = 1 << 11;

  // Both flags should be set to zero, indicating clear conditions.
  var mask = qa.bitwiseAnd(cloudBitMask).eq(0)
    .and(qa.bitwiseAnd(cirrusBitMask).eq(0));

  return image.updateMask(mask).divide(10000);
}

var dataset = ee.ImageCollection('COPERNICUS/S2_SR')
  .filterDate('2020-01-01', '2020-01-30')
  // Pre-filter to get less cloudy granules.
  .filter(ee.Filter.lt('CLOUDY_PIXEL_PERCENTAGE', 20))
  .map(maskS2clouds);

var visualization = {
  min: 0.0,
  max: 0.3,
  bands: ['B1', 'B3', 'B8'],
};

Map.setCenter(83.277, 17.7009, 12);
```

Fig. 4 Snip of code for preprocessing

```
import ee from 'ee4j';
var geometry = ee.Geometry.Rectangle([83.277, 17.7009, 83.277, 17.7009]);
var qa = image.select('QA60');

// Bits 10 and 11 are clouds and cirrus, respectively.
var cloudBitMask = 1 << 10;
var cirrusBitMask = 1 << 11;

// Both flags should be set to zero, indicating clear conditions.
var mask = qa.bitwiseAnd(cloudBitMask).eq(0)
  .and(qa.bitwiseAnd(cirrusBitMask).eq(0));

return image.updateMask(mask).divide(10000);

// Map the function over the granules and take the median.
var dataset = ee.ImageCollection('COPERNICUS/S2_SR')
  .filterDate('2020-01-01', '2020-01-30')
  .filter(ee.Filter.lt('CLOUDY_PIXEL_PERCENTAGE', 20))
  .map(maskS2clouds);

var viz = {
  min: 0.0,
  max: 0.3,
  bands: ['B1', 'B3', 'B8']
};

Map.setCenter(83.277, 17.7009, 12);
Map.addLayer(dataset.median().viz(viz));
```

Inspector Console Tasks

Use print(...) to write to this console.

* ImageCollection COPERNICUS/S2 (54 elements) 250M

type: ImageCollection

id: COPERNICUS/S2

version: 1606926331397205

bands: []

features: list (54 elements)

properties: object (20 properties)

Fig. 5 Image collection with band, features and properties of the image

5.2 Chlorophyll-a

Figure 7 shows us the zone wise distribution of Chlorophyll-a during year 2018 to year 2020. In zone 1 and 10, the value is increasing. In zone 2, 4, 8, the value has increased from 2018 to 2019 then decreased in 2020. In zone 3, the value is almost equal in 2018 and 2020 but decreased in 2019. In zone 6, the value is decreasing. In zone 5 and 11, the value is decreasing in 2018 to 2019 then increasing again in 2020. In zone 7, there is a sudden increase in value from 2019 to 2020. In zone 9, there is a sudden decrease in value from 2019 to 2020 (Figs. 6 and 8).

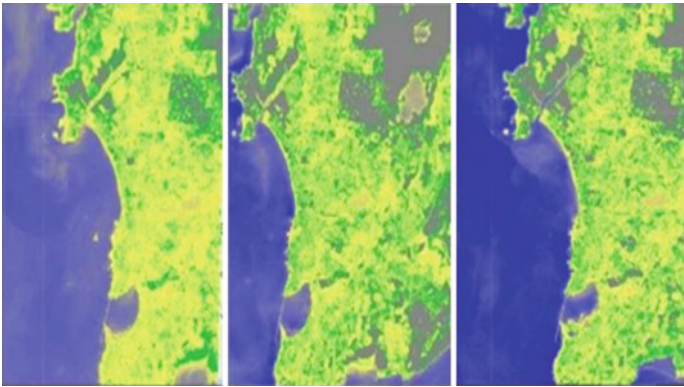


Fig. 6 Chl-a observed in December 2018, 2019 and 2020

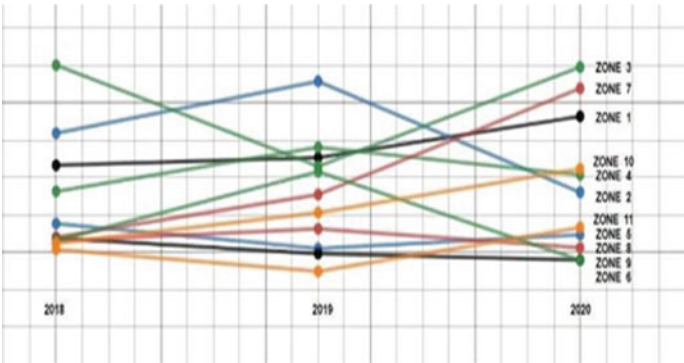


Fig. 7 A graph showing Chlorophyll-a trends from year 2018 to 2020 for all 11 zones

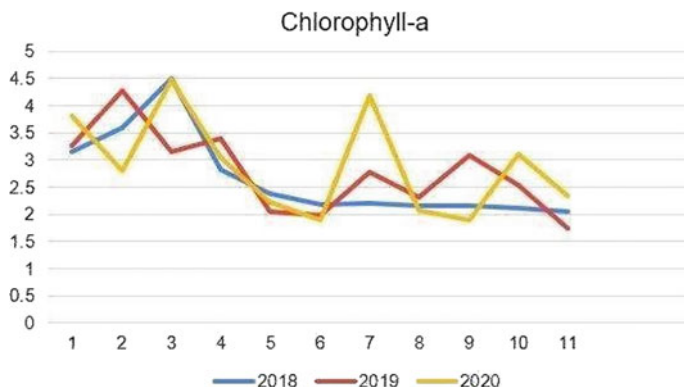


Fig. 8 A graph showing Chlorophyll-a trends from year 2018 to 2020

5.3 Biological Oxygen Demand

Equation (4) is originally derived for Landsat satellite. It is converted for sentinel 2 bands which use reflectance without atmospheric correction Eq. (7) instead of spectral radiance. Thus, the value obtained is negative. The negative sign of the value is irrelevant for the study. After normalization, the BOD obtained is approximately 1.5–8 mg/l which concludes that the water in River Mithi is highly contaminated and unsuitable for living organisms. The concentration of BOD also varies in different zones. BOD is more where toward the lower part and less near the origin (Fig. 9).

Figure 10 resembles a ‘Inverted V’ structure, indicating that the BOD values were high in the year 2019 and lower in the year 2018 and 2020. This trend can be seen clearly in zone 1, 2, 3, 4, 5, 6, 7, 9 and 11. There is a regular increment in the value of BOD over the years in the zone 8 and 10. However, on comparing the values of BOD in the year 2018 and 2020, it is evident that the BOD has increased in all the zones with gradual increase in few zones and steep increase in other zones (Fig. 11).

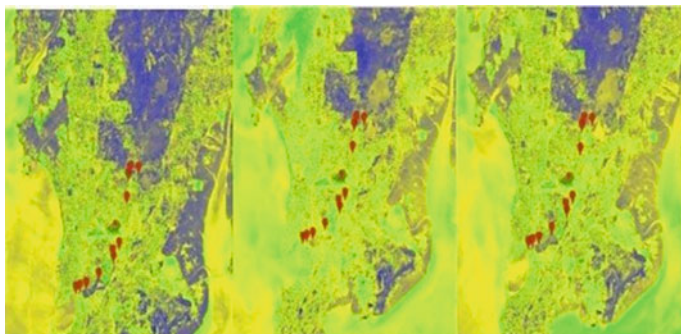


Fig. 9 BOD of 11 zones in December 2018, 2019 and 2020

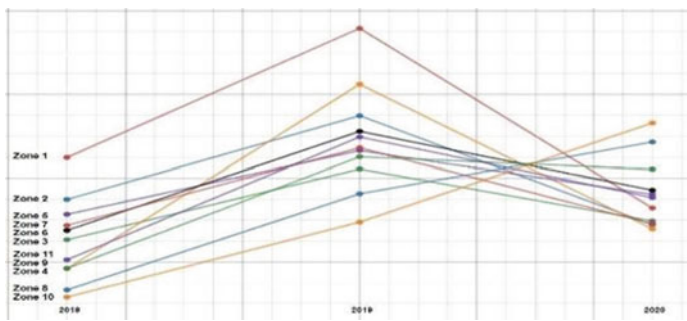


Fig. 10 A graph showing BOD trends from year 2018 to 2020 for all 11 zones



Fig. 11 Zonal trends in BOD for year 2018, 2019 and 2020

5.4 Chemical Oxygen Demand

Equation (5) was originally used in [17] for Landsat ETM and is converted for Sentinel-2 MSI surface reflectance in Eq. (8) in the paper to produce the COD index of Dec 2018, 2019 and 2020, respectively, as shown below. In the Inspector window, the COD index value in each position can be found out. A collection of such values will be helpful to further find patterns and to estimate future values of COD index using machine learning algorithms (Figs. 12 and 13).

The COD values are further plotted to analyze from 2018 to 2020. The trends help us understand and further study the real reasons behind the food or bad practices which would make us aware of the consequences (Fig. 14).

Figure 15 is a zone wise distribution of COD index from 2018 to 2020. There is a clear trend in zones 1, 2, 4, 5, 7, 9, 10, 11. The COD values in these zones were lower in 2019 than in 2018 and rose again in the year 2020 due to which there is a valley shape in the graph of these zones. Zones 6 and 8 have their COD values higher in 2018 as compared to 2019 and 2020. The values decreased in 2019 and further in 2020 as well. Zone 3 has a very unique trend where in the COD value in the year 2018 was lower than in 2019, which further increased in 2020. In majority

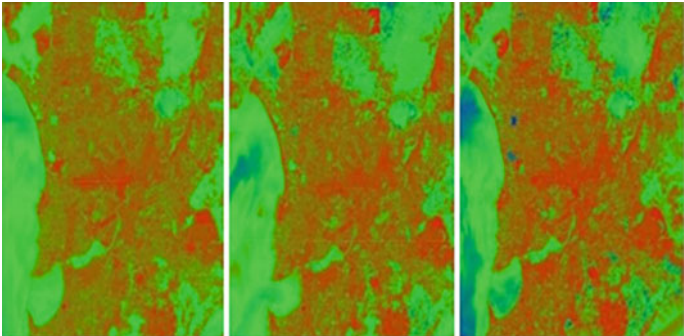


Fig. 12 COD observed as per sentinel-2 in Dec 2018, 2019 and 2020

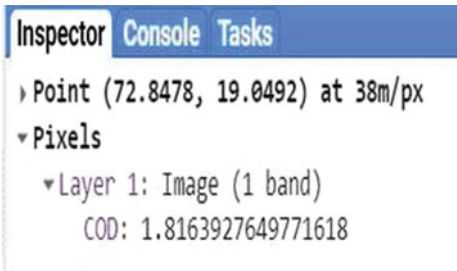


Fig. 13 COD between the zones 2 and 3

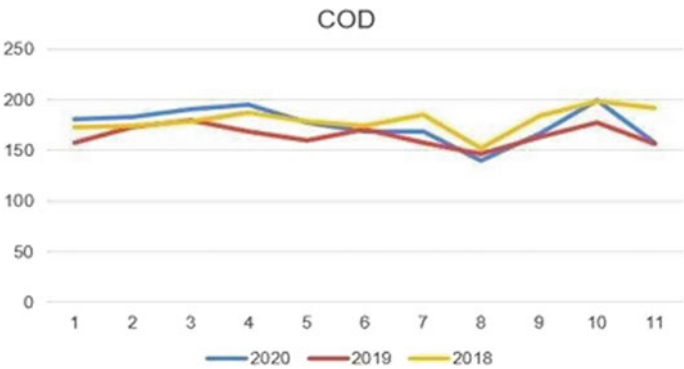


Fig. 14 COD variation of 3 years

of the cases, COD values have increased dramatically in the year 2020. Zonal analysis and surveys let us the different possible reasons due to which this has happened, which further lets us understand the problem and amend our practices.

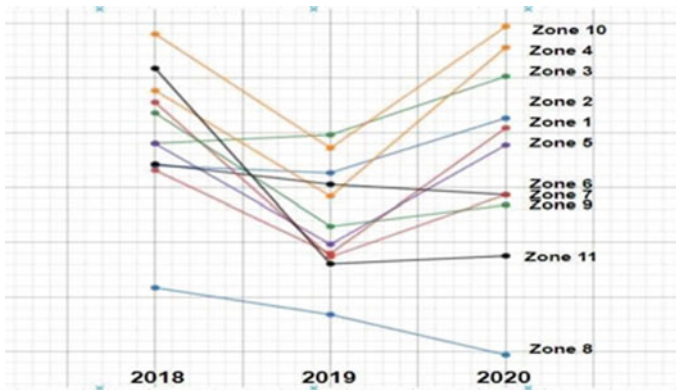


Fig. 15 Zone wise distribution of COD

6 Conclusion

From the graph, we can say that there are different trends in different zones for Chlorophyll-a value. In most of the areas, value is increasing from 2018 to 2019. In some areas, there is a sudden drop in 2020. However, this is not same in the case of BOD. From the analysis done, we can say that the trends in BOD show an overall increase. The BOD was lower in 2018 as compared to 2019 but has decreased again in 2020. Based on the data obtained and algorithms applied, COD index has mostly decreased from 2018 to 2019 and then increased again from 2019 to 2020.

7 Future Scope

Data from the eleven zones will be divided into training data and testing data. Using training data multiple regression analysis will be carried out to determine the model coefficient [24].

$$WQI = a + b * x1 + c * x2 + d * x3 \quad (9)$$

where $x1$ -BOD, $x2$ -COD, $x3$ -Chlorophyll-a.

Further, parameters can be added like TSS [25], SDT, turbidity, etc., which will be combined with the current parameters to improve the WQI [24]. Then, based on the final WQI results, specific regions can be analyzed- the industries, the various activities can be carefully placated for the betterment of that region.

References

1. https://en.wikipedia.org/wiki/Mithi_River
2. <https://www.thehindu.com/news/cities/mumbai/how-the-mithi-was-destroyed/article26298525.ece>
3. <https://www.usgs.gov/faqs/what-remote-sensing-and-what-it-used>
4. https://en.wikipedia.org/wiki/Remote_sensing#:~:text=Remote%20sensing%20is%20the%20acquisition,acquiring%20information%20about%20the%20Earth
5. <https://developers.google.com/earth-engine/datasets/catalog/sentinel-2>
6. Comprehensive study/profiling of Mithi River: Report by Maharashtra Pollution Control Board (2014)
7. <https://www.soft.farm/en/blog/vegetation-indices-ndvi-evi-gndvi-cvi-true-color-140>
8. Gholizadeh, M.H., Melesse, A.M., Reddi, L.: A Comprehensive Review on Water Quality Parameters Estimation Using Remote Sensing Techniques. <https://doi.org/10.3390/s16081298>
9. Gitelson, A.: The peak near 700 nm on radiance spectra of algae and water: relationships of its magnitude and position with chlorophyll concentration. *Int J Remote Sens* **13**, 3367–3373 (1992). <https://doi.org/10.1080/01431169208904125>
10. https://www.usgs.gov/special-topic/water-science-school/science/biological-oxygen-demand-bod-and-water?qt-science_center_objects=0#qt-science_center_objects
11. Ansper, A., Alikas, K.: Retrieval of Chlorophyll a from Sentinel-2 MSI Data for the European Union Water Framework Directive Reporting Purposes. <https://doi.org/10.3390/rs11010064>
12. https://www.researchgate.net/post/What_is_the_relationship_between_the_COD_and_BOD_values_in_Waste_water#:~:text=COD%20or%20Chemical%20Oxygen%20Demand,present%20in%20water%20%2F%20waste%20water
13. Sheela, A.M., Letha, J., Joseph, S., Ramachandran, K.K., Justus, J.: Assessment of pollution status of a Coastal Lake system using satellite imagery. *J. Remote Sens. GIS*. <https://doi.org/10.4172/2169-0049.1000110>
14. Lv, J.J., Yang, H., Chen, J., Gao, L., Xu, X.F., Liu, Z.Q.: China. *Environ. Sci.* **24**, 307–310 (2004)
15. Yan, Z., Xie, Z.W., Zhou, N., Feng, L., Dan, D.Z.: *Chem. Res. Appl.* **18**, 455–458 (2006)
16. Huang, M.F., Qi, X.P., Yu, W.Y., Zhang, Y.M.: *Arid. Land. Geog.* **29**, 885–893 (2006)
17. Yang, B., Liu, Y., Ou, F., Yuan, M.: Temporal and spatial analysis of COD concentration in East Dongting Lake by using of remotely sensed data. In: 3rd International Conference on Environmental Science and Information Application Technology (2011). <https://doi.org/10.1016/j.proenv.2011.09.420>
18. Wang, X.J.: *T. Ma. Environ. Sci* **11**, 65–68 (2000)
19. Zeng, N., Liu, Z., Miao, Z., Wei, Y.: Design and implementation of Chlorophyll a and eutrophication remote sensing monitoring system based on ArcGIS Engine. <https://doi.org/10.1109/ETTandGRS.2008.254>
20. Kaymaz, Ş.M., Ates, E.: Estimating Chlorophyll-A Concentration using Remote Sensing Techniques. <https://doi.org/10.19080/ARR.2018.04.555633>
21. <https://www.envexp.com/labmatters/236-understanding-biochemical-oxygen-demand-bod>
22. <https://developers.google.com/earth-engine/tutorials/community/sentinel-2-s2cloudless>
23. https://developers.google.com/earth-engine/tutorials/tutorial_global_surface_water_01
24. Erhan Alparslan, H., Coskun, G., Alganci, U.: Water Quality Determination of Küçükçekmece Lake, Turkey by Using Multispectral Satellite Data. <https://doi.org/10.1100/tsw.2009.135>
25. Topliss, B.J., Almos, C.L.: *Int. J. Remote Sens.* **11**, 947–966 (1990)

Human-Sensing Technologies for Business Solutions



Rajeev Tiwari[✉], Kamal Kumar, Satyam Kumar, and Shelly[✉]

Abstract Detection of human presence can be used for intelligently switching on and off devices. This will save a lot of electricity as well as help in building an intuitive experience for smart homeowners. In the future, technologies like artificial intelligence may also benefit from this information by taking smart decisions and providing more contextual responses. One can find many research proposals and commercial products for efficiently counting humans. However, these systems are very costly, extremely difficult to install, and many a time obstructs people. It is the reason why they have still not made it to residential homes yet. In this paper, we have discussed some of the most cutting-edge technologies that can be used for sensing humans. We analyze them based on six factors and determine how economic and easy to deploy they are. Some of the solutions deliver promising results and have the potential of becoming a mass-market product.

Keywords Human counting · Person detection · Sensing · Noise · Environment

1 Introduction

The smart home market is expected to be doubled by the year 2024 [1]. Detection of human presence is something that is still missing from the category of smart electronic devices being sold. There have been studies that recorded a 25% reduction in energy consumption [2] when HVAC systems are efficiently managed. It must be noted that the calculation of the number of people in individual rooms and commercial offices is a crucial factor for efficiently managing HVAC systems. Another study in the United States of America found that around 40% of energy is

R. Tiwari · Shelly (✉)

Department of Virtualization, University of Petroleum and Energy Studies, Dehradun, India

e-mail: shelly@ddn.upes.ac.in

K. Kumar · S. Kumar

National Institute of Technology, Srinagar, Uttarakhand, India

e-mail: kamalkumar@nituk.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

513

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,

Lecture Notes on Data Engineering and Communications Technologies 73,

https://doi.org/10.1007/978-981-16-3961-6_42

wasted by residential homes and commercial buildings [3]. Room occupancy can be used for safety purposes. It will open new opportunities for building futuristic experiences by making artificial intelligence-powered agents more aware of the context.

Many researchers have tried to use various detecting techniques to get an accurate count of the number of persons in a room. The most widely used and very cheap solution is a pyroelectric infrared sensor [4]. It can be easily found in modern washrooms, being used to automatically switch the lights when a person enters or exits the room. Detecting techniques commonly used by researchers as well as industry professionals include RGB cameras, laser beams (when combined in form of a linear array at the doorway), infrared cameras, ultrasonic sensors, light sensors, vibration sensors, piezoelectric crystals, etc. Multiple authors [5, 6] have tried to accumulate works and compare these methodologies based on scalability, cost, counting, functionality, location, and identity detection capabilities. In recent years, there has been a surge in the number of research articles and patents based on technologies that use disturbances in radio signals emitted by Wi-fi routers [7–11], changes in CO₂ levels, and air pressure sensing [12], etc., that have not been discussed by the authors. New researches have been made possible due to the increased penetration of smart gadgets and the internet.

This paper accumulates the various technologies available and discusses on drawbacks and unique offerings of each technology. We also compare them based on counting capability, accuracy, or reliability, ease of installation, and economic feasibility. Our goal is to investigate the new solutions being proposed by researchers as well as examine the results of combining multiple technologies for greater accuracy and reliability.

2 Challenges

Common challenges that are faced when detecting humans are listed below.

2.1 *Environment*

Designing a system that automatically adapts to any environment or works irrespective of surroundings is somewhat difficult to build. In real-world conditions, any sudden or unexpected changes in the surroundings contribute the most to dropping the accuracy rate of any system. For example, PIR sensors might be affected by the presence of hot objects inside the room/building, or by heat currents flowing in centralized air conditioners, or even by hot weather. Image processing-based systems can be easily affected by lighting conditions moving objects and shadows.

2.2 Noise

Depending on how well the sensor hardware is, the sensor data obtained is usually affected by noise. Most sensors make use of small entities (like photons are used by camera sensors). This makes them prone to errors like statistical fluctuations in the speed with which particles arrive. A good sensor design configuration can easily remove noises like pink noise and thermal noises.

2.3 Similarity

There can be similarities in detecting background signals and humans. The primary component of most human detection techniques is to differentiate between the background environment with humans. Since the real-world environment can be very complex, it becomes difficult to get things working outside laboratory conditions.

To sensors, different people seem similar. It becomes very difficult to identify and track people. This makes it challenging to count the number of people in the room. Image processing systems find it very challenging when all the people in the room are wearing similar dresses for example in a gathering with a strict dress code.

3 Factors Considered

We analyze different human-sensing techniques based on the following six factors.

3.1 Presence

This criterion is used to check whether there is any person in the room. Presence is the most trivial criteria that any human-sensing technology must have. PIR sensors are the most commonly deployed sensors that are used to detect human presence and can be easily found in modern-day washrooms. In places where humans can be provided with wearable devices, solutions like radio frequency identification, i.e., RFID can be easily deployed, for example, incorporate buildings. Detection of presence can then be used for applications like automatically switching on and off lights, air conditioners, fans, televisions, projectors and other electric appliances and devices. It will certainly help Smart home manufacturers create intuitive experiences for their consumers as well.

3.2 Counting

This factor determines if we can accurately count the number of people present inside a particular room. Counting the number of people in an environment can be done by either the sensors that observe the entire room or by deploying special sensors that only count people when they are entering and exiting the room. The person count can be used to smartly control electronic devices like air conditioners depending on the number of people that are present in the room. It can also have several commercial applications like determining the rush, counting the exact number of people which is not possible manually in a crowded place, etc.

3.3 Tracking

This factor helps us determine if any particular human tracking system can distinguish and efficiently track different humans. It also includes reporting the entry and exit times of a particular person. The person, however, can be labeled with temporary person IDs and tracking may be anonymous. The temporary identification can be lost when a person leaves the room and re-enters the scene later. This will help futuristic artificial intelligence-powered agents to provide much more contextual information.

3.4 Adaptability

This criterion is used to check if the system can be easily adapted to any new environment without any need for customization. It plays an important role in checking if the system is versatile enough to perform well outside laboratory conditions and handle complex environmental uncertainty. As we will discuss, some systems require automatic training before they can start functioning. In this study, we will still consider such systems as adaptable because they do not require any customization by the installation engineer and can be used easily by a normal person. It is a key factor to consider when we are looking at the commercial scalability of any particular system.

3.5 Cost

This factor determines how much resources and manpower does a particular system required to be built installed. If the system is costly, it could only be used by premium segment or by commercial owners. On the other hand, the system is

cheaper it can be easily used by the mass public like PIR sensors for example. The economic feasibility of any technology determines if it has the potential to become widely popular and used as a consumer device.

3.6 Ease of Installation

This criterion determines how easy is it to install a human tracking system at a location without any prior experience or expertise. Any system which is easy to install must also be adaptable at the same time. However, vice versa may not be true. If any system cannot be easily installed by a non-technical person, then it attracts additional installation charges which automatically adds to the overall cost of the system. This factor plays an important role in deciding scalability and feasibility of the solution is.

An interesting property to note is that if factor 3 is satisfied, then factor 2 gets automatically satisfied. This is because if we can individually track humans, then trivially we will also be able to count the number of people in a room. Similarly, if factor 2 is satisfied, then factor 1 automatically gets satisfied. Factor 2 can be seen as a more generalized measurement of factor 1 for count >1 .

4 Survey of Technologies

We classify the human-sensing technologies in to natural characteristic-based and motion-based sensing methods.

4.1 Natural Characteristic-Based Sensing

These technologies detect the presence of one or more humans based on natural characteristics of human body like emission of CO₂ or absorption of radio signals by human body.

Wi-Fi. Multiple researchers [7–11] have proposed ways to count the number of people by using Wi-Fi signals. The basic idea behind these types of approaches is that humans create disturbances in received Wi-Fi signals. These disturbances are then processed by either advanced algorithms (based on some complex mathematical calculations [7, 8, 10] or neural networks [9–11]) which then determine the number of people inside the room. It must be noted that the receiver must be stationary, and hence, a device like a smartphone cannot be used for the same purpose. This microcontroller or computer runs the algorithms or neural networks and yields the count of people as output.

Light Sensing. It works on the principle that the presence of humans reduces the intensity of light in the room. Photodetectors are used to convert light signals into electrical signals, and then, a device like ADC is used to convert electric signal to digital signal which can be easily processed by a microcontroller [13–15]. There are two light-based sensing techniques for recognizing any human activity which are as follows:

Active sensing. The user wears a device/or a simple LED that emits light of a specific frequency. This emitted light is then used to track the position of a person using a camera or a photodiode [13, 14].

Passive sensing. It doesn't require people to wear any special device. Photodetectors installed at some places in the room are used to sense ambient light and any flickering frequencies for the reconstruction of human blueprint and indoor location [15].

CO₂ levels. Humans produce carbon dioxide due to the natural respiration process. This increases the percentage of carbon dioxide in the atmosphere which can be used to identify the presence of humans in a room. Some of the systems require machine learning-based model training for each environment before it can start producing results [12]. Due to the slow speed of diffusion of carbon dioxide in the air, it takes some time before the carbon dioxide released by human beings reaches the designated sensor. Hence, it is not suitable for applications that need instant feedback on whether a human is present or not.

4.2 Motion-Based Sensing

These technologies detect the motion of people and use it to detect the presence or count and track the persons inside a room.

Beam Break Sensor. A beam break sensor is used to detect the entrance and exit of humans at doorways. They work by having an emitter on one side that emits light and a receiver on the other side which measure the amount of light incident on it. These types of sensors are also commonly found in lifts, metro token pathways, etc. However, they have very strict installation requirements and cannot detect when multiple people pass by simultaneously. We also need at least two beam break sensors installed perpendicular to the direction pathway for identifying the direction of movement. Under properly managed situations, these do a wonderful job of counting the number of people present inside the room. However, they have very strict installation requirements and cannot detect when multiple people pass by simultaneously.

Sensing Air Pressure. This system work on the principle that when human move between rooms because of disturbances in airflow at the ductwork of air conditioning (HVAC) systems found in many buildings and houses. Human movement

changes the static pressure in the HVAC air handling unit. A significant change in pressure is noticed when doors are opened or closed and when people go from one room to another. The pressure variation is noted by sensors installed at air filters which are then used to classify the movement events [16]. Ongoing research is going on for testing similar systems at various places. The accuracy level is lower compared to the technologies discussed above.

Array of IR Cameras. This system works on the principle that human presence causes a sudden change in temperature patterns recorded by infrared sensors. In [17], the authors used an array of very low-cost IR imaging devices at the doorway for counting entry and exit events. As with break beam sensors, this method also fails to identify events when multiple people enter and exit simultaneously and pose similar installation challenges.

Image Processing. RGB cameras are widely used by machine learning and image processing enthusiasts [18, 19] for counting and tracking people. This method can achieve high levels of accuracy at places where a complete field of view is available. In environments where it works, it can track different persons very effectively. It, however, fails to work under dark lighting conditions and poses some serious privacy issues at some obvious places.

Ultrasonic Sensors. Multiple research groups [20–23] have investigated the use of ultrasonic waves for solutions that count the number of people. The underlying idea is that the human body actively reflects any ultrasonic waves incident on it. It is recommended to use sensors [24, 25] that are capable of generating higher frequencies because they tend to be more accurate than cheaper ones that do not produce such high frequencies. This method can count the number of people; however, tracking is not possible. Data generated can become big data, so analytical techniques can also be useful for such big data [26–28].

5 Discussion

We have investigated the different human-sensing technologies available for precise estimation of people count. Unlike many researchers that have shared their opinions on the technologies for measuring the human presence, we have taken into account the economic, technological, and operational feasibility. There has been very little or no discussion on newer technologies like differential air pressure sensing, and CO₂ reading in existing researches. We have taken into consideration the perspective of smart device manufacturers and business owners (Table 1).

In this paper, we have given the reader understanding of how these technologies work and discussed the potential of them becoming a reality. Talking in terms of cost, break beam sensors, IR array and PIR sensors remain to be the most cost-effective solutions to date. Technologies like Wi-Fi signals demonstrate the

Table 1 Summary of discussed sensing technologies

Technology	Presence	Count	Track	Adaptable	Cost	Ease of deployment
Wi-Fi	Yes	Yes	No	No	Med	Easy
CO ₂	Yes	Yes	No	Yes	High	Easy
Active light sensing	Yes	Yes	Yes	No	High	Hard
Passive light sensing	Yes	No	No	Yes	Low	Easy
Beam break sensor	Yes	Yes	No	Yes	Med	Hard
Air pressure sensing	Yes	No	–	–	High	Hard
IR camera array	Yes	Yes	No	Yes	Med	Hard
Image pro-cessing	Yes	Yes	Yes	Yes	Med	Easy
Ultrasonic sensors	Yes	Yes	No	Yes	Med	Hard

huge potential for becoming a mass-market technology provided further research makes it adaptable to real-world environments outside laboratories.

6 Conclusion

Similar to how computing devices transitioned from desks to people’s pockets. In the world we live in, there will be an increasing demand for more powerful artificially intelligent agents. In this paper, we examined and discussed the pros and cons of the existing methods to acquire such information. We anticipate that future human presence detecting systems will likely consist of a mixture of one or more technologies discussed in the paper. With the current advancements in technology, we are more hopeful than ever to see people counting devices making their way to residential homes and commercial buildings.

References

1. MARKETSandMARKETS: Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment, Smart Speaker, Home Healthcare, Smart Kitchen, Home Appliances, and Smart Furniture), Software & Services, and Region-Global Forecast to 2024 <https://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html> (2018)

2. Beltran, A., Erickson, V.L., Cerpa, A.E.: Thermosense: occupancy thermal based sensing for HVAC control. In: Proceedings of the 5th ACM Workshop on Embedded Systems for Energy-Efficient Buildings, pp. 1–8. ACM (2013)
3. Buildings Energy Data Book. 2011: Energy Efficiency and Renewable Energy. US Department of Energy (2011)
4. Moghavvemi, M., Seng, L.C.: November. Pyroelectric infrared sensor for intruder detection. In: 2004 IEEE Region 10 Conference TENCON 2004, vol. 500, pp. 656–659. IEEE (2004)
5. Teixeira, T., Dublon, G., Savvides, A.: A survey of human-sensing: methods for detecting presence, count, location, track, and identity. *ACM Comput. Surv.* **5**(1), 59–69 (2010)
6. Mohammadmoradi, H., Yin, S., Gnawali, O.: Room occupancy estimation through wifi, UWB, and light sensors mounted on doorways. In: Proceedings of the 2017 International Conference on Smart Digital Environment, pp. 27–34 (2017)
7. Depatla, S., Muralidharan, A., Mostofi, Y.: Occupancy estimation using only WiFi power measurements. *IEEE J. Sel. Areas Commun.* **33**(7), 1381–1393 (2015)
8. Depatla, S., Mostofi, Y.: Crowd counting through walls using WiFi. In: IEEE International Conference on Pervasive Computing and Communications (PerCom) 2018 Mar 19, pp. 1–10. IEEE
9. Tiwari, R., Kumar, N.: Minimizing query delay using cooperation in IVANET. *Procedia Computer Science* **57**, 84–90 (2015)
10. Yang, Y., Cao, J., Liu, X., Liu, X.: Wi-Count: Passing People Counting with COTS WiFi Devices (2018). <https://doi.org/10.1109/ICCCN.2018.8487420>
11. Sobron, I., Del Ser, J., Eizmendi, I., Velez, M.: A Deep Learning Approach to DeviceFree People Counting from WiFi Signals. In: Del Ser, J., Osaba, E., Bilbao, M., SanchezMedina, J., Vecchio, M., Yang, X.S. (eds.) *Intelligent Distributed Computing XII. IDC 2018. Studies in Computational Intelligence*, vol 798. Springer (2018)
12. Arief-Ang, I.B., Salim, F.D., Hamilton, M.: DA-HOC: semisupervised domain adaptation for room occupancy prediction using CO₂ sensor data. In: Proceedings of the 4th ACM International Conference on Systems for Energy-Efficient Built Environments (BuildSys '17), pp. 1–10. Association for Computing Machinery, New York, NY, USA, Article 1 (2017)
13. Kuo, Y.-S., Pannuto, P., Hsiao, K.-J., Dutta, P.: Luxapose: Indoor positioning with mobile phones and visible light. In: *MobiCom'14*, pp. 447–458. ACM (2014)
14. Li, L., Hu, P., Peng, C., Shen, G., Zhao, F.: Epsilon: A Visible Light Based Positioning System. In: *NSDI'14*, pp. 331–343. USENIX Association, Seattle, WA. <https://www.usenix.org/conference/nsdi14/technical-sessions/presentation/li> (2014)
15. Zhang, C., Zhang, X.: LiTell: robust indoor localization using unmodified light fixtures. In: *MobiCom'16*, pp. 230–242. ACM (2016)
16. Sharma, I., Tiwari, R., Anand, A.: Open source big data analytics technique. In: Proceedings of the International Conference on Data Engineering and Communication Technology. Springer, Singapore (2017)
17. Mohammadmoradi, H., Munir, S., Gnawali, O., Shelton, C.: Measuring people-flow through doorways using easy-to-install ir array sensors. In: 2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 35–43. IEEE (2017)
18. Barandiaran, J., Murguia, B., Boto, F.: Real-time people counting using multiple lines. In: 2008 Ninth International Workshop on Image Analysis for Multimedia Interactive Services, pp. 159–162. IEEE (2008)
19. Zhao, X., Delleandrea, E., Chen, L.: A people counting system based on face detection and tracking in a video. In: Sixth IEEE International Conference on Advanced Video and Signal Based Surveillance, 2009 (AVSS'09), pp. 67–72. IEEE (2009)
20. Hnat, T.W., Griffiths, E., Dawson, R., Whitehouse, K.: Doorjamb: unobtrusive room-level tracking of people in homes using doorway sensors. In: *SenSys'12*, pp. 309–322. ACM (2012)
21. Nasir, N., Palani, K., Chugh, A., Prakash, V.C., Arote, U., Krishnan, A.P., Ramamritham, K.: Fusing sensors for occupancy sensing in smart buildings. In: *ICDCIT'15*, pp. 73–92. Springer (2015)

22. Shih, O., Rowe, A.: Occupancy estimation using ultrasonic chirps. In: ICCPS'15, pp. 149–158. ACM (2015)
23. Mishra, D., Khan, A., Tiwari, R., Upadhyay, S.: Automated irrigation system-IoT based approach. In: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1–4. IEEE (2018)
24. Tiwari, R., Kumar, N.: A novel hybrid approach for web caching. In: 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. IEEE (2012)
25. Sharma, I., Tiwari, R., Rana, H.S., Anand, A.: Analysis of mahout big data clustering algorithms. In: Intelligent Communication, Control and Devices, pp. 999–1008. Springer, Singapore (2018)
26. Anand, A., et al.: Comparative analysis between proprietary software vs. open-source software vs. free software. In: 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE (2018)
27. Kumar, S., Tiwari, R.: Optimized content centric networking for future internet: dynamic popularity window based caching scheme. *Comput. Netw.* **179**, 107434 (2020)
28. Khan, E., et al.: Automated toll tax collection system using cloud database. In: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). IEEE (2018)

Identification and Minimization of Churn Rate Through Analysing Financial Routines Using Machine Learning



Rahul Pahuja, Niket Dheeryan, Lovish Sethi, Preeti Nagrath, and Rachna Jain

Abstract In recent years, source of revenue for companies across all industries is subscription products. Hence, it is crucial to know the user area of interest so that customer churn from the company is minimized. Machine learning is gaining scope day by day. Its application has also found a way to predict and analyse the churn rate. The model is build using logistic regression and support vector machine (SVM) algorithms. Objective of the model is to predict which user is likely to cancel product subscription. Accuracy obtained in the model using logistic regression was found to be 61.2 and using SVM was found to be 60.7%.

Keywords Churn · Prediction · Accuracy · Logistic regression · SVM

1 Introduction

This research paper with the churn analysis of subscription products. This involves identifying user's area of interest and behavioural patterns that acts as rapid fire in disengagement of a particular product. Every company wants that subscription to the products should not be cancelled and for that they first need to identify which services provided by them is fulfilling the need of customer or not. Efforts are made accordingly by providing new features to the user like low interest rate for loans. Machine learning has recently advanced with a great pace. Logistic regression one of the algorithms is applied in this model and prediction of churning is obtained for all the users using the features. Logistic regression is used to identify statistical probability in form of binary variables whether churn will take place or not.

R. Pahuja · N. Dheeryan · P. Nagrath · R. Jain
Department of C.S.E., Bharati Vidyapeeth College of Engineering, New Delhi 110063, India
e-mail: preeti.nagrath@bharatividyaapeeth.edu

R. Jain
e-mail: rachna.jain@bharatividyaapeeth.edu

L. Sethi (✉)
Department of IT, Bharati Vidyapeeth College of Engineering, New Delhi 110063, India

Features which are important to predict the response variable were analysed in this model building process so that amendment can be made in those services and company minimize the cancelling of subscription and hence retain the customers. Churning of customers depends on quality of services provided to them. Many churn predicting models based on machine learning has been designed in past few years, but all models cannot work efficiently. If best services are provided to the customers at proper time, then chances of retaining the customers to a product increase with great pace. Machine learning models can easily predict the parameters which are forcing the user to leave the product. Although we can see that machine learning is advancing and used in almost every area, it suffers from few following limitations:

1. Problem of overfitting arises when generally small datasets are used.
2. Large possibility of errors.
3. Training data that is used for fitting the model must be unbiased and should be of best quality.

Machine learning has proved to be very helpful to the big companies and businessmen as they get to know which factor is making competitions high among the markets.

Support vector machine (SVM)—It is supervised machine learning algorithm that is used mainly for classification purposes. In this algorithm, every data point of dataset is plotted in n dimensional space where n is number of features in dataset with each feature's value being the value of a particular coordinate. It consists of a hyperplane to differentiate and perform classification.

Various classification techniques serve the purpose of determining the chances of churning. Banking systems are also applying random forest algorithms along with hyper tuning of dataset to classify the churn possibility of the users. Standardization and Normalization of data has to be done to get effective results of prediction. Feature extraction is necessary to determine which features have to be used for prediction in machine learning models. In machine learning, most of the dataset can be read through pre-existing pandas and Sklearn library.

Logistic regression is one of classification algorithm that uses a logistic sigmoid function to return probability value that maps to discrete classes.

1.1 Motivation

Determination of churning of user from the company or from subscription products is the major demand of every company in order to increase the profit. By knowing the areas in which users are churning the most, they can introduce new features to the products.

Various authors have made efforts in this area in past few years. Different methodologies have been adopted for making prediction. Authors in [1] have

designed a hybrid model (a two-stage model). Other works include the use of different algorithms like decision tree, SVM, fuzzy c means algorithm. Hybrid approaches gave much better result as compared to single algorithm. Machine learning is a growing field of science and it contains various algorithms which need to be explored further.

1.2 Contribution

In this paper two machine learning algorithms, i.e. Logistic regression and support vector machine (SVM) are proposed for predicting the churning of user. The proposed approach uses various techniques in model building like pre-processing, plotting various plots for getting distribution of features, One hot encoding, Feature scaling and balancing, Feature selection using RFE function. Accuracy obtained with this approach was found to be 61.2% on Fintech dataset for 27,000 users using logistic regression while SVM algorithm has provided accuracy of 60.7%.

Following are the contributions of paper:

1. Histograms and pie charts are plotted to get distribution of various features of dataset.
2. Effect of various features on churning of user is determined using correlation plot.
3. Efficiency of algorithms is enhanced by extracting few features which are necessary for accomplishing objective of prediction.

1.3 Uniqueness of the Paper

1. Relationship between different features and churning of user is studied using correlation plots. This gives a brief overview that whether churning is positively related to that feature or negatively related.
2. Feature selection technique is applied to achieve top best feature required for making prediction which increases the efficiency of algorithms.

1.4 Organisation

The remaining part of the paper is organized as follows. Section 2 contains the related works that have been done for churn prediction in different areas using various approaches. Section 3 describes the proposed approach. Performance evaluation of the proposed approach is indicated in Sect. 4. Section 5 is the concluding part of the paper.

2 Related Works

Weighted voting method was used to build a final decision tree from several small decision trees in the work by Wei et al. [2] in 2002. Final classification of churning users was obtained using the decision tree obtained. Decision tree's ability to classify better even in presence outliers has made it a recursively used algorithm.

Hadden et al. [3] had published a work in 2006 in which they are identifying the most important variables to identify churn possibility. Artificial neural network, decision trees and regression were used to model the data. Churn risk plot made in artificial neural network predicted the result to 72% accuracy. Highest accuracy found for the model was from decision trees.

Qi et al. [4] in 2006 had built Tree Logit model consist of logistic regression and A D-tree (decision tree with boosting algorithm). Logistic model was built for every decision tree that is obtained after categorization to make customer churning prediction.

In 2007, probability of churning is predicted using self-organizing map (an artificial neural network) by Chu et al. [5]. Clustering of subscribers according to important characteristics was done. SOM layers size was fixed so to build an effective model better version of SOM was used, i.e. GHSOM with 85% accuracy.

In another work done by Zhao and Dang [1] in 2008, that used SVM with 4 kernels for prediction of customers churning from bank and then compared it with different classifiers like logistic regression, Naïve Bayes, ANN. In the analysis, SVM gave highest prediction accuracy of 59.74%.

Various algorithm was analysed like regression, Naïve Bias, decision tree, support vector machine (SVM) was applied by Coussement and Van den Poel [6] for classification of most important feature in churn minimization. To handle the nonlinear relationships between independent fields of the dataset, RBF kernel was used for SVM model implementation. This model worked well with newspaper subscription dataset and prediction was accurate to great extent. PCC metric was used to determine the probability of most likely churning user to the least likely churning user, hence making subscription analysis effective in that model.

Churn prediction in retail banking was determined using Fuzzy c means clustering by Popovic and Dalbelo Basic [7] in 2009. It was the more accurate algorithm as compared to hierarchical methods and k means clustering. It was operated well on the outliers existing in dataset.

Hybrid model was built in 2009 by Bose and Chen [8]. This model involved two stages. In first stage, various clustering algorithms like KMD, KM, SOM, BIRCH, FCM were applied. Second stage was the final prediction stage which used decision tree (C 5.0) along with boosting procedure. Decision tree was used because when compared to other algorithms as it is faster approach.

Neural network based on genetic algorithm was proposed by Pendharkar [9] in 2009. Managing hidden nodes effectively played an important role in making churn predictions. Efficient feature selection in GANN had enabled it to make more accurate predictions.

Another work by Bangzhu [10] in 2010 includes the use of Least Square Support Vector Machines, Rough sets in addition to SMC for predicting Churn rate of customers. Accuracy of the model was somewhat higher in this model. LSSVM worked well with inseparable data and was able to make prediction better than SVM.

Data mining techniques were applied to telecom dataset by Umayaparvathi and Iyakutti [11] in 2012. Performance of decision tree and a neural network was analysed and decision tree was found to be more efficient in predicting users more likely to churn. Neural network and decision tree were trained using rules defined for the features of dataset.

Qureshi et al. [12] in 2013, had analysed and classified active telecom customers and churn customers using various approaches. Linear regression, Artificial neural networks, 4 types of decision trees, i.e. CART (Classification and regression tree), CHAID (Chi-squared automatic interaction detector), Exhaustive CHAID and QUEST (Quick unbiased and efficient statistical tree) were used. Exhaustive CHAID was the most efficient version of decision tree with 70% accuracy.

In 2014 another work done by Zhao [13] was able to predict the ecommerce customer churning rate using Artificial Neural Network and SVM. Genetic algorithm was used which means result of SVM prediction and artificial neural network were combined and passed to SVM model again to obtain better results. Since ecommerce data was highly nonlinear, model using single algorithm could not give efficient result in that scenario and time consumed was also higher.

Data mining was used for predicting churn of telecom user in the work presented by Dahiya and Talwar [14] in 2015.

Khan et al. [15] had obtained 90% accuracy in 2015. Subscribers churning from a telecom industry using different algorithms like Linear Regression, SVM, KNN, random forest. Trees that were trained using K fold cross-validation-based approach were used for feature selection.

Predicting the next activity and its timestamp can be accomplish using LSTM (long short-term memory). LSTM was used by Tax et al. [16] in their project to predict remaining cycle time and next process on the basis of past activity in 2016. It worked well for prediction as LSTM is special RNN which has long-term dependencies power. LSTM may have very long training time which is the limitation for its working.

Churn prediction in telecom industry was performed by Dalvi et al. [17] which incorporated the use of two algorithms, i.e. decision tree and logistic regression in 2016 with a speciality that the system can be used with any type of data. System consists of 3 modules for providing different functionalities. First module was for providing interface, second for extracting features and third for making predictions.

Role of attributes selection in making prediction of customers churn from telecom industry was analysed with data mining techniques by Umayaparvathi and Iyakutti [18] in 2016. Gradient boost algorithm has given highest accuracy of 73 and 95% on two datasets out of 7 classifiers used for prediction.

Jain et al. [19] had made an effort in 2017 to predict churn using decision tree along with classification approach. Decision tree proves to be an efficient approach while making prediction as it studies every node and considers all possible outcomes. RMD metric was used to predict, how much accurate the model was. Pruning technique was used to improve the results of decision tree. Hence, number of churning user was determined by the model. Data needs to be properly managed as changes make decision tree unstable.

K means clustering was combined with many classifiers like Naïve Bayes, random forest, decision tree, SVM in 2017 by Rajamohamed and Manokaran [20]. Rough k means clustering algorithm with SVM was able to achieve highest accuracy of 96%. Single classification algorithms were less accurate as compared to hybrid models.

Improvement in FCM algorithm was provided by Cui et al. [21] in 2017 to overcome the previous inefficiencies in the algorithm like inability to predict number of clusters for making final customer churn prediction. The prediction accuracy was obtained to be 80.3% by enhanced algorithm.

Four algorithms, i.e. logistic regression, SVM, gradient boost and random forest for prediction of churn were used in the work suggested by Gaur and Dubey [22] in 2018. Analysis of area under curve (AUC) values has proved gradient boost to be most accurate method for prediction with its value being 84.59.

Artificial neural network can also be used for classification of churn. The most popular work was done in the paper by Xia and He [23] in which the use of BP neural network was incorporated with SVM to predict the churn. Various plots were plotted between different commodities and churn. Results of combined algorithms proved to be efficient with accuracy of 93%. But on the other side rate of convergence of BP neural network is quite slow and also numerical stability of predicted results is poor for this algorithm.

In 2018 Sahu et al. [24] had made an effort to predict churn of telecom customers using data mining techniques. Pattern among the already churned customers was found. LASSO was used to penalize the regression coefficient size. Then Lasso was fitted to logistic regression to evaluate the result. Decision tree used in the model was more effective than logistic regression.

Factors responsible for churning were determined, and churning chances of users were determined for telecom using neural network with an 80% accuracy by Agrawal et al. [25] in 2018.

Logistic regression was incorporated for making prediction in the model developed by Sai and Sasikala [26] in 2019. ROC was used for model evaluation and value of Area under curve was determined to be 0.83 while making prediction with value of threshold being 0.5.

In 2019, behaviour of ecommerce customers was analysed to predict the churn rate using K Nearest neighbour and decision trees. Hybrid approach was followed in this model by Kareena [27]. In the beginning, relationship was determined between response and features using decision tree (Base Classifier). Then final classification of customers into different categories was made using KNN (Meta Classifier). This is known as hybrid approach.

Table 1 Comparative analysis of various works

Reference no.	Year	Algorithm used	Accuracy (%)
[3]	2006	1. Decision tree	82
		2. Regression	81
		3. Artificial Neural Network	74
[5]	2007	1. Self-organizing map	85
[1]	2008	1. SVM	59.74
		2. Logistic regression	58.90
		3. Naïve Bayes	55.49
		4. ANN	54.79
[11]	2012	1. Decision tree	98.88
		2. Neural network	98.43
[15]	2015	1. SVM	89.4
		2. Random forest	88.4
		3. KNN	88.2
		4. AdaBoost	89.2
		5. Logistic regression	89.3
[20]	2017	1. KNN	76.05
		2. DT	83.7
		3. SVM	93.2
		4. RF	85.6
		5. NB	77.9
[27]	2019	1. Naïve Bayes	74.11
		2. Hybrid model (Decision tree and KNN)	90.75

Random forest was used in the work suggested by Zhou and Yang [28] in which review helpfulness was predicted using textual and numerical features. In this analysis, review length was found to be crucial criteria for prediction (Table 1).

3 Proposed Approach

Machine learning is a subfield of artificial intelligence. It provides computer the ability to learn and practise without being explicitly programmed. Machine learning contains many algorithms with which it passes data and trains from it. One of the machine learning algorithms known as logistic regression is used in this model to predict whether a user will churn or not.

3.1 Reading Dataset

Dataset is read using Pandas library. Pandas is an open source library whose key feature is the data frames (manipulation is done in form of rows and columns) read function is used to read the file.

Description of dataset: Dataset used for model building is a Fintech Company dataset that provides financial services to the customers. Dataset contains information of the 27,000 users using different services from the company. Number of features in the dataset is 31 out of which some contains binary data and some contain numerical data. Dataset contains user identification number for identification of the services used by the user. Source: <https://www.kaggle.com/niketdheeryan/fintech-users-data>.

3.2 *Cleaning of Data*

Data cleaning is very crucial step in implementing machine learning algorithms. Null values in the given dataset are checked using prebuilt ISNA () function. If a particular column contains large number of null values, then that particular column is dropped using drop () function in order to accomplish model building process.

3.3 *Plotting Histograms and Pie Chart*

Histograms and pie chart are plotted to get the distribution of various features of dataset.

Histogram plots the data by dividing into interval called bins as shown in Fig. 1. Distribution obtained from histograms is less informative as binary variables are not

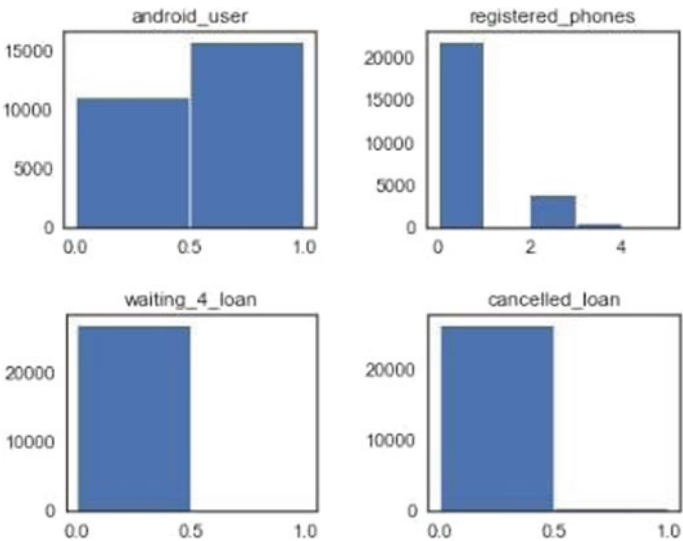


Fig. 1 Histogram for Fintech users' dataset

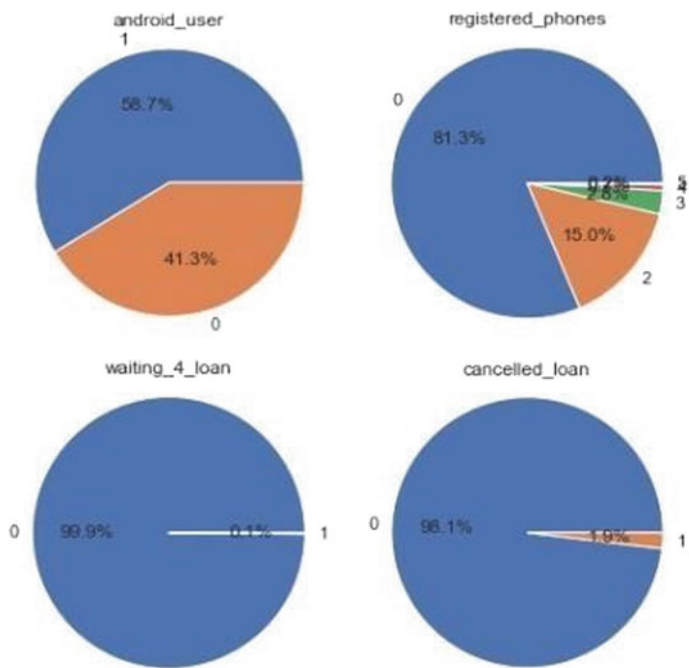


Fig. 2 Pie Chart for Fintech user’s dataset

properly examined in histograms. So, pie chart is plotted in order to obtain better visualization in form of percentages.

In Fig. 2, depicting pie chart for Fintech user’s dataset, fields which are evenly distributed (i.e. 50%–50% or 40%–60%) are not of much concern. Small subsets have to be explored further in order to know whether they are useful for prediction or not. For example, `android_user` plot is evenly distributed and there is nothing to worry about those distributions. On the other hand `waiting_4_loan`, `registered_phones`, `cancelled_loan` have subsets which are very small have to be taken care off because there are not enough results for those small subsets to include both rows where churn variable is 0 and 1.

3.4 Correlation Plot

This plot is used to gaze the correlation between independent and dependent variables of dataset. Categorical variables are removed and binary variables are kept because this correlation plot requires numeric value fields. In Fig. 3 showing the correlation plot among various fields and churning possibility, the fields whose bar plot is below origin line are negatively correlated with the churn chance.

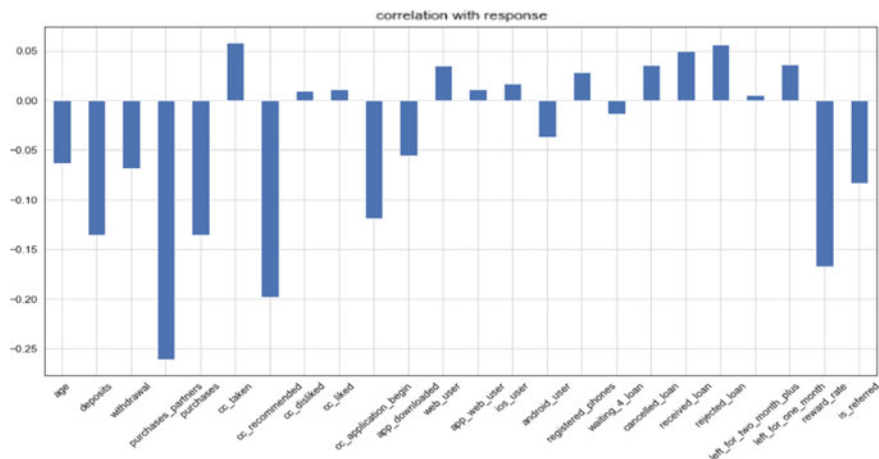


Fig. 3 Correlation plot for Fintech user's dataset

For example, smaller the number of deposits more is the chance of user to be churn. age, deposit, withdrawal, purchases_partner, purchases, cc_recommended, app_downloaded are also negatively correlated to churn. This means less activity a person is having in particular field; he is more likely to churn. In case of cc_recommended, if more recommendations are provided, more likely the user will stay with the company. In a similar manner, cc_taken, web_user, app_web_user, ios_user, registered_phones are positively correlated to response variable, i.e. churn. It is giving an insight that people are not satisfied with these features and enhancement has to be done to prevent churn of users.

3.5 One Hot Encoding

It converts all categorical variables into their own independent binary variables because python models cannot read categorical variables. One hot encoding is done by getting dummies () function present in panda library. Correlation among the one hot encoded column is dropped using drop () function.

3.6 Splitting the Dataset into Train Set and Test Set

train_test_split () is a function in Sklearn model selection for splitting data arrays into two subsets: train set and test set. Test set is used to predict the accuracy of the designed model while train set is used to train the model.

3.7 *Feature Scaling and Balancing*

Balancing the amount of zeroes and ones that training set has in its response variable guarantees that whatever accuracy we are getting is result of model itself rather than random permutation of how many zeroes or ones are present in training set.

Feature scaling is a pre-processing step applied to features of dataset. It normalizes all numerical fields in such a way that its weight is not too large in equation of logistic regression standard scalar present in sklearn pre-processing standardize features by removing the mean and scaling to unit variance.

3.8 *Feature Selection Process*

Top best features were selected from the dataset. Useful attributes can be extracted to minimize the time taken for machine learning algorithm. RFE function present in sklearn feature selection is used for that purpose. RFE support used in the project returns list of Boolean values meaning that these values are actually mapping which columns are to be included in final result.

3.9 *Fitting Model to Training Set*

Logistic regression (LR) is a statistical method similar to linear regression since LR finds an equation that predicts an outcome for a binary variable, Y from one or more response variables X .

Modelling of model is done in such a way that probability maps to either 0 or 1.

Now let us consider a generalized model having parameter θ then we have function,

$$h_{\theta}(X) = 1 / (1 + e^{-\theta^T X}) = \Pr(Y = 1 | X; \theta) \quad (1)$$

exponent is used in modelling logistic regression because probability is always greater than 0.

Hence,

$$\Pr(Y = 0 | X; \theta) = 1 - h_{\theta}(X) \quad (2)$$

$$\text{And since } Y \in \{0, 1\}, \text{ therefore } \Pr(y | X; \theta) = h_{\theta}(X)^y (1 - h_{\theta}(X))^{1-y} \quad (3)$$

Now assumption is made that all observations are Bernoulli distributed, likelihood function is given as:

$$L(\theta|y; x) = \Pr(Y|X; \theta) \quad (4)$$

$$= \prod_i \Pr(y_i|x_i; \theta) \quad (5)$$

$$= \prod_i h_\theta(x_i)^{y_i} (1 - h_\theta(x_i))^{1-y_i} \quad (6)$$

log likelihood is maximized,

$$N^{-1} \log L(\theta|y; x) = N^{-1} \sum_{i=1}^N \log \Pr(y_i|x_i; \theta) \quad (7)$$

Gradient descent is used to maximize Eq. (7).

Now (x, y) pair are drawn in uniform manner from distribution, Applying limit to N ,

$$\lim_{n \rightarrow \infty} \sum_{i=1}^N \log \Pr(y_i|x_i; \theta) \quad (8)$$

$$= \sum_{x \in X} \sum_{y \in Y} \Pr(X = x; Y = y) \log \Pr(Y = y|X = x; \theta) \quad (9)$$

$$= \sum_{x \in X} \sum_{y \in Y} \Pr(X = x, Y = y) \left(-\log \frac{\Pr(Y = y|X = x)}{\Pr(Y = y|X = x; \theta)} + \log \Pr(Y = y|X = x) \right) \quad (10)$$

$$= -D_{\text{KL}}(Y||Y_\theta) - H(Y|X) \quad (11)$$

where D_{KL} is the Kullback Leiber divergence and $H(X|Y)$ is conditional entropy. The odds of any event in logistic regression are given by:

$$p/1 - p = e^{w_0 + w_1 x_1 + \dots + w_n x_n} \quad (12)$$

which is further log transformed.

Now to define log likelihood we take log of Eq. (12)

$$\log(p/1 - p) = w_0 + w_1 x_1 + \dots + w_n x_n \quad (13)$$

3.10 *Predicting Output for Test Set and Evaluation of Accuracy*

Test data is fed to predict function of the classifier and predicted values are determined. Accuracy of model is an important parameter for evaluation of any model. Various accuracy scores are imported using sklearn metrics.

Accuracy score is defined as:

$$\text{Accuracy Score} = \frac{\text{TRUE POSITIVE} + \text{TRUE NEGATIVE}}{\text{TRUE POSITIVE} + \text{TRUE NEGATIVE} + \text{FALSE POSITIVE} + \text{FALSE NEGATIVE}}$$

Precision score is defined as:

$$\text{Precision Score} = \frac{\text{TRUE POSITIVE}}{\text{TRUE POSITIVE} + \text{FALSE POSITIVE}}$$

Precision score is the ability of classifier not to label as positive if sample is negative.

Recall score is defined as how many relevant items are selected.

$$\text{Recall Score} = \frac{\text{TRUE POSITIVE}}{\text{TRUE POSITIVE} + \text{FALSE NEGATIVE}}$$

Diagrammatic representation of model building process.

Figure 4 depicts the flow of steps involved in model building. Initially, dataset is read using read function in step 1. Then in step 2 pre-processing (cleaning) of dataset is done. Distribution of various features is plotted using various plots in steps 3 and 4. In step 5, One hot encoding is applied. In step 6, we split data into two sets—train and test. Then feature scaling and balancing is applied for normalising the fields in step 7. Best features are then selected in step 8. After that model was fitted to training set. In last step, evaluation of model is done.

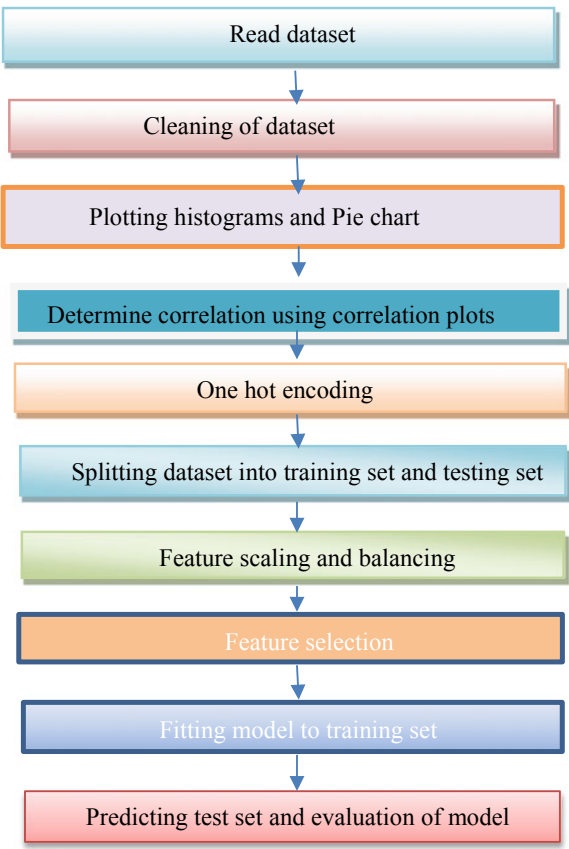
4 Performance Evaluation

4.1 *Discussion on Results*

For building the project standard libraries like Sklearn, Pandas, NumPy, seaborn, matplotlib were used.

Sklearn is used because it supports python numerical libraries like NumPy and is freely available machine learning library for python. matplotlib pyplot is used for plotting various plots to get distribution of various fields in the dataset.

Fig. 4 Flow chart for model building process



Pandas library is most popular library and is used because its key feature includes Dataframe and helps to manipulate data in form of rows and columns.

Dataset imported was splitted into two parts in order to train the model and then evaluate on test data. Model was fitted to logistic regression and accuracy score was calculated. Accuracy Score is the important parameter for evaluation of model (Table 2).

The heat map is the representation of matrix data in a graphical form. It is used to represent the confusion matrix or any two-dimensional data in form of colour.

Table 2 Various accuracy scores obtained on testing

Algorithm used	Accuracy score	Precision score	Recall score	F1 score
Logistic regression	61.2	55.4	74.8	61.4
SVM	60.75	51.6	75.4	61.5

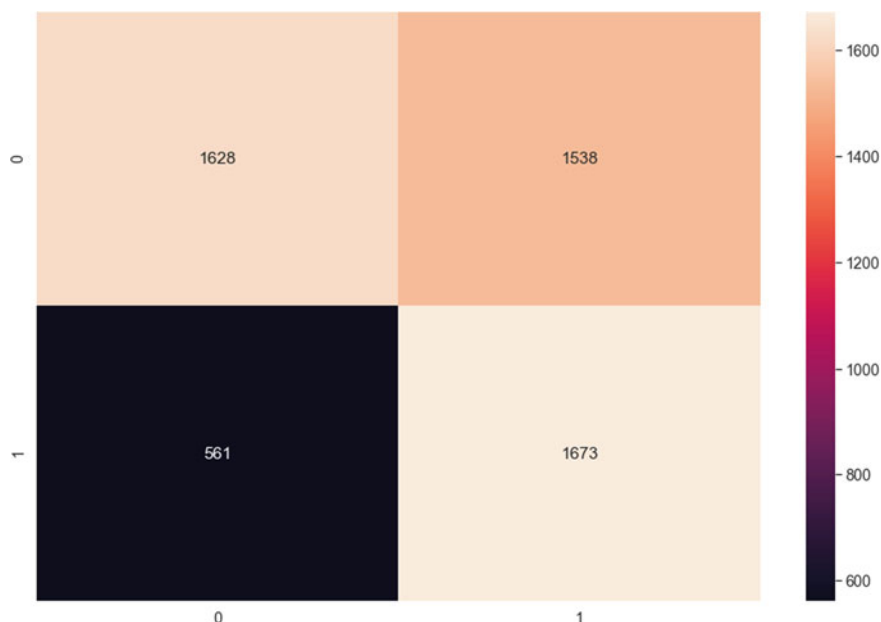


Fig. 5 Heat map for confusion matrix

In Fig. 5, Heat map representing the confusion matrix is shown. It has successfully able to identify 1665 true positives, 1541 false positives, 1625 true negatives and 569 false negatives.

The accuracy can be further improved in future by designing hybrid models which involve combining two or more algorithms together to form an efficient model and also by applying neural networks and deep learning algorithms. Hybrid approach gives better result as compared to single algorithm.

5 Conclusion

This paper has justified the need of churn analysis in order to minimize the customer loss from the subscription to the particular product. Simple model using logistic regression, SVM algorithm was built to identify the areas in which churning from the company has occurred. This is the need of every company to know area of interest of user using the product so as to retain their customers. The current model build using machine learning has involved data cleaning and other pre-processing steps like feature scaling which need to be minimized further. In future, this process may be implemented through other models like artificial neural networks, deep learning. Models should be built in such a manner that pre-processing steps like feature scaling, balancing steps are minimized to greater extent in order to ensure effectiveness of the model.

References

1. Zhao, J., Dang, X.: Bank customer churn prediction based on support vector machine: taking a commercial bank's VIP customer Churn as the example. In: 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, pp. 1–4 (2008). <https://doi.org/10.1109/WiCom.2008.2509>
2. Wei, C.-P., Chiu, I.-T.: Turning telecommunications call details to churn prediction: a data mining approach. *Expert Syst. Appl.* **23**(2), 103–112 (2002)
3. Hadden, J., Tiwari, A., Roy, R., Ruta, D.: Churn prediction: does technology matter. *Int. J. Intell. Technol.* **1**(1), 104–110 (2006)
4. Qi, J.Y., Zhang, Y.M., Zhang, Y.Y., Shi, S.: TreeLogit model for customer churn prediction. In: Proceedings of the 2006 IEEE Asia-Pacific Conference on Services Computing, Guangzhou, China, pp. 70–75, 12–15 Dec. 2006
5. Chu, B.-H., Tsai, M.-S., Ho, C.-S.: Toward a hybrid data mining model for customer retention. *Knowl. Based Syst.* **20**(8), 703–718 (2007)
6. Coussement, K., Van den Poel, D.: Churn prediction in subscription services: an application of support vector machines while comparing two parameter-selection techniques. *Expert Syst. Appl.* **34**(1), 313–327 (2008)
7. Popovic, D., Dalbelo Basic, B.: Churn prediction model in retail banking using Fuzzy C-means clustering. *Eng. Comput.* 036–130 (2009)
8. Bose, I., Chen, Xi.: Hybrid models using unsupervised clustering for prediction of customer churn. *J. Organ. Comput. Electron. Commer.* **19**, 133–151 (2009)
9. Pendharkar, P.C.: Genetic algorithm based neural network approaches for predicting churn in cellular wireless network services. *Expert Syst. Appl.* **36**(3), 6714–6720 (2009)
10. Bangzhu, Z.: The prediction of e-business customer churn based on smc-rs-lssvm model. *Syst. Eng. Theor. Pract.* **11**, 1960–1967 (2010)
11. Umayaparvathi, V., Iyakutti, K.: Applications of data mining techniques in telecom churn prediction. *Int. J. Comput. Appl.* (2012)
12. Qureshi, S.A., Rehman, A.S., Qamar, A.M., Kamal, A., Rehman, A.: Telecommunication subscribers churn prediction model using machine learning. In: Digital Information Management (ICDIM), 2013 Eighth International Conference, pp. 131–136 (2013)
13. Zhao, X.: Research on E-commerce customer churning modeling and prediction. *Open Cybern. Syst. J.* **8**, 800–804 (2014)
14. Dahiya, K., Talwar, K.: Customer Churn prediction in telecommunication industries using data mining techniques—a review. In: International Journal of Advanced Research in Computer Science and Software Engineering (2015)
15. Khan, M.R., Manoj, J., Singh, A., Blumenstock, J.: Behavioral modeling for churn prediction: early indicators and accurate predictors of custom defection and loyalty. In: Proceedings of the IEEE International Congress on Big Data, BigData Congress 2015, pp. 677–680 (2015)
16. Tax, N., Verenich, I., La Rosa, M., Dumas, M.: Predictive Business Process Monitoring with LSTM Neural Networks (2016)
17. Dalvi, P.K., et al.: Analysis of customer churn prediction in telecom industry using decision trees and logistic regression. In: 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, pp. 1–4 (2016). <https://doi.org/10.1109/CDAN.2016.7570883>
18. Umayaparvathi, V., Iyakutti, K.: Attribute selection and customer Churn prediction in telecom industry. In: 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), Ernakulam, India, pp. 84–90 (2016) <https://doi.org/10.1109/SAPIENCE.2016.7684171>
19. Jain, R., Rajpoot, V., Richhariya, V.: Predicting Churn in Telecom Sector Using Classification & Decision Tree, vol. 3(5) (2017). ISSN: 2395-3853
20. Rajamohamed, R., Manokaran, J.: Improved credit card churn prediction based on rough clustering and supervised learning techniques. *Cluster Comput.* **21**, 65–77 (2017)

21. Cui, S., Ding, N.: Customer Churn prediction using improved FCM algorithm. In: 2017 3rd International Conference on Information Management (ICIM), Chengdu, pp. 112–117 (2017). <https://doi.org/10.1109/INFOMAN.2017.7950357>
22. Gaur, A., Dubey, R.: Predicting customer Churn prediction in telecom sector using various machine learning techniques. In: International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal, India, pp. 1–5 (2018). <https://doi.org/10.1109/ICACAT.2018.8933783>
23. Xia, G., He, Q.: The research of online shopping customer Churn prediction based on integrated learning. In: 2nd International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2018), China
24. Sahu, M.K., Pandey, R., Silakari, S.: Analysis of customer Churn prediction in telecom sector using logistic regression and decision tree. *J. Appl. Sci. Comput.* **5** (2018)
25. Agrawal, S., Das, A., Gaikwad, A., Dhage, S.: Customer Churn prediction modelling based on behavioural patterns analysis using deep learning. In: 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, pp. 1–6 (2018). <https://doi.org/10.1109/ICSCEE.2018.8538420>
26. Sai, B.N.K., Sasikala, T.: Predictive analysis and modeling of customer Churn in telecom using machine learning technique. In: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, pp. 6–11 (2019). <https://doi.org/10.1109/ICOEI.2019.8862625>
27. Kareena, R.K.: A consumer behavior prediction method for E-Commerce application. *Int. J. Recent Technol. Eng. (IJRTE)*. **8**(2S6) (2019). ISSN: 2277-3878
28. Zhou, Y., Yang, S.: Roles of review numerical and textual characteristics on review helpfulness across three different types of reviews. *IEEE Access* **7**, 27769–27780 (2019)

Machine Learning-Based Predictive Analysis to Abet Climatic Change Preparedness



Abra Shafiq Siddiqi, Md. Afshar Alam, Deepa Mehta,
and Sherin Zafar

Abstract Global warming and the corresponding climatic changes have affected the world adversely. Climatic changes encompass the soaring temperatures, extremity in weather phenomenon, disrupting habitats, rising water levels in seas, and plenty of other impacts. As these changes emerge, the humans attempt to reduce the carbon emissions. This research paper aims to study the changing temperatures as a result of the industrial activities and greenhouse effect over the last 5 decades. The analysis utilizes data analytic tools to analyze the percentage at which the decades are affected as we moved into technologically advanced era. After studying the effects, the research paper also aims to predict the changes in the mean temperatures for the next decade using the time series prediction model with the help of machine learning algorithms. The dataset includes monthly temperatures for about 150 countries for a period of 58 Years, and machine learning algorithms aim to predict the rise and fall of temperatures for the next decade successfully.

Keywords Global warming · Prediction analysis · Time series · Machine learning

1 Introduction

AI and man-made consciousness are required to give huge new experiences into understanding environmental change and how to battle it, as indicated by an investigation distributed today in Environmental Research Letters. Studies give a convincing contention that AI (ML) and man-made reasoning (AI) can fill a portion

Present Address:

A. S. Siddiqi · Md.A. Alam · S. Zafar (✉)
Jamia Hamdard, New Delhi, India
e-mail: sherin.zafar@jamiahamdard.ac.in

Md.A. Alam
e-mail: aalam@jamiahamdard.ac.in

D. Mehta
GD Goenka University, Sohna, Haryana, India

of the holes that exist in environment science. Educator Chris Huntingford, from the Center for Ecology and Hydrology, is the investigation's lead creator. He said: "In spite of the fact that environment research is by and large viewed as a cycle drove movement, it is likewise incredibly complex, thus the use of measurably based AI calculations will clarify new climate examples and associations."

Co-creator Professor Mike Bonsall said: "ML calculations have progressed significantly lately, and have empowered momentous discoveries in other examination sec-peaks. There is each motivation to expect they can be utilized to help environment analysis." Co-creator Hannah Christensen added: "There is a wide scope of potential uses of ML in the environment sciences. While a few people stay wary of ML, truth be told climate researchers have been utilizing attempted and tried ML strategies for a long time with-out acknowledging it. We feature this in our paper, just as point out new zones where ML could change our field." Co-creator Dr. Hui Yang remarked: "Planet Earth is observed at extraordinary levels, and particularly by satellites gathering tremendous quantities of environment-related information. Specialists need further developed calculations and techniques to utilize such enormous measures of information, to describe patterns, practices and interconnections."

To represent explicit capability of ML and AI, the analysts inspected three test plea where they could be utilized to acquire knowledge into environment occasions—the UK summer 2018 dry season; the environment "break"; and earthbound biological system condition fabricating—for instance how plant nourishment interfaces with environment and impacts the measure of carbon that can be put away on the land surface. Favorable to Professor Huntingford said: "regarding understanding the 'rest', it is fundamental that for an environment highlight so unmistakable, we join all strands of proof to create a complete clarification. As the rest is likely an element of concurrent cooperation's in the environment framework, ML can help describe these, and highlight any environment model lacks [1–3]."

Co-creator Dr. Elizabeth Jeffers said: "In biological system condition building, ML can help distinguish which plant synthetic characteristics and natural conditions are driving input to the nitrogen and carbon cycles, empowering the improvement of interaction-based conditions for use in demonstrating supplement restriction." Co-writer Thomas Lees said: "Our examination sums up where explicit environment framework segments have just been researched with ML". Our call is to go a lot further and utilize ML techniques to the whole the Earth framework, with an accentuation on surveying its inner associations. Supportive of Professor Huntingford summed up: "Environment demonstrating needs a stage change to lessen vulnerability in projections—ML probably has a significant job in accomplishing that" [4–6].

In the upcoming sections in this paper, authors will focus on machine learning-based predictive analysis to abet climatic change preparedness, various research issues and questions are discussed in Sect. 2. Methods and results are presented in Sects. 3 and 4 that will highlight on the model building for predictive analysis, followed by conclusion and references.

2 Research Problem and Research Questions

2.1 Research Problem

In the utilization of AI-based examination, is there a methodology that can be effortlessly utilized by amateurs to make information investigation and the understanding of results workable for individuals not familiar with programming? Moreover, is there a doable route for fledglings to play with explicit factors in different PC reenactment situations utilizing easy to use AI programming? How might the bits of knowledge from the investigated information be passed on in natural non-specialized terms that others, e.g., strategy producers, who are more worried about the “generally speaking greater picture,” can plainly get it? Creators propose that there is an answer that can be utilized to determine these previously mentioned issues. The easy to use AI-empowered methodology that will be used in this paper depends on Bayesian network (BN) probabilistic thinking [7, 8]. It very well may be applied utilizing a product bundle that is appropriate for fledglings, as it doesn’t need any product programming abilities. Utilizing this methodology, people can start to lead the pack and consider over the predictive models produced by AI. Probabilistic thinking utilizing BN models is more intuitive for speaking with numerous partners across multidisciplinary area verticals, as deduction as far as likelihood is nearer to normal human idea, compared to utilizing old style frequentist connections or p-values [9–12]. The models in the current paper will likewise encourage openings for exploring different avenues regarding, e.g., how the change of ecological factors could foresee various results of climatic changes [13–15].

2.2 Research Questions

The qualities of the unique worldwide climatic changes framework are investigated utilizing these examination questions:

RQ1: What are the elements that add to the current conditions that characterize the worldwide climatic changes?

RQ2: What are the prescient effects of the direst outcome imaginable in the versatility of the normal assets on the result of climatic changes, with the goal that strategy producers can be educated and endeavor to stay away from them?

3 Methods

Analysis involves the publicly available dataset from National Aeronautics and Space Administration Goddard Institute for Space Studies (NASA-GISS). The dataset describes the surface temperature changes across various countries.

The FAOSTAT temperature change domain includes the temperature change pertaining to each country, with updates provided annually. The available dissemination involves details from the year 1961–2019.

Data analysis is performed using pandas library in python. Analysis studies the effect of global warming over the three decades. The yearly data available from 1961 to 2019 are divided into six decades. The temperature trends are studied for India during the summer, winter, fall and spring. After, studying the effects on temperatures in the Indian subcontinent. The analysis further investigates the effect on the 190 countries.

The countries around the world are investigated for the changes in temperatures over the similar 6 decades. After the analysis, the final section involves the use of time series prediction algorithm to predict the temperature changes in the coming decade. The involvement of Time series prediction is due to the fact that it:

Time series permits understanding and comparison while assuring that none of the extremely relevant information is lost with respect to the background of “time.” Time series also enables forecasting.

The time series prediction includes the use of Facebook’s open-source library prophet. Prophet renders the ability to permit time series predictions with great accuracy with the use of simple yet intuitive parameters. The following section discusses the results achieved.

4 Result Analysis

Global warming has been on the rise particularly during the last decade, and this research investigates the effect of this on the Indian subcontinent during the last decade compared to the previous five decades. In Fig. 1, the graph indicates that the summer temperatures have risen considerably in the last decade. Figure 2 indicates a sharp decline in the winter temperatures during the last two decades. While spring also has similar fluctuation to winter, fall has a similar trend to summer as depicted by Figs. 3 and 4. Results are indicative of the last decade that is 2010–2019 has been among the ten hottest years on record in terms of mean annual temperatures.

Figure 5 depicts the pair plot analysis of the six decades and their correlation. A pair plot is indicative of the relationships between the decades.

The animation map in Fig. 6 demonstrates the seriousness of the rising temperatures year after year. From our above analysis result, I came up winter season getting hotter. The results are a proof of global warming that is severely affecting the global temperatures across the countries.

Figure 7 enables the visualization of the temperature trends across the six decades within the 190 countries across the world. The darker areas indicate rising temperatures across last two decades as a result of global warming.

Figures 8 and 9 predicts the temperatures expected in the next two decades from 1970 to 2040. The predictions indicate that temperatures will rise further drastically in case of absence of significant effects to abet the climate changes. The reason for

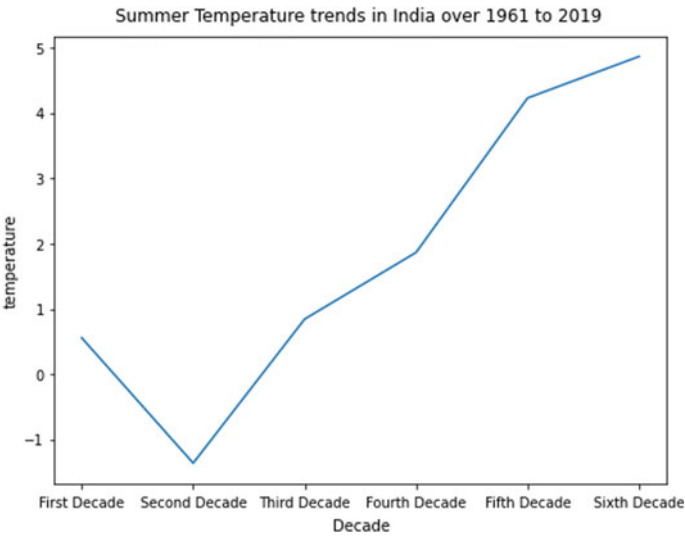


Fig. 1 Summer temperature trends in India over 1961–2019

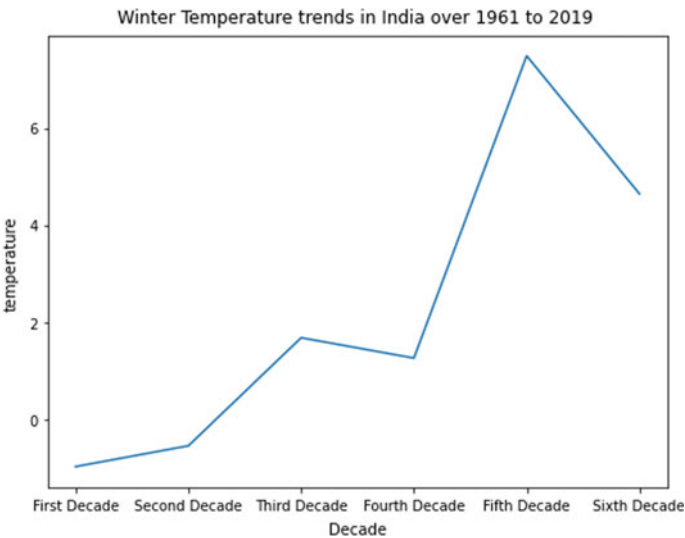


Fig. 2 Winter temperature trends in India over 1961–2019

the drastic changes Earth’s climate during the last decade is contributed by human activities which are increasing the heat trapped and therefore, increased greenhouse gas levels in Earth’s atmosphere, increasing Earth’s average surface temperature.

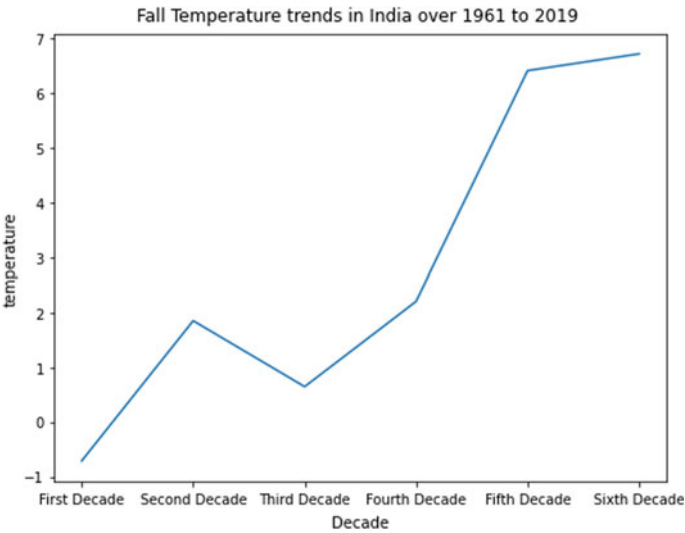


Fig. 3 Fall temperature trends in India over 1961–2019

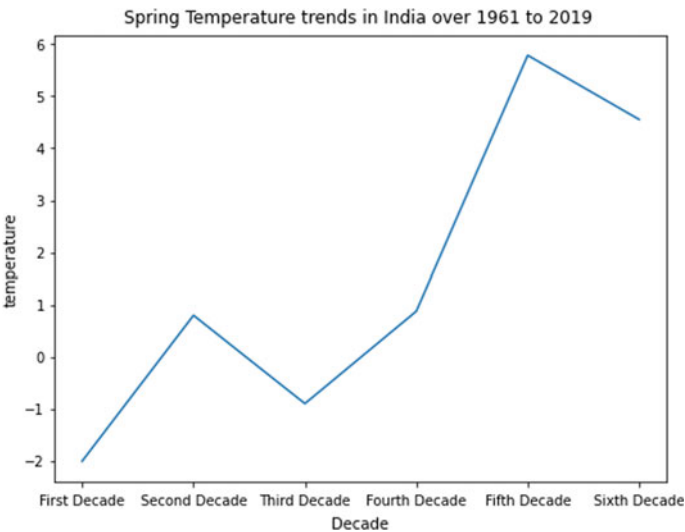


Fig. 4 Spring temperature trends in India over 1961–2019

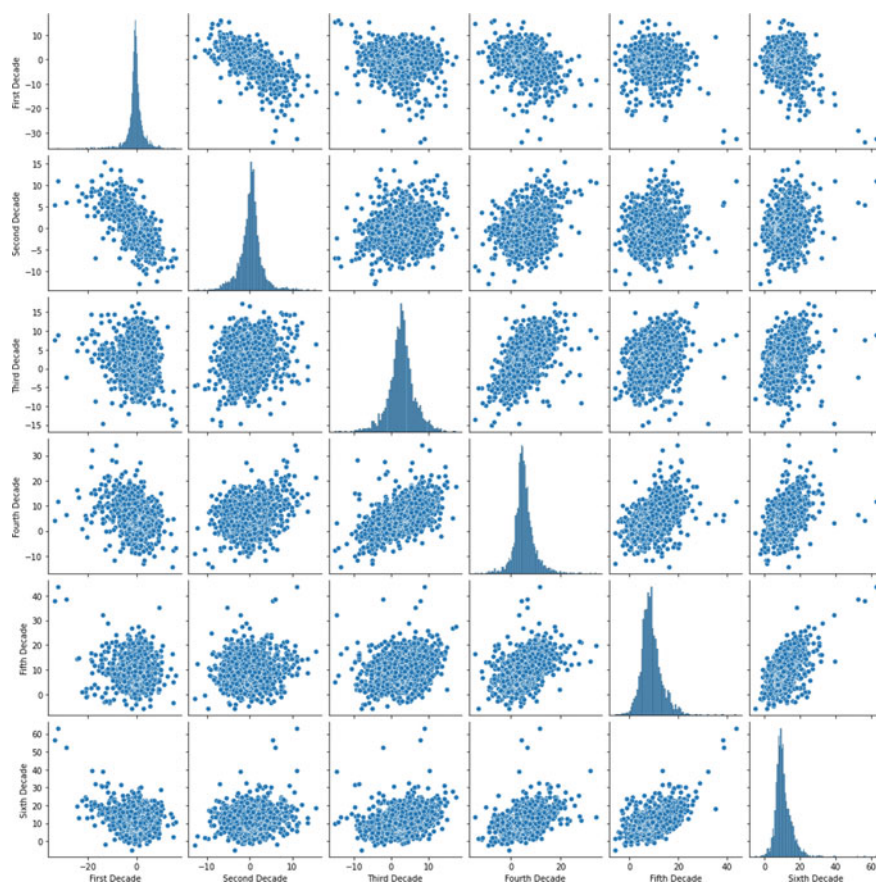


Fig. 5 Pair plot analysis of all decades

5 Conclusion and Future Scope

This study proposes a machine learning (ML) model to abet climatic change preparedness. In this study, data analysis is performed using pandas library in python. Analysis studies the effect of global warming over the three decades. The yearly data available from 1961 to 2019 are divided into six decades. The temperature trends are studied for India during the summer, winter, fall and spring. After, studying the effects on temperatures in the Indian subcontinent. The analysis further investigates the effect on the 190 countries. The countries around the world are investigated for the changes in temperatures over the similar 6 decades. After the analysis, the final section involves the use of time series prediction algorithm to predict the temperature changes in the coming decade. The accuracy of the model was validated using the historical records, and the results produced predictive

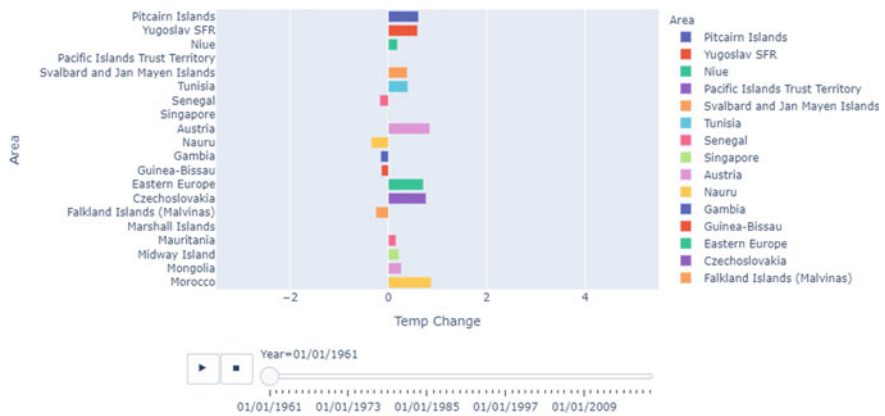


Fig. 6 Varying temperatures across the world

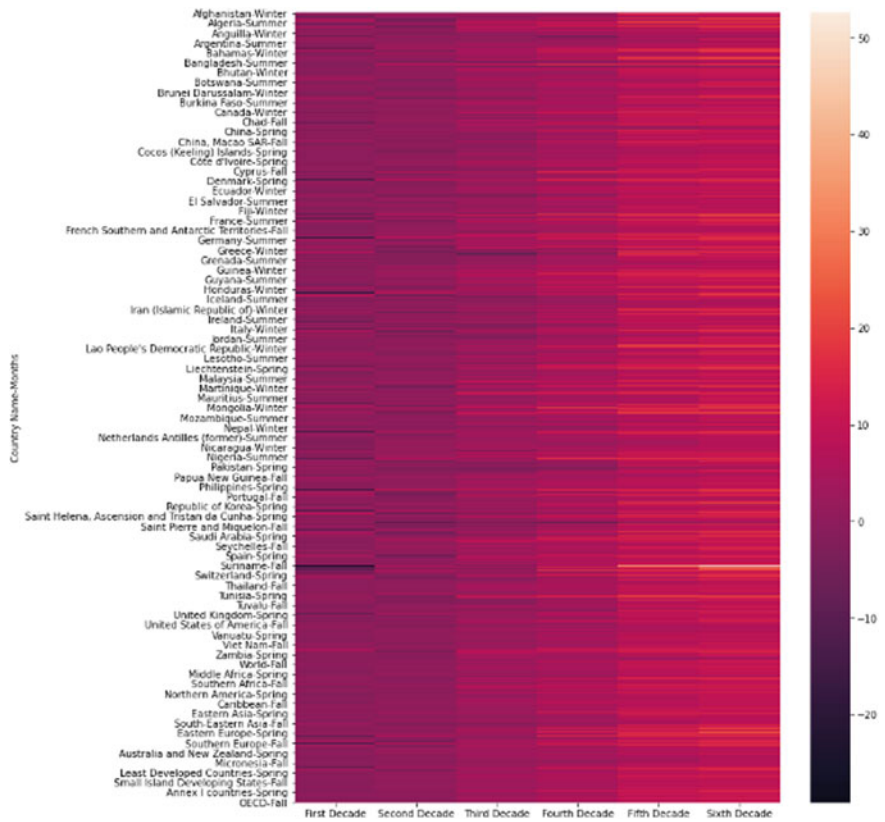


Fig. 7 Rising temperatures over the six decades across the world

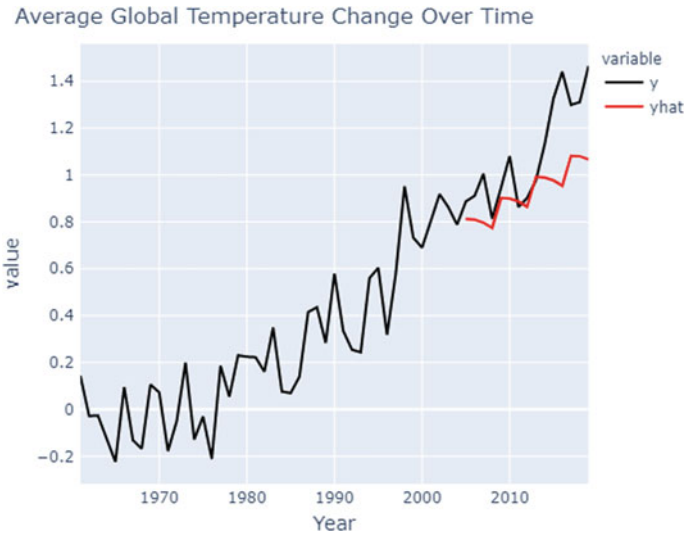


Fig. 8 Average global temperature change over time (1970–2010)

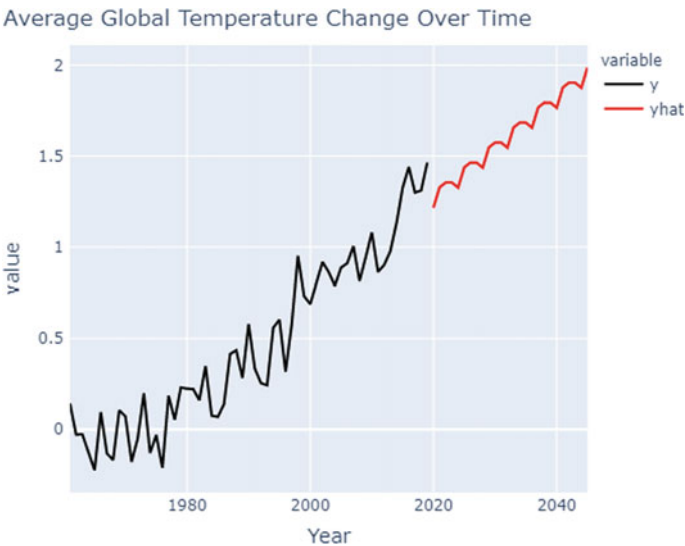


Fig. 9 Average global temperature change over time (1980–2040)

analysis model for optimized model generation. The predictions indicate that temperatures will rise further drastically in case of absence of significant effects to abet the climate changes. The reason for the drastic changes Earth’s climate during the last decade is contributed by human activities which are increasing the heat

trapped and therefore, increased greenhouse gas levels in Earth's atmosphere, increasing Earth's average surface temperature. Climatic change preparedness is a very important aspect in many countries, especially during pandemic like covid-19. Therefore, this research study will prove to be a great advantage for performing predictive analysis and generating machine learning models for weather forecasting, climate change awareness and for many other changes also.

References

1. Pearl, J.: Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann, San Francisco (1988)
2. Wulff, S.S.: Time series analysis: forecasting and control. *J. Qual. Technol.* **49**(4), 418 (2017)
3. Taylor, S.J., Letham, B.: Forecasting at scale. *Am. Stat.* **72**(1), 37–45 (2018)
4. Schervish, M.J.: P values: what they are and what they are not. *Am. Stat.* **50**(3), 203–206 (1996)
5. Scher & Messori.: How global warming changes the difficulty of synoptic weather forecasting. *Geophys. Res. Lett.* **46**(5), 2931–2939 (2019)
6. FAOSTAT.: Temperature change [Online]. <http://www.fao.org/faostat/en/#data/ET>, last accessed 2021/02/10
7. Hwang, Y., Carbone, G.J.: Ensemble forecasts of drought indices using a conditional residual resampling technique. *J. Appl. Meteorol. Climatol.* **48**(7), 1289–1301 (2009)
8. Al-Obeidat, F., Spencer, B., Alfandi, O.: Consistently accurate forecasts of temperature within buildings from sensor data using ridge and lasso regression. *Future Gener. Comput. Syst.* (2018)
9. Manogaran, G., Lopez, D.: A survey of big data architectures and machine learning algorithms in healthcare. *Int. J. Biomed. Eng. Technol.* **25**(2–4), 182–211 (2017)
10. Aybar-Ruiz, A., et al.: A novel grouping genetic algorithm–extreme learning machine approach for global solar radiation prediction from numerical weather models inputs. *Sol. Energy* **132**, 129–142 (2016)
11. Yin, C., et al.: A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **5**, 21954–21961 (2017)
12. Borthakur, D., et al.: Smart fog: fog computing framework for unsupervised clustering analytics in wearable internet of things. In: 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), IEEE (2017)
13. Ardabili, S., Mosavi, A., Dehghani, M., Várkonyi-Kóczy, A.R.: Deep Learning and machine learning in hydrological processes climate change and earth systems a systematic review. In: Várkonyi-Kóczy, A. (eds.) *Engineering for Sustainable Future. INTER-ACADEMIA 2019. Lecture Notes in Networks and Systems*, vol. 101. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-36841-8_5
14. Gopirajan, P.V., Gopinath, K.P., Sivaranjani, G., et al.: Optimization of hydrothermal liquefaction process through machine learning approach: process conditions and oil yield. *Biomass Conv. Bioref.* (2021). <https://doi.org/10.1007/s13399-020-01233-8>
15. Anuj, K., Kumar, V.: Big data in climate: opportunities and challenges for machine learning. In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '17). Association for Computing Machinery, New York, NY, USA, 21–22 (2017). <https://doi.org/10.1145/3097983.3105810>

Deep Learning Approaches for Anomaly and Intrusion Detection in Computer Network: A Review



Khushnaseeb Roshan and Aasim Zafar

Abstract In recent years, a great deal of attention has been given to deep learning in the field of network and information security. Any intrusion and anomaly in the network can significantly impact many areas, such as security of the private and social data, national security, social and financial concerns, etc. Therefore, network and information security are a broad research domain for which researchers are actively utilizing the functionally improved, emerging deep learning technique and report the improved result. In this review paper, we have analysed several deep learning methods in the area of network anomaly, intrusion detection, network traffic analysis and its classification. We have presented a comprehensive review of widely known deep learning approaches. And then, we conclude with open research challenges and unresolved issue for further study. This review paper provides an overall background for the researchers interested in network anomaly and intrusion detection based on deep learning methods.

Keywords Deep learning · Intrusion detection · Network anomaly · Network attack · Network security

1 Introduction

Network and communication security is an important part of our daily life, and its protection has continuously emerged as a major concern. Also, the global accessibility of the network exposes individuals and organizations to network attack. Antivirus software, firewalls, Intrusion detection, and anomaly detection methods are various approaches to protect network and individual from attack [1]. Network traffic analysis and classification are also important for network anomaly detection, which try to identify the signs of intrusion and abnormal behaviour using profiling method (IDS anomaly based) [2].

K. Roshan (✉) · A. Zafar
Aligarh Muslim University, Aligarh, Uttar Pradesh 202002, India
e-mail: azafar.cs@amu.ac.in

Moreover, outsiders can cause security instances and network anomalies, such as any suspicious activity aiming to disable the services, steal private data and information. Other reasons like server crashes, power outages, link congestion are known as inside factors. And these factors significantly impact on network and communication security [3].

The recent rise of interest in deep learning (DL) algorithms resulted in major advancements in network security and anomaly detection methods. Also, the availability of the extensive computational power encourages researchers to adopt deep learning techniques for attack detection, network intrusion and anomalies detection [4–6].

This review paper has mainly used journal and conference articles in network anomaly detection (attack, intrusion and abnormal behaviour) and network traffic analysis. This review article organizes as follows: Section 1 presents a brief introduction. Section 2 provides a detailed description of various deep learning methods applied in network anomaly and intrusion detection. Section 3 discusses open research challenges and issue for future work with suggestions. Section 4 concludes this review paper.

2 Deep Learning for Network Anomaly and Intrusion Detection

Deep learning methods are very effective to discover the relationship in highly complex data without human intervention. Feature learning and data classification are the main task of DL methods and hence very useful in handling complex network traffic data. This review analysis provides a complete overview of DL methods with their advantages and challenges for future exploration.

As shown in Fig. 1, deep learning architecture broadly classified into three categories, i.e. generative, discriminative and hybrid. Each category has its working advantages and disadvantage that we have included in Table 1.

2.1 Autoencoder (AE)

Autoencoder networks were initially developed as compression techniques that aim to covertly give input to output with the least amount of distortion. This compression achieves by using less number of nodes than the nodes used in the hidden layer. Autoencoders are theoretically simple and widely used for unsupervised anomaly detection. In high dimensional data, these networks are used for feature extraction (reduction in dimensionality) by the hidden layer between the encoder and decoder [7].

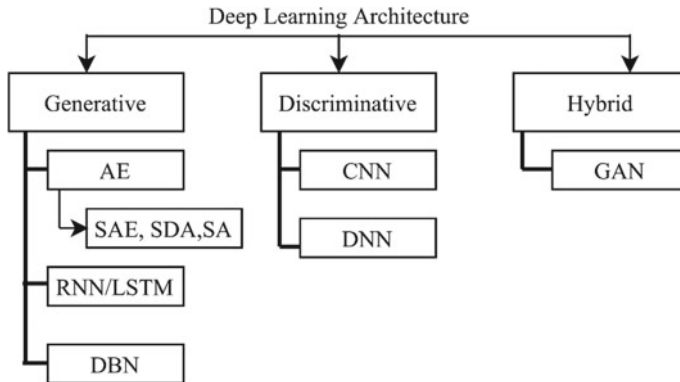


Fig. 1 Deep learning architecture

The authors of [8] proposed IDS model using autoencoder for cybersecurity. The model was capable enough to detect not only malicious packets but also classify specific types of attacks with 81.31% recognition accuracy. In the study of [9], a new IDS model based on autoencoder proposed, this model has been trained and tested on two popular benchmark network datasets, i.e. KDD99 and NSL-KDD. The model successfully achieved a recall of 98.11%. The authors also used the memetic algorithm for final classification.

In the latter study, the authors of [10] proposed a deep learning framework named SU-IDS. They used both semi-supervised and unsupervised technique to develop the Intrusion Detection System using autoencoder. The experimental results on NSL-KDD and CICIDS2017 dataset were quite acceptable. The model achieved approximately 99.65% accuracy for intrusion detection. Then other effective deep learning approach proposed in [11], authors used sparse autoencoder mechanism for feature selection and SVM for final classification, which improved its detection capability for intrusion and classification accuracy. Moreover, the results of the proposed approach are also compared with other classification methods, such as SVM, naive Bayesian, random forest and J48.

2.2 Convolutional Neural Networks (CNNs)

Convolutional neural networks are the advanced version of ANNs and were initially developed for pattern recognition task within complex images. CNNs are formed by stacking three layers, namely convolutional layers, pooling layers and fully connected layers. These networks extract higher resolution features and then convert them into more complex features at a coarser resolution in image classification task [12]. However, in some recent research, they are also performed well in classifying non-image data (like network traffic data, anomaly detection).

Table 1 Single DL techniques

Detection category	DL approach	Datasets used	Measurement metrics used in papers	Performance	Workings and purpose of the methods
IDS, Cyber Security (2017) [8]	AE	KDD-CUP99, NSL-KDD	ACC	90.12% ACC	AEs are generative or unsupervised deep learning methods, mainly used for unlabelled datasets, also used for dimensionality reduction in highly complex data like network traffic datasets
IDS (2017) [9]	AE	KDD-CUP99, NSL-KDD	DR, CR	0.98 DR	
IDS (2018) [31]	AE	NSL-KDD, CICIDS2017	ACC, DR, FAR	0.99DR	
IDS (2018) [11]	AE	NSL-KDD	ACC, P, R, F	99.396% ACC	CNNs are discriminative or supervised deep learning methods used for labelled datasets in prediction and classification purposes, very efficient in image classification
NTC (2017) [13]	CNN	USTC-TFC2016 (Self-collected)	ACC, P, R, F	99.41% ACC	
IDS (2018) [14]	CNN	NSL-KDD	ACC, P, R, F	81.84%ACC	
IDS (2018) [15]	CNN	ISCX2012	ACC, DR, FAR	99.21%	DBNs are unsupervised methods based on RBMs, can be used for dimensionality reduction, can also be used for classification purpose with an additional discriminative layer
IDS (2017) [17]	DBN	KDD-CUP99, NSL-KDD	ACC, P, R, F	99.7% ACC	
IDS (2017) [18]	DBN	KDD-CUP99	ACC, DR, FAR	99.04% ACC	
IDS (2017) [20]	LSTM	KDD-CUP99	ACC, P, DR, FAR	97.54% ACC	LSTMs are generative methods, very efficient for time-series data, LSTM uses a feedback loop in its hidden cells, makes it capable of learning timestamps and sequential data
NTC (2020) [21]	LSTM	NSL-KDD	ACC, DR, FPR	84.25% ACC	
IDS (2020) [22]	LSTM	NSL-KDD	ACC, P, R, F, FPR	83.85%ACC	
NTC (2017) [23]	SAE	AWID	DR, FPR	92.7% DR	SAEs are unsupervised methods and a variant of AEs, composed of many hidden layers, performed better in terms of accuracy with raw data like network traffic, can also reduce high dimensional data with few features
NTC (2017) [24]	SAE	AWID	ACC, DR,F, FAR	99.91 ACC%	
NTC (2017) [25]	SAE	AWID + Emulated	ACC	98.66% ACC	
NTC (2016) [26]	SAE	Simulated Environment	ACC, TPR, FPR	99.99% ACC	
IDS (2019) [27]	SAE	KDD-CUP99, UNSW-NB15	ACC, P, R, F, FAR	99.99% ACC	

(continued)

Table 1 (continued)

Detection category	DL approach	Datasets used	Measurement metrics used in papers	Performance	Workings and purpose of the methods
IDS (2017) [28]	SDA	CTU-13 + UNB ISCX IDS 2012 dataset	ACC, P, R, F	99.48% ACC	Another variant of AEs, used to produce refined data from corrupted and noisy input data
IDS (2016) [29]	SA	NSL-KDD	ACC, P, R, F	95.95% DR	Another variant of AEs, have only one hidden layer in its architecture
IDS (2020) [30]	GAN + AE	NSL-KDD, UNSW-NB15	ACC, P, R, F	95.19% ACC	GANs are hybrid methods, i.e. composed of both generative and discriminative techniques
GAN —Generative Adversarial Network; CNN —Convolutional Neural Network; RNN —Recurrent Neural Network; LSTM —Long Short-Term Memory; AE —Autoencoder; SAE —Stacked AE; DBN —Deep Belief Network; SVM —Support Vector Machine; SDA —Stacked Denoising Autoencoder; SA —Sparse AE; RBM —Restricted Boltzmann Machine; DBM —Deep Boltzmann Machine; DNN —Deep Neural Network; DL —Deep learning; DT —Decision Tree; RF —Random Forest; ACC —Accuracy; FAR —False alarm rate; DR —Detection Rate; R —Recall; P —Precision, F —F-measure; FPR —False positive rate; TPR —True positive rate; NTC —Network traffic classification					

The authors of [13] presented a novel representation learning approach using CNNs and applied it on network traffic data to detect malware. The model has trained on raw network traffic data by converting it into images and achieved an average accuracy of 99.41%. However, the authors used only spatial feature in the training process and ignored the temporal feature completely, which is the major drawback of the method. In the latter study [14], the same approach is applied to IDSs, where the authors used NSL-KDD dataset and graphics conversion technique to train the model on transformed data. The model used the full feature set as input and performed well as compared to standard classifier but did not improve the state-of-the-art method. Future work can improve the graphical conversion technique for better result.

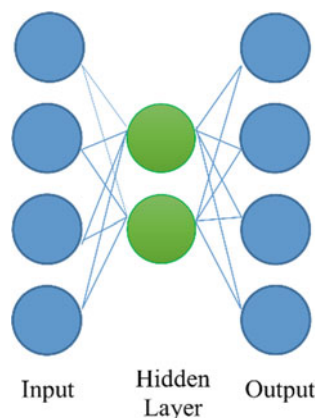
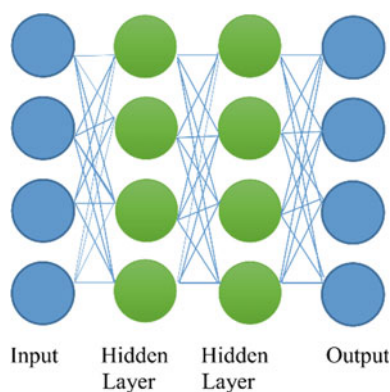
The authors of [15] presented a new model named TR-IDS to detect network intrusion. The model utilizes both statistical and payload data for better result. Word embedding and text-convolutional neural are two modern NLP techniques adopted by the model to extract feature from payloads, and ISCX2012 dataset was used for training. Furthermore, the RF algorithm was used in the final classification, and the detection rate achieved by the model was 99.26%.

2.3 *Deep Belief Networks (DBNs)*

A deep belief network is generated by stacking restricted Boltzmann machine (RBM), and the input of an RBM is the result of earlier RBMs. These networks contain a layer of visible nodes and layers of hidden nodes like other neural network architecture. All layers are connected with a unidirectional connection, except for the top two layers, which provide a two-way connection [16].

The authors of [17] suggested a new method based on DBN and PNN (probabilistic neural network) for intrusion detection, which also addressed the problem of falling into local optimal. This method somehow shortens the model's training and testing time by converting raw network data into a low dimension. The benchmark dataset KDD CUP-1999 is used for testing the performance of the method, and results were compared with traditional methods like PNN, PCA-PNN and un-optimized DBN-PNN. However, the actual network environment is more complex than the dataset used; therefore, further, improvement can be applied in real network traffic as an enhancement.

The latter study [18] compares deep and shallow network architecture in network anomaly identification. Authors distinguished between the normal and attack connection. Additionally, model was capable of categorizing an attack to its corresponding category. Experimental results showed that deep networks are essential for real-time anomaly identification (Figs. 2 and 3).

Fig. 2 Autoencoder**Fig. 3** Deep belief network

2.4 Recurrent Neural Networks (RNNs)

These networks contain at least one cycle in its connection graph, and these nodes are also known as the recurrent cell (or nodes). This network architecture can adopt the internal memory to process random sequences of inputs. This architecture is required to perform a complex task. This technique is good for handling real-time learning and processing time-series data. Presently, RNN based on Long Short-Term Memory (LSTM) is a widely known architecture [19].

The authors of [20] proposed a classification model for IDS. This model is based on LSTM-RNN and nadam optimizer as optimizing technique. The experimental results successfully achieved an accuracy of 97.54%. The false alarm rate of 9.98% is also quite acceptable, having a detection rate of 98.95%. Recently, a novel model named BAT-MC was proposed by combining bidirectional Long Short-Term memory (BLSTM) and attention mechanism [21]. The model well-described network traffic behaviour and improved the detection rate and accuracy. The model was tested on KDDTest+ and KDDTest-21 dataset, including NSL-KDD.

The authors of [22] suggest another approach for cyber-attack detection, and the model named HLSTM was capable enough to learn temporal hierarchical features of the complex network traffic data. The detection rate of the system has been greatly improved on the benchmark datasets. The multi-classification accuracy of 83.85% and 69.73% was achieved on both the dataset, namely KDDTest+ and KDDTest-21.

2.5 *Stacked Autoencoder (SAE)*

Stacked autoencoder is generated by adding (stacking) more hidden layer using the greedy approach and can be trained using the same methods for each additional layer. SAE is ideal for transforming the original feature set into more meaningful representation and proved useful for unsupervised learning. SAE efficiently extract feature in unlabelled and complex data, i.e. raw network traffic data. And this unsupervised learning capability is important to detect unknown attacks.

The authors of [23] presented an optimized method to detect impersonation attack in Wi-Fi network using ANN and SAE by selecting the abstract features. The proposed approach successfully achieved a quite acceptable result. But this approach is limited to detect specific attack only. In a latter study, the authors of [24] presented a novel method called deep feature extraction and selection (D-FES). They combined both stacked and weighted feature selection approach to collect meaningful, relevant information from raw network traffic data. The proposed method achieved the most accurate results in detection accuracy and false alarm rate in detecting impersonation attacks in Wi-Fi networks, i.e. 99.918% and 0.012%, respectively. However, future work can enhance the model to detect more attack classes and not limit it for impersonation attacks.

The method presented by [25] is not just limited to impersonation, which was the drawback of the previously mentioned approaches. Here, they presented a solution based on anomaly detection and considered a multi-class problem, i.e. flooding, injection, normal traffic and impersonation attack. The proposed frameworks were developed using the SAE architecture with two and three hidden layers. The model achieved an accuracy of 98.67%, which is quite acceptable as compared to other state-of-the-art methods. A new approach based on anomaly detection to identify DoS attacks in encrypted network traffics was presented [26]. The authors tested this technique on a realistic cyber environment that generated realistic traffic patterns. However, the study can be improved in terms of accuracy and can be tested to perform better in the bigger dataset, i.e. by capturing the network traffic data for several days.

Recently, a model is proposed named TSDL based on deep stacked autoencoder. This model contains two stages and two hidden layers at each stage with softmax classifier. The model is trained in a semi-supervised manner [27]. Results were quite impressive; model achieved good recognition rates of 99.99% and 89.13% for both KDD99 and UNSW-NB15 dataset, respectively, with a low false alarm rate.

Furthermore, future work can improve its performance by combining the proposed approach with novel reinforcement learning.

2.6 Stacked Denoising Autoencoder (SDA)

A new approach in session-based Intrusion Detection System model was presented by the authors of [28]. They implemented an SDA-based deep architecture, and used botnet traffics dataset for evaluation. Researchers obtained relatively impressive results, but the future study can use the network application layer's complete payload data for further improvement.

2.7 Sparse Autoencoder

A Network Intrusion Detection System (NIDS) is suggested using the concept of self-taught learning (STL) and a deep learning-based architecture, i.e. sparse autoencoder [29]. The benchmark dataset, NSL-KDD were used for evaluation. The model performed well, but it has been observed that the proposed technique can be improved by using other deep learning architecture. Additionally, instead of using the derived feature, future work can be done to learn feature from raw network traffic headers on the go.

2.8 Generative Adversarial Network

GANs are composed of two neural networks, i.e. Generator and Discriminator. Generators generate the sample data and discriminators distinguish it from actual data. GANs are based on hybrid deep learning method which utilizes generative features at initial layers and discriminative data at later stages. The authors of [30] proposed intrusion detection model based on GAN and AE named as SAVAER-DNN. The issue of imbalance nature of network traffic data is also addressed by generating new attack samples.

3 Open Issues, Findings and Future Directions

Although, a number of deep learning methods have been presented in this review paper for network anomaly and intrusion detection, still so many unresolved issues and challenges are open for future work.

We found that single deep learning methods explored earliest, but now day's researchers are exploring hybrid deep learning methods. We would also like to encourage researchers to leverage hybrid deep learning methods such as GANs to move towards effective and efficient solutions. Further exploration of hybrid deep learning methods would be worthwhile as they have shown quite acceptable and promising results [30, 32–34].

3.1 Datasets Challenges

There are several publically available network traffic and intrusion detection datasets as shown in Table 1. But most of them are problematic and do not even simulate the real network environment. Also, the attacking scenario is constantly advancing due to which feature selection for one attack situation might not work effectively for others. The other issue is the lack of availability of labelled dataset. And creating the labelled dataset through testbed or simulated environment gathered over a long period is also troublesome.

The Imbalance and the diverse nature of the network traffic datasets are another obstacle for anomaly detection. It will change the actual perspective of the data and might increase false alarm rate. However, the majority of the researchers used KDD99 and its modified version NSL-KDD dataset for intrusion and anomaly detection. Still, both are unreliable and less application in a real network environment. Furthermore, the benchmarks datasets are very old, do not have real-time scenarios and recent traffic behaviour.

As a solution, we would like to encourage researchers to use network traffic from the simulated environment. Real-world and big datasets are also recommended to enhance the performance and detection accuracy of the model. The authors also developed a method based on deep learning and tested it on real-world environment [33].

3.2 Security Challenges

Security for every device existing over the internet is crucial as they are prone to be hacked or attacked at any time. To secure the network, deep learning model should be capable enough to detect all attack, whether successful or unsuccessful immediately. It is critical to secure the network (NIDS) to protect all devices such as hosts, various resources and servers. Furthermore, a powerful threat or attack detection can be achieved through better detection techniques and hence an improved IDS and anomaly detection method based on deep learning would be a key solution to improve the security of the network.

Anomaly-based hybrid deep learning methods can overcome some security issues as they are capable enough to reduce false alarm rate and have a good detection rate for both known and unknown attacks.

3.3 Real-Time Performance

Real-time implementation of anomaly detection model is an important issue to be addressed. Also, the nature of the network anomalies keeps changing with time. Hence, whenever unknown attacks are detected, it is important to update the profile in real-time without compromising the performance.

Deep learning methods are highly computation intensive and required high-performance CPUs and GPUs. Therefore, the improved performance methods can achieve real-time detection of unknown attacks. There are various deep learning techniques like SAE, DBN, etc. that proved efficient for unsupervised feature extraction of network traffic data. The authors of [35] suggested using multi-core CPU and GPU, with highly complex data, like network traffic data for intrusion detection system and anomaly detection methods.

3.4 Complexity of Network Traffic Data

The network traffic data's scale and density are very complex and rapidly growing over the years. To handle such large traffic volume and highly diverse data distribution is very challenging. To reduce network traffic data complexity, developing the appropriate and fast feature selection deep learning techniques would be a key solution.

This survey aimed to provide the complete understating of network anomaly, network traffic classification, intrusion detection problems, and its various aspects. It also includes multiple deep learning methods proposed in this domain with its advantage, drawbacks and improvements for further research.

4 Conclusion

This review paper has explained the importance of computer network security from anomalies, intrusion and various network attacks (like User to Root (U2R), Remote to Local (R2L), Trojan, Probe, etc.). Then we have reviewed and analysed several deep learning methods, techniques in network anomaly and intrusion detection. Two broad categories were identified, i.e. single and hybrid deep learning methods. In this review paper, we have included only single DL approaches. We will also review hybrid deep learning methods in our further study. Finally, we have

discussed open issues and recommendations for researchers and practitioners who are willing to work for network anomaly detection and its security. Even though several open issues and challenges need to be addressed, in contrast, researchers should also keep in mind the quite promising guidelines for further investigation in this domain.

References

1. Choo, K.K.R.: The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **30**(8), 719–731 (2011)
2. Iglesias, F., Zseby, T.: Analysis of network traffic features for anomaly detection. *Mach. Learn.* **101**(1–3), 59–84 (2015)
3. Löf, A., Nelson, R.: Annotating network trace data for anomaly detection research. In: *Proc. Conf. Local Comput. Networks, LCN*, vol. 2014-Novem, no. November, pp. 679–684 (2014)
4. Saied, A., Overill, R.E., Radzik, T.: Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing* **172**, 385–393 (2016)
5. Kang, M.-J., Kang, J.-W.: Intrusion detection system using deep neural network for in-vehicle network security. *PLoS One*, **11**(6), e0155781 (2016)
6. Naseer, S., et al.: Enhanced network anomaly detection based on deep neural networks. *IEEE Access* **6**(8), 48231–48246 (2018)
7. Yu, Y., Long, J., Cai, Z.: Network intrusion detection through stacking dilated convolutional autoencoders. *Secur. Commun. Netw.* **2017** (2017)
8. Alom, M.Z., Taha, T.M.: Network intrusion detection for cyber security on neuromorphic computing system. In: *Proc. Int. Jt. Conf. Neural Networks*, vol. 2017-May, pp. 3830–3837 (2017)
9. Mohammadi, S., Namadchian, A.: A new deep learning approach for anomaly base IDS using memetic classifier. *Int. J. Comput. Commun. Control* **12**(5), 677–688 (2017)
10. Long, E.M.B.J., Liu, Q., Cui, J., Cai, Z.: *SU-IDS : A Semi-supervised and Unsupervised Framework for Network Intrusion Detection*, vol. 1. Springer International Publishing (2018)
11. Al-qatf, M., Lasheng, Y.U., Al-habib, M., Al-sabahi, K.: *Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection*, vol. 6 (2018)
12. O’Shea, K., Nash, R.: *An Introduction to Convolutional Neural Networks*, pp. 1–11 (2015)
13. Wang, W., Zhu, M., Zeng, X., Ye, X., Sheng, Y.: *Malware Traffic Classification Using Convolutional Neural Network for Representation Learning* (2017)
14. Li, Z., Qin, Z., Huang, K., Yang, X., Ye, S.: Intrusion detection using convolutional neural networks for representation learning. In: *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10638 LNCS, pp. 858–866 (2017)
15. Min, E., Long, J., Liu, Q., Cui, J., Chen, W.: TR-IDS : anomaly-based intrusion detection through text-convolutional neural network and random forest. *Secur. Commun. Netw.* **2018** (2018)
16. Ferrag, M.A., Maglaras, L., Janicke, H., Smith, R.: *Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis*, pp. 126–136 (2019)
17. Zhao, g., Zhang, c., Zheng, l.: Intrusion detection using deep belief network and probabilistic neural network. In: *Proc. 2017 IEEE Int. Conf. Comput. Sci. Eng. IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput. CSE EUC 2017*, vol. 1, pp. 639–642 (2017)
18. Vinayakumar, R., Soman, K.P., Poornachandran, P.: Evaluating effectiveness of shallow and deep networks to intrusion detection system. In: *2017 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2017*, vol. 2017-Janua, pp. 1282–1289 (2017)

19. Ferrag, M.A., Maglaras, L., Janicke, H., Smith, R.: Deep learning techniques for cyber security intrusion detection: a detailed analysis. In: 6th International Symposium for ICS & SCADA Cyber Security Research 2019 6, pp. 126–136 (2019)
20. Le, T.T.H., Kim, J., Kim, H.: An effective intrusion detection classifier using long short-term memory with gradient descent optimization. In: 2017 Int. Conf. Platf. Technol. Serv. PlatCon 2017 - Proc., pp. 0–5 (2017)
21. Su, T., Sun, H., Zhu, J., Wang, S., Li, Y.: BAT: deep learning methods on network intrusion detection using NSL-KDD dataset. *IEEE Access* **8**, 29575–29585 (2020)
22. Hou, H., et al.: Hierarchical long short-term memory network for cyberattack detection. *IEEE Access* **8**, 1–1 (2020)
23. Oh, E., Kim, T., Cho, T.: Detecting impersonation attack in WiFi networks using deep learning approach. *Wisa* **1**, 186–197 (2017)
24. Aminanto, M.E., Choi, R., Tanuwidjaja, H.C., Yoo, P.D., Kim, K.: Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Trans. Inf. Forensics Secur.* **13**(3), 621–636 (2017)
25. Thing, V.L.L.: IEEE 802.11 network anomaly detection and attack classification: a deep learning approach. In: 2017 IEEE Wirel. Commun. Netw. Conf., pp. 1–6 (2017)
26. Zolotukhin, M., Hamalainen, T., Kokkonen, T., Siltanen, J.: Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic. In: 2016 23rd Int. Conf. Telecommun. ICT 2016 (2016)
27. Khan, F.A., Gumaee, A., Derhab, A., Hussain, A.: TSDL: a two-stage deep learning model for efficient network intrusion detection. *IEEE Access* **7**, 30373–30385 (2019)
28. Yu, Y., Long, J., Cai, Z.: Session-Based Network Intrusion Detection Using a Deep Learning Architecture, no. January, pp. 144–155 (2017)
29. Niyaz, Q., Sun, W., Javaid, A.Y., Alam, M.: A deep learning approach for network intrusion detection system. In: EAI Int. Conf. Bio-inspired Inf. Commun. Technol. (2015)
30. Yang, Y., Zheng, K., Wu, B., Yang, Y., Wang, X.: Network intrusion detection based on supervised adversarial variational auto-encoder with regularization. *IEEE Access* **8**, 42169–42184 (2020)
31. Min, E., Long, J., Liu, Q., Cui, J., Cai, Z., Ma, J.: Su-ids: a semi-supervised and unsupervised framework for network intrusion detection. In: International Conference on Cloud Computing and Security, pp. 322–334 (2018)
32. Zhang, H., Li, Y., Lv, Z., Sangaiah, A.K., Huang, T.: A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. *IEEE/CAA J. Autom. Sin.* **7**(3), 790–799 (2020)
33. Kim, A., Park, M., Lee, D.H.: AI-IDS: application of deep learning to real-time web intrusion detection. *IEEE Access* **8**, 70245–70261 (2020)
34. Zhong, Y., et al.: HELAD: a novel network anomaly detection model based on heterogeneous ensemble learning. *Comput. Netw.* **169**, 107049 (2020)
35. Potluri, S., Diedrich, C.: Accelerated deep neural networks for enhanced intrusion detection system. In: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8 (2016)

Forest Cover Change Detection Using Satellite Images



Achal Kalwar, Rohan Mathur, Shubham Chavan,
and Chhaya Narvekar

Abstract Deforestation, which has contributed to adverse effects on the natural environment, is one of the challenges to reducing biodiversity and global climate change. Thus, early detection of deforestation is of utmost importance. Inspired by the above situation, this work provides an examination of the automated deforestation detection method. Change detection is used to figure out whether or not the changes occurred using remote sensing images at two different times. This work proposes an idea of effective method for detecting relevant changes in the equivalent scene between two temporally different images. This research analyzes image data from a remote sensing satellite called Landsat-8 in order to track changes in forest cover over a period of time. The findings of such a study will lead to taking steps to conserve the environment.

Keywords Remote sensing · Multi-temporal · Landsat-8 · QGIS · Change detection

1 Introduction

Forests provide us with essential ecological and economic services like clean water and air, soil conservation, climate modulation, timber, food, and shelter for the animals. Forest cover changes are dynamic, expedite, and extensive process [1]. Owing to climate change and man-made factors, the forest cover regions in many parts of the world have been forced to degrade. Development in a metropolitan city like Mumbai comes at the cost of degradation of forest covers. Many forest areas of Mumbai have been forced to deteriorate due to the development of infrastructure. Mumbai's economic development poses a danger to the ecological balance of the forests. Many scientists have predicted that in the coming few decades, and the city will lose its green lungs.

A. Kalwar (✉) · R. Mathur · S. Chavan · C. Narvekar
Xavier Institute of Engineering, Mumbai, India
e-mail: chhaya.n@xavier.ac.in

Remote sensing is acquiring information about objects or areas without making physical contact with the object [2]. One of the commonly used applications of remote sensing is tracking of the forest covers. Remote sensing forms to be an economic tool for forest mapping as it is cheaper and also faster compared to other methods of surveying. Change detection using remote sensing technique is based on a series of multi-temporal satellite images which uses various classification algorithms along with geographic information system (GIS) tool that provides a suitable platform for data analysis. The paper mainly focuses on studying and monitoring the pattern of forest cover change using temporal satellite data from different time periods and deep learning image classification techniques.

2 Problem Definition

Around 3.4 billion hectares of the world is covered by forest. For development purposes, 15,000 km² of forests have been diverted in the past three decades [3]. There is not any continuous monitoring system for forest cover change which includes forest inventory or geographical information system which keeps track of land use which can give actual figures. This lack of the system and great concern involved in the increased destruction of forest cover change has led to the need to propose a system for the proper forest, management, and decision improvement [4].

Due to this lack of the system and great concern involved in the increased destruction of forest cover change has led to the need to propose a system for proper forest management and decision improvement. From the above context, the following problems are identified:

- Decline in the area under forest.
- Loss of biodiversity and habitat.
- Transformation of the reserved and protected forest areas into developed and agricultural areas [5].

The proposed system is designed to tackle the above-mentioned problems by studying the change cover detection of forest areas over the past few years. Remote sensing (RS)-based tools along with deep learning techniques are used to classify the multi-temporal Landsat 8 images.

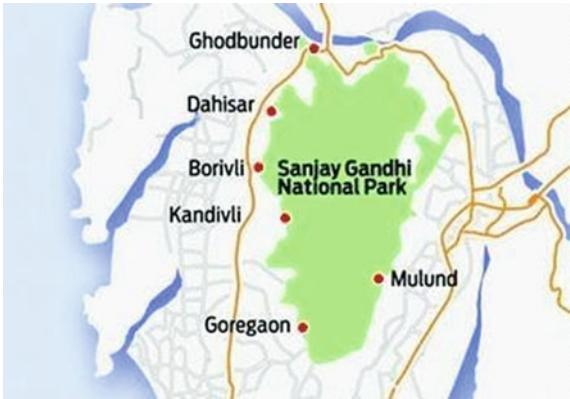
3 Data and Study Area

The research area is Sanjay Gandhi National Park, a protected area spread over approximately 87 km² in Mumbai. It covers a geographical location between 19° 8' N 72° 53' E and 19° 21' N 72° 58' E. The park occupies the majority of the northern suburbs of Mumbai. The suburbs Goregaon, Malad, Kandivali, Borivali,

Table 1 Satellite data details

Date	Satellite/Sensor
November 19, 2013	Landsat 8 OLI
November 01, 2018	Landsat 8 OLI

Fig. 1 Study area



and Dahisar lie to the west. Bhandup and the Mulund suburbs lie to the east [4] and to the south lie Aarey Milk Colony. The forest enters Thane City in the north. The Sanjay Gandhi National Park is home to more than 270 bird species, 35 mammal species (including leopards), and 1300 plant species [6].

Landsat 8 OLI multi-temporal remote sensing data for November 2013 and November 2018 has been acquired. The remote sensing data was gathered from the geological survey of the United States (USGS) archives [7, 8]. Table 1 provides the details of satellite data used (Figs. 1, 2 and 3).

4 Literature Survey

Usually, current change detection techniques adopt one of two ways, using either post classification analysis or analysis of difference image. Owing to the high-resolution nature of satellite images, these approaches are also resource-intensive and time-intensive. The post classification method would first classify the two temporally distinct images of the equivalent scene and then compare them to determine the changes. The second approach is comparative study, which produces a difference image (DI). In order to determine the extent of the changes, further DI research is then undertaken [9, 10].

Deep learning (DL) methods have recently been successfully applied to the image processing of remote sensing (RS). It is possible to learn several layers of data representation using deep neural networks (DNNs) and extract more robust and abstract features, which typically offer more useful knowledge than hand-crafted

Fig. 2 Satellite view of Sanjay Gandhi National Park

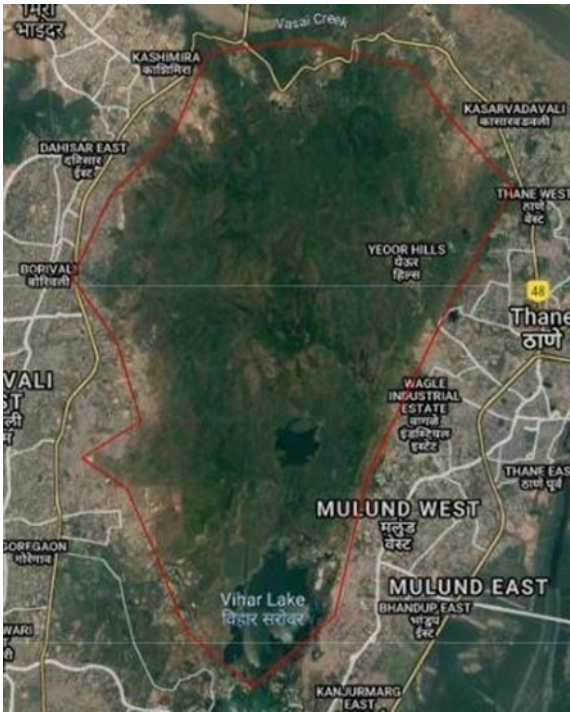
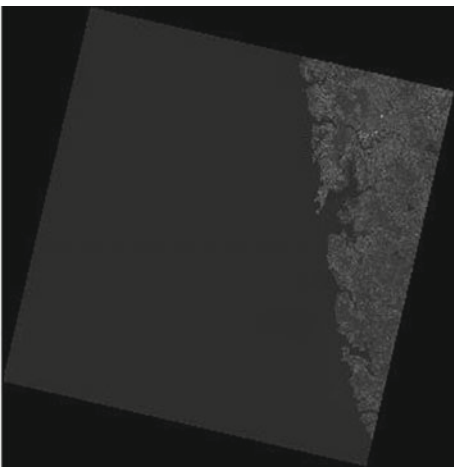


Fig. 3 Raw satellite image downloaded from USGS



ones. In this context, variants of DNNs are possible candidates for automatic deforestation detection, such as convolutional neural networks (CNNs) and Siamese networks [11, 12].

In remotely sensed data, the prevalent approaches to change detection can be classified into two main classes—low-level local approaches and object-based approaches. Low-level approaches allow use of statistical indexes extracted from spectral image pixel values. Object-based methods take qualitative information into account by focusing on homogeneous pixels, which are typically clustered together on the basis of their appearance, position, and/or temporal properties [13].

Before detecting the change, the feature extraction stage is necessary when using machine learning algorithms. The feature extraction step is used to improve multispectral image precision. But, when using deep learning algorithms, no separate feature extraction process is necessary. The accuracy of the classification is dependent on the algorithms used to classify the changes, as well as the resolution of the images. We also concluded that deep learning algorithms have provided higher accuracy than techniques for machine learning [14].

Image processing techniques, image fusion, fuzzy clustering, and difference image (DI) are the earlier methods of change detection. The traditional methods are not very accurate in detecting the changes from the satellite images. Change detection methods can be classified as either supervised or unsupervised. To derive an appropriate training set, the supervised approach requires a ground truth. The unsupervised method, by allowing a simple comparison of multi-temporal images without adding any additional detail, performs change detection [3, 15].

In general, relative to other machine learning approaches, the drawbacks of deep learning are the need for large and high-quality training data, as well as hardware restrictions related to GPU computing capacity. The most notable benefit of deep learning is the degree of automation and the high ability to generalize by using large quantities of representative training data, which, however, may not always be available, particularly with regard to ground-truth labels that might be scarce or not exist at all [16, 17].

5 Methodology

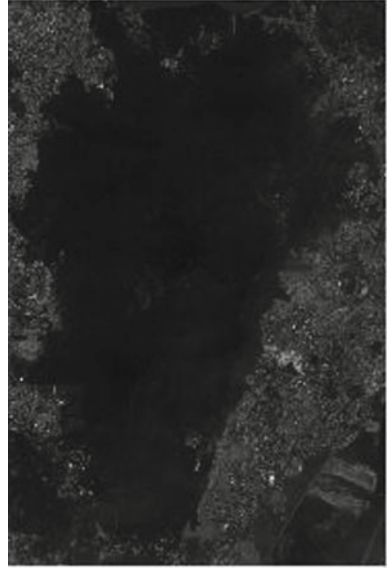
5.1 *Extraction of Study Area*

The initially downloaded multi-temporal satellite images were clipped, and the area of Sanjay Gandhi National Park was extracted with the help of QGIS clipper tool [18].

QGIS is a free and open-source cross-platform desktop geographic information system (GIS) program that facilitates accessing, editing, and analyzing geospatial data [19].

The clipped images were further processed to make several atmospheric corrections. Clipped images were the input source for the QGIS semi-automatic classification plugin tool, which generated reflectance images as its output [18]. Reflectance images typically contain spectral details of the specified area and are

Fig. 4 Clipped image



used for image classification or image processing. Figure 4 shows the raw satellite image of the study area which is clipped using the QGIS clipper tool.

5.2 *Study of Spectral Bands*

A spectral band is a matrix of points identified by three dimensions, their coordinates, and their radiance-related strength [20]. In different combinations, the multispectral image bands were combined and applied to the obtained reflectance images. To get the final processed image, the band combination 5-4-3 was used. The 5-4-3 band combination uses the near-infrared band (NIR), which is more useful for showing and distinguishing land cover from urban and agricultural areas [21, 22].

6 Conclusion

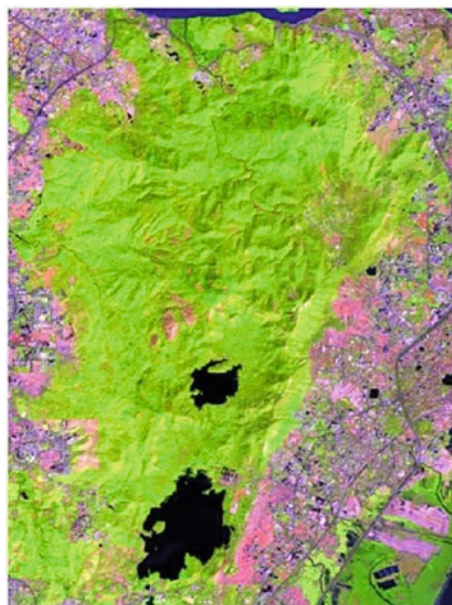
The dataset has been acquired successfully from the USGS website. We have performed preprocessing on the data and have successfully extracted the area of study by clipping the initially acquired images for the year 2013 and 2018 and also applied a band combination 5-4-3 using QGIS. It is possible to monitor forest cover changes using satellite images [23]. This study tests the technological potential of satellite imagery to quantify and monitor forest cover along with the use of deep

learning techniques to classify multi-temporal satellite images to assess if there has been some change in the forest cover being analyzed. This research will help to take precautions to conserve forests. Government agencies should take adequate steps to conserve the environment in Mumbai and not allow it to be sacrificed at the cost of urban development (Figs. 5 and 6).

Fig. 5 Satellite image of November 19, 2013



Fig. 6 Satellite image of November 01, 2018



7 Future Scope

The satellite images obtained after performing preprocessing steps, extracting the area of interest, applying atmospheric the correction, and using a suitable band combination are the final images that will be used as an input to the convolutional neural network (CNN) model. Further, a CNN model will be developed using a suitable activation function and optimization algorithms [24]. To learn the sequence of information compared to the global pattern of a conventional neural network, CNN uses filters on the raw pixel of an image [25]. This model will extract features from each input image and will compare them for image classification. The image classification will result in an output image that will display the pattern of forest cover change over the years.

References

1. <http://www.fao.org/3/XII/0586-C1.htm>, last accessed 2020/09/23
2. https://en.wikipedia.org/wiki/Remote_sensing, last accessed 2020/02/11
3. <https://www.encyclopedia.com/environment/energy-government-and-defense-magazines/forest-resources>, last accessed 2020/03/13
4. https://en.wikipedia.org/wiki/Sanjay_Gandhi_National_Park, last accessed 2020/04/25
5. Yismaw, A., Gedif, B., Addisu, S., Zewudu, F.: Forest cover change detection using remote sensing and GIS in Banja district, Amhara region, Ethiopi. *Int. J. Environ. Monit. Anal.*, 23 Dec 2014
6. <https://mumbaimirror.indiatimes.com/mumbai/cover-story/park-in-peril/articleshow/62773396.cms>, last accessed 2020/08/11
7. <https://earthexplorer.usgs.gov/>, last accessed 2020/04/11
8. <https://www.usgs.gov/core-science-systems/nli/landsat/landsat-8-data-users-handbook>, last accessed 2020/12/11
9. de Jong, K.L., Bosman, A.S.: Unsupervised Change Detection in Satellite Images Using Convolutional Neural Networks, 21 Mar 2019
10. Boriah, S., Mithal, V., Garg, A., Steinbach, M., Kumar, V.: Automated Detection of Forest Cover Changes. *Igarss* (2010)
11. Ortega, M.X., Bermudez, J.D., Happ, P.N., Gomes, A., Feitosal, R.Q.: Evaluation of deep learning techniques for deforestation detection in the amazon forest. *ISPRS Ann. Photogram. Remote Sens. Spat. Inf. Sci.* **IV**-2/W7 (2019)
12. Bragilevsky, L., Bajic', I.V.: Deep Learning for Amazon Satellite Image Analysis. *IEEE* (2017)
13. Khan, S.H., He, X., Porikli, F., Bennamoun, M.: Forest change detection in incomplete satellite images with deep neural networks. *IEEE Trans. Geosci. Remote Sens.* (August 2018)
14. Vignesh, T., Thyagarajan, Ramya, K.: Change detection using deep learning and machine learning techniques for multispectral satellite images. *UJITEE*, **9**(Issue-IS) (November 2019). ISSN: 2278–3075
15. Henderson, J., Piwowar, J.: Analysis of Changes in Vegetation Condition in Grasslands National Park Using Remote Sensing. *IEEE* (2006)
16. Hamdi, Z.M., Brandmeier, M., Straub, C.: Forest Damage Assessment Using Deep Learning on High Resolution Remote Sensing Data, *MDPI*, 22 Aug 2019
17. Bhatt, A., Ghosh, S.K., Kumar, A.: Automated Change Detection in Satellite Images Using Machine Learning Algorithms for Delhi, India. *IGARSS* (2015)

18. <https://plugins.qgis.org/plugins/SemiAutomaticClassificationPlugin/>, last accessed 2020/11/06
19. <https://en.wikipedia.org/wiki/QGIS>, last accessed 2020/05/16
20. <https://www.sciencedirect.com/topics/earth-and-planetary-sciences/spectral-band>, last accessed 2020/06/21
21. <https://openweather.co.uk/blog/post/satellite-imagery-landsat-8-and-its-band-combinations>, last accessed 2020/06/01
22. Dsouza, H., Gupta, S.: A study in change in vegetation cover in an urban environment: a multi-spectral, multitemporal analysis of Mumbai suburban district using remote sensing. *J. Agroecol. Nat. Resour. Manage.* **3**(2) (July-September 2016)
23. Coppin, P.R., Bauer, M.E.: *Change Detection in Forest Ecosystems with Remote Sensing Digital Imagery* (1996)
24. Hu, F., Xia, G.-S., Hu, J., Zhang, L.: Transferring Deep Convolutional Neural Networks for the Scene Classification of High-Resolution Remote Sensing Imagery", *MDPI*, November 2015
25. <https://www.guru99.com/convnet-tensorflow-image-classification.html>, last accessed 2020/10/19

FPGA-Based Design Architecture for Fast LWE Fully Homomorphic Encryption



Sagarika Behera  and Jhansi Rani Prathuri 

Abstract A high-speed field-programmable gate array (FPGA) implementation architecture is purposed to implement fast learning with error (LWE) fully homomorphic encryption. Currently, there are many security issues with conventional cryptosystems. In addition, encrypting and decrypting a large volume of data consume enormous computing time which makes the conventional cryptosystems ineffective. In this work, a novel fully homomorphic encryption algorithm, LWE, has been analyzed using linear algebraic equations. The same has been simulated in Python. In addition, to map the LWE scheme in the FPGA, digital circuits are conceptualized to implement mathematical operations such as modulo adder, multiplier, and noise generator.

Keywords Field programmable gate array (FPGA) · Learning with error (LWE) · Modulo adder · Multiplier · Noise generator

1 Introduction

In this new digital era of transmission, communication, and storing of data in the cloud, cryptography plays a major role. Various industries produce massive quantities of data every day, which is then processed in the cloud. Industries such as financial sectors, health industries, stock markets, defense sectors, IoT applications, IT industries, and power sectors generate large volume of data every day. Various cloud service providers (CSP) are used by various industries to save their information in the cloud. As a result, cloud computing has become increasingly important in the digital age. Since data are stored in some other location that is not in control of the client, the CSP is responsible to secure the client information. User encrypts his or her data before uploading it to the cloud server. CSP maintains privacy of the user and the secrecy of the data. Cryptography is required for all

S. Behera (✉) · J. R. Prathuri
CMR Institute of Technology, Bengaluru, India
e-mail: sagarika.b@cmrit.ac.in

these operations. Cloud computing provides different types of services such as PaaS, SaaS, IaaS, and XaaS with less price. With these services, cloud computing also provides a powerful computing model with low cost. Cloud computing is facing various security issues such as data leakage, the privacy of sensible data, cyber-attacks, and account hijacking. If the client wants to do some computing on the encrypted data saved on the server in the cloud, then the client has to share the private key with the server to decrypt the encrypted data. This may lead to different types of data security issues. To avoid this type of situation, many prefer smart computation on encrypted data. In this computation method, the client will not share the secret key with the third party. Computation on encrypted data will be carried out, and the encrypted form will be the output of the operation. Homomorphic encryption (HE) enables encrypted data to work in such a way. This enables the cloud server to compute the encrypted data without accessing the customer's secret key. This technology came to the picture just 12 years back. Since then, more researchers started working in this area. In the cloud computing and big data environment, customers are accepting this technology, since they are not going to lose the confidentiality and secrecy of their critical and sensitive data. Fully homomorphic encryption (FHE) is the most common type of homomorphic encryption technique as it allows various operations without decrypting the encrypted data. It enables arbitrary circuits of unbounded depth to be evaluated. The basic concept of FHE is shown in Fig. 1 and explained below.

Let $M1$ and $M2$ are two messages, op is an operator and R is the result one gets after performing the operation, and $R1$ is holding the encrypted form of the result.

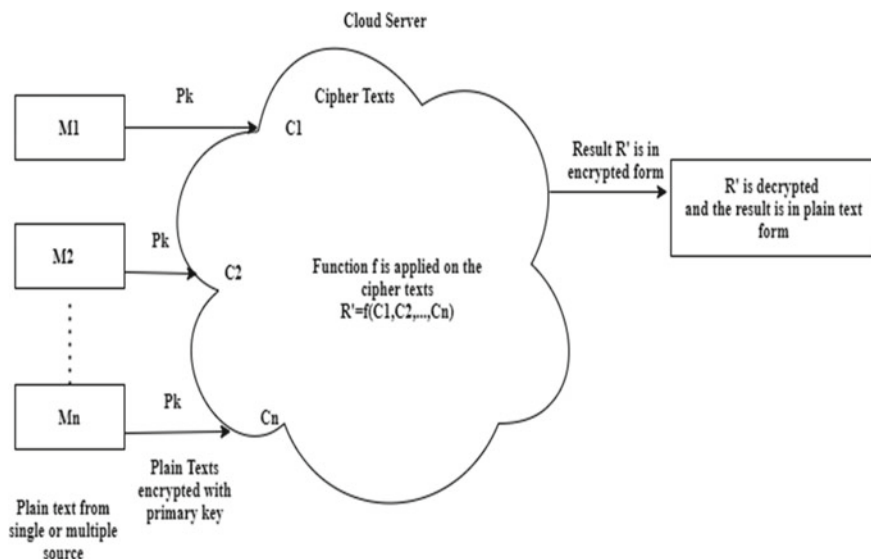


Fig. 1 FHE processing on the cloud data

$$R = M1 \text{ op } M2 \quad (1)$$

$$R1 = \text{Encrypted}(R) = \text{Encrypted}(M1 \text{ op } M2) \quad (2)$$

Let $C1$ and $C2$ be the encrypted versions of $M1$ and $M2$, respectively. Same operation has been carried out on the encrypted form. The result is denoted by R' .

$$R' = C1 \text{ op } C2 \quad (3)$$

As per the homomorphic encryption scheme, Eq. (2) = Eq. (3)

$$\text{Encrypted}(M1 \text{ op } M2) = \text{Encrypted}(M1) \text{ op } \text{Encrypted}(M2) = C1 \text{ op } C2 \quad (4)$$

After decryption the result R' will be equivalent to R .

$$\text{Decr}(C1 \text{ op } C2) = M1 \text{ op } M2 \quad (5)$$

There are four steps involved in the FHE scheme. So the FHE scheme can be represented as the quadruplet of algorithms (KeyGen, Encr, Eval, Decr).

- KeyGen(r): It is an algorithm for generating keys. It takes a random number r as input and returns Pk as a public key and Sk as a secret key as output.
- Encr(M, Pk): Encryption algorithm takes two inputs: a plain text message M and a public key Pk . As an output, it generates ciphertext C .
- Eval($f, C1, C2, \dots, Cn$): It is an evaluation algorithm. This is a homomorphic-specific operation, which takes cipher texts $C1, C2, \dots, Cn$ as input and applies the function f on those ciphertexts. The output of the operation will be in encrypted form. The most important point is that here, the format of the output after the evaluation process should be preserved in order to decrypt it correctly.
- Decr(C, Sk): Decryption algorithm accepts the C as ciphertext and the secret key Sk as inputs and plain text M is retrieved.

2 Related Work

In the year 2009, Craig Gentry [1] gave the most powerful smart computation FHE concept to the research community. Since then, researchers are working in this field to make it more efficient. Before that, homomorphic encryption concept was there, but all of them were partial homomorphic encryption. Partial homomorphic encryption method supports only one type of operation (multiplication or addition).

Some cryptographic algorithms which support partial homomorphic encryption are RSA, ElGamal, and Paillier encryption methods. RSA and ElGamal encryption methods support the multiplicative homomorphic property. Paillier encryption method supports the additive homomorphic property. Gentry [1] gave an FHE scheme which is lattice-based homomorphic encryption. However, as the depth of the circuit grows, so does the noise. He then modified his scheme and made it bootstrapping. In bootstrapping scheme, a class of circuit also contains its own decryption circuit. Van Dijk et al. [2] proposed an FHE scheme which is based on the concept of partially homomorphic encryption over integers. Two types of the gate (addition and multiplication) can be evaluated by somewhat homomorphic encryption scheme. The complete working model of FHE scheme was proposed by Gentry and Halevi [3]. Halevi [4] explained all the concepts of different types of the homomorphic encryption schemes.

Without bootstrapping, Brakerski et al. [5] proposed a fully homomorphic concept. For constructing leveled fully homomorphic encryption schemes, this scheme uses learning with error (LWE) and ring-LWE (RLWE). Brakerski and Vaikuntanathan [6] improved the scheme presented in [5]. They stated that the ciphertext generated by their proposed scheme is shorter and can be used for the single-server private data retrieval (PIR) protocol based on LWE. Chatterjee and Aung [7] explained the different types of homomorphic encryption schemes with circuit and their application in the real world. Yi et al. [8] briefed about the homomorphic encryption schemes and their applications. Su et al. [9] proposed FPGA-based architecture for ring-LWE (RLWE) problem.

Luo et al. [10] made a learning with rounding (LWR)-based FHE scheme to eliminate the tangly modulus problem using approximate eigenvector method. They extended their scheme to construct multi-key FHE which is an alternative to LWE-based multi-key FHE. They claimed that their scheme can be applied to multiparty computation with high efficiency. LWE-based FHE scheme presented in [5, 6] is more secure and efficient compared to the scheme presented in [1, 2, 11, 12]. Kim et al. [13] performed a secure search operation on encrypted genomes which were encrypted using homomorphic encryption. Applications of homomorphic encryption in different fields such as privacy preserving data mining, private data retrieval, privacy preserving prediction, multiparty computation, and training neural networks over encrypted data are given in [14–17]. Since 2009, after Gentry's FHE scheme [1], many researchers are working in this area to improve the performance. Fan et al. [18] compared LWE scheme with RLWE scheme. They have analyzed various homomorphic operations such as multiplication and bootstrapping and derived worst case bounds on the noise caused by these operations. In the paper [19], the authors claimed that their modified LWE scheme which is based on approximate eigenvector method is easier to understand and asymptotically faster than the previous LWE scheme. Ducas et al. [20] claimed that their bootstrapping method for homomorphic encryption takes about half a second to run on a personal computer. Fast fully homomorphic encryption (TFHE) [21] is the improvement of FHE scheme which is based on GSW and its ring variants.

The authors of the paper [21] demonstrated a new bootstrapping circuit that converts LWE ciphertexts to low-noise RingGSW ciphertexts in few milliseconds.

LWE, a modern fully homomorphic encryption algorithm, is analyzed using linear algebraic equations in this paper. The same has been simulated in Python. Further, this LWE has been converted to binary strings, and mathematical circuits such as modulo adder, multiplier, and a noise generator are conceptualized to map the LWE scheme in the FPGA architecture.

In Sect. 3, LWE-based homomorphic encryption scheme is explained. In Sect. 4, the design architecture for the FPGA-based LWE scheme is covered. Section 5 explains the implementation and simulation result of the LWE scheme. Finally, the paper is concluded in Sect. 6.

3 LWE-Based Homomorphic Encryption Scheme

Oded Regev first proposed the LWE problem in 2005. After that, it is put to use in a public key cryptosystem. Brakerski et al. [6] proposed a LWE-based fully homomorphic encryption scheme. First, we will describe the LWE problem, and then, we will describe how to do encryption with LWE.

This is how the LWE problem is described. Let $\mathbb{Z}_q$ be the ring of modulo q integers and $\mathbb{Z}_q^n$ be the set of n number of vectors over $\mathbb{Z}_q$. There is an unknown linear function f , defined as $f: \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$. The LWE problem takes a pair $(\mathbf{x}, \mathbf{y})$ as input, $\mathbf{x} \in \mathbb{Z}_q^n$ and $\mathbf{y} \in \mathbb{Z}_q$. As a result $y = f(\mathbf{x})$ having high probability. Due to some minor error, some deviation will be there from the equality.

Now we will describe how to create a FHE scheme using this LWE concept. Let $\vec{S}$ is a secret vector and $\vec{S} \in \mathbb{Z}_q^n$, A is a uniform matrix and $A \in \mathbb{Z}_q^{n \times M}$, $\vec{\eta}$ is a small noise vector where $\vec{\eta} \in \mathbb{Z}_q^M$ and the elements of this noise vector are very small, where $|\eta_i| \leq \alpha q$ and α are very tiny. $\vec{S}$ and $\vec{\eta}$ are selected randomly. The secret vector is multiplied with the uniform matrix and noise is added to it. We got another vector $\vec{b}$ and $\vec{b} \in \mathbb{Z}_q^M$.

$$\vec{b} = \vec{S}.A + \vec{\eta} \quad (6)$$

So Eq. (6) tells that if we have a random noisy linear equation with mod integer (q), then it is computationally indistinguishable from the uniform equation.

Now we will consider a new matrix $(-A)$ where $A \in \mathbb{Z}_q^{(n+1) \times M}$ and 1 is concatenated with $\vec{S}$. So the new secret vector $\vec{S} \in \mathbb{Z}_q^{n+1}$.

$$\vec{\eta} = \vec{b} - \vec{S}.A \quad (7)$$

So small noise vector can be written as $\vec{S}.A = \vec{\eta}$. Now we will discuss how the encryption of the message can be performed from LWE.

Here matrix A is the public key and $\vec{S}$ is the secret key. A uniform binary vector $\vec{r}$ is multiplied with A and encoded message $\vec{y}$ is added to it, and we got the cipher text $\vec{C}_y$. So the cipher text is

$$\vec{C}_y = A. \vec{r} + \vec{y} \quad (8)$$

So the attacker can see the public key and the cipher text. It will be difficult for the attacker to find the message since it cannot find out the secret key. If we want to encrypt "0," then $\vec{y}$ will be 0. If we want to encrypt "1," then $\vec{y}$ will be a random vector. Now we will discuss the decryption process. We will multiply the secret key with the cipher text.

$$\vec{S} \vec{C}_y = \vec{S} A. \vec{r} + \vec{S} \vec{y} = \vec{\eta} \vec{r} + \vec{S} \vec{y} \quad (9)$$

In Eqs. (8) and (9), we have shown the encryption and decryption processes for the vector. Now it can be generalized to matrices where A , R , and Y are the matrices.

So the encryption process will be $A R + Y = \vec{C}_y$ where R is the binary matrix consists of $\{0,1\}$ of size $M \times N$, and Y is the encoded message of size $(n + 1) \times N$. Decryption process will be $\vec{S} \vec{C}_y = \vec{\eta} R + \vec{S} Y$.

Now we will discuss the eigenvector method and approximate eigenvector, and then, how to perform encryption and decryption on approximate eigenvector. It was observed that if C_1 and C_2 are two matrices with same eigenvector $\vec{S}$ and m_1, m_2 are respective eigenvalues with respect to same eigenvector $\vec{S}$, then it holds the following properties.

1. $C_1 + C_2$ has eigenvalue $(m_1 + m_2)$ with respect to same eigenvector $\vec{S}$.
2. $C_1.C_2$ has eigenvalue $m_1 m_2$ with respect to same eigenvector $\vec{S}$.

It is satisfying the fully homomorphic properties, but it is not secure. Eigen vector can be easily calculated. So we will take approximate eigenvector where secret key $\vec{S}$ is the eigenvector and C is the cipher text, m is the encoded message and $\vec{e}$ is small noise or error. The corresponding linear equation is given below.

$$\vec{S}.C = m\vec{S} + \vec{e} \quad (10)$$

It is decryptable if $|\vec{e}| < q$. Fully homomorphic properties of approximate eigenvector are given below. Let C_1 and C_2 are two cipher texts. Applying Eq. (10) on C_1 and C_2 , we got the following two equations.

$$\vec{S}C_1 = m_1\vec{S} + \vec{e1} \quad \text{and} \quad \vec{S}.C_2 = m_2\vec{S} + \vec{e2}$$

After performing addition operation on these two cipher texts

$$\begin{aligned} C_{\text{add}} &= C_1 + C_2, \Rightarrow \vec{S} \cdot (C_1 + C_2) = \vec{S} \cdot C_1 + \vec{S} \cdot C_2 \Rightarrow m_1 \vec{S} + \vec{e}_1 + m_2 \vec{S} + \vec{e}_2 \\ &\Rightarrow (m_1 + m_2) \vec{S} + (\vec{e}_1 + \vec{e}_2) \end{aligned} \quad (11)$$

After addition of two cipher texts, noise grows a little. Now we will perform the multiplication operation on these two cipher texts.

$$\begin{aligned} C_{\text{mult}} &= C_1 \cdot C_2 \Rightarrow \vec{S} \cdot (C_1 \cdot C_2) \Rightarrow (m_1 \vec{S} + \vec{e}_1) C_2 \Rightarrow m_1 C_2 \vec{S} + C_2 \vec{e}_1 \Rightarrow m_1 (m_2 \vec{S} + \vec{e}_2) + C_2 \vec{e}_1 \\ &\Rightarrow m_1 m_2 \vec{S} + (m_1 \vec{e}_2 + C_2 \vec{e}_1) \end{aligned} \quad (12)$$

Compared to addition operation, noise grows more in multiplication operation. If we will generalize the growth of noise during homomorphic circuit evaluation, then it can be represented as below.

The noise increases by the factor $(N + 1)$ at each step. At depth “ d ,” noise will grow by $(N + 1)^d$, where N is the size of polynomial. For decryption, we need the noise to be small.

4 FPGA-Based Design Architecture for LWE Scheme

FPGA-based design architecture for LWE scheme contains three blocks as shown in Fig. 2. The components and functions of three blocks are explained below.

- **Key Generator:** It contains true randomness generator (TRG), which generates a symbol series that resembles a uniformly random sequence. It generates the public key matrix A . Polynomial multiplier multiplies A with the secret key S . The modular operation is performed on the output of the multiplier, and it is added to the noise e . So the output of the polynomial adder is the public key b . The output of the key generator is two public keys A and b .
- **Encryption:** This is the second module which takes input message m and gives the encrypted message in the form (u, v) . Public key A is multiplied with r (binary uniform vector), and a modular operation is performed on it to get u . Message m and $q/2$ are multiplied by scalar multiplier, and the result is added to public key b and modular reduction is applied on it to get the value v .
- **Decryption:** In this module, u and S are multiplied, and the result is subtracted from v . If the result is less than $q/2$, it is 0 otherwise 1.

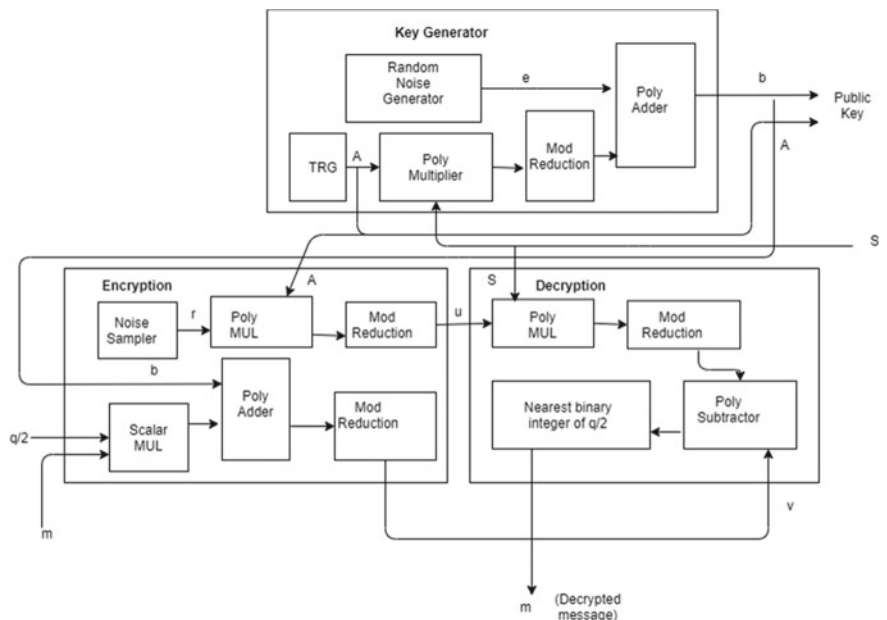


Fig. 2 FPGA-based design architecture for LWE scheme

5 Result and Implementation

Implementation of LWE and the result are discussed here. First, a random series of values are selected for our public key A . We have selected 20 random values in the range of 0–137.

Public key (A): [4, 46, 82, 132, 117, 10, 28, 47, 75, 7, 125, 45, 22, 104, 16, 57, 65, 18, 48, 122]

Prime number q is 137, the secret key S is 43, and e is small error values.

Error vector (e): [2, 2, 2, 1, 1, 2, 2, 2, 3, 1, 2, 1, 2, 1, 1, 2, 3, 2, 2, 1]

List B is generated using the method $B_i = A_i S + e_i \pmod{q}$

List (B): [37, 62, 103, 60, 100, 21, 110, 105, 77, 28, 34, 18, 126, 89, 4, 124, 58, 91, 11, 41]

We took two message values 9 and 5 for encryption.

Bits to be ciphered: [1, 0, 0, 1, 0, 0, 0, 0], [1, 0, 1, 0, 0, 0, 0, 0]

We calculated two values u and v using the following method. Where $u = \sum A_i \pmod{q}$ and $v = \sum B_i + q/2.M \pmod{q}$. The encrypted message sample (u, v) is given below.

[11, 9], [3, 5], [14, 8], [11, 4], [0, 9], [17, 1], [12, 6], [16, 6]

For decryption, we have used the following calculation.

$$\text{Decr} = v - Su(\text{mod } q)$$

If $\text{Decr} < q/2$, then the message bit is 0 else it is 1.

Result bit0 is: 0, result bit1 is: 0, result bit2 is: 1, result bit3 is: 1

6 Conclusion and Future Work

Mathematical analysis and simulation of a fully homomorphic LWE algorithm have been carried out in order to map all the mathematical expressions into FPGA. It is concluded that the mathematical operations namely polynomial adder, subtractor, multiplier, modulo reduction, and random number generator for a large length of binary strings can easily be implemented in modern FPGA. FPGA-based architecture also implements a large amount of mathematical operations which are typical for LWE fully homomorphic encryption. The computation is also faster compared to central processing unit (CPU), graphics processing unit (GPU), and general purpose computing on graphics processing unit (GPU). Our future work will be the simulation of LWE in VHDL and real-time implementation in FPGA board to quantify the claim of this work.

References

1. Gentry, C.: Fully Homomorphic Encryption Scheme. Stanford University (2009)
2. Van Dijk, M., Craig Gentry, Halevi, S., Vaikuntanathan V.: Fully homomorphic encryption over the integers. In: Proceedings of Advances in Cryptology, pp. 24–43, EUROCRYPT'10 (2010)
3. Gentry, C., Halevi, S.: Implementing Gentry fully homomorphic scheme. In: Proceedings of Advances in Cryptology, EUROCRYPT'11, pp. 129–148 (2011)
4. Halevi, S.: Homomorphic Encryption, In: *Tutorials on the Foundations of Cryptography*, pp. 219–276. Springer Cham (2017)
5. Brakerski, Z., Craig Gentry, Vaikuntanathan, V.: Fully homomorphic encryption without bootstrapping, In: *Innovations in Theoretical Computer Science (ITCS'12)* (2012)
6. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (Standard) LWE. *SIAM J. Comput.* **43**(2), 831–871 (2014)
7. Chatterjee, A., Aung, K.M.M.: Fully Homomorphic Encryption in Real World Applications. <http://www.springer.com/series/15213>
8. Yi, X., Paulet, R., Bertino, E.: Homomorphic Encryption and Applications. <https://www.springer.com/series/10028>
9. Su, Y., Yang, B., Yang, C., Tian, L.: FPGA-based hardware accelerator for leveled ring-LWE fully homomorphic encryption, 168008–168025. *IEEE Access* **8** (2020)
10. Luo, F., Wang, F., Wang, K., Li, J., Chen, K.: LWR-Based Fully Homomorphic Encryption, Revisited, *Security and Communication Networks* (2018). <https://doi.org/10.1155/2018/5967635>

11. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Annual Cryptography Conference, vol. 6841 of Lecture Notes in Computer Science, pp. 505–524, Springer, Heidelberg, Berlin, Germany (2011)
12. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes, Public Key Cryptography, vol. 6056 of Lecture Notes in Computer Science, pp. 420–443, Springer, Berlin, Germany (2010)
13. Kim, M., Song, Y., Cheon, J.H.: Secure searching of biomarkers through hybrid homomorphic encryption scheme. BMC Med. Genomics, **10**(2), 42 (2017)
14. Yi, X., Kaosar, M.G., Paulet, R., Bertino, E.: Single database private information retrieval from fully homomorphic encryption. IEEE Trans. Knowl. Data Eng. **25**(5), 1125–1134 (2012)
15. Bos, J.W., Castryck, W., Iliashenko, I., Vercauteren, F.: Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling. In: International Conference on Cryptology in Africa, Springer, pp. 184–201 (2017)
16. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., Wemsing, J.: Cryptonets: applying neural networks to encrypted data with high throughput and accuracy. In: International Conference on Machine Learning, pp. 201–210 (2016)
17. Xu, R., Joshi, J.B., Li, C.: CryptoNN: training neural networks over encrypted data. In: IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 1199–1209 (2019)
18. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption, IACR Cryptol. 144 (2012)
19. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Annual Cryptology Conference, Springer, pp. 75–92 (2013)
20. Ducas, L., Micciancio, D.: FHEW: bootstrapping homomorphic encryption in less than a second. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 617–640 (2015)
21. Chillotti, I., Gama, N., Georgieva, M., Izabachene, M.: TFHE: fast fully homomorphic encryption over the torus. J. Cryptol. **33**(1), 34–91 (2020)
22. Clear, M., McGoldrick, C.: Multi-identity and multi-key leveled FHE from learning with errors. In: Proceedings of the Annual Cryptography Conference, pp. 630–656, Springer, Heidelberg, Berlin, Germany (2015)

Hierarchal Communication Architecture for Multi-level Energy Harvesting Support in Underwater Sensor Network



Anuradha, Amit Kumar Bindal, Devendra Prasad,
and Afshan Hassan

Abstract Communication by using an energy-saving approach is a vital requirement of an energy-constrained underwater sensor network. The underwater acoustic communication technique ordinarily governs the usage of clout. The network's capability to communicate the collected facts is affected due to minimal renewing capacity in case of the underwater wireless sensor network. The proposed work describes the reliable resources available in underwater for the sensors. The proposed scheme provides the mechanism for energy harvesting from tidal energy into electrical energy to charge the Li-ion cells used in sensors. To cover the maximum area of the ocean sensor, the data aggregators are deployed at three different levels (i.e. bottom, middle and top levels). The sensors deployed in oceans at the top level are static, whereas they are mobile at middle and bottom levels.

Keywords Underwater sensor network (UWSN) • Energy harvesting • Li-ion • Underwater acoustic sensor networks (UW-ASNs)

Anuradha

ECE Department, M. M. Engineering College, M. M. (Deemed To Be University) Mullana, Ambala, Haryana, India

A. K. Bindal (✉)

Department of Computer Science and Engineering, M. M. Engineering College, M. M. (Deemed to be University) Mullana, Ambala, Haryana, India
e-mail: amitbindal@mmumullana.org

D. Prasad • A. Hassan

Institute of Engineering and Technology, Chitkara University, Chandigarh, Punjab, India
e-mail: devendra.prasad@chitkara.edu.in

A. Hassan

e-mail: afshan.hassan@chitkara.edu.in

1 Introduction

The current era of learning of UWSNs has appealed speedily mounting interests [1–3]. UWSNs are the arising and inspiring frameworks that entitle an extensive range of energetic short-term and long-term applications like distributed tactical surveillance, disaster preclusion, ecological monitoring, oceanographic statistics and abetted navigation [4]. Untethered sensor nodes are used in the disposition in such challenging to reach localities. The major constraint related to unleashed nodes is restricted battery volume which means nodes will work for a predetermined period. Numerous practices have been introduced to increase the lifetime of SNs powered by the battery. To lengthen the network life, essential energy is kept in the hardware in any form. If the category of battery is preferred, the Li-ion battery is the utmost capable technology for UWSNs because of their greater energy yield and power density in comparison to nickel–cadmium and nickel–metal hydride [5]. An alternative way of solving energy problems is the energy harvesting approach, which generates energy by itself. Harvesting energy means the restoration of power by absorbing it from the atmosphere or using other energy sources, such as the heat of a body, stroke of a finger and tidal energy [6–8].

2 Literature Review

Communication Architecture

Following communication, architectures are considered for UWSNs, i.e. 2D and a 3D architecture [9].

(i) *Two-Dimensional (2-D) UW-ASNs*

As shown in Fig. 1, the 2D architecture is affixed in the lowermost of the marine. UW-SNs are associated with one or more UW-gateways by acoustic transmission media.

The surface station, fortified by an acoustic transceiver, which might be capable of handling bar scores of corresponding communication with the UW-gateways and by a long-range radio or satellite transmitter, desires communication with onshore or surface sink [9].

(ii) *Three-Dimensional (3-D) UW-ASNs*

Figure 2 shows 3D architecture; in this structural design, sensors sink at dissimilar depths [9]. In the design of 3D architecture, the problem of coverage area is a little bit resolved. We cover more areas by deploying the sensors in

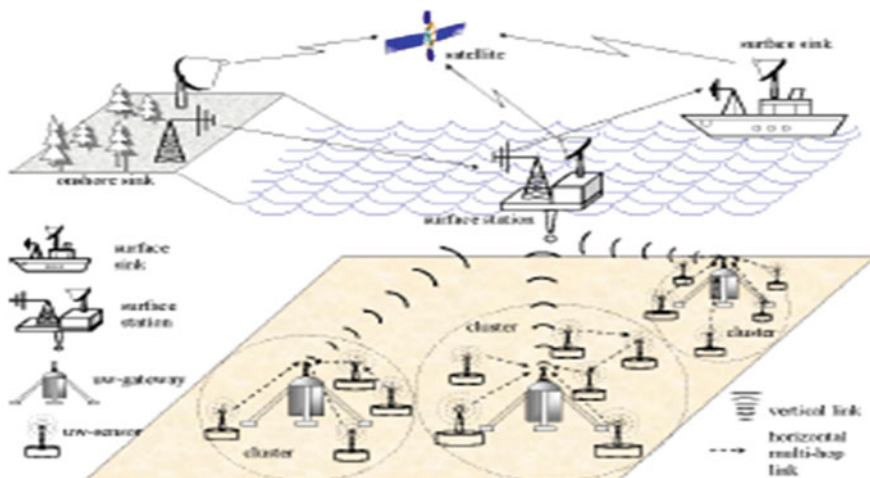


Fig. 1 2-Dim UW-ASNs architecture [9]

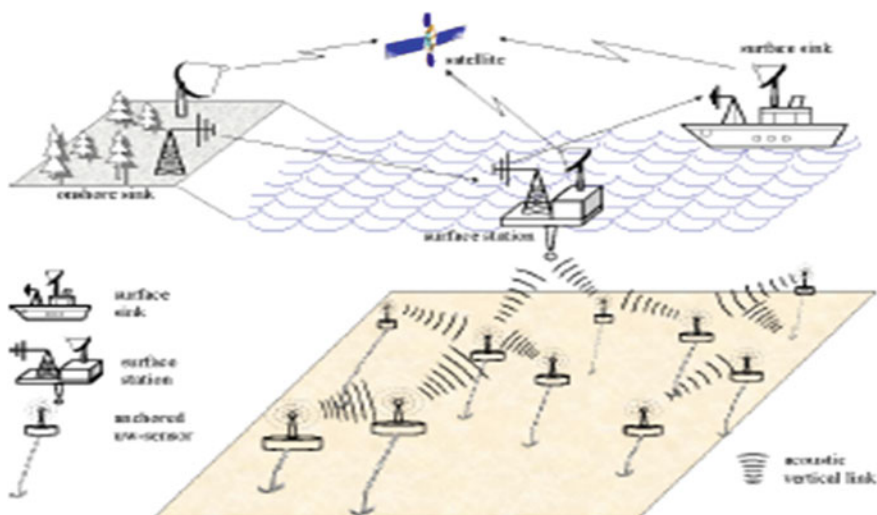


Fig. 2 3-Dim UW-ASNs architecture [9]

depth of the ocean, but the energy issue is there. This problem arises due to more energy consumption because each node is working as a gateway in 3 D architecture.

Acoustic and Radio Energy Analysis

The use of energy by the acoustic and radio modem is computed in this section. As radio requires surfacing, the requirement of the energy of any node in order to travel upward to the surface is also considered. The calculation uses pragmatic inputs that match our observed energy utilization. The maximum transmission power of the acoustic modem is around 10 W. The acoustic power (P_a) per bit is computed as:

$$P_a = 5 \text{ W} / (5.5 * 8 \text{ bits/s}) = 113.6 \text{ mJ/bit.} \quad (1)$$

The approximate data rate for the radio is given in Eq. (2) accordingly per bit of power consumed (P_r) using the radio is given by Eq. (3).

$$76,800 / 6 / 2 \text{ bits/s} = 6400 \text{ bits/s} \quad (2)$$

$$P_r = 1 \text{ W} / 6400 \text{ bits/s} = 0.16 \text{ mJ/bit} \quad (3)$$

However, the SN must go up to the surface first, with the help of a depth adjustment system, to transmit data. This arrangement consumes around 0.6 watts and moves at a speed of 2.4 m per minute. The power per meter is calculated by Eq. (4).

$$P_w = 0.6 \text{ W} / 0.04 \text{ m/s} = 15,000 \text{ mJ/m} \quad (4)$$

In Eq. (5), P_{rw} is total power required for transmitting k bits from a depth of d meters, using depth adjustment and radio system (pretentious that node will relocate to the same point post transmission), is given by Eq. (5).

$$P_{rw} = 2 d P_w + k P_r = 2 d \leftarrow 15000 \text{ mJ} + k \leftarrow 0.16 \text{ mJ} \quad (5)$$

3 Proposed Model

(C) System Model

The model recommended in this paper is heterogeneous that entails three different types of sensor nodes (SNs), i.e. ordinary SNs used to sense the phenomenon that occurred as aggregators accumulate the data from ordinary SNs and BS receives the data from aggregators and use for scrutiny.

(D) Network architecture

In the proposed model, SNs are deployed at 3 layers, i.e. top, middle and bottom layer. Individual layer comprises of data aggregator accompanied by ordinary SNs, as shown in Fig. 3. The base station (BS) is floating on the surface of the water. Sensors are fitted out with the depth acclimation system, which strengthens the network.

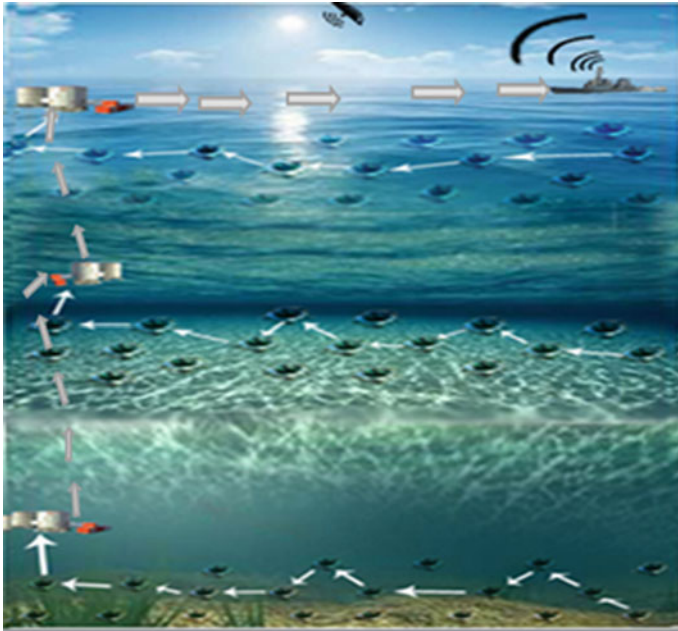


Fig. 3 Network architecture of the proposed model

(E) Data dissemination mechanism

To deliver the data from the various layers to the BS, the data aggregator deployed at bottom level transfers the data to the data aggregator at middle level, middle-level data aggregator transfers the data to the top-level data aggregator, and top-level data aggregator node transfers the data to the floating BS. Finally, the BS delivers data to the data centre through satellite as shown in Fig. 3. In the process, data is delivered to the BS from various layers using shortest path (computed through any standard algorithm).

(F) Energy Model

The sensors deployed at various levels keep on watching its energy level. If the remaining energy (E_r) goes below some threshold energy (E_{th}), sensors open their charging circuitry and start charging without interrupting their communication. Once its battery is full, the sensor closes its charging circuitry. In the proposed model, tidal energy is converted into electrical energy and provide to the sensor's circuitry for charging purpose.

(i) **Acoustic Energy Consumed**

As TDMA slot is capable of sending as well as receiving data packet of 20 bytes, containing 14 bytes of payload, in every 4 s; hence, the throughput is 7 bytes/s. The acoustic power per bit is computed as in Eq. (6).

$$P_{pb} = 5 \text{ W} / \left(7 * \frac{8 \text{ bits}}{\text{sec}} \right) = 89.29.4 \text{ mJ/Bit} \quad (6)$$

(ii) **Acoustic Energy Gain through Tidal Energy**

The primitive equation of tidal energy is given by Eq. (7).

$$e = \frac{1}{2} * a_{\text{layer}} * \rho_{sw} * g * h_t^2 \quad (7)$$

where e is the energy, a_{layer} is an area of the basin, ρ_{sw} is water density (1025 kg/m³), g is the acceleration due to gravity (9.81 m/s²), and h_t is the height of the tide in the ocean. The equation is implemented only if it is dimensionally correct.

$$e = m^2 * \frac{\kappa g}{m^3} * \frac{m}{s^2} * m^2 \quad (8)$$

$$e = \mathcal{K}g \left(\frac{m^2}{s^2} \right)$$

$$\mathcal{K}.\mathcal{E}. = 1/2 \ m \ v^2 \quad (9)$$

Similarly, by putting the units of various parameters in Eq. (9), the dimensionality comes out to be as given in Eq. (10).

$$\mathcal{K}.\mathcal{E}. = \mathcal{K}g \left(\frac{m^2}{s^2} \right) \quad (10)$$

After comparing the dimensionality of tidal energy and kinetic energy, we can conclude that Eq. (7) used in the proposed model is correct. As only 30% of the total energy can be utilized, the net energy available can be calculated as below:

$$e = 0.15 * a_{\text{layer}} * \rho_{sw} * g * h_t^2 \quad (11)$$

After substituting the value of ρ_{sw} and g in Eq. (11), the tidal energy is coming out to be as given in Eq. (12).

$$e = 0.15 * a_{\text{layer}} * 1025 * 9.81 * h_t^2$$

$$e = 1508.29 * a_{\text{layer}} * h_t^2 \quad (12)$$

From Eq. (12), we conclude that the tidal energy is directly proportional to the area of the basin and the square of the height/depth.

- (i) **Computation of energy at various levels:** Eq. (12) can be used to find the energy produced by tide at any layers.

• **Top Level**

The height of the tide at top level is 1 m. The energy available at top level (E_{top}) for sensors can be computed by putting the value of the height of tide at the top level and basin area in Eq. (12).

$$E_{\text{top}} = 1508.29 * 2.5 * 10^5 * 1^2 \text{ J} = 3.8 * 10^{11} \text{ mJ} \quad (13)$$

Equation (13) gives the energy available for all sensors deployed in the entire area. So the energy available for a single sensor

$$E_{\text{single\_top}} = 3.8 * 10^{11} / 500 \text{ mJ} = 7.6 * 10^8 \text{ mJ} \quad (14)$$

According to the principle of energy conservation, the energy supplied by the tidal waves will be related to the electrical energy produced by the transducers. So electrical energy generated by a single transducer at the top level will be equal to $7.6 * 10^8 \text{ mJ}$.

To charge a 5 V Li-ion cell, 1500 mA of current is required. The total power (T_{ptl}) produced for Li-ion cell, at top level, is computed by Eq. (15).

$$T_{\text{ptl}} = E/C = 0.6 * 10^8 / 1 = 7.6 * 10^8 \text{ V} \quad (15)$$

• **Middle Level**

Similarly, for the middle level, the value of E_{mid} , $E_{\text{single\_mid}}$ and T_{pml} are computed as above and given by Eq. (16) through Eq. (18).

$$\begin{aligned} E_{\text{mid}} &= 1508.29 * 2.5 * 10^5 * 3^2 \text{ J} = 3770.7 * 10^5 * 3^2 \text{ J} = 33.9 * 10^8 \text{ J} \\ &= 33.9 * 10^{11} \text{ mJ} \end{aligned} \quad (16)$$

$$E_{\text{single\_mid}} = 33.9 * 10^{11} / 500 \text{ J} = 6.78 * 10^9 \text{ mJ} \quad (17)$$

$$T_{\text{pml}} = E/C = 6.78 * 10^9 / 1 = 6.78 * 10^9 \text{ V} \quad (18)$$

• **Bottom Level**

By putting the value of the basin area and height of the tide at the bottom level, the value of E_{bot} , $E_{\text{single\_bot}}$ and T_{pbl} are computed as earlier and given by Eq. (19) through Eq. (21).

$$E_{\text{bot}} = 1508.29 * 2.5 * 10^5 * 5^2 = 94.3 * 10^8 \text{J} = 94.3 * 10^{11} \text{mJ} \quad (19)$$

$$E_{\text{single\_bot}} = 94.3 * 10^{11} / 500 = 18.86 * 10^9 \text{mJ} \quad (20)$$

$$T_{\text{pbl}} = E/C = 18.86 * 10^9 / 1 = 18.86 * 10^9 \text{ V} \quad (21)$$

4 Simulation Result and Discussion

Figures 4, 5 and 6 represent the energy consumption in various slots under proposed work. From various figures, we can observe that the energy consumption in the proposed work is very less as compared to the existing schemes for all levels, i.e. at the top, middle and bottom level.

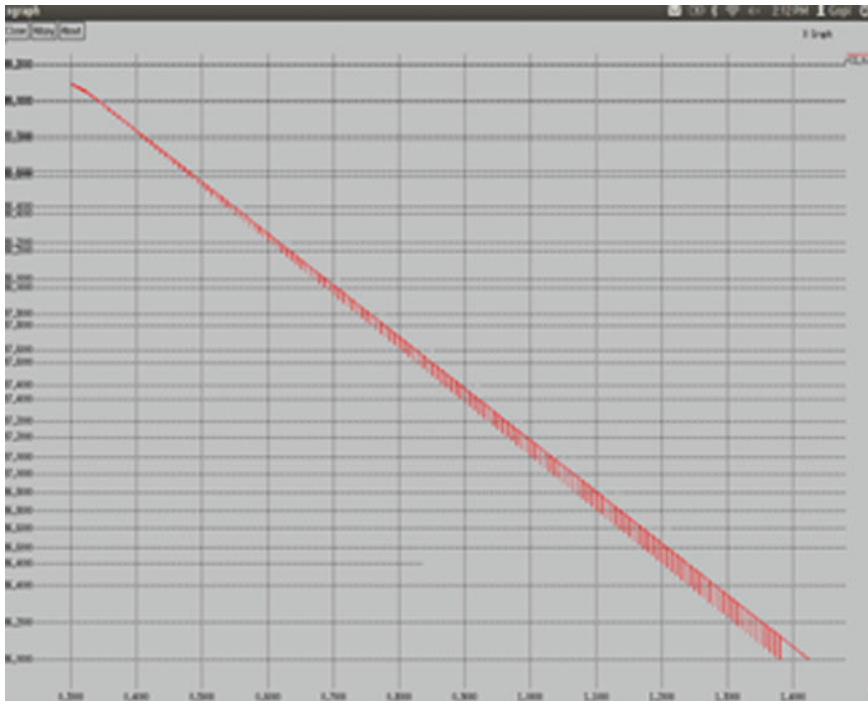


Fig. 4 Energy consumed at top level

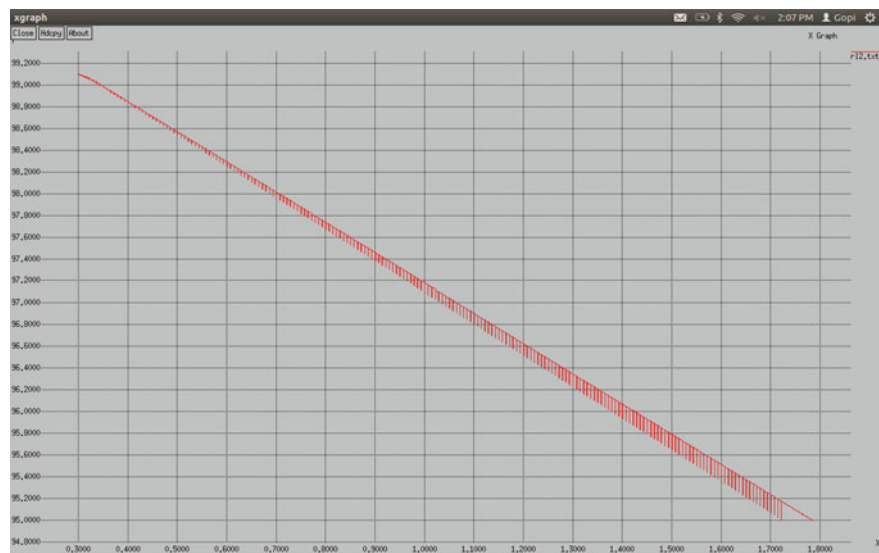


Fig. 5 Energy consumed at middle level

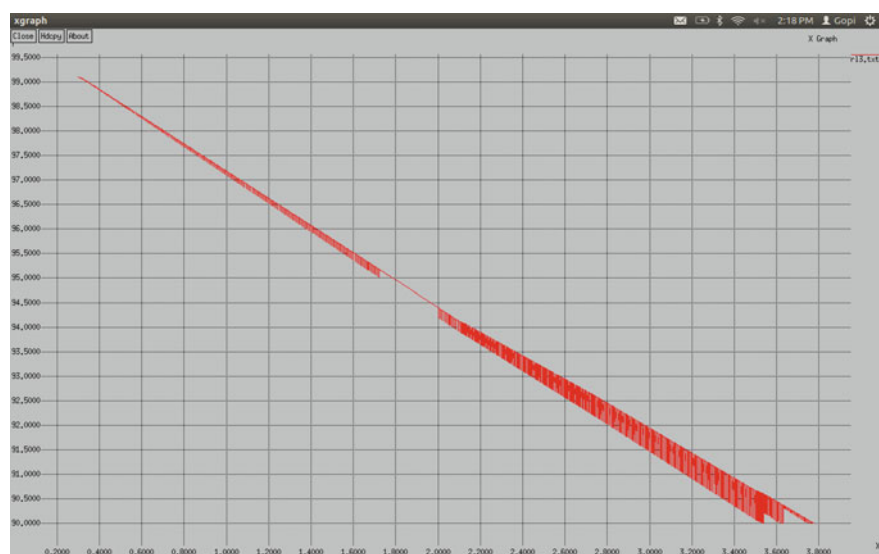


Fig. 6 Energy consumed at bottom level

As in the proposed work, we are providing the concept of energy harvesting to resolve the reliable resource of energy for charging the battery of sensors at various levels. We observed from the simulation that there is a huge amount of energy gain at bottom level as compared to the middle and top levels; the amount of gain in

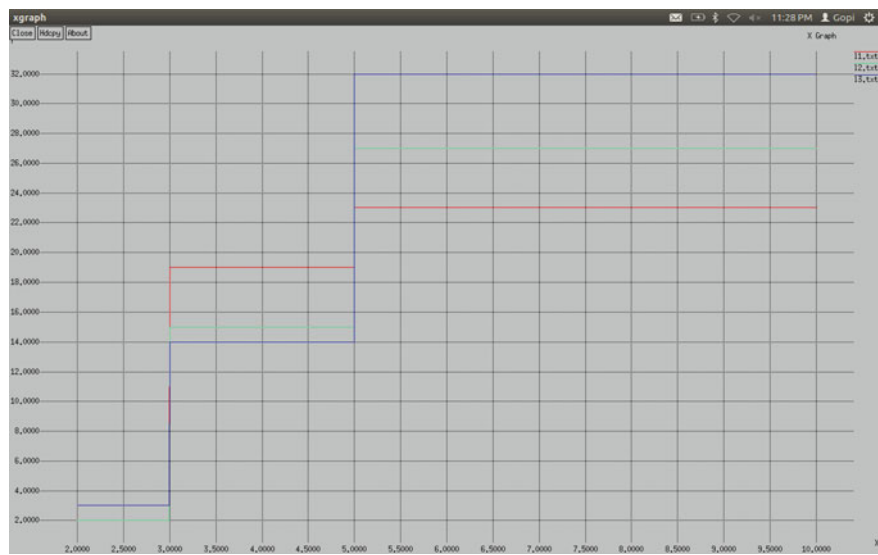


Fig. 7 Energy gain at top level, middle level and bottom level

energy at middle level is more as compared to the top level. In Fig. 7, energy gain at the bottom level is presented by the blue line, at the middle level presented by the green line and the top level is presented by the red line.

5 Conclusion

This work proposed a layered architecture to monitor the activities underwater. In the presented work, data of the various levels are collected through aggregator deployed at various levels. In the process of data dissemination, energy consumption at various levels is observed. As the energy consumption at the bottom levels is very high as compared to the top level, for prolonging the network life, the density of sensors at the bottom level should be very less as compared to the top-level.

As future work, researchers may analyse the effect of sensor density on the amount of tidal energy required for recharging the Li-ion cell so that network should work continuously without any disaster occurs. One can also investigate the various parameters that must be considered in the conversion of tidal energy into electrical energy.

References

1. Goel, K., Bindal, A.: Energy issues in underwater wireless sensor network: a survey report. *IJRSR*, **3**(2), 1–4 (2014)
2. Yang, H., Ren, F., Lin, C., Liu, B.: Energy efficient cooperation in underwater sensor networks. In: *IEEE 18th International Workshop on Quality of Service (IWQoS)* (2010). <https://doi.org/10.1109/IWQoS.2010.5542761>
3. Pompili, D., Akyildiz, I.: Overview of networking protocols for underwater wireless communications. *Commun. Mag. IEEE* **47**(1), 97–102 (2009)
4. Xu, J., Li, K., Min, G., Lin, K., Qu, W.: Energy-efficient tree-based multipath power control for underwater sensor networks. *IEEE*, **23**(11), 2107–2116 (2012)
5. Ovaliadis, K., Savage, N., Kanakaris, V.: Energy efficiency in underwater sensor networks: a research review. *JESTR*, **3**(1), 151–156 (2010)
6. Sudevalayam, S., Kulkarni, P.: Energy harvesting sensor nodes: survey and implications. *IEEE*, **13**(3), 443–461 (2011)
7. Pompili, D., Melodia, T., Akyildiz, I.F.: Deployment analysis in underwater acoustic wireless sensor networks. In: *1st ACM International Workshop on Underwater Networks*, Los Angeles, California, USA, pp. 48–55 (2006)
8. Bindal, A.: 3-tier architecture for sustainable underwater wireless sensor networks. *Adv. Math.: Sci. J.* **9**(3), 1205–1212 (2020)
9. Detweiler, C., O'Rourke, M., Basha, E.: Multi-model communications in under water sensor networks using depth adjustment. *ACM 978–1–4503–1773–3–3/12/11, WUWNet'12*, Los Angeles, California, USA, pp. 1–5 (2012)

Review of Evolutionary Algorithms for Energy Efficient and Secure Wireless Sensor Networks



Rajiv Yadav, S. Indu, and Daya Gupta

Abstract Wireless sensor network (WSN) finds vast real-world applications in the field of energy control, security, health care, defense, and environment monitoring. WSNs are subduced by limited power with a specific battery backup. Due to the large distance between sensor nodes and sink, more consumption of power takes place in the sensors. Limited energy of sensor nodes is a major drawback to empower a large network coverage area. Therefore, the battery life and location of cluster heads play an important role in increasing the efficiency and lifetime of sensor nodes for long-term operation in WSNs. While there are many algorithms leading to the optimization of performance using convergence, comparison of such algorithms and their advantages and challenges is addressed. Different types of attacks and security goals are described for high-level security and privacy in WSNs. This paper tabulates a systematic survey of the evolutionary algorithms of WSNs based on nature. This paper also intends to reflect on the security challenges of WSN and proposes effective techniques to address them.

Keywords GA · PSO · ACO · BBO · GWO · Energy utilization · Wireless sensor network · IoT

1 Introduction

Wireless sensor networks (WSNs) having a group of sensor nodes through which these nodes communicate with each other to identify useful information and data. The primary target of WSN is to detect the behavior of the current event and transmits its information to the sink. This phenomenon of distribution protects the loss of data in a specific coverage area. Due to the large distance, more consumption

R. Yadav (✉) · S. Indu
Department of ECE, Delhi Technological University, Delhi, India
e-mail: s.indu@dce.ac.in

D. Gupta
Department of CSE, Delhi Technological University, Delhi, India

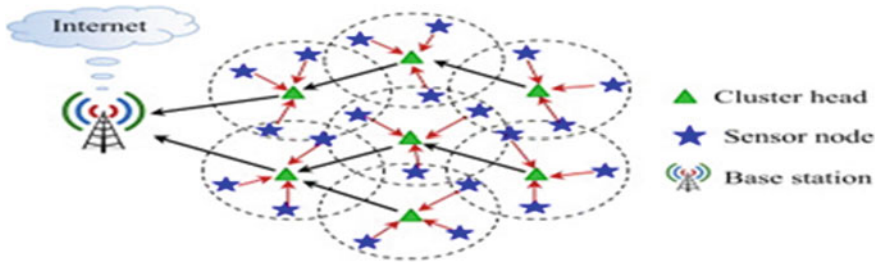


Fig.1 Wireless sensor network topology

of power takes place in the sensors. Limited energy of sensor nodes is a major drawback to empower a large network coverage area. The lifetime of a WSN depends on the CH lifetime, which makes optimum use of CH battery an important parameter for an energy-efficient WSN.

In designing a sensor network, the focus must be on utilizing energy consumption and battery lifetime. The existing WSN model is presented in Fig. 1 [1]. Previous researches on WSN gave different ideas to extend network lifetime by utilizing the present resources. Clustering and routing algorithms also have a specific contribution to the process. There are many performance matrices associated with the efficient working of a WSN. For an energy-efficient network, optimum use of the CH battery is essential, load balancing is important for the stability of the WSN, and the hole-free deployment of sensor nodes is essential for the uninterrupted coverage of the surveillance region.

The introduction of IoT-based applications demands a new algorithm to ensure the efficient working of WSN. In WSN, different objects at different places are empowered to transmit and receive the signals generated by them. High security and privacy are required in WSN through the environment. Information storage, authentication, and management are the main issues in security concerns. Different types of layers can be designed for the safety of WSN, in which the first layer includes many sensors and actuators for taking the information from different functionalities. The main security concerns that the network layer has faced are access attacks, data transit attacks, routing attacks, and unlawful attacks.

2 State of Art

2.1 Energy Efficiency in WSN

The selection of cluster heads randomly from sensor nodes with less residual energy is defined by LEACH [2]. There have been other differences in LEACH with respect to WSN performance enhancement. The fuzzy logic-based clustering

algorithm in [3] contains three: fuzzy node energy, centrality, and concentration variables. But a big problem faced by this logic is the involvement of a single cluster in the process. Authors in [4] worked on energy dissipation of the network, but the distance parameter is not mentioned. This avoidance of the distance parameter creates unbalancing in the network. Authors in [5] considered only one parameter node centrality to minimize energy consumption. Other important parameters like load balancing, transmission distance, and uniformity in deployment are not considered. A novel algorithm in [6] is presented to minimize the distance between sink and CH. The transmission distance is specified in this algorithm, but the communication distance between sensor nodes and CHs is not considered.

To enhance the lifetime of a WSN, a partial swarm optimization (PSO) in [7] is used. In PSO, they consider the fitness function parameters like network lifetime and cluster head to sink distance to achieve an energy-efficient network. But the sensor node to CH distance is not considered in PSO. Energy description during the process is also not considered. Authors in [8] proposed a significant algorithm to tackle optimization problems. This algorithm is highly flexible and more desirable for automatically configured techniques. In complex applications, ACO can be used. Changes such as new distances may be adjusted. It can also search among a population in parallel. The challenges faced are probability distribution changes for each iteration. ACO has a difficult theoretical analysis and uncertain time to convergence.

A new nature influenced by the authors in [9] suggested a technique of optimization based on biogeography (BBO-C) in WSN for energy-efficient clustering. To maximize the performance of the network, a complex and effective fitness feature is used. Authors in [10] proposed a clustering and routing algorithm (EBBO-CR) for extending the lifetime of WSN. It also minimizes the distance from its respective CHs and the number of hops required to move data from CH to sink. But in exploiting the solutions, BBO and EBBO are bad. They have no provision for selecting each generation's best members and the resulting fitness solution.

A novel version of BBO was proposed by the authors in [11]. The implementation of the age-structured BBO (ASBBO) is the impact of people's age on the migration method. Individuals are implemented to capture age-related trends of birth rates and survival rates. Age systems enable information to be shared not only on the basis of the present goodness. In [12], the writers mimic the leadership structure and hunting method of gray wolves. Four forms of the gray wolves were used to determine their fitness, i.e., alpha, beta, delta, and omega. For the energy-efficient WSNs and load balancing of the cluster heads, they suggested DBSCDS-GWO and DBSC-GWO. Yeah, but the author does not take WSN's accuracy and convergence.

2.2 Load Balancing in WSN

Recent researches described many algorithms to enhance the performance of a network. In [13], the authors described a breadth-first tree using a clustering algorithm to find the gateway which is at low load. The drawback of this algorithm is the time of execution while calculating large computations. Authors in [14] build a load-balanced CDS using GA and load-balanced allocation of a sensor node to cluster heads. Before this, a limited study has been done to achieve a load-balanced CDS WSN. The problem that is to be observed in this algorithm is high energy dissipation and slow convergence rate. LEACH-C with GA has been proposed later to minimize energy dissipation for the entire network. For congestion management of wireless sensor networks, a load-balancing protocol inspired by GA [15] has been introduced. A fuzzy-based PSO routing algorithm was proposed by the authors in [16] to balance the load and scalability of the network. The authors improved three important factors like density, energy consumption, and transmission distance by using FBPSO. They also balanced the cluster heads' energy dissipation and increased the lifespan of WSNs. The choice of cluster head and network stability was not considered by them.

Authors in [17] proposed a data dissemination strategy using nature-inspired ant colony optimization (ACO) named TMLBS. This paper identified three load balancing systems, which are the system of load decentralization, the system of maintenance, and the system of load diversion. The authors tried to create multiple transmission paths for the entire network at different places. In these schemes, they implemented multipath subtrees to avoid excessive load, pheromone update mechanism, and paths with low data load, respectively. But they did not focus on the lifetime of the network and convergence speed. New nature-inspired techniques have been proposed by authors in [18] biogeography-based optimization (BBO-C and BBO-CR) for WSN energy production. This leads to better sensor distribution and a well-balanced method of clustering. But there is no provision for the BBO-C and BBO-CR to pick the best members from each generation. The resulting fitness solution could not be concluded when too many alternatives were produced.

The authors in [19], proposed DBSCDS-GWO and DBSC-GWO to calculate the distance of transmission and balance the load on the network. A selection of dominator nodes is deterministically chosen by DBSCDS-GWO, and the meta-heuristic method GWO is used to find the optimal location. Authors have also tried to minimize the effective transmission distance (ETD) parameter, as follows:

$$ETD = \Phi \text{ or } \eta(\text{whichever is shorter}) \quad (1)$$

Authors achieved stability and balanced the load of the network up to an extent, but GWO has a bad local searching ability, low solving precision, and low speed of convergence.

2.3 *Security Enhancement in WSN*

In the past years, a large increment has been seen in the field of WSNs devices. These devices are connected wirelessly with each other and communicate wirelessly without any human intervention. During transmission of data or information from sensor node to sink, security can be compromised. WSN protection is very important. Otherwise, it can lead to significant losses of property and life as well. Data or information can be modified or removed by the attackers to break the security of WSNs. Attackers try some specific attacks (active or passive) to alter the specifications of the network. These attacks are classified according to the layers of WSNs. Each wireless environment consists of the following four layers on which different types of attacks are imposed in [20–23].

To protect these layers from attacks and alterations, there is a need to follow some security protocols. So, three main factors need to describe the security of WSNs, which are:

- **Attacks in WSNs:** There are primarily two kinds of attacks: active (aggressive) attacks and passive attacks. Active attacks are DOS attack, physical attack, routing attack, node replication attack, node outage attack, node malfunction attack, false node, etc. Passive attacks are traffic monitoring, traffic analysis, and eavesdropping.
- **Security goals of WSNs:** WSN security goals are divided into two parts, i.e., primary and secondary goals. Primary goals are mainly confidentiality, authentication, integrity, and availability. Secondary goals are secure localization and resilience to attacks.
- **Security protocols for WSNs:** Authors have identified various types of protection in [24, 25]. WSN protocols based on SPIN, line-selected multicast (LSM) [26], randomized efficient and distributed (RED) [25], CRS-A [27], logical key hierarchy-based model (LKHM) [28], localized encryption and authentication protocol (LEAP), certificate-less effective key management (CL-EKM) [29], low-storage clone detection (LSCD) [30].

2.3.1 *Security in IoT*

IoT is the upcoming era of communication. According to recent reports, there will be around 9.5 billion connected devices in 2020. IoT applications are rapidly increasing all over the world but are majorly used in North America, Western Europe, and China. To expand the digital economy, IoT is the major upcoming market, according to data declares in reports. Recent and existing applications of IoT are highly promising and more efficient for the users, but high-level privacy and authentication for these applications are required. Existing solutions using different technologies like machine learning, fog computing, edge computing, and blockchain are implemented for high-level security and privacy in IoT, as discussed in Table 1.

Table 1 Comparison of security techniques in IoT

Blockchain technique-based solutions	Fog computing-based solutions	Machine learning-based solutions	Edge computing-based solutions
1. WSNs are vulnerable to exposing private data. Then, by using permission blockchain, WSNs can be secured 2. Moving toward decentralization using blockchain, exponential growth can be handled in WSNs 3. Data available on different nodes of the network by blockchain technique. Hence, no distinct failed node is observed	1. Verifiable computation is proposed by fog computing 2. Server-aided exchange and data analytics provided by fog computing 3. Sharing data securely and designing protocols are also provided by fog computing 4. Identity recognition and access management are also done by using fog computing	1. Machine learning techniques help to secure the network from attacks and in increasing accuracy 2. Machine learning helps us to prevent the devices from eavesdropping 3. Machine learning helps us to increase detection and classification accuracy 4. The techniques of machine learning also help reduce the false alarm rate and the average error rate	1. Edge computing eliminates the transit of data and thus avoids the possibility of data theft and data breaches 2. Organizations can manage the data within their boundaries using edge computing to ensure data enforcement 3. Using edge computing, surveillance cameras can also be empowered to achieve faster response time

3 Comparison of Evolutionary Algorithms

3.1 Genetic Algorithm (GA)

The authors in [31] suggested GA for distance-conscious routing. They used this algorithm to choose the head of the cluster and to achieve the calculation of fitness. Authors in [32] used GA for node deployment. They found efficient positions for sensor nodes by using this algorithm. The authors mainly focused on three factors in this paper which are to minimize no. of sensor nodes, maximize connectivity and maximize coverage region. Authors in [33, 34] proposed GA for routing of WSN. In choosing the cluster head, they considered three weaknesses and achieved a prolonged network lifetime. Authors in [35] used GA for load balancing of the network. They also identified a prolonged lifetime of the network after simulation. Authors in [36, 37] GA is used to schedule the set cover problem and to minimize the exposure path. They scheduled the sensors for better conservation of energy and approached redundant trend scheduling. They also implemented a cross-over operator for exploitation purposes and an upside-down operator to avoid premature convergence. In order to find a new generation with better fitness appeal, GA effectively explores the new combinations with the information available.

3.2 Particle Swarm Optimization (PSO)

Since its introduction in 1995, particle swarm optimization (PSO) [38] has undergone many improvements. They have derived new models, developed new implementations, and published theoretical studies on the effects of different parameters and aspects of the algorithm as researchers have learned about the technique. Authors in [7, 39] proposed PSO for routing of the wireless sensor network. They used an unsupervised learning technique to achieve efficient routing between sensor nodes. They also used PSO to find routing paths for data transfer and to balance the load of WSN. Using PSO, the authors also found optimal solutions by implementing double-layer encoding. Authors in [40] proposed discrete PSO to overcome the scheduling problem in PSO. The proposed model of discrete PSO improved task allocation and utilization of available resources. Authors in [41, 42] proposed a new methodology to reduce the overhead of CH named cluster assistant node (CAN). They also focused on coverage area and node positioning of sensor nodes under CHs to minimize energy dissipation. In recent work, it is observed that PSO has few parameters to adjust and short computational time.

3.3 Ant Colony Optimization (ACO)

Authors in [1] proposed ACO for the deployment of sensor nodes. They achieved maximum coverage by allocating the nodes using a probability distribution. Another technique, greedy migration, was also implemented by authors for fast convergence. Authors in [43] proposed ACO in terms of QoS-based routing. They considered energy consumption and network performance for finding a highly efficient route from sensor nodes to sink. They achieved a better ratio of packet delivery and low consumption of energy by using this algorithm. Authors in [44] proposed ACO for routing based on trust values of sensor nodes. The authors also considered number of hops and re-laid nodes for balance the network and secure transfer of data. In recent research, it is found that ACO can be used in complex applications. Changes such as new distances may be adjusted. It can also perform simultaneous searches among a population.

3.4 Biogeography-Based Optimization (BBO)

BBO is an evolutionary algorithm that is applied to preserve population diversity through the transfer of species from one habitat to another habitat. A person is represented by habitat in the BBO. There can be multiple environments in a group, such as chromosomes in genetic algorithms. Habitat suitability index (HSI) values

are determined for every habitat. In this way, several changed vectors/habitats allocated to sensor nodes will be obtained. For all these resulting ecosystems, measure HSI values again. Retain the best HSI value for the habitat. If after adjustment, the HSI value is higher than the HSI value before modification, the output of the batter network is achieved. The entire situation is then simulated and optimal efficiency is achieved. In [45], the authors suggested the algorithm (MSDR-BBO) to pick the optimal routing CHs in MSWSN according to the data transfer requirements of SNs and CHs.

3.5 *Gray Wolf Optimization (GWO)*

Authors in [46] proposed recent work (2014–2017) based on GWO. They described GWO based on wolf hunting behavior which shows their domination while hunting their food. The key phases of hunting, which track, chase, and approach the prey, were also explained by the authors. They found problems such as cost estimation, parameter tuning, economic dispatch problems, and classification of genes in this research. GWO is also capable of addressing both single and multi-objective questions. To solve the distinct optimization problem, improved and hybrid GWO are increasing. A hybrid protocol MLHP was proposed by the authors in [47] to centralize selection processes for the selection of suitable CH, and deterministic selection at levels two and three. The algorithm used in this paper performed 500 times better as compare to LEACH in terms of the lifetime of WSN.

Authors in [49, 50] focused on localization problems and energy utilization of WSNs. They also achieved the fitness criteria by which nodes consumed desired energy. Network lifetime, stability, residual energy, and performance are considered during the entire implementation of the methodology. In a recent study, it is observed that GWO provides automatic configuration of the set of parameters in a manner to balance the load. It also provides more accuracy instability and energy efficiency as compared to previously used algorithms. The comparison and contribution of previously used evolutionary algorithms are described in Table 2.

4 Conclusion and Future Directions

The main purpose of this paper is to review various algorithms and clustering routing protocols used to improve the energy efficiency of WSNs. Recently, many algorithms are described in WSN in order to improve the stability and lifetime of WSN. Now, a better methodology or hybrid approach is required to increase energy efficiency. Hence, this paper elaborates various evolutionary algorithms and clustering routing protocols to enhance the energy efficiency in WSN. This survey also describes the security techniques of IoT in different scenarios. An introduction on energy efficiency, load balancing, and security of WSNs has been described. Some

Table 2 Comparison of evolutionary algorithms [48]

Algorithms	Contribution
GA	1. Used to find the efficient location of sensor nodes and CHs 2. Used for whole area coverage by using less number of sensor nodes 3. Used to prolong the network lifetime and exploitation purposes
PSO	1. Used for exploration and perform better than GA 2. Used routing to minimize the number of hops and efficient data transfer 3. Used double-layer encoding to find the optimal solution
ACO	1. Used probability distribution to achieve maximum coverage for the network 2. Used multiple constraints for multi-hop routing 3. Achieved better packet delivery ratio and energy consumption
BBO	1. The introduced phenomenon of extinction and evolution of species 2. Used nonlinear mapping used to enhance the stability of the network 3. Achieved gateways optimum location faster to reduce energy dissipation
GWO	1. Achieved a more stable and energy-efficient network using DBSCDS-GWO and DBSC-GWO 2. Used to reduce effective transmission distance (ETD) 3. Overall performance of GWO is better than previously used algorithms

advantages and challenges for evolutionary algorithms are explained in the paper to optimize future problems. Table 1 shows a comparison of security techniques-based solutions for IoT. The review paper mainly comprises of the research articles published in the past few years and the details of many other surveys are also described here. In the future, the hybridization technique in the above-discussed algorithms can be implemented to obtain better results. This paper also can be expanded in the future for the hybridization of evolutionary algorithms.

References

1. Liu, X., He, D.: Ant colony optimization with greedy migration mechanism for node deployment in wireless sensor networks. *J. Netw. Comput. Appl.* **39**, 310–318 (2014). <https://doi.org/10.1016/j.jnca.2013.07.010>
2. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: *Proc. Annu. Hawaii Int. Conf. Syst. Sci.* 2000-Janua, 1–10 (2000)
3. Gupta, I., Riordan, D., Sampalli, S.: Cluster-head election using fuzzy logic for wireless sensor networks. In: *Proc. 3rd Annu. Commun. Networks Serv. Res. Conf.* 2005, pp. 255–260 (2005). <https://doi.org/10.1109/CNSR.2005.27>
4. Tamandani, Y.K., Bokhari, M.U.: SEPFL routing protocol based on fuzzy logic control to extend the lifetime and throughput of the wireless sensor network. *Wirel. Netw.* **22**, 647–653 (2016). <https://doi.org/10.1007/s11276-015-0997-x>
5. AbdulAlim, M.A., Wu, Y.C., Wang, W.: A fuzzy based clustering protocol for energy-efficient wireless sensor networks. *Adv. Mater. Res.* 760–762, 685–690 (2013). <https://doi.org/10.4028/www.scientific.net/AMR.760-762.685>

6. Gupta, S.K., Kuila, P., Jana, P.K.: GAR: an energy efficient GA-based routing for wireless sensor networks. In: *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. 7753 LNCS, pp. 267–277 (2013). https://doi.org/10.1007/978-3-642-36071-8_21
7. Kuila, P., Jana, P.K.: Energy efficient clustering and routing algorithms for wireless sensor networks: particle swarm optimization approach (2014)
8. Blum, C., López-Ibáñez, M.: Ant colony optimization. *Intell. Syst.* (2016). <https://doi.org/10.4249/scholarpedia.1461>
9. Kaushik, A., Indu, S., Gupta, D.: Optimizing and enhancing the lifetime of a wireless sensor network using biogeography based optimization. *Commun. Comput. Inf. Sci.* **899**, 260–272 (2019). https://doi.org/10.1007/978-981-13-2035-4_23
10. Zhang, S., Xu, S., Zhang, W., Yu, D., Chen, K.: A hybrid approach combining an extended BBO algorithm with an intuitionistic fuzzy entropy weight method for QoS-aware manufacturing service supply chain optimization. *Neurocomputing* **272**, 439–452 (2018). <https://doi.org/10.1016/j.neucom.2017.07.011>
11. Shukla, K., Verma, M., Gupta, D.: Age-Structured Biogeography-based Optimization, pp. 339–346 (2020)
12. Kaushik, A., Indu, S., Gupta, D.: A grey wolf optimization approach for improving the performance of wireless sensor networks. *Wirel. Pers. Commun.* 1429–1449 (2019). <https://doi.org/10.1007/s11277-019-06223-2>
13. Low, C.P., Fang, C., Ng, J.M., Ang, Y.H.: Efficient load-balanced clustering algorithms for wireless sensor networks. *Comput. Commun.* **31**, 750–759 (2008). <https://doi.org/10.1016/j.comcom.2007.10.020>
14. He, J., Ji, S., Yan, M., Pan, Y., Li, Y.: Load-balanced CDS construction in wireless sensor networks via genetic algorithm. *Int. J. Sens. Netw.* **11**, 166–178 (2012). <https://doi.org/10.1504/IJSNET.2012.046331>
15. Raha, A., Kanti Naskar, M., Paul, A., Chakraborty, A., Karmakar, A.: A genetic algorithm inspired load balancing protocol for congestion control in wireless sensor networks using trust based routing framework (GACCTR). *Int. J. Comput. Netw. Inf. Secur.* **5**, 9–20 (2013). <https://doi.org/10.5815/ijenis.2013.09.02>
16. Balaji, S., Julie, E.G., Rajaram, M., Robinson, Y.H.: Fuzzy based particle swarm optimization routing technique for load balancing in wireless sensor networks. *Int. J. Comput. Inf. Eng.* **10**, 1418–1427 (2016)
17. Liu, X., Qiu, T., Wang, T.: Load-balanced data dissemination for wireless sensor networks: a nature-inspired approach. *IEEE Internet Things J.* **6**, 9256–9265 (2019). <https://doi.org/10.1109/IIOT.2019.2900763>
18. Kaushik, A., Indu, S., Gupta, D.: A novel load balanced energy conservation approach in WSN using biogeography based optimization. *AIP Conf. Proc.* **1884**, 1–4 (2017). <https://doi.org/10.1063/1.5002507>
19. Bozorg-Haddad, O.: *Studies in Computational Intelligence—Advanced Optimization by Nature-Inspired Algorithms* (2018)
20. Lghd, V., Wkh, D., Fkdooqhjhv, I., Dqg, J., Glvdvwhu, F., Lqirupdwlrq, E., Dqg, F., Lpsruwdqfh, P., Wkh, V.R., Fkdudfwhuv, X., Wkhvh, R.I., Wkh, D.Q.G., Sxusrvhv, D., Xvhg, D.U.H., Surylgh, W.R., Iru, W., Dqg, L., Dwwdfnv, R., Wkhuh, Q.W., Whupv, D.U. H., Whup, Q., Xvhg, L. V, Wkh, D.L., Wkh, S.: \$ 6xuyh\ rq 6hfxulw\ \$wwdfnv lq :luhohvv 6hqvr u lhwzrunv. 536–539 (2016)
21. Wang, Q., Zhang, T.: A survey on security in wireless sensor networks. *Secur. RFID Sens. Networks.* 293–320 (2016). <https://doi.org/10.5121/ijnsa.2017.9103>
22. Karakaya, A., Akleylek, S.: A survey on security threats and authentication approaches in wireless sensor networks. In: *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018—Proceeding. 2018-Janua*, 1–4 (2018). <https://doi.org/10.1109/ISDFS.2018.8355381>
23. Teymourzadeh, M., Vahed, R., Alibeygi, S., Dastanpor, N.: Security in Wireless Sensor Networks: Issues and Challenges. *arXiv* (2020)

24. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: SPINS: security protocols for sensor networks. *Wirel. Netw.* **8**, 521–534 (2002). <https://doi.org/10.1023/A:1016598314198>
25. Conti, M., Di Pietro, R., Mancini, L., Mei, A.: Distributed detection of clone attacks in wireless sensor networks. *IEEE Trans. Dependable Secur. Comput.* **8**, 685–698 (2011). <https://doi.org/10.1109/TDSC.2010.25>
26. Gligor, V.D.: Emergent properties in ad-hoc networks: a security perspective. In: *Proc. 2006 ACM Symp. Information, Comput. Commun. Secur. ASIACCS '06*. 2006, 1 (2006). <https://doi.org/10.1145/1128817.1128819>
27. Ren, J., Zhang, Y., Zhang, K., Shen, X.: Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **15**, 3718–3731 (2016). <https://doi.org/10.1109/TWC.2016.2526601>
28. Di Pietro, R., Mancini, L. V., Law, Y.W., Etalle, S., Havinga, P.: LKHW: a directed diffusion-based secure multicast scheme for wireless sensor networks. In: *Proc. Int. Conf. Parallel Process. Work.* 2003-Janua, pp. 397–406 (2003). <https://doi.org/10.1109/ICPPW.2003.1240395>
29. Seo, S.H., Won, J., Sultana, S., Bertino, E.: Effective key management in dynamic wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **10**, 371–383 (2015). <https://doi.org/10.1109/TIFS.2014.2375555>
30. Dong, M., Ota, K., Yang, L.T., Liu, A., Guo, M.: LSCD: a low-storage clone detection protocol for cyber-physical systems. *IEEE Trans. Comput. Des. Integr. Circuits Syst.* **35**, 712–723 (2016). <https://doi.org/10.1109/TCAD.2016.2539327>
31. Bhatia, T., Kansal, S., Goel, S., Verma, A.K.: A genetic algorithm based distance-aware routing protocol for wireless sensor networks. *Comput. Electr. Eng.* **56**, 441–455 (2016). <https://doi.org/10.1016/j.compeleceng.2016.09.016>
32. Gupta, S.K., Kuila, P., Jana, P.K.: Genetic algorithm approach for k-coverage and m-connected node placement in target based wireless sensor networks. *Comput. Electr. Eng.* **56**, 544–556 (2016). <https://doi.org/10.1016/j.compeleceng.2015.11.009>
33. Shokouhifar, M., Jalali, A.: A new evolutionary based application specific routing protocol for clustered wireless sensor networks. *AEU Int. J. Electron. Commun.* **69**, 432–441 (2015). <https://doi.org/10.1016/j.aeue.2014.10.023>
34. Khalesian, M., Delavar, M.R.: Wireless sensors deployment optimization using a constrained Pareto-based multi-objective evolutionary approach. *Eng. Appl. Artif. Intell.* **53**, 126–139 (2016). <https://doi.org/10.1016/j.engappai.2016.03.004>
35. Pal, V., Yogita, Singh, G., Yadav, R.P.: Cluster head selection optimization based on genetic algorithm to prolong lifetime of wireless sensor networks. *Procedia Comput. Sci.* **57**, 1417–1423 (2015). <https://doi.org/10.1016/j.procs.2015.07.461>
36. Zhang, X.Y., Zhang, J., Gong, Y.J., Zhan, Z.H., Chen, W.N., Li, Y.: Kuhn-Munkres parallel genetic algorithm for the set cover problem and its application to large-scale wireless sensor networks. *IEEE Trans. Evol. Comput.* **20**, 695–710 (2016). <https://doi.org/10.1109/TEVC.2015.2511142>
37. Ye, M., Wang, Y., Dai, C., Wang, X.: A hybrid genetic algorithm for the minimum exposure path problem of wireless sensor networks based on a numerical functional extreme model. *IEEE Trans. Veh. Technol.* **65**, 8644–8657 (2016). <https://doi.org/10.1109/TVT.2015.2508504>
38. Kiranyaz, S.: Particle swarm optimization. *Adapt. Learn. Optim.* **15**, 45–82 (2014). https://doi.org/10.1007/978-3-642-37846-1_3
39. Taherian, M., Karimi, H., Kashkooli, A.M., Esfahanimehr, A., Jafta, T., Jafarabad, M.: The design of an optimal and secure routing model in wireless sensor networks by using PSO algorithm. *Procedia Comput. Sci.* **73**, 468–473 (2015). <https://doi.org/10.1016/j.procs.2015.12.028>
40. Guo, W., Li, J., Chen, G., Niu, Y., Chen, C.: A PSO-optimized real-time fault-tolerant task allocation algorithm in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **26**, 3236–3249 (2015). <https://doi.org/10.1109/TPDS.2014.2386343>

41. Rejinaparvin, J., Vasanthanayaki, C.: Particle swarm optimization-based clustering by preventing residual nodes in wireless sensor networks. *IEEE Sens. J.* **15**, 4264–4274 (2015). <https://doi.org/10.1109/JSEN.2015.2416208>
42. Yan, Z., Goswami, P., Mukherjee, A., Yang, L., Routray, S., Palai, G.: Low-energy PSO-based node positioning in optical wireless sensor networks. *Optik (Stuttg.)* **181**, 378–382 (2019). <https://doi.org/10.1016/j.ijleo.2018.12.055>
43. Wang, Y.L., Song, M., Wei, Y.F., Wang, Y.H., Wang, X.J.: Improved ant colony-based multi-constrained QoS energy-saving routing and throughput optimization in wireless Ad-hoc networks. *J. China Univ. Posts Telecommun.* **21**, 43–53 (2014). [https://doi.org/10.1016/S1005-8885\(14\)60267-3](https://doi.org/10.1016/S1005-8885(14)60267-3)
44. Sun, Z., Wei, M., Zhang, Z., Qu, G.: Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. *Appl. Soft Comput. J.* **77**, 366–375 (2019). <https://doi.org/10.1016/j.asoc.2019.01.034>
45. Kaushik, A., Indu, S., Gupta, D.: Adaptive mobile sink for energy efficient WSN using biogeography-based optimization. *Int. J. Mob. Comput. Multimed. Commun.* **10**, 1–22 (2019). <https://doi.org/10.4018/IJCMCMC.2019070101>
46. Hatta, N.M., Zain, A.M., Sallehuddin, R., Shayfull, Z., Yusoff, Y.: Recent studies on optimisation method of Grey Wolf Optimiser (GWO): a review (2014–2017). *Artif. Intell. Rev.* **52**, 2651–2683 (2019). <https://doi.org/10.1007/s10462-018-9634-2>
47. Al-Aboody, N.A., Al-Rawashidy, H.S.: Grey Wolf optimization-based energy-efficient routing protocol for heterogeneous wireless sensor networks. In: 2016 4th Int. Symp. Comput. Bus. Intell. ISCBI 2016, pp. 101–107 (2016). <https://doi.org/10.1109/ISCBI.2016.7743266>
48. Balasubramanian, D., Govindasamy, V.: Study on evolutionary approaches for improving the energy efficiency of wireless sensor networks applications. *EAI Endorsed Trans. Internet Things.* **5**, 164856 (2020). <https://doi.org/10.4108/eai.13-7-2018.164856>
49. Rajakumar, R., Amudhavel, J., Dhavachelvan, P., Vengattaraman, T.: GWO-LPWSN: grey wolf optimization algorithm for node localization problem in wireless sensor networks. *J. Comput. Networks Commun.* **2017** (2017). <https://doi.org/10.1155/2017/7348141>
50. Sharawi, M., Emary, E.: Impact of grey Wolf optimization on WSN cluster formation and lifetime expansion. In: 9th Int. Conf. Adv. Comput. Intell. ICACI 2017, pp. 157–162 (2017). <https://doi.org/10.1109/ICACI.2017.7974501>

Utilization and Energy Consumption Optimization for Cloud Computing Environment



Rajeev Tiwari[✉], Roohi Sille, Nilima Salankar, and Pardeep Singh

Abstract In a cloud environment, the workload that has to be maintained using visualization is limited by the available hardware resources of virtual machines (VMs). So utilization of VMs becomes significant to do more work with lesser infrastructure. Thus, in recent times, major thrust was shown by researchers in the field of task allocation algorithms on VMs. There are many techniques discussed in the literature, which uses different allocation methods, which can improve the performance by changing the working of cloud environment. In this research work, analysis, implementation and performance comparison of the existing allocation techniques have been performed using CloudSim. So performance tuning is being done analytically and practically for the task allocation algorithm. VMs and cloudlets are configured for experimental purposes and parameter results are obtained. Parameters recorded are execution time, makespan, utilization ratio and power consumption. A new algorithm is proposed for task allocation algorithm (Tiwari et al in *Int J Adv Intell Syst Comput*, 2016 (Tiwari and Kumar in *Telecommun. Syst.* 62:149–165, 2016)). These parameters are calculated for FCFS, SJF, Hungarian and the proposed algorithm. Then, result analysis is done and majorly got a speedup in utilization ratio of the proposed algorithm *w.r.t.* to FCFS as 53.20%, 18.08% *w.r.t.* to SJF and 10.52% *w.r.t.* to Hungarian. For power consumption, the algorithm has shown a significant decrease in power consumption from 37.21, 16.52 and 10.52% *w.r.t.* to FCFS, SJF and Hungarian algorithms.

Keywords Cloud environment • Optimization • Utilization rate • Energy consumption • Virtualization • Speedup percentages

R. Tiwari (✉) · R. Sille · N. Salankar · P. Singh (✉)
School of Computer Science, UPES, Dehradun, India
e-mail: rajeev.tiwari@ddn.upes.ac.in

P. Singh
e-mail: pardeep.singh@ddn.upes.ac.in

1 Introduction

Cloud computing [1–3] is enabling any infrastructure, development environment and software as a services on-demand basis. These are provisioned rapidly through web enablement using a shared pool of resources like compute, storage, network etc. with minimum manual intervention. This is considered as resource management, which is a current research topic in cloud [4]. Any application can be deployed in cloud environment, and this environment is a complex system that works with a number of configurations requirements. For researches and testing purposes, a tool is created called CloudSim [5] where any workload that needs to be executed is termed as cloudlet. It needs to be allocated on virtualized hardware through virtual machines [6]. Any application service that needs to be executed is to be allocated on virtual machines in such a way that load can be managed dynamically and provisioned rapidly. This application allocation policy of cloudlet on virtual machine is termed as task allocation policy (TAP) [7, 8]. There are many number of TAPs available for different metrics like work load, utilization, energy consumption, more throughput, etc.

Using TAP in a cloud environment, executions can be done fast, and throughput can be increased significantly [8], with proper utilization of resources. So most of the researches are going in the direction of optimization of performance parameters for cloud environment.

Other most common and effective method of performance tuning for such environments is in network caching, where caches are deployed on nodes for prefetching and forwarding required data. So optimization in terms of power consumption and utilization is also given by authors in ACIT [9] and ECCI [10] techniques.

2 Literature Review

There are a number of scheduling algorithms being proposed by researchers in history. A few are being discussed in the coming sections. First scheduling algorithm is famous for its simplicity, i.e. first come first serve scheduling algorithm (FCFS), shortest job fastest resource (SJFR), longest job fastest resource (LJFR), min–min algorithm and max–min algorithms are evolved as per their need. As these algorithms consider all processes of same priority to execute at same time, while this is not the case in in real scenarios. So different cloudlets with workloads may have different significance and priority, so another pool of algorithms is designed. Some algorithm [11] offers first preference to a high-complexity job, and other has given high priority to level of parallelism. However, due to preference of high priority jobs by these algorithms, there is a limitation of increase in waiting time for low priority jobs.

First come first serve (FCFS) [12] is the simplest version of task allocation algorithms. Processes are allocated to VMs as per their order of arrival in queue. It is a non-preemptive algorithm. FCFS is the default technique for task allocation scheduling. But due to its simplicity, waiting time of processes may increase rapidly. It considers all processes as equal, but process or workload may be of different significance, so it may exhibit losses in business.

In Shortest Job First (SJF) algorithm [11, 13] or Shortest-Process-Next (SPN) algorithm, out of number of work processes waiting for execution, a smallest length cloudlet process is selected to be allocated to available virtual machine. It is a non-preemptive algorithm. The SJF algorithm is suitable for batch jobs, with predefined execution times. Since this type of scheduling results in the lower average time, it is optimal in nature. However, the algorithm should have a prior information of time required by each cloudlet for executing completely. This prediction about execution time of each cloudlet prior to its actual execution is a major task and is an overhead to system. Then at times, estimation can be erroneous if some new type of workload is to be executed whose history is not well known.

The Hungarian algorithm [14] uses combinatorial optimization for allocating cloudlets on VMs. This can optimize the whole task execution, proposed by Harold Kuhn. Another advancements done in the same field by James Munkres which found that it is strongly polynomial. So using combinations, it can solve any non-polynomial problem in polynomial times, so this was an optimization achieved in utilization of resources, and their efficiency in execution. In CloudSim, the Hungarian method is used for having least cost for whole cloudlet execution for an objective to attain with whole VMs to run effectively [15]. Then, some recent research works are also done which optimize the cloud performance on time constraints as given in [16]. Another optimization approach that is suitable for clouds is using Cournot and Bertrand games utilized for resource management in the federated cloud as proposed in [17].

3 Problem Formulation

In a cloud environment, hardware is associated with virtual machines (VM) which are the working units in cloud environment. Task allocation algorithms are mechanisms for allocating workloads on these VMs. A number of algorithms and techniques are discussed in previous section. For the main theme of cloud computing, resource utilization must be maximized for better worth of infrastructure of VMs, as per their capabilities. Optimization of servers to lessen the energy resources and proper tuning of energy usage in these active resources is the prime concern nowadays. So this work has proposed an algorithm for tuning of energy consumed and the resource usage in task allocation algorithm. Optimization through this work may result in good performance for a cloud environment. It can be done by making modifications in parameters like execution time of the cloudlets, which in turn will affect makespan and may change throughput, energy consumed and utilization ratio of the hardware resources [18, 19].

3.1 *Open Issues*

According to research literature discussed in section 2 above, a number of research gaps are identified, in which direction future researches can be perused. Following are the areas of interest in this field.

- Power consumption is the main area in allocation algorithms for work; system should consume power efficiently.
- Cloud demands a dynamic and rapid provisioning of services through infrastructure. So faster response time is always a requirement for good cloud environment.
- Explored techniques have achieved lesser makespan but have utilized more power consumption.
- Makespan and execution time must be approaching to each other, lesser the gap better is the algorithm.
- The price/performance ratio helps estimate the cost and further design the service catalogue.

3.2 *Contributions*

1. As per problem statement, an objective function is defined with all assumptions and constraint fixed for scenario.
2. Designed algorithm is implemented on CloudSim.
3. Execution time of cloudlets is reduced.
4. Reduction in energy consumption is attained.
5. Then, performance of proposed work with respect to peer techniques is shown for execution time, makespan, utilization ratio and power consumption parameters.

3.3 *Objective Function*

For the optimization of the task scheduling technique, in the given cloud environment, the resources allotted need to be used to their maximum efficiency. For maximizing the utilization ratio (UR), we have proposed an objective function given below in equation no. 1, subject to constraints followed. Table 1 describes various symbols and their meaning used in this paper.

Table 1 Utilization ratio per VM in each technique

	FCFS SJF Hungarian proposed			
VM0	1	1	0.84	1
VM1	0.42	0.95	1	0.95
VM2	0.42	0.45	0.60	0.89

$$\text{Maximize}\{UR\} \text{ Subject to: } \begin{cases} ET: \text{minimized} \\ MS - ET \rightarrow 0 \\ ET \propto \frac{1}{IT} \\ P_{\text{cons}}: \text{minimized} \\ S_{\text{up}}: \text{increased} \\ POW_{\text{rate}} \propto UR \end{cases} \quad (1)$$

where $UR \rightarrow$ utilization ratio, $ET \rightarrow$ execution time, $MS \rightarrow$ makespan, $P_c \rightarrow$ power consumed, $S_{\text{up}} \rightarrow$ speedup percentage, $POW_{\text{rate}} \rightarrow$ rate of power consumed, and $IT \rightarrow$ ideal time.

For maximization of utilization ratio, following constraints are being followed like: execution time needs to be minimized, difference between makespan and execution time should limit towards zero, i.e. makespan and execution times should be same. Execution time is inversely proportional to ideal time. P_{cons} should be minimized and S_{up} should be more for a suitable viable algorithm.

3.4 Problem Statement

For the main theme of cloud computing, resource utilization must be maximized for better worth of infrastructure of VMs, as per their capabilities. Due to the depletion of energy from the servers, proper energy tuning approach is required in server optimization, this is a scope of research in this area. So this work has implemented an algorithm for tuning of energy consumed and the resource usage in task allocation algorithm. Optimization of these techniques results in performance tuning of the cloud environment by affecting parameters such as execution time of the cloudlets, which in turn affects makespan and may change throughput, energy consumed and utilization ratio of the hardware resources.

3.5 Methodology

For having tuning of parameters for a task allocation algorithm, we have to design a new algorithm for task allocation. Our proposed algorithm was given in [20]. For implementing and testing the performance of this proposed algorithm with its peer

algorithms, CloudSim tool [5, 21] is used. Its performance parameters are computed, noted and calculated for peer comparison on same platform. Techniques for comparison taken are FCFS, SJF and Hungarian matching.

4 Implementation and Output

In this section, implementation description of our algorithm and its peers is discussed. Then, its output is measured and given.

4.1 Proposed Solution

The proposed technique aims to tune the performance of the cloud environment by reducing the execution time of the cloudlets on VMs and the energy consumption of the system. For the implementation of our goal, we have considered the following performance parameters like execution time of the cloudlets, makespan, throughput of the system, utilization ratio of the hardware resources, rate of energy consumption of the system and total energy consumed by the system.

Overview Task allocation should be done in a cloud environment such that high performance can be achieved. For this requirement, a new algorithm is proposed. The proposed algorithm is a hybrid algorithm with a function for weights to allocate workload with VMs capabilities. It allocates the appropriately biased application with suitable VM. Like VMs with high memory are being offered with cloudlets of high memory requirements. VMs with more IOs are offered with cloudlets with more IOs requirements. So workload nature-wise biasing is being done by heuristic function. So proper utilization of VMs resources can be done.

Flowchart The proposed algorithm can be depicted using flowchart as shown in Fig. 1.

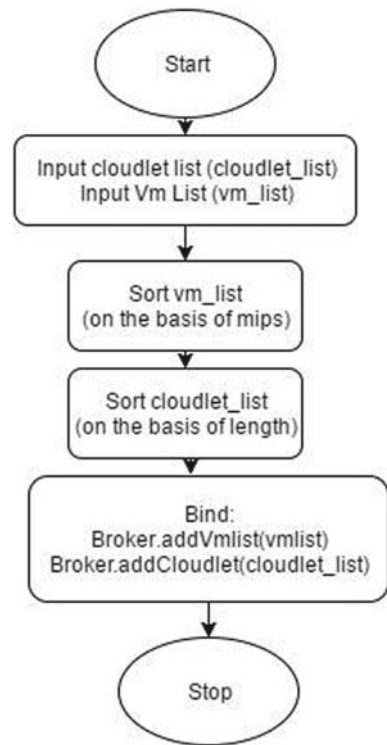
Output The output screen on implementing the proposed technique is shown in Fig. 2.

As a result utilization ratio is more and power consumption would be lesser. As a result, utilization ratio is more and power consumption would be less. Same can be evident from implementation and performance parameter values.

5 Performance Testing

The following performance parameters are taken into account:

- Execution time of the cloudlets
- Makespan

Fig. 1 Working flowchart

- Throughput of the system
- Utilization ratio of the hardware resources
- Rate of energy consumption of the system
- Total energy consumed by the system

All the techniques have been tested with the same cloudlet and VM configurations and compared for performance, and the results have been represented graphically [22].

5.1 Configurations of VMs and Cloudlets

The virtual machines and the cloudlets that have been used for experimentation have the configurations [22].

VMs are configured with MIPS of 250, 150 and 200 with a size of 10,000, RAM is 512, bandwidth is 1000, processing elements are 1000, and virtual machine manager is Xen hypervisor in each instance.

While **Cloudlets** are configured with one processing element, length is 250,000, 350,000 and 200,000, respectively. File size and output size parameters are both set to 300.

```

Initialising...
Starting CloudSim version 3.0
Datacenter_0 is starting...
Broker is starting...
Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)
0.0: Broker: Trying to Create VM #0 in Datacenter_0
0.0: Broker: Trying to Create VM #2 in Datacenter_0
0.0: Broker: Trying to Create VM #1 in Datacenter_0
0.1: Broker: VM #0 has been created in Datacenter #2, Host #0
0.1: Broker: VM #2 has been created in Datacenter #2, Host #0
0.1: Broker: VM #1 has been created in Datacenter #2, Host #0
0.1: Broker: Sending cloudlet 2 to VM #0
0.1: Broker: Sending cloudlet 0 to VM #2
0.1: Broker: Sending cloudlet 1 to VM #1
1250.1: Broker: Cloudlet 0 received
1333.433333333332: Broker: Cloudlet 1 received
1400.097333333332: Broker: Cloudlet 2 received
1400.097333333332: Broker: All Cloudlets executed. Finishing...
1400.097333333332: Broker: Destroying VM #0
1400.097333333332: Broker: Destroying VM #2
1400.097333333332: Broker: Destroying VM #1
Broker is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.

===== OUTPUT =====
Cloudlet ID   STATUS   Data center ID   VM ID   Time   Start Time   Finish Time
0             SUCCESS   2                2       1250   0.1          1250.1
1             SUCCESS   2                1       1333.33  0.1          1333.43
2             SUCCESS   2                0       1400    0.1          1400.1
Proposed Algorithm Executed!

```

Fig. 2 Output results from CloudSim

5.2 Utilization Ratio

The ratio of time taken by a cloudlet to execute completely to the total time a VM runs is known as the utilization ratio of that VM. The utilization ratio of each VM in the techniques implemented has been shown in Table 1.

5.3 Power Consumption

Studies [23, 24] have shown that on average, when an idle server is fully utilized, it consumes almost 70% of the total power consumed. Further, these studies additionally demonstrate that this power consumption can be accurately described by a linear relationship [25] between the CPU utilization (utilization ratio) and power consumption. Therefore, for our experimental studies, we define the power consumption as a function of the CPU utilization (Pow_{rate}):

$$\text{Pow}_{\text{rate}}(t) = i * P_{\text{max}} + (1 + i) * P_{\text{max}} * UR \quad \text{Pow}_{\text{rate}}(t) = P_{\text{max}} * (0.7 + 0.3 * UR)$$

where

I = power consumed by an idle server in fraction; UR = CPU utilization (utilization ratio) where P_{max} is assumed as:

250 mW/ms for VM0

200 mW/ms for VM1

230 mW/ms for VM2

Thus, total power consumed is shown in Fig. 3.

The rate of power consumption per VM for each technique considered can be seen in Table 2.

Due to variations in the workload, the utilization ratio may change over time and is, thus, defined as a function of the time: $UR(t)$. Therefore, to define the total energy consumption (P_{consumed}) by a server we use [26]:

$$P_{\text{consumed}} = \int_0^t \text{Pow}_{\text{rate}}(t) dt$$

Thus, to reduce the total energy consumption, we improve the utilization ratio.

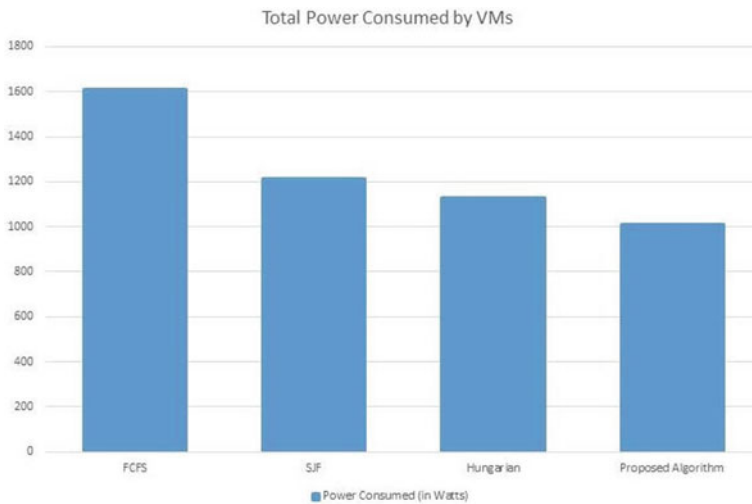


Fig. 3 Total power consumed by each technique

Table 2 Rate of power consumption per VM for each technique

FCFS SJF Hungarian proposed				
VM0	250	250	237.99	250
VM0	250	250	237.99	250
VM1	165.71	197.14	200	197.14
VM2	190.57	192.54	202.39	222.60

Table 3 Speedup of proposed algorithm versus FCFS, SJF and Hungarian for various parameters

FCFS			SJF Hungarian
Execution time (%)	8.07	5.53	2.04
Makespan (%)	39.99	20	16
Utilization ratio (%)	53.20	18.08	16.60
Power consumption (%)	37.21	16.52	10.52

6 Conclusion

In this paper, various task-scheduling algorithms are studied, mainly FCFS, SJF and Hungarian in cloud environment. A new task allocation algorithm is proposed for achieving higher utilization and lesser energy consumption. Due to the hybrid allocation function of proposed algorithm, appropriate allocations of workloads are being done on cloudlets due to which utilization of infrastructure of VM is increased and power consumption is decreased. Such parameter results and speedups are shown after calculating from CloudSim parameters. Thus, the proposed objective function is justified with results and analytically. Speedups of proposed technique *w.r.t.* FCFS, SJF and Hungarian algorithm in terms of execution time, makespan, utilization ratio and power consumption are given in Table 3.

While in terms of speedups, decrement percentages of execution times, makespan and power consumption are given while increment percentage of utilization ratio is given.

References

1. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. In: Grid Computing Environments Workshop, pp. 1–10 (2008)
2. Sim, K.M.: Agent-based cloud computing. *IEEE Trans. Serv. Comput.* **5**, 564577 (2012)
3. Mell, P.M., Grance, T.: The NIST Definition of Cloud Computing. NIST special publication 800-145 (2011)
4. Wang, X., et al.: Online cloud resource prediction via scalable window waveform sampling on classified workloads. *Future Gener. Comput. Syst.* **117**, 338–358 (2021)
5. Beloglazov, A., Buyya, R.: CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Wiley Online Library (wileyonlinelibrary.com) (2010)

6. Theja, P.R., Khadar Babu, S.K.: Resource optimization for dynamic cloud computing environment: a survey. *Int. J. Appl. Eng. Res.* **9**(24) (2014). ISSN 0973-4562
7. Lei, J., et al.: Cloud task and virtual machine allocation strategy in cloud computing environment. In: *Network Computing and Information Security, Second International Conference, NCIS Proceedings* (2012)
8. Tayal, S.: Tasks scheduling optimization for the cloud computing systems. (IIAEST) *Int. J. Adv. Eng. Sci. Technol.* **5**(2) (2011)
9. Tiwari, R., Kumar, N.: An adaptive cache invalidation technique for wireless environments. *Telecommun. Syst.* **62**(1), 149–165 (2016)
10. Tiwari, R., Kumar, N.: Cooperative gateway cache invalidation scheme for internet-based vehicular adhoc networks. *Wireless Pers. Commun.* **85**(4), 1789–1814 (2015). <https://doi.org/10.1007/s11277-015-2867-3>
11. Rekha, S., Santhosh Kumar, R.: MJHP—job scheduling algorithm for cloud environment. *Int. J. Tech. Res. Appl.* (2014). e-ISSN: 2320-8163
12. Yahyapour, R., Schwiegelshohn, U.: Analysis of first-come-first-serve parallel job scheduling. In: *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms* (1998)
13. Hong, C., Caesar, M., Godfre, P.: Finishing flows quickly with preemptive scheduling. *SIGCOMM Comput. Commun. Rev.* (2012)
14. Kunh, H.W.: The Hungarian method for the assignment problem. *Naval Res. Logistics Q.* **1**, 83–97 (1955)
15. Kushang, P., et al.: Virtual machine allocation policy in cloud computing using CloudSim in Java. *Int. J. Grid Distrib. Comput.* (2015)
16. Halima, R.B., Kallel, S., Gaaloul, W., Maamar, Z., Jmaiel, M.: Toward a correct and optimal time-aware cloud resource allocation to business processes. *Future Gener. Comput. Syst.* **112**, 751–766 (2020)
17. Khorasani, N., Abrishami, S., Feizi, M., Esfahani, M.A., Ramezani, F.: Resource management in the federated cloud environment using Cournot and Bertrand competitions. *Futur. Gener. Comput. Syst.* **113**, 391–406 (2020)
18. Vijindra, Shenai, S.: Survey on scheduling issues in cloud computing. *Procedia Eng.* **38** (2012)
19. Endo, P.T.: Resource allocation for distributed cloud: concept and research challenges. *IEE*, 42–46
20. Tiwari, R., Lal, G., Goel, T.: Published paper “Performance tuning approach for cloud environment”. *Int. J. Adv. Intell. Syst. Comput.* (2016)
21. Ranbhise, S.M., Joshi, K.K.: Simulation and analysis of cloud environment. *Int. J. Adv. Res. Comput. Sci. Technol.* (2014)
22. Majumdar, S.: Resource management on cloud: handling uncertainties in parameters and policies. *CSI Commun.* 16–19 (2011)
23. Fan, X., et al.: Power provisioning for a warehouse-sized computer. In: *Proc. of the 34th Annual International Symposium on Computer Architecture*, pp. 13–23 (2007)
24. Kusic, D., et al.: Power and performance management of virtualized computing environments via look ahead control. *Clust. Comput.* **12**(1), 1–15 (2009)
25. Beloglazov, A., Buyya, R.: Adaptive threshold-based approach for energy efficient consolidation of virtual machines in cloud data centers. In: *Proceedings of the 8th International Workshop on Middleware for Grids, Clouds and E-Science—MGC '10* (2010)
26. Beloglazov, A., Buyya, R.: Energy efficient resource management in virtualized cloud data centers. In: *2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing* (2010)

Author Index

A

Agarwal, Aviral, 31
Aggarwal, Himani, 75
Agrawal, Akshat, 99, 309
Ahlawat, Prachi, 321
Ahuja, Aarush, 179
Alam, Md. Afshar, 445, 541
Anuradha, 143, 585
Arora, Akash, 401
Arora, Ritika, 87
Arpitha Shankar, S.I., 213
Azubuike, Ezenwoke, 99

B

Baghel, R.K., 479
Bahuguna, Varun, 75
Bajaj, Parv, 87
Behera, Sagarika, 575
Bindal, Amit Kumar, 585
Bindlish, Sanya, 423
Booba, B., 351
Budhani, Sandeep Kumar, 21

C

Charan Kumari, A., 199
Chaubey, Ashish, 3
Chaudhary, Kavita, 53
Chavan, Shubham, 565
Chhabra, Sargam, 423

D

Damasevicius, Robertas, 99, 309
Deshmukh, Saumya, 501
Dheeryan, Niket, 523
Dinesha, P., 213

Dua, Devansh, 31

E

Ezra, Paul Joan, 309

G

Ganesan, Sumathi, 129
Girija, R., 289
Gonsai, Atul, 301
Goswami, Radha Tamal, 11
Goyal, Gaurav, 3
Gryzunova, Darina, 191
Gryzunov, Vitaly, 191
Gupta, Daya, 597
Gupta, Rahul, 31
Guru Prasad, U., 289

H

Harish, D., 487
Hassan, Afshan, 585

I

Iftekhar, Nida, 445
Indu, S., 597

J

Jain, Achin, 391
Jain, Rachna, 75, 523
Jain, Vanita, 179, 391
Jayalakshmi, S. L., 289
Jha, Atul, 11

K

Kalra, Vaishali, 381
Kalwar, Achal, 565

Kanisk, 401
 Kapur, Saniya, 75
 Karkera, Shrishti, 501
 Kaur, Amandeep, 65
 Kaur, Parmeet, 153
 Kaushik, Keshav, 3, 265
 Khanna, Kavita, 321
 Khan, Samia, 445
 Khurana, Mehak, 45, 87
 Khurana, Mridul, 391
 Kumar, Kamal, 513
 Kumar, Nitin, 433
 Kumar, Satyam, 513
 Kumar, Shailender, 401
 Kumar, Vinay, 53
 Kumar, Vinod, 433

M

Maan, Priyanka, 199
 Mahajan, Shilpa, 87
 Makani, Ruchi, 113
 Maskeliunas, Rytis, 99, 309
 Mathur, Rohan, 565
 Mehta, Deepa, 541
 Mehta, Kshitij, 423
 Misra, Sanjay, 99, 309
 Mittal, Puneet, 143
 Mondal, Avijit, 11
 Murugappan, K., 231

N

Nagrath, Preeti, 75, 523
 Narvekar, Chhaya, 501, 565

O

Oluranti, Jonathan, 309

P

Pahuja, Rahul, 523
 Parthasarathy, Akaash R., 239
 Patel, Jatin, 161
 Prasad, Devendra, 585
 Prathuri, Jhansi Rani, 459, 575
 Puri, Vartika, 153

R

Rahunathan, L., 487
 Raj, Akanshu, 391
 Rani, Seema, 65
 Rathee, Tripti, 371

Rathod, Chetan, 301
 Rawale, Prachi, 501
 Reddy, B.V.R., 113
 Renuka, P., 351
 Roshan, Khushnaseeb, 551
 Rotimi, Olasina Jamiu, 99

S

Sachdeva, Shelly, 153
 Saini, Dharmender, 179
 Salankar, Nilima, 609
 Samson, A. Antony, 487
 Sapra, Pooja, 381, 423
 Sarfaraz, Aatif, 11
 Saxena, Vineeta, 479
 Sejwal, Simran, 381
 Sethi, Lovish, 523
 Sharma, Asmit Kumar, 3
 Sharma, Bhawna, 253, 273
 Sharma, Gargeya, 3
 Sharma, Geeta, 53
 Sharma, Sandeep, 321
 Sharma, Sukhwinder, 143
 Shelly, 513
 Dr.Sheth, Ravi, 161
 Siddiqi, Abra Shafiq, 445, 541
 Sille, Roohi, 609
 Singh, Hukum, 45, 199
 Singh, Pardeep, 609
 Singh, Parvinder, 273, 371
 Sivabalaselvamani, D., 487
 Sonakshi, 341
 Sree Kala, T., 231
 Surana, Sneha, 265

T

Tanwar, Abhishek, 391
 Tewari, Naveen, 21
 Tijare, Poonam Vijay, 459
 Tiwari, Rajeev, 513, 609

U

Ullah, Syed Uvaid, 479

V

Vaid, Rohit, 253
 Vedhapriyavadhana, R., 289
 Verma, Pawan Kumar, 433
 Verma, Seema, 341
 Vivek Raj, K., 213

Y

Yadav, Ankit, [31](#)
 Yadav, Rajiv, [597](#)

Z

Zafar, Aasim, [551](#)
 Zafar, Sameena, [479](#)
 Zafar, Sherin, [445](#), [541](#)