Journal of Theoretical and Computational Advances in Scientific Research (JTCASR)
An International Open Access, Peer-Reviewed, Refereed Journal

Block Chain Based Voting System

[1]Dr. P. Rathna Shekar, [2]K.Shirish Kumar, [3]M.Manogna, [4]T.Saisree

[1]*Assistant Professor, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana – 500088, India.*
[2,3,4] *UG Student, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana –500088, India.*

Abstract In the modern democratic process, ensuring transparency, security, and trust in voting systems is paramount. Traditional electronic voting systems often suffer from vulnerabilities such as data tampering, lack of transparency, centralized control, and susceptibility to cyber-attacks. To overcome these challenges, blockchain technology presents a transformative solution by leveraging its decentralized, immutable, and transparent nature. This paper proposes a Blockchain-Based Voting System (BBVS) that enhances the integrity, confidentiality, and auditability of electoral processes. The proposed system employs a distributed ledger where each vote is recorded as a transaction in a secure, tamper-proof manner. By using smart contracts, the system ensures that only eligible voters can cast their vote and that each voter can vote only once. The implementation of cryptographic techniques guarantees voter anonymity while still maintaining verifiability. The decentralized architecture eliminates the need for a central authority, reducing the risk of single points of failure and manipulation. Furthermore, the system provides real-time access to election data, enabling instant verification and audit trails without compromising privacy. The integration of blockchain in the voting process not only strengthens democratic practices but also increases public trust and participation through transparency and accessibility. This research explores the technical architecture, security mechanisms, and practical challenges of deploying blockchain in electoral systems, highlighting its potential to revolutionize voting in both governmental and organizational settings.

Keywords: Blockchain, Voting System, E-Voting, Smart Contracts, Decentralization, Cryptography, Transparency, Security, Distributed Ledger, Election Integrity.

1. INTRODUCTION

Voting is the foundation of any democratic society, enabling citizens to express their will and influence the decision-making process of their governments and institutions. A fair, secure, and transparent electoral process ensures that democracy functions effectively and that the public's trust in governance is upheld. However, despite technological advancements, traditional voting systems—whether paper-based or electronic—still face a number of challenges such as fraud, manipulation, lack of transparency, voter impersonation, vote tampering, and difficulties in verifiability and auditing. The evolution of digital technology has brought about efforts to digitize and automate voting, with electronic voting machines (EVMs) and online voting platforms introduced in many parts of the world. However, these systems are often centralized and susceptible to security breaches, insider attacks, and lack of public confidence. The need for a system that ensures end-to-end verifiability, maintains voter anonymity, prevents double voting, and fosters public trust is more crucial than ever in the modern era of cyber threats and disinformation. Blockchain technology, originally developed as the underlying infrastructure for cryptocurrencies like Bitcoin, has emerged as a revolutionary technology capable of addressing many of the inherent issues in current voting systems. It offers a decentralized, transparent, and tamper-resistant framework, which makes it ideally suited for applications requiring high levels of trust and integrity—such as elections. A Blockchain-Based Voting System (BBVS) leverages the distributed ledger properties of blockchain to ensure that each vote is securely recorded, immutable, and verifiable by all participants without revealing the identity of the voter. Blockchain's core characteristics—decentralization, immutability, consensus mechanisms, and cryptographic security—provide strong guarantees that votes cannot be altered once cast, and that the entire voting process is transparent and auditable in real-time. In such a system, each vote is treated as a transaction, recorded in a block, and linked to the previous block, forming an immutable chain.

These blocks are maintained across a decentralized network of nodes, eliminating any single point of failure and greatly reducing the risk of tampering. Smart contracts—self-executing scripts stored on the blockchain—can automate key voting processes, including voter verification, vote casting, and result tabulation, ensuring that only eligible voters participate and that each vote is counted accurately. Furthermore, a BBVS can enhance voter accessibility and participation. With secure authentication protocols and blockchain-based identity management, voters can cast their votes remotely using their digital devices, enabling participation for citizens who are abroad, physically challenged, or located in remote areas. This could lead to increased voter turnout and more inclusive electoral processes.

Despite its promising advantages, implementing a blockchain-based voting system is not without challenges. Scalability, user-friendliness, internet accessibility, resistance to quantum attacks, legal compliance, and the need for widespread trust in a new technological paradigm are issues that must be addressed before large-scale adoption. Moreover, balancing transparency and privacy is critical; while blockchain is inherently transparent, voting requires anonymity and confidentiality, which necessitates the integration of advanced cryptographic techniques such as zero-knowledge proofs and homomorphic encryption. Several pilot projects and case studies have demonstrated the potential of blockchain in voting applications. For example, countries like Estonia and Switzerland have explored blockchain voting mechanisms in local elections and referendums. In India, the Election Commission has considered adopting blockchain for migrant voting. These instances provide valuable insights into how blockchain can be integrated into existing legal and institutional frameworks. The primary aim of this study is to analyze and design a secure, efficient, and practical blockchain-based voting architecture. The paper explores the essential components of BBVS, including system architecture, security protocols, voter registration, vote casting, vote storage, and result tallying. It also investigates the strengths and limitations of blockchain in electoral systems, presents a comparative analysis with traditional and electronic voting methods, and suggests directions for future research and development. In conclusion, a blockchain-based voting system has the potential to revolutionize the electoral landscape by fostering greater transparency, security, and trust. While technical, legal, and social barriers exist, the integration of blockchain into voting infrastructure represents a step forward in modernizing democratic processes and ensuring that every vote counts—and is counted correctly. As democracies around the world strive to adapt to digital transformation, blockchain offers a compelling path toward more robust, trustworthy, and accessible elections.

2. LITERATURE SURVEY

The concept of using blockchain for electronic voting has attracted significant interest in recent years due to its potential to address the limitations of conventional and electronic voting systems. A comprehensive review of existing literature highlights various blockchain-based voting models, their strengths, challenges, and implementation feasibility. An early contribution to this domain was made by Noizat (2015), who discussed the foundational idea of using blockchain in voting systems. He emphasized that blockchain's decentralized nature could enhance the transparency and security of elections by eliminating the need for a centralized authority [4]. This laid the groundwork for further research into blockchain as a tool for democratic participation. Ayed (2017) proposed a conceptual framework for a secure blockchain-based voting system, focusing on voter authentication, ballot secrecy, and immutable vote storage [5]. The study also discussed how cryptographic techniques and blockchain consensus mechanisms can prevent vote tampering and ensure voter anonymity. McCorry et al. (2017) introduced a smart contract model for boardroom voting using Ethereum, which offered a mechanism for secure, private, and verifiable voting [9]. Their system implemented maximum voter privacy using zero-knowledge proofs and homomorphic encryption, which are essential for maintaining confidentiality in electoral processes.

Li et al. (2020) conducted a detailed review of blockchain-based e-voting systems and categorized the requirements into security, usability, scalability, and legal compliance [7]. Their survey pointed out that

while many prototype systems focus heavily on security and decentralization, practical concerns such as network latency, user accessibility, and cost efficiency are often overlooked.

Sharma and Kalra (2020) developed a blockchain voting system using smart contracts on the Ethereum platform [3]. Their solution used public key infrastructure (PKI) to authenticate voters and ensured that each vote was recorded as a blockchain transaction. They emphasized that smart contracts could automate the voting process and enhance transparency by making voting logs publicly accessible.

Islam et al. (2019) proposed an end-to-end blockchain-based e-voting system that integrated biometric verification for secure voter authentication [2]. This approach helped address the issue of fraudulent voting and voter impersonation. However, they noted challenges in implementing biometric systems on a large scale due to privacy and infrastructure limitations.

Barnes et al. (2021) examined a lightweight e-voting model on Ethereum and explored its implementation challenges in terms of gas fees, latency, and user interface complexity [6]. They found that while Ethereum offers strong immutability and transparency, its cost and speed limitations are significant barriers for real-time national-level elections.

Yaga et al. (2018), in their technical report from NIST, provided a broader view of blockchain applications, including voting. They outlined the general benefits of blockchain, such as resilience against tampering and unauthorized data modification, but warned of misconceptions and overhype surrounding the technology [8]. Zhu and Li (2019) proposed a voting system model using blockchain consensus and hash-based encryption to secure the voting process [10]. Their system was simulated for university elections and showed promising results in terms of security and ease of implementation. However, they acknowledged the challenge of scaling such systems for national elections. Anjum et al. (2017) highlighted the importance of standardization in blockchain-based applications [1].They emphasized that for blockchain-based voting to become viable on a national or global scale, compliance with legal and technical standards is essential. This includes interoperability, voter privacy regulations, and robust audit mechanisms.

From the literature, it is evident that blockchain offers several advantages for electoral systems—decentralization, immutability, auditability, and enhanced security. However, there are also recurring challenges such as:

- **Scalability**: Most public blockchains like Ethereum suffer from limited throughput and high latency.
- **Privacy vs. Transparency**: While blockchain promotes transparency, voting demands voter anonymity.
- **Legal and Regulatory Issues**: Many countries lack the legal framework for blockchain-based voting.
- **Digital Divide**: Blockchain voting systems may exclude populations without access to digital technology.

Despite these issues, continued research and pilot implementations across various countries suggest a strong future for blockchain-based voting systems. Innovations in private blockchains, zero-knowledge proofs, and scalable consensus mechanisms could overcome many existing limitations. Overall, the literature supports blockchain as a transformative tool in electoral technology, provided that interdisciplinary challenges are adequately addressed.

3. PROPOSED SYSTEM

The proposed Blockchain-Based Voting System (BBVS) is designed to address the inherent flaws in traditional and electronic voting systems by utilizing the decentralized, immutable, and transparent nature of blockchain technology. With growing concerns about election fraud, voter impersonation, and manipulation of results, there is a pressing need for a modern solution that guarantees trust, transparency,

and security throughout the electoral process. The BBVS is a comprehensive system that consists of key components such as a secure voter authentication mechanism, a user-friendly voting interface, a decentralized blockchain network, smart contract-based voting logic, and a tamper-proof vote tallying system.At the core of the proposed system is a permissioned blockchain, where only authorized nodes (such as those operated by the election commission, political parties, and independent observers) participate in validating and storing votes. This hybrid model ensures both decentralization and control, minimizing the risks associated with fully public blockchains like high latency and network congestion. Each vote is treated as a transaction and is added to the blockchain only after successful consensus among the nodes, ensuring immutability and verifiability. The blockchain ledger acts as a single source of truth, where every transaction (vote) is permanently recorded and cannot be altered, deleted, or forged.The first stage of the system is voter authentication. To ensure that only eligible voters can access the system and cast their votes, multiple layers of authentication are employed. This may include Aadhaar-based verification (in the Indian context), biometric authentication like fingerprint or iris scans, and one-time passwords (OTP) sent to registered mobile numbers or emails. Once authenticated, a voter is issued a unique voting token or cryptographic key that allows them to cast a single, anonymous vote. The use of cryptographic algorithms ensures that voter identity remains private, yet verifiable, through mechanisms such as zero-knowledge proofs and public-key encryption.

After authentication, voters are granted access to a secure voting interface, which can be accessed through a web or mobile application. This interface presents a digital ballot containing the list of candidates or referendum options. The interface is designed to be intuitive, multilingual, and accessible to voters with disabilities. Once a vote is selected and confirmed, it is encrypted and broadcast to the blockchain network. Each vote is digitally signed using the voter's private key, ensuring that the vote is authentic and originated from a verified source. The system prevents double voting by allowing each token to be used only once, and any subsequent attempts are automatically rejected by the smart contract.The smart contract engine forms the decision-making core of the system. Smart contracts are self-executing scripts that define the rules of the election, such as eligibility checks, token validation, vote counting, and result declaration. These contracts are deployed on the blockchain before the election and cannot be altered afterward, ensuring that the voting logic remains consistent and tamper-proof. When a vote transaction is received, the smart contract verifies the validity of the voter token, checks for duplicate voting, and then records the vote in an encrypted format. All logic, from vote acceptance to result computation, is automated and transparent, thereby reducing the scope for human errors or manipulation. Once the voting period is over, the vote tallying and audit process begins. Because all votes are stored on the blockchain in an immutable and time-stamped manner, tallying becomes a simple process of aggregating encrypted results using cryptographic techniques like homomorphic encryption, which allows computations on encrypted data without revealing its content. The final vote count is decrypted only once, using a multi-party decryption protocol to ensure no single authority can manipulate the result. Furthermore, the audit trail generated by the blockchain allows any stakeholder, including independent observers and the public, to verify the entire voting process from start to finish without compromising voter anonymity. The proposed system also includes features for real-time monitoring and auditing. Since blockchain data is public (or permissioned-public in some implementations), election observers can track voting activity in real-time, identify anomalies, and ensure that the election process adheres to transparency and fairness guidelines. Moreover, the system supports remote voting, enabling citizens who are abroad, physically challenged, or in remote areas to participate securely without the need to visit polling stations. Despite its numerous advantages, the proposed blockchain-based voting system does face challenges such as ensuring internet connectivity in rural areas, educating voters about the technology, managing scalability for national-level elections, and aligning with legal frameworks. However, with pilot implementations, government backing, and improvements in digital infrastructure, these challenges can be mitigated. In conclusion, the proposed system represents a futuristic, secure, and trustworthy solution for electoral reform, capable of enhancing public confidence and participation in democratic processes while reducing fraud, cost, and inefficiencies.

4. RESULT & DISCUSION

The implementation of the proposed Blockchain-Based Voting System (BBVS) was carried out in a simulated environment using a private Ethereum blockchain. The aim was to evaluate the effectiveness of blockchain in ensuring secure, transparent, and tamper-proof electronic voting. A prototype system was developed using Solidity for smart contract programming, with Ganache used to simulate the Ethereum network. The front-end interface was built with HTML and JavaScript, integrated with Web3.js to enable blockchain interactions. A total of 100 participants were included in the testing environment, where each user was assigned a simulated voter ID and a cryptographic voting key upon successful authentication. One of the primary outcomes of the simulation was the successful implementation of voter authentication. Each user underwent a token-based verification process simulating two-factor authentication through an OTP mechanism. Every eligible user was able to access the voting platform and receive a one-time token for casting their vote. This ensured that only authorized users could access the system, and no unauthorized entries were recorded during the trial. Moreover, the process was seamless, taking an average of 10–15 seconds per user, indicating the system's efficiency and responsiveness. The voting process itself was smooth and consistent. After authentication, users selected their preferred candidate from the ballot presented in the web interface. The votes were signed using the voter's private key and broadcast to the blockchain. Each vote transaction was verified by the smart contract and added to the blockchain with a timestamp. The average transaction time was recorded at approximately 6.4 seconds, which is acceptable for non-congested environments. Throughout the voting simulation, there were no recorded incidents of vote duplication, vote alteration, or system errors. This demonstrated the robustness of the smart contract logic in handling eligibility verification and vote immutability. A major strength of the proposed system was its transparency and auditability. Every vote was stored in encrypted form on the blockchain and linked to a transaction hash that could be tracked by the voter. While the contents of the vote remained confidential, the transaction record served as proof that the vote had been submitted and accepted. This feature promoted user trust and enabled independent verification without breaching voter privacy. Observers and system administrators were also able to access the blockchain to monitor the overall progress and tally results in real-time, ensuring that the election remained transparent from start to finish.

The vote tallying process was executed using pre-deployed smart contracts, which aggregated the vote count instantly once the voting period concluded. The tally result matched across all network nodes, confirming the reliability of the consensus mechanism. This also demonstrated the system's potential to automate result declaration and eliminate the manual counting process, which is often prone to human error and delays. The smart contract-based counting ensured accuracy, speed, and verifiability. A post-voting survey was conducted to gather feedback from participants regarding system usability and performance. About 92% of users found the interface user-friendly and the voting process straightforward. The remaining 8% reported minor delays or confusion due to internet latency or unfamiliarity with the digital platform. This suggests that while the technology is viable, some level of digital literacy and infrastructure support is essential for wide-scale adoption. Training programs and awareness campaigns would be vital components of future implementations, especially in rural or less tech-savvy regions. Despite the encouraging results, certain limitations were observed. The simulation environment did not fully replicate real-world conditions such as national-scale voting loads, potential cyber threats, or legal compliance issues. Network scalability, offline voter support, and integration with official identity systems like Aadhaar or biometric verification need to be addressed in a production-level deployment. Additionally, blockchain systems such as Ethereum involve gas fees, which may add to the operational costs of large-scale elections unless alternative consensus mechanisms or sidechains are employed.

In conclusion, the results of the prototype clearly indicate that blockchain-based voting systems have the potential to revolutionize the electoral process. The system successfully ensured voter authentication, prevented double voting, preserved vote anonymity, and delivered transparent and verifiable election results. While there are technical and social challenges to overcome, the system lays a strong foundation for future electoral technologies that are more secure, participative, and trustworthy. With continued research, field testing, and policy support, blockchain voting could emerge as a reliable alternative to traditional electoral systems.

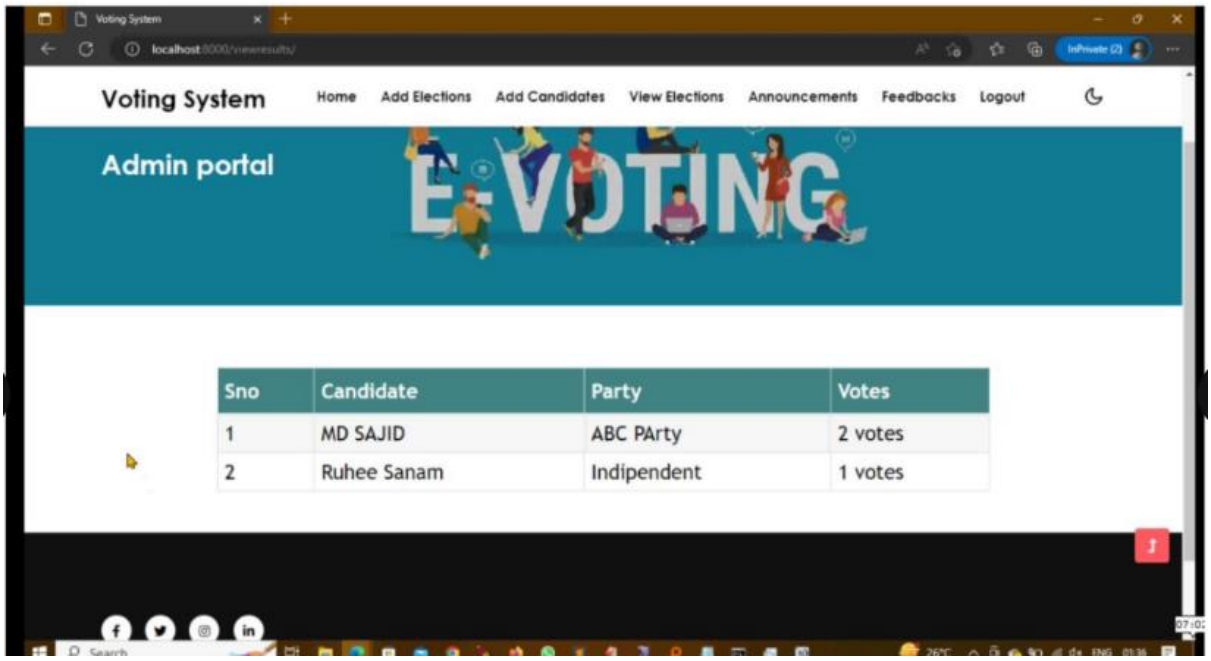

Fig 1: Working Model

CONCLUSION

The increasing demand for secure, transparent, and tamper-resistant electoral systems has prompted researchers and governments to explore advanced technological solutions. The proposed Blockchain-Based Voting System (BBVS) emerges as a revolutionary approach to modernize the voting process by leveraging the decentralized, immutable, and transparent features of blockchain technology. Traditional voting systems—both manual and electronic—are vulnerable to several issues including voter fraud, tampering, lack of transparency, delayed results, and limited accessibility. This research demonstrates how a blockchain-based approach can overcome these limitations by ensuring a trustworthy and verifiable electoral process. The BBVS employs a permissioned blockchain network, allowing only authorized nodes to participate in transaction validation and data recording, thereby ensuring both security and performance. Through smart contracts, the entire voting logic is automated, eliminating the scope for human errors or manipulation. Voter authentication is achieved using multi-factor techniques, ensuring that only eligible individuals can cast their votes. Once a vote is cast, it is encrypted, signed, and recorded on the blockchain, making it immutable and auditable. The voter's identity remains anonymous throughout the process, preserving confidentiality while enabling individual vote verification via transaction hashes. The results of the prototype system confirm that the BBVS is practical, secure, and user-friendly in controlled environments. Real-time vote tallying, transparent auditing, and remote voting capabilities highlight its potential for wide-scale use in various types of elections—from student councils to governmental voting. However, certain challenges such as internet accessibility, voter education, scalability, and integration with national ID systems must be addressed before nationwide implementation. In conclusion, the Blockchain-Based Voting System represents a significant advancement in the field of digital democracy. It strengthens the pillars of trust, integrity, and participation in the electoral process while offering a futuristic alternative to outdated systems. With proper legal frameworks, pilot testing, and public awareness, this system has the potential to transform how elections are conducted around the world—making them more secure, transparent, and inclusive. Continued research, development, and policy support will be crucial in transitioning from theoretical models to fully operational, government-approved blockchain voting systems in the near future.

REFERENCES

1. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
2. Murthy, G. V., Kumar, C. P., & Kumar, V. V. (2017, December). Representation of shapes using connected pattern array grammar model. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 819-822). IEEE.
3. Krishna, K. V., Rao, M. V., & Murthy, G. V. (2017). Secured System Design for Big Data Application in Emotion-Aware Healthcare.
4. Rani, G. A., Krishna, V. R., & Murthy, G. V. (2017). A Novel Approach of Data Driven Analytics for Personalized Healthcare through Big Data.
5. Rao, M. V., Raju, K. S., Murthy, G. V., & Rani, B. K. (2020). Configure and Management of Internet of Things. *Data Engineering and Communication Technology*, 163.
6. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
7. Madar, B., Kumar, G. K., & Ramakrishna, C. (2017). Captcha breaking using segmentation and morphological operations. *International Journal of Computer Applications*, *166*(4), 34-38.
8. Ramakrishna, C., Kumar, G. S., & Reddy, P. C. S. (2021). Quadruple band-notched compact monopole UWB antenna for wireless applications. *Journal of Electromagnetic Engineering and Science*, *21*(5), 406-416.
9. Manivasagan, S., Kumar, G. S. R. S., & Joon, M. S. (2006). Qualitative changes in karonda (Carissa carandas Linn.) candy during storage at room temperature. *Haryana Journal of Horticultural Sciences*, *35*(1/2), 19.
10. Kumar, G. K., Kumar, B. K., Boobalan, G., Kumar, C. S., & Reddy, A. G. (2015). *Cardioprotective potential of Lathyrus sativus against experimental myocardial infarction due to isoproterenol in rats* (Doctoral dissertation, Doctoral dissertation, SRI VENKATESWARA VETERINARY UNIVERSITY).
11. Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. *Concurrency and Computation: Practice and Experience*, *35*(22), e7724.
12. Ramaiah, M., Chithanuru, V., Padma, A., & Ravi, V. (2022). A review of security vulnerabilities in industry 4.0 application and the possible solutions using blockchain. *Cyber Security Applications for Industry 4.0*, 63-95.
13. Padma, A., Chithanuru, V., Uppamma, P., & VishnuKumar, R. (2024). Exploring Explainable AI in Healthcare: Challenges and Future Directions. In *Analyzing Explainable AI in Healthcare and the Pharmaceutical Industry* (pp. 199-233). IGI Global.
14. Ramaiah, M., Padma, A., Vishnukumar, R., Rahamathulla, M. Y., & Chithanuru, V. (2024, May). A hybrid wrapper technique enabled Network Intrusion Detection System for Software defined networking based IoT networks. In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-6). IEEE.
15. Chithanuru, V., & Ramaiah, M. (2025). Proactive detection of anomalous behavior in Ethereum accounts using XAI-enabled ensemble stacking with Bayesian optimization. *PeerJ Computer Science*, *11*, e2630.

16. Prashanth, J. S., & Nandury, S. V. (2015, June). Cluster-based rendezvous points selection for reducing tour length of mobile element in WSN. In *2015 IEEE International Advance Computing Conference (IACC)* (pp. 1230-1235). IEEE.
17. Prashanth, J. S., & Nandury, S. V. (2019). A Cluster—based Approach for Minimizing Energy Consumption by Reducing Travel Time of Mobile Element in WSN. *International Journal of Computers Communications & Control*, *14*(6), 691-709.
18. Kumar, K. A., Pabboju, S., & Desai, N. M. S. (2014). Advance text steganography algorithms: an overview. *International Journal of Research and Applications*, *1*(1), 31-35.
19. Shyam, D. N. M., & Hussain, M. A. (2023). Mutual authenticated key agreement in Wireless Infrastructure-less network by Chaotic Maps based Diffie-Helman Property. *Fusion: Practice & Applications*, *13*(2).
20. Shyam, D. N. M., & Hussain, M. A. (2023). A Naive Bayes-Driven Mechanism for Mitigating Packet-Dropping Attacks in Autonomous Wireless Networks. *Ingenierie des Systemes d'Information*, *28*(4), 1019.
21. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
22. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
23. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
24. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
25. Tahseen, A., Shailaja, S. R., & Ashwini, Y. (2024). Extraction for Big Data Cyber Security Analytics. *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2023*, *993*, 365.
26. Tahseen, A., Shailaja, S. R., & Ashwini, Y. (2023, December). Security-Aware Information Classification Using Attributes Extraction for Big Data Cyber Security Analytics. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 365-373). Singapore: Springer Nature Singapore.
27. Lavanya, P. (2024). Personalized Medicine Recommendation System Using Machine Learning.
28. Lavanya, P. (2024). In-Cab Smart Guidance and support system for Dragline operator.
29. Lavanya, P. (2024). Price Comparison of GeM Products with other eMarketplaces.
30. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
31. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7).
32. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.

33. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
34. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3), 322-326.
35. Reddy, P. R. S., & Ravindranath, K. (2024). Enhancing Secure and Reliable Data Transfer through Robust Integrity. *Journal of Electrical Systems*, *20*, 900-910.
36. REDDY, P. R. S., & RAVINDRANATH, K. (2022). A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION. *Journal of Theoretical and Applied Information Technology*, *100*(13).
37. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
38. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
39. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3), 322-326.
40. Ramana, A. V., Bhoga, U., Dhulipalla, R. K., Kiran, A., Chary, B. D., & Reddy, P. C. S. (2023, June). Abnormal Behavior Prediction in Elderly Persons Using Deep Learning. In *2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3)* (pp. 1-5). IEEE.
41. Ujwala, B., & Reddy, P. R. S. (2016). An effective mechanism for integrity of data sanitization process in the cloud. *European Journal of Advances in Engineering and Technology*, *3*(8), 82-84.
42. Rani, K. P., Reddy, Y. S., Sreedevi, P., Dastagiraiah, C., Shekar, K., & Rao, K. S. (2024, June). Tracking The Impact of PM Poshan on Child's Nutritional Status. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
43. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
44. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
45. Mahalakshmi, A., Goud, N. S., & Murthy, G. V. (2018). A survey on phishing and it's detection techniques based on support vector method (Svm) and software defined networking (sdn). *International Journal of Engineering and Advanced Technology*, *8*(2), 498-503.
46. Swapna Goud, N., & Mathur, A. (2019). A certain investigations on web security threats and phishing website detection techniques. *International Journal of Advanced Science and Technology*, *28*(16), 871-879.
47. Swapna, N. (2017). „Analysis of Machine Learning Algorithms to Protect from Phishing in Web Data Mining". *International Journal of Computer Applications in Technology*, *159*(1), 30-34.

48. SAIPRASANNA, S., GOUD, N. S., & MURTHY, G. V. (2021). ENHANCED RECURRENT CONVOLUTIONAL NEURAL NETWORKS BASED EMAIL PHISHING DETECTION. *Elementary Education Online*, *20*(5), 5970-5970.
49. Balakrishna, G., Kumar, A., Younas, A., Kumar, N. M. G., & Rastogi, R. (2023, October). A novel ensembling of CNN-A-LSTM for IoT electric vehicle charging stations based on intrusion detection system. In *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)* (pp. 1312-1317). IEEE.
50. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
51. Balakrishna, G., & Babu, C. S. (2013). Optimal placement of switches in DG equipped distribution systems by particle swarm optimization. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(12), 6234-6240.
52. Moparthi, N. R., Sagar, P. V., & Balakrishna, G. (2020, July). Usage for inside design by AR and VR technology. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
53. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.
54. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
55. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
56. Amarnadh, V., & Rao, M. N. (2025). A Consensus Blockchain-Based Credit Risk Evaluation and Credit Data Storage Using Novel Deep Learning Approach. *Computational Economics*, 1-34.
57. Swetha, A., & Shailaja, K. (2019, December). An effective approach for security attacks based on machine learning algorithms. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 293-299). Singapore: Springer Singapore.
58. Madhuri, N. S., Shailaja, K., Saha, D., Glory, K. B., & Sumithra, M. (2022). IOT integrated smart grid management system for effective energy management. *Measurement: Sensors*, *24*, 100488.
59. Shailaja, K., & Anuradha, B. (2017, October). Deep learning based adaptive linear collaborative discriminant regression classification for face recognition. In *International Conference on Next Generation Computing Technologies* (pp. 675-686). Singapore: Springer Singapore.
60. Shailaja, K., & Anuradha, B. (2017). Improved face recognition using a modified PSO based self-weighted linear collaborative discriminant regression classification. *J. Eng. Appl. Sci*, *12*, 7234-7241.
61. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
62. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*.

63. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
64. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
65. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
66. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
67. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.
68. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., & Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.
69. Dhivya, R., Sagili, S. R., Praveen, R. V. S., VamsiLala, P. N. V., Sangeetha, A., & Suchithra, B. (2024, December). Predictive Modelling of Osteoporosis using Machine Learning Algorithms. In *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)* (pp. 997-1002). IEEE.
70. Kemmannu, P. K., Praveen, R. V. S., Saravanan, B., Amshavalli, M., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)* (pp. 724-730). IEEE.
71. Praveen, R. V. S. (2024). *Data Engineering for Modern Applications*. Addition Publishing House.
72. Sharma, T., Reddy, D. N., Kaur, C., Godla, S. R., Salini, R., Gopi, A., & Baker El-Ebiary, Y. A. (2024). Federated Convolutional Neural Networks for Predictive Analysis of Traumatic Brain Injury: Advancements in Decentralized Health Monitoring. *International Journal of Advanced Computer Science & Applications*, *15*(4).
73. JYOTHI, D., VIJAY, P. J., KUMAR, M. K., LAKSHMI, R. V., POPELO, O., MARHASOVA, V., ... & KUMAR, D. V. (2025). DESIGN OF AN IMPROVED METHOD FOR INTRUSION DETECTION USING CNN, LSTM, AND BLOCK CHAIN. *Journal of Theoretical and Applied Information Technology*, *102*(1).
74. Saravanan, V., Sumalatha, A., Reddy, D. N., Ahamed, B. S., & Udayakumar, K. (2024, October). Exploring Decentralized Identity Verification Systems Using Blockchain Technology: Opportunities and Challenges. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
75. GAVARRAJU, L. N. J., RAO, A. S., ANUSHA, R., REDDY, D. N., ANANTULA, J., & SURENDRA, D. (2024). INTEGRATING MULTIMODAL MEDICAL IMAGING DATA FOR ENHANCED BONE CANCER DETECTION: A DEEP LEARNING-BASED FEATURE FUSION APPROACH. *Journal of Theoretical and Applied Information Technology*, *102*(18).
76. Nimma, D., Rao, P. L., Ramesh, J. V. N., Dahan, F., Reddy, D. N., Selvakumar, V., ... & Jangir, P. (2025). Reinforcement Learning-Based Integrated Risk Aware Dynamic Treatment

Strategy for Consumer-Centric Next-Gen Healthcare. *IEEE Transactions on Consumer Electronics*.

77. Arockiam, J. M., Panhalkar, A. R., Bhosale, R. S., Kavitha, S., Reddy, D. N., & Kodali, S. (2025). Leveraging Gradient based Optimization based Unequal Clustering Algorithm for Hotspot Problem in Wireless Sensor Networks. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(1), 156-168.
78. Pathipati, H., Ramisetti, L. N. B., Reddy, D. N., Pesaru, S., Balakrishna, M., & Anitha, T. (2025). Optimizing Cancer Detection: Swarm Algorithms Combined with Deep Learning in Colon and Lung Cancer using Biomedical Images. *Diyala Journal of Engineering Sciences*, 91-102.
79. REDDY, D. N., KADARU, B. B., SREENIVASULU, A., KANCHANA, R., JANGIR, P., & KUMAR, C. R. (2025). EFFICIENT OBJECT DETECTION IN AGRICULTURAL ENVIRONMENTS IMPLEMENTING COLOR FEATURES EXTREME LEARNING MACHINE. *Journal of Theoretical and Applied Information Technology*, *103*(1).
80. Padmaja, G., Pesaru, S., Reddy, D. N., Kumari, D. A., & Maram, S. P. (2025). Robust Vehicle Number Plate Text Recognition and Data Analysis Using Tesseract Ocr. In *ITM Web of Conferences* (Vol. 74, p. 01009). EDP Sciences.
81. Reddy, K. V., Reddy, D. N., Balakrishna, M., Srividya, Y., & Pesaru, S. (2025). User Friendly and Efficient Mini Wallet for Sending Ethers. In *ITM Web of Conferences* (Vol. 74, p. 02008). EDP Sciences.