IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14233

E-Voting Using Blockchain: A Secure and Transparent Approach

Dr. T. Subbareddy[1], MahendraSakhamuri[2], KunduruPratap[3], TiramdasuNithin[4], Parakandla Durgaganesh[5]

Associate Professor of CSE-Data Science, KKR & KSR Institute of Technology and Sciences,
Guntur, Andhra Pradesh, India[1]

B. Tech CSE-Data Science, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India[2-5]

Abstract: Voting is an essential part of any democracy but traditional methods based on paper ballots often face risks like security breaches, fraud, and voter intimidation. The opportunity to solve these issues comes with applying blockchain technology where voting is decentralized, secure, and transparent. This document analyzes how block chain can facilitate e-voting while dealing with problems such as voter impersonation, ballot secrecy, and election fraud. Utilizing crypto security, smart contracts, and decentralization, trust and accessibility of the electorate can surely be improved. We evaluated blockchain e-voting systems and their pros and cons as well as innovations that will follow in these systems. Voter impersonation and tampering have been long standing issues in electioneering and voting and recently emerged electronic voting scheme provides a possible solution to these problems. However, it has introduced complicated issues regarding security, credibility, transparency, functionality and most importantly, reliability. Using blockchain technology in e- voting improves security by effectively addressing threats of fraud and vote tampering. Such systems are virtually impossible to hack as the vote ledger is decentralized and can be verified by anybody.

Keywords: Blockchain; E-Voting; Decentralization; Smart Contracts; Cryptographic Security

1. INTRODUCTION

Elections are central towards governance and policy systems of a state which makes voting an important element of a country's politics. On the contrary, traditional voting systems face sophisticated challenges like voter fraud, ballot tampering and issues of very limited scope of accessibility. These areas shave improved thanks to technology as e-voting became possible, however it raised additional concerns in terms of security. It can serve as the foundation for a new, secure, transparent and immutable e-voting system. Gland and Liou's paper present a blockchain- based e-voting system that incorporates measures for voter authentication, prevents any form of tampering and maintains privacy. The system employs cryptographic techniques and smart contracts for secure vote casting and counting. The feasibility and the ability of blockchain to resize the electoral systems is proven through analysis of real worlds scenarios and the technical frameworks. "Blockchain has the great power to change elections as we know them, as e-voting is one of the most prominent areas where the technology is… applied" securing ballots is one of the simplest tasks that needs to be addressed. Seemingly easy task is what people voting online e.g. supporting the election of a candidate is a concern. Users need to be assured that the system will not be abused by advanced technologies. In recent years block chain is often mentioned as an example of secure technology used in an online environment. Oure-voting system uses blockchain to manage all election processes.

The intertwining of digital transformation with several industry areas that has governance and election systems has unfolded in a big way. Voting in every form (paper and electronic) has notable weaknesses associated with vote manipulation, coercion, and significant transparency issues. With its decentralized and immutable ledger, blockchain technology solves these problems head on. This project seeks to build integrities within a blockchain system for electronic voting to ensure safety, privacy and record verification during elections. "Public sectors, such as e-voting, stands to benefit from the advancement of blockchain technologies," All of this is easier said than done. New challenges such as ensuring safe guarding in the election which is at least as safe as the classic voting systems with ballots, emerge. This is exactly the reason why we set out to build worry free blockchain based secure elections. As a secure technology that guarantees safe online transactions, block chains has been the go to technology for many years now. All election processes in my proposed e-voting system are handled through the block chain. The lack of trust concerning the Centralized authority in charge of creating and supervising elections and the additional concern of the

DOI: 10.17148/IJARCCE.2025.14233

authority altering the election's results sets my solution apart from the rest. Particularly in the formoftraditionalmeansofdirectvoting,votingisalready the foundation and stream of democracy-commraising the integralrightsofeverycitizentodeterminetheir representatives and democratic process of ruling. The said mechanisms,dealingwithvoting-varyingfrompaperballots to electronic-are scarcely freefromrigors.Suchvexations mightinvolve,interalia,with certain canvasserstampering with votes, the lack of transparency in the voting process, and logisticaldifficulties-vis-à-visthosethatwouldcomeintoplay in the virtual setting for such a large-scale election.Thiswill include things like voter fraud, double-toting, coercive voting, and inefficiencies in counting the votes, all of which would greatly undermine confidence in an election process.With changing technologies, electronic voting has become a reasonableoptionforallof thesequestions.Whilethe electronic voting systems improve ease of access and flow of voting, they are principally centralized and prone to security threats, be it through hacking or direct manipulations. A very secure, transparent, andverifiablevoting systemproposes to useblockchaintechnology.Animmutable,decentralized, secure production environment of trust and transparency will support Blockchain in a wide variety of application areas.By using Blockchain, an e-Voting system may assure data is not susceptibletoalteration,keepstheintegrityofvotes,and allows voters to trust the systemmore. Ethereumsmartcontracts act as an important tool for the automation of the election process.

The primary objectives of this project are:To develop a decentralized e-voting system that ensures security, transparency, andverifiability.Topreventvotemanipulation andensurethatvotesremainimmutableoncecast.To enhance voter anonymity while maintaining the integrity of the election.To allow real-time vote counting and reduce human intervention in the process.To make the system accessible and easy to use while ensuring its scalability for large-scale elections.This project aims to bridge the gap betweentraditional voting systems and modern technological advancements by providing a solution that can be implemented at different levels, from student council elections to national- level democratic elections.The following sections will provide an in-depth analysis of existing work, the proposed system architecture, security features, challenges, testing methodologies, and future enhancements to improve the efficiency and reliability of blockchain based e-voting systems.Key cryptographic techniques employed include zero- knowledgeproofs, which bolster voter privacy, and securehash algorithms like SHA-384, SHA-256, Zero Knowledge Proofs (ZKPs), Digital Signatures(ECDSA, RSA, Ed25519),Smart Contracts, Public Key Cryptography (PKC), which safeguard data integrity and uses consensus algorithms likeProof ofWork (POW): Ensures tamper-resistance but is energy- intensive. Proof of Stake (POS): Reduces energy costs while maintaining security. Additionally, link-ablering signaturesare implemented to maintain voter anonymity while preventing double voting. The primary objective of integrating blockchain into voting is to establish a trustworthy, tamper-resistant platform that upholds voter confidentiality and enhances public confidence in democratic processes. Additionally, integrating blockchain with a modern frontend framework such as Next.js allows for a user-friendly and interactive voting experience.Its main advantage is that there is no need for confidence in the centralized authority that created the elections. This authority cannot affect the election results in our system. Another challenge in e voting is the lack of transparency in the functioning of the system, leading to a lack of confidence in voters.

2. RELATED WORK

Many studies have discussed how blockchain can revolutionize e-voting. Reports indicate that the use of decentralized ledgers would greatly reduce the possibility of electoral fraud and improve transparency [1]. Thefirstmajorsuchimplementationontheotherhandwasi-Voting inEstonia,which,althoughitisverycapable,hasa centralized structure [2]. Other works have examined the privacy-preservingtechnologiescapableofoffering anonymity to voters like zero-knowledge proofs [3]. Beyondallthis,severalopenresearchissuesremain: scalability,voterauthentication,andresistancetocyber-attacks.Inrecent years electronic voting systems have succeeded ineasing the voting process and attracting increased voter participation. In spite of this fact, opponents have continued containing criticism for hacking and other forms of interference that primarily discourage their acceptability.This project is anattempt to try to address these issues inwhichasecureandtamper-proofe-votingplatformis secured on blockchain. The project uses four frameworks: Truffle, Web3, Solidity programming language. Because it is too easy to alter the data in conventionale-voting systems, it becomes inherently allthemoreimportantto beabletoguaranteeauthenticityandintegrityinthe voting process through the technology-based e-voting process.Ganacheisablockchainsimulatorthatisused for testing and validation, thus ensuring the robustness ofthe application before deployment. Unlike the traditional electronic voting system, this blockchain-based solutionwill guarantee transparency, immutability, and protection fromelectionfraud.Besidessustainingvoterconfidence, it facilitates healthier electoral processes, hence laying a basis for a modern-day responsive democracy.Voting systems are in need of urgent improvement due to the aforementionedproblems.Thewaytocounteractthiscan be by overthrowing the ongoing system by a newsystemthatlimitsthechancesofvotingfraudsand makes the voting and counting much more efficient. Our main aim is to put blockchain technology to resolve the problems related to conventional voting systems.

DOI: 10.17148/IJARCCE.2025.14233

OurelectronicvotingsystemusingBlockchainwilllimit voting fraud and increase voterturnout.Using aBlockchainwillsatisfyalltherequirementsofanyvoting system.

Thesystemprovidesfortheverificationoftotalvotescast, which establishes transparency and accountability. The objectives: to develop a smart contract, would make it transparent, immutable, and accurate using Solidity languages. Migrate users into a secured mechanism for registration and login where voting verification will be through the Aadhaar card. This would bring an end to multiple voting possibilities or the generation of fake votes. Develop a web application that provides the ability for the user tologontoandcasthis/her voteinthee-votingsystem. In order toachievetheintegrationrequiredbetween theweb application and the blockchain platform, both Web3.js and Ganachewillbeemployed.Theimplementationwillallowus to run smart contracts and save voting data securelyThe systemprovidesfortheverification oftotalvotescast,which establishes transparencyand accountability. The objectives: to develop a smart contract, would make it transparent, immutable, and accurate using Solidity languages. Migrate users into a secured mechanism for registration and login where voting verification will be through the Aadhaar card. This would bring an end to multiple voting possibilities or thegeneration offakevotes. Develop a webapplication that provides theabilityfor the user to log on to and cast his/her vote in the e-voting system. In order to achieve the integration required between the web application and the blockchain platform, both Web3.js and Ganache will be employed. The implementation will allow us to run smart contracts and save voting data securely.

The process of testing comprises engaging in activities related to the identification of errors, bugs or defects in a software product. It requires the execution of software or systems under specific conditions to observe their behavior and functionality. It also checks whether the product (i.e., the system) has met the functional, performance, design, and implementationspecificationsregisteredinthe specification documents. Testing may happen at any stage within the software development life cycle, from the initialstage down to maintenance. The testing can be done on a manualbasis,thatis,donebyhumanbeings,oran automated basis, with the help of testing tools or scripts.Testing enables identifying the problems early in the development cycle, thus ensuring higher quality and more reliable software, reduced costs, and greater customer satisfaction. To conclude, the purpose of testing is thediscoveryoferrorswheretestingreferstoattemptsto disclose any possible defect in a product. Testing provides a local vantage to check for components, subassemblies, assemblies, and/or a complete product. Testing refers to the processoftherequiredexecutionofsoftwareforthe purpose of establishing that the software system satisfies the requirements of both the user and the final specification andthatitdoesnotproduceunacceptablefailures.Varioustypes of tests exist, each attending to a specific subclass of testing requirements.Further,theproblemsof security, anonymity, and user accessibility relative to broad penetration must bedealt with. Future developments in blockchain scalability, cryptographic privacy solutions, and AI-based verification will fortify e-voting systems.Some have developed a blockchain- based e-voting system as a secure, transparent, and decentralized alternative to the traditional methods of voting. Blockchain technology assures that votes are formed in an immutable manner: this assures integrity, prevents tampering, and allows verification. Smart contracts automate votecounting, thus reducing human interference and potentialhuman errors. The integration of biometric verification and AI- enabled fraud checks enhances security and obnoxiouslyhinders the prospect of identity fraud.

3. SYSTEM ARCHITECTURE

Voter Registration: Users register using a cryptographic keypair toverifyidentitywhilepreservinganonymity.Vote Casting: Votes are encrypted and recorded on a blockchain ledger through smart contracts.Vote Counting and Verification: The blockchain network ensures that votes are immutable and publicly auditable without revealing individual voter identities.

Smart Contract Implementation

Smart contracts automate key election processes such as Ballot creation and distribution Vote encryption and validationReal- time vote tallying with consensus mechanismsUse Cases for Xception in E-Voting&Blockchain :Voter IdentityVerification Use Xception for facial recognition to verify voter identity before allowing them to cast a vote.Prevents identity fraud by ensuring only registered voters can access the system.Signature or Document Verification Train Xception to validate digital signatures or scanned voter ID documents. Ensures authenticity of voter registration. Fraud Detection &Anomaly Detection. Use deep learning to detect irregular voting patterns in a blockchain-based system. Identify potential double voting or unauthorized access. CAPTCHA or Anti-Bot Measures Prevent bots from spamming the blockchain voting system by using Xception to validate human users.

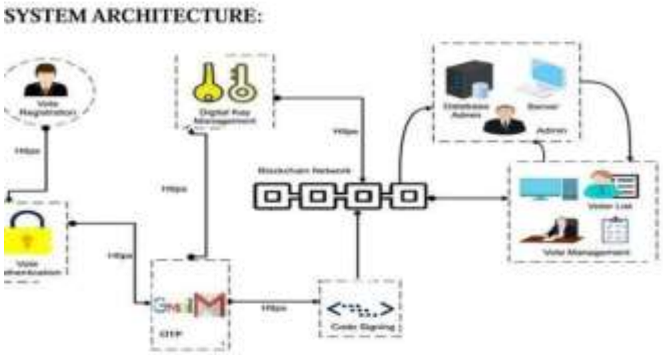

Figure: System Architecture

SECURITYMEASURES

To ensure the security of an E-voting system, strong cryptographic measures are needed: VoterAuthentication,Public-key cryptography ensures the authentication of voter identity without revealing personal data. Multi-factor authentication increases the level of security. Data Integrity and Transparency:Being decentralized, the block-chain ensures that once votes are recorded, they cannot be changed or deleted, therefore preventing vote manipulation. Privacy Preservation: Homomorphic encryption and zero-knowledge proofs preserve voter anonymity while allowing for safe verification of the votes. Blockchain technology, being used in the form of smart contracts for e-voting, guarantees transparency, immutability and great security during the elections. This factoring negates central authority control, prevent stampering, and provides verifiable results once elections are over. Completion of the dot point is a list of the following challenges and limitations: Scalability Public blockchains might, therefore, have issues with very high transaction volumes, particularly in the case of national elections. Voter coercion risks alone cannot be prevented by blockchain. Technical barriers Mean while, voter education with regards to the blockchain-based systems and access to them remain serious impediments, especially in areas of low digital literacy.

4. FUTURE DIRECTIONS

Future research that may further enhance blockchain-basede-voting may focus on Layer 2 solutions such as off-chain voting verification for scalability, integration withbiometrics for authentication, and hybrid approaches that combine blockchain with traditional voting methods.

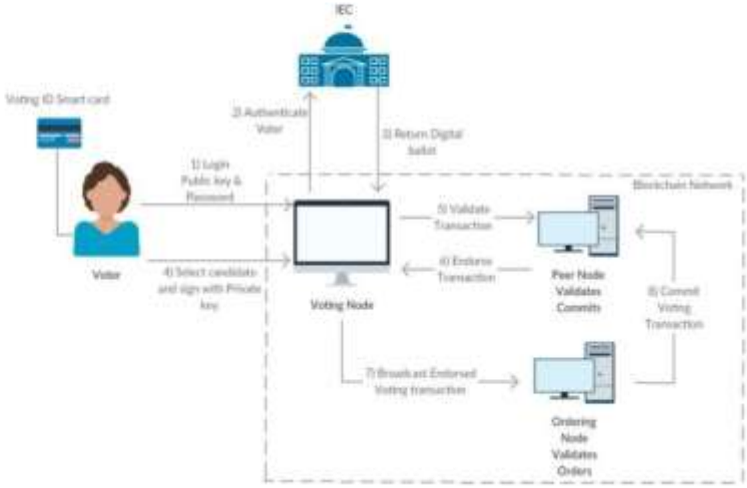
IEC
Voting ID Smart card
2) Authenticate Voter
3) Return Digital ballot
1) Login Public key & Password
Blockchain Network
5) Validate Transaction
6) Endorse Transaction
Voter
4) Select candidate and sign with Private key
Voting Node
Peer Node Validates Commits
8) Commit Voting Transaction
7) Broadcast Endorsed Voting transaction
Ordering Node Validates Orders

Figure: E-voting workflow

5. CLASSIFICATION

We now turn to the second problem of detecting trading malpractices like hoarding. We first identify cases of hoarding and weather related anomalies using newspaper reports. We isolate the reports into hoarding incidents irrespective of a weather event, and weather events when no hoarding

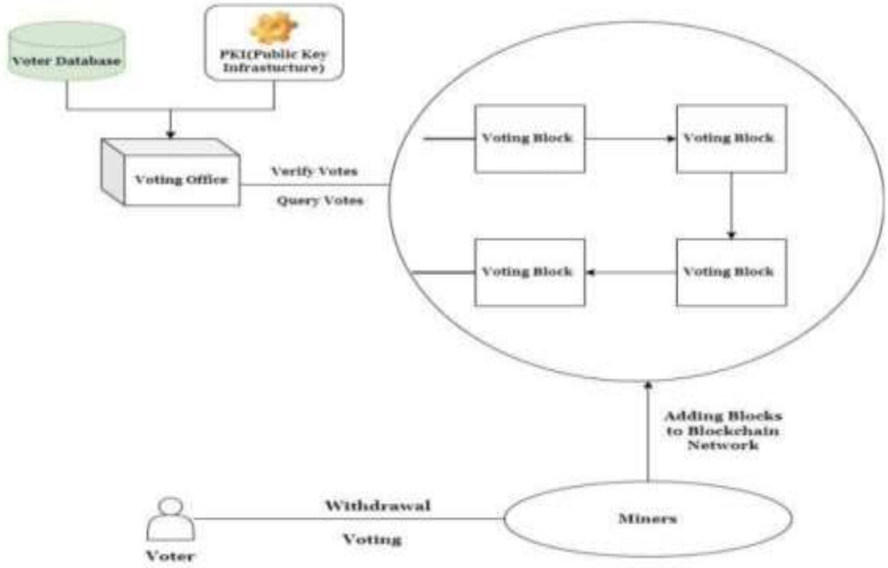

Figure: Classification diagram

6. DISCUSSION AND CONCLUSIONS

Blockchain-based e-voting is a secure, transparent, and decentralized alternative to conventional voting methods. Thanks to blockchain technology, voting can also be written onto an immutable land register, thereby maintaining its integrity, preventing it from being tampered with, and enabling its verifiability. All votes are counted automatically-by the smart contract-with very little human intervention, which reduces the possibility for human error. In addition, AI-based fraud detection along with biometric verification can greatly improve system security and protect against identity fraud. However, the stated barriers do include user accessibility, privacy mediation, and scalability issues. Other advanced resilience mechanisms may include future advancements in blockchain scalability, cryptographic privacy solutions, and AI-based verification, which could further cement the security ofe-voting systems.

The further development of blockchain e-voting can revolutionize elections, providing security, efficiency, and trust worthiness. E- voting based on blockchain technology represents a radical change in the election system, targeting essential issues like security, transparency, and voter confidence. Conventional voting methods, either paper, electronic or even online, get mired in uncertainty in their conclusions because of fraud and manipulation. The decentralized and immutable nature of blockchain comes to help in these cases by guaranteeing a secure voting process where each vote is secured in register and can't be altered or deleted. Although challenges remain, developments in cryptography and blockchain scalability will help resolve the current limitations; thus, it is the view of many that e-voting using blockchain has the capability to make the process secure, transparent and trustworthy. Governments will be able to enhance the integrity of elections and the confidence of voters in democratic processes by employing blockchain-based voting.

7. ACKNOWLEDGEMENTS

We would like to thank **Dr.B .Bhanu Prakash** sir Head of the Department(HOD),**Dr.T. Subbareddy** sir and the Trainers Especially, a special thanks to Teja Kavali sir for their continuous support, encouragement, and guidance throughout the project.

REFERENCES

[1] E. Laan, “Estonia’si-VotingSystem: LessonsandChallenges,” Journal of Digital Democracy, 2018.

[2] A. Smith, “Privacy-Preserving Voting with Blockchain,” International Conference on Cryptographic Security, 2021.

[3] Nakamoto, S. “Bitcoin: A Peer-to-Peer ElectronicCash System,” 2008.

[4] Zyskind, G., Nathan, O., & Pentland, A. “Decentralizing Privacy: Using Blockchain toProtect Personal Data,”IEEESecurity & Privacy Workshops, 2015.

[5] Pilkington, M. “Blockchain Technology: Principles and Applications,” Research Handbook on Digital Transformations, 2016.

[6] Bonneau,J.,Miller,A., Clark, J.,Narayanan, A.,Kroll, J.A., & Felten, E. W. “Research Perspectives and Challenges for Bitcoinand Cryptocurrencies,” IEEE Security & Privacy, 2015

[7] Swan, M. “Blockchain: Blueprint for a New Economy,”O’Reilly Media, 2015.

[8] Yavuz, E. A., Kaan, K., Sert, H., & Dalkılıç, G. “TowardsSecure E-Voting Using Blockchain in P2P Networks,” International Symposium on Computer and Information Sciences, 2018

[9] Xia, Z., Wang, X., Sun, X., & Wang, Q. “A Secure and Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data,” IEEE Transactions on Parallel and Distributed Systems, 2016.

[10] Sharma, T., Joshi, S., & Sood, S. K. “Blockchain-based Efficient Voting System,” International Journal of Information Management, 2021.

[11] Wang, H., Xu, X., & Yang, L. T. “Secure Voting System Design Based on Blockchain,” IEEE Transactions on Computers, 2021.

[12] Singh, R., & Chatterjee, S. “Secure and Transparent Election Process Using Blockchain,” Journal of Computing and Security, 2020.

[13] Noizat, G. “Blockchain Electronic Vote,” Handbook of Digital Currency, 2015

[14] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” IEEE International Congress on Big Data, 2017.

[15] Ruffing, T., Moreno-Sanchez, P., & Kate, A. “CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin,” European Symposium on Research in Computer Security, 2014.

[16] Kiayias, A., Russell, A., David, B., & Oliynykov, R. “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” Advances in Cryptology, 2017.

[17] International Journal on “Wielding Neural Networks to Interpret Facial Emotionsin Photographswith Fragmentary Occlusion”, on American Scientific Publishing Group (ASPG) Fusion: Practice and Applications(FPA) ,Vol. 17, No. 01, August, 2024, pp. 146-158.

[18] International Journal on “Prediction of novel malware using hybrid convolution neural network and long short-term memory approach”, on International Journal of Electrical and Computer Engineering (IJECE),Vol. 14, No. 04, August, 2024, pp. 4508-4517.

[19] International Journal on “Cross-Platform Malware Classification: Fusion of CNN and GRU Models”,on International Journal of Safety and Security Engineering (IIETA),Vol. 14, No. 02, April, 2024, pp. 477-486.

[20] International Journal on “Enhanced Malware Family Classification via Image-Based Analysis Utilizing a Balance-Augmented VGG16 Model,onInternational information and Engineering Technology Association (IIETA),Vol. 40, No. 5, October, 2023, pp. 2169-2178.=

[21] International Journal on “Android Malware Classification Using LSTM Model, International information and Engineering Technology Association (IIETA)Vol.36,No.5,(October,2022),pp.761–767.Android Malware Classification Using LSTM Model | IIETA.

[22] International Journal on “Classification ofImage spam Using Convolution NeuralNetwork”,TraitementduSignal, Vol. 39, No. 1, (February 2022), pp. 363-369 .

[23] InternationalJournalon“MedicalImageClassification Using Deep Learning Based Hybrid Model with CNN and Encoder”, International information and Engineering Technology Association (IIETA), Revue d'IntelligenceArtificiellVol.34,No.5,(October,2020),pp.645 –652.

[24] International Journal on “Prediction of Hospital Re- admission Using Firefly Based Multi-layer Perception, International information and Engineering Technology Association(IIETA)Vol.24,No.4,(sept,2020), pp.527–533.

[25] International Journal on “Energy efficient intrusion detection using deep reinforcement learning approach”,Journal ofGreen Engineering (JGE),Volume-11, Issue-1,January2021.625-641.

[26] International Journal on “Classification of High Dimensional Class Imbalance Data Streams UsingImproved Genetic Algorithm Sampling”, International JournalofAdvanced ScienceandTechnology, Vol. 29, No. 5, (2020), pp. 5717 – 5726.

[27] Dr. M. Ayyappa Chakravarthi etal. published Springer paper “Machine Learning-Enhanced Self-Management for Energy-Effective and Secure Statistics Assortment in UnattendedWSNs”inSpringer Nature(Q1),Vol6,Feb4th 2025.

[28] Dr. M. Ayyappa Chakravarthi etal. published Springer paper “GeoAgriGuard AI-Driven Pest and Disease Management with Remote Sensing for Global Food Security” in Springer Nature (Q1), Jan 20th 2025.

[29] Dr. M. Ayyappa Chakravarthi etal. presented and published IEEE paper “Machine Learning Algorithms for Automated Synthesis of Biocompatible Nanomaterials” , ISBN 979-8-3315-3995-5, Jan 2025.

[30] Dr. M. Ayyappa Chakravarthi etal. presented and published IEEE paper “Evolutionary Algorithms for Deep Learning in Secure Network Environments” ISBN:979-8- 3315-3995-5, Jan 2025.

[31] International Journal on “Wielding Neural Networks to Interpret Facial Emotions in Photographs with Fragmentary Occlusion”, on American Scientific Publishing Group (ASPG) Fusion: Practice and Applications(FPA) ,Vol. 17, No. 01, August, 2024, pp. 146-158.

DOI: 10.17148/IJARCCE.2025.14233

[32] International Journal on “Prediction of novel malware using hybrid convolution neural network and long short-term memory approach”, on International Journal of Electrical and Computer Engineering (IJECE),Vol. 14, No. 04, August, 2024, pp. 4508-4517.

[33] International Journal on “Cross-Platform Malware Classification: Fusion of CNN and GRU Models”,on International Journal of Safety and Security Engineering (IIETA),Vol. 14, No. 02, April, 2024, pp. 477-486

[34] International Journal on “Enhanced Malware Family Classification via Image-Based Analysis Utilizing a Balance-Augmented VGG16 Model,onInternational information and Engineering Technology Association (IIETA),Vol. 40, No. 5, October, 2023, pp. 2169-2178

[35] International Journal on “Android Malware Classification Using LSTM Model, International information and Engineering Technology Association (IIETA) Vol. 36, No. 5, (October, 2022), pp. 761 – 767. Android Malware Classification Using LSTM Model | IIETA.

[36] International Journal on “Classification of Image spam Using Convolution Neural Network”, Traitement du Signal, Vol. 39, No. 1, (February 2022), pp. 363-369 .

[37] International Journal on “Medical Image Classification Using Deep Learning Based Hybrid Model with CNN and Encoder”, International information and Engineering Technology Association (IIETA), Revue d'IntelligenceArtificiellVol. 34, No. 5, (October, 2020), pp. 645 – 652.

[38] International Journal on “Prediction of Hospital Re-admission Using Firefly Based Multi-layer Perception, International information and Engineering Technology Association (IIETA) Vol. 24, No. 4, (sept, 2020), pp. 527 – 533.

[39] International Journal on “Energy efficient intrusion detection using deep reinforcement learning approach”,Journal of Green Engineering (JGE),Volume-11, Issue-1,January 2021.625-641.

[40] International Journal on “Classification of High Dimensional Class Imbalance Data Streams Using Improved Genetic Algorithm Sampling”, International Journal of Advanced Science and Technology, Vol. 29, No. 5, (2020), pp. 5717 – 5726.

[41] Dr. M. Ayyappa Chakravarthi etal. published Springer paper “Machine Learning-Enhanced Self-Management for Energy-Effective and Secure Statistics Assortment in Unattended WSNs” in Springer Nature (Q1), Vol 6, Feb 4th 2025

[42] Dr. M. Ayyappa Chakravarthi etal. published Springer paper “GeoAgriGuard AI-Driven Pest and Disease Management with Remote Sensing for Global Food Security” in Springer Nature (Q1), Jan 20th 2025.

[43] Dr. M. Ayyappa Chakravarthi etal. presented and published IEEE paper “Machine Learning Algorithms for Automated Synthesis of Biocompatible Nanomaterials” , ISBN 979-8-3315-3995-5, Jan 2025.

[44] Dr. M. Ayyappa Chakravarthi etal. presented and published IEEE paper “Evolutionary Algorithms for Deep Learning in Secure Network Environments” ISBN:979-8-3315-3995-5, Jan 2025.

[45] Dr. Ayyappa Chakravarthi M. etal, published Scopus paper “Time Patient Monitoring Through Edge Computing: An IoT-Based Healthcare Architecture” in Frontiers in Health Informatics (FHI), Volume 13, Issue 3, ISSN-Online 2676-7104, 29th Nov 2024.

[46] Dr. Ayyappa Chakravarthi M. etal, published Scopus paper “Amalgamate Approaches Can Aid in the Early Detection of Coronary heart Disease” in Journal of Theoretical and Applied Information Technology (JATIT) , Volume 102, Issue 19, ISSN 1992-8645, 2nd Oct 2024.

[47] Dr. Ayyappa Chakravarthi M, etal, published Scopus paper “The BioShield Algorithm: Pioneering Real-Time Adaptive Security in IoT Networks through Nature-Inspired Machine Learning” in SSRG (Seventh Sense Research Group) -International Journal of Electrical and Electronics Engineering (IJEEE), Volume 11, Issue 9, ISSN 2348-8379, 28th Sept 2024.

[48] Ayyappa Chakravarthi M, Dr M. Thillaikarasi, Dr Bhanu Prakash Battula, published SCI paper “Classification of Image Spam Using Convolution Neural Network” in International Information and Engineering Technology Association (IIETA) - “Traitement du Signal” Volume 39, No. 1

[49] Ayyappa Chakravarthi M, Dr. M. Thillaikarasi, Dr. Bhanu Praksh Battula, published Scopus paper “Classification of Social Media Text Spam Using VAE-CNN and LSTM Model” in International Information and Engineering Technology Association (IIETA) - Ingénierie des Systèmes d’Information (Free Scopus) Volume 25, No. 6.

[50] Ayyappa Chakravarthi M, Dr. M. Thillaikarasi, Dr. Bhanu Praksh Battula, published Scopus paper “Social Media Text Data Classification using Enhanced TF_IDF based Feature Classification using Naive Bayesian Classifier” in International Journal of Advanced Science and Technology (IJAST) 2020

[51] Ayyappa Chakravarthi M. presented and published IEEE paper on “The Etymology of Bigdata on Government Processes” with DOI 10.1109/ICICES.2017.8070712 and is Scopus Indexed online in IEEE digital Xplore with Electronic ISBN: 978-1-5090-6135-8, Print on Demand(PoD) ISBN:978-1-5090-6136-5, Feb’2017.

[52] Subba Reddy Thumu & Geethanjali Nellore, Optimized Ensemble Support Vector Regression Models for Predicting Stock Prices with Multiple Kernels. Acta Informatica Pragensia, 13(1), x–x. 2024.

[53] Subba Reddy Thumu, Prof. N. Geethanjali. (2024). "Improving Cryptocurrency Price Prediction Accuracy with Multi-Kernel Support Vector Regression Approach". International Research Journal of Multidisciplinary Technovation 6 (4):20-31.

[54] Dr syamsundararaothalakola et.al. published Scopus paper "An Innovative Secure and Privacy-Preserving Federated Learning Based Hybrid Deep Learning Model for Intrusion Detection in Internet-Enabled Wireless Sensor Networks " in IEEE Transactions on Consumer Electronics 2024.

[55] Dr syamsundararaothalakola et.al. published Scopus paper "Securing Digital Records: A Synerigistic Approach with IoT and Blockchain for Enhanced Trust and Transparency " in International Journal of Intelligent Systems and Applications in Engineering 2024.

[56] Dr syamsundararaothalakola et.al. published Scopus paper "A Model for Safety Risk Evaluation of Connected Car Network " inReview of Computer Engineering Research2022.

[57] Dr syamsundararaothalakola et.al. published Scopus paper "An Efficient Signal Processing Algorithm for Detecting Abnormalities in EEG Signal Using CNN" in Contrast Media and Molecular Imaging 2022.

[58] Dr. Ayyappa Chakravarthi M. etal, published Scopus paper "Time Patient MonitoringThrough Edge Computing: An IoT-Based Healthcare Architecture" in Frontiers in Health Informatics(FHI), Volume13,Issue3,ISSN-Online 2676-7104, 29th Nov 2024.

[59] Dr. Ayyappa Chakravarthi M. etal, published Scopus paper "Amalgamate Approaches Can Aid in the Early Detection of Coronary heart Disease" in Journal of Theoreticaland Applied Information Technology(JATIT) , Volume 102, Issue 19, ISSN 1992-8645, 2nd Oct 2024.

[60] Dr. Ayyappa Chakravarthi M, etal, published Scopus paper "The BioShield Algorithm: Pioneering Real-Time AdaptiveSecurityin IoTNetworksthrough Nature-Inspired Machine Learning" in SSRG (Seventh Sense Research Group) -International Journal of Electrical and Electronics Engineering(IJEEE),Volume11,Issue9,ISSN2348-8379,28thSept2024.

[61] Ayyappa Chakravarthi M, Dr M. Thillaikarasi, Dr BhanuPrakash Battula,published SCIpaper "Classification of Image Spam Using Convolution Neural Network" in International Information and Engineering Technology Association (IIETA) - "Traitement du Signal" Volume 39, No. 1.

[62] Ayyappa Chakravarthi M, Dr. M. Thillaikarasi, Dr. Bhanu Praksh Battula, published Scopus paper "Classification of Social Media Text Spam Using VAE- CNN and LSTM Model" in International Information and Engineering Technology Association (IIETA) - Ingénierie des Systèmes d'Information (Free Scopus) Volume 25, No. 6.

[63] Ayyappa Chakravarthi M, Dr. M. Thillaikarasi, Dr. Bhanu Praksh Battula, published Scopus paper "Social Media Text Data Classification using Enhanced TF_IDF based Feature Classification using Naive Bayesian Classifier"in International Journal of Advanced Science and Technology (IJAST) 2020.

[64] Ayyappa Chakravarthi M. presented and published IEEEpaper on "TheEtymologyofBigdata on Government Processes"with DOI 10.1109/ICICES.2017.8070712andis Scopus Indexed online in IEEE digital Xplore with Electronic ISBN: 978-1-5090-6135-8, Print on Demand(PoD) ISBN:978-1-5090-6136-5, Feb'2017.

[65] Subba Reddy Thumu & Geethanjali Nellore, Optimized Ensemble Support Vector Regression Modelsfor Predicting Stock Prices with Multiple Kernels. Acta Informatica Pragensia, 13(1), x–x. 2024.

[66] Subba Reddy Thumu, Prof.N. Geethanjali (2024). "ImprovingCryptocurrencyPricePredictionAccuracywith Multi-Kernel Support Vector Regression Approach". InternationalResearchJournalofMultidisciplinary Technovation 6 (4):20-31.

[67] Dr syamsundararaothalakolaet.al. published Scopus paper "An Innovative Secure and Privacy-Preserving FederatedLearningBasedHybridDeepLearningModelfor Intrusion Detection in Internet-Enabled Wireless Sensor Networks "in IEEE Transactions on ConsumerElectronics 2024.

[68] Dr syamsundararaothalakolaet.al. published Scopus paper "Securing Digital Records: A Synerigistic Approach with IoT and Blockchain for Enhanced Trust and Transparency "in International Journal of Intelligent Systems and Applications in Engineering 2024.

[69] Dr syamsundararaothalakolaet.al. published Scopus paper "A Model for Safety Risk Evaluation of Connected Car Network "inReview of Computer Engineering Research2022.