Anusandhanvallari
Vol 2025, No.1
January 2025
ISSN 2229-3388

A Review on Fraud Detection Techniques in Iot-Enabled Voting Systems

Shambhavi Holay [1]

Research Scholar

Dr. Diwakar Ramanuj Tripathi [2]

Research Supervisor

1,2 Department of Electronics and Computer Science

Rashtrasant Tukdoji Maharaj,Nagpur University,

Nagpur

Abstract: The integration of Internet of Things (IoT) in the electronic voting systems has improved the efficiency, accessibility of the electoral process and transparency of the voting process to a large extent but it has also come with its own security vulnerabilities and risks associated with fraudulent activities. IoT-enabled voting systems rely on interconnected devices, wireless-based communication, and real-time data transfer, which increase the attack surface and expose the system to various risks, including voter impersonation, vote manipulation, replay attacks, denial-of-service attacks, insider fraud, etc. This review paper presents a comprehensive discussion of fraud detection methods used in the IoT-enabled voting systems. It critically analyzes the cryptographic and blockchain-based security solutions, fraud detection models that can utilize machine learning, and hybrid systems that can combine various methods. The research paper provides the advantages and disadvantages of both methods based on their strength in security, scalability, cost of computation, and detection ability. Comparison of the results in tables and graphical representations shows that hybrid fraud detection architectures provide better robustness and detection rates as they are a composite of secure communication, data integrity and smart anomaly detection. Such challenges as scalability, preserving privacy or resource constraints are also highlighted in the review and give the insights on the possible direction of future research about the creation of secure and trustworthy IoT-based voting infrastructures.

Keywords: IoT-Enabled Voting Systems, Fraud Detection, Electronic Voting, Machine Learning, Blockchain Technology, Hybrid Security Frameworks.

1. INTRODUCTION

The democratic systems rely on elections, and the security and reliability of voting systems is the national concern. Although most commonly used, traditional and paper-based system of voting have known inefficiencies, they are expensive to operate and logistical problems. To eliminate these shortcomings, electronic voting systems were adopted to provide a quicker method of casting and counting votes. The Internet of Things (IoT) technologies have recently been integrated again to change the electronic voting process by introducing smart voting machines, biometric authentication hardware, interlinked sensors, and real-time data exchange.

IoT voting systems should help increase voter access, improve transparency, and decrease human involvement. In spite of these benefits, the use of IoT integration increases greatly the attack surface because of the heterogeneity of the devices, wireless channels of communication, and cloud infrastructure dependency. Such weaknesses make voting systems susceptible to advanced fraud and cyber-attacks, such as vote manipulation, identity spoofing, unauthorized access, and system malfunction.

Voting systems based on IoT have become an important part of secure voting systems therefore, fraud detection is now a critical component of secure IoT-based voting systems. Researchers have suggested diverse approaches

including the conventional cryptographic protection to sophisticated data orientation models like machine learning and blockchain-based verification system. The review paper is a critical analysis of these techniques, and the comparison of their effectiveness and their suitability to real world electoral environment.

This study differs from the current literature, which mainly concentrates on the performance of individual security methods. The study compares cryptographic, blockchain, machine learning, and hybrid methods of fraud detection in IoT-supported voting processes. It identifies the merits and demerits of each security method as well as the challenges related to the scalability and privacy of the proposed security measures.

2. REVIEW METHODOLOGY

The structured literature review technique was used in this review to evaluate fraud detection mechanisms for IoT-based voting systems. The selected scholarly works related to this topic were retrieved from various electronic databases, such as IEEE Xplore, Scopus, SpringerLink, ScienceDirect, and Web of Science, using terms like "IoT-enabled voting systems," "electronic voting security," "blockchain voting," "machine learning for voting security," and "IoT cybersecurity."

The review focused on studies that have been conducted from the years 2020 to 2025. Studies that are related to cryptographic techniques, blockchain architecture, machine learning algorithms, and hybrid security system were selected, whereas those studies which are redundant and not relevant were omitted.

This review adopted the PRISMA approach for the study identification, screening, eligibility, and selection process.

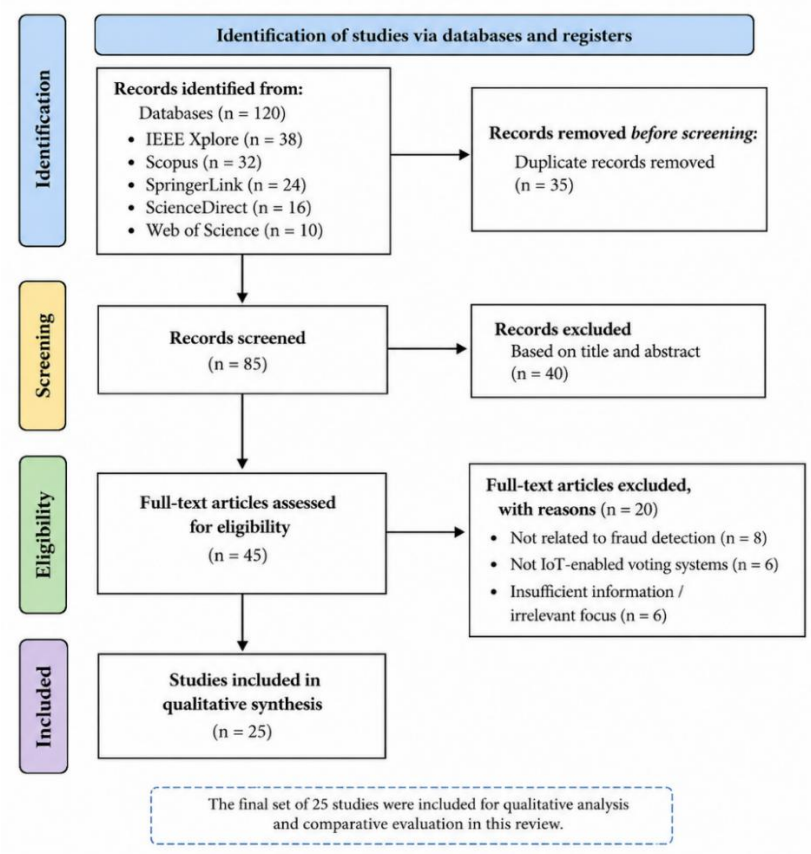

Figure 1: PRISMA Flow Diagram for Literature Selection

3. LITERATURE REVIEW

Abubakar et al. (2024) reviewed how Artificial Intelligence of Things (AIoT) can be applied to improve the process of electronic voting, particularly focusing on departmental association elections in Covenant University. Their article showed that e-voting systems that use AIoT led to increased transparency and efficiency and increased voter turnout and met the goals of Sustainable Development Goal 16 that focuses on peace, justice, and strong institutions. The authors emphasized the fact that the combination of intelligent sensing, data analytics, and automated decision-making decreased human involvement and minimized electoral malfunctions.

Al-Farouni et al. (2025) presented an open and hack-resistant electronic voting system as an attempt to enhance election security. They worked on filling the most important weak areas of traditional e-voting systems with the help of secure authentication and data structures protecting the integrity of the information stored in the system. The offered system focused on the transparency and anti-vote manipulation feature and showed enhanced trustworthiness in contrast with traditional models of electronic voting.

Ashraf and Ahmad (2025) explored a customized e-voting system which incorporated blockchain technology and IoT-based social networks through graph theory within a distributed microservices-grounded cloud-fog architecture. Their paper demonstrated the increased data integrity, transparency, and the benefits of graph-theoretic models in the analysis of voter personalization and interaction through the improved use of decentralized blockchain structure. The suggested solution was successful in overcoming the problem of tampering of votes and unauthorized access in distributed environments.

The reviewed studies indicate that recent research trends in IoT-enabled voting systems are shifting from standalone security mechanisms toward integrated hybrid frameworks combining blockchain, biometric authentication, cryptographic protection, and machine learning-based anomaly detection. Blockchain-based solutions primarily improve transparency and vote integrity, while machine learning techniques enhance adaptive fraud detection capabilities. However, existing studies still face challenges related to scalability, computational overhead, privacy preservation, and resource limitations in large-scale electoral environments. These limitations highlight the need for lightweight and efficient hybrid fraud detection architectures for future secure voting systems.

4. ARCHITECTURE OF IOT-ENABLED VOTING SYSTEMS AND SECURITY THREATS

IoT-based voting systems typically are run on a multi-layered architecture that includes voting devices, communication networks, processing platforms, and application services. Smart voting machines, biometric scanners, RFID cards, and sensors are installed at the device level to check the voter and record the votes. Such devices communicate either by wired or wireless network i.e., Wi-Fi, Bluetooth or cellular networks to a centralized or distributed server.

The distributed nature of IoT-enabled voting systems presents a number of security challenges. IoT devices have limited computing power, which limits the application of sophisticated security algorithms. The wireless communication channels are susceptible to eavesdropping attack, replay attack and data interception.

IoT-based voting systems can be subject to many types of fraud, such as voter impersonation with stolen credentials, tampering of the vote during transmission or storage, replay attacks, which duplicate valid votes, and denial-of-service attacks, which cause a voter to be unable to cast their vote. Understanding these threats is essential in order to come up with efficient fraud detection systems.

Table 1: Major Fraud Types and Threats in IoT-Enabled Voting Systems

Fraud Type	Description	Potential Impact

Voter impersonation	Unauthorized use of voter identity	Invalid vote casting
Vote tampering	Alteration of vote data	Election result manipulation
Replay attacks	Reuse of legitimate vote packets	Multiple voting
DoS attacks	System unavailability	Voter disenfranchisement
Insider fraud	Abuse of authorized privileges	Loss of public trust

5. CRYPTOGRAPHIC AND BLOCKCHAIN-BASED FRAUD DETECTION TECHNIQUES

Studies that focused on the security of electronic voting systems laid the foundation for cryptographic methods for privacy and data security. This is evidenced by the contributions made by Chaum (1981) and Benaloh (1987). Chaum (1981) presented methods of secure communication in electronic transactions whereas Benaloh (1987) developed homomorphic encryption algorithms for e-voting systems.

In IoT-enabled voting systems cryptographic techniques are used as the basic level of security. Vote confidentiality in transmission and storage is guaranteed by encryption techniques and voter authenticity and integrity of data by use of digital signatures and hash functions. More complex cryptographic protocols, like homomorphic encryption, can be used to count the votes without disclosing voting data, thus maintaining voter privacy.

Even though cryptographic techniques are effective, they can have a significant computational overhead and complicated key management, which they may not be appropriate with resource-limited IoT devices. Blockchain technology has been used as an additional solution to overcome these shortcomings. Blockchain offers a decentralized and tamper-resistant ledger of votes that are stored as transactions and thus post-election interventions are virtually impossible.

Smart contracts that run on blockchain-based systems automatically check voting regulations and identify anomalies including vote faking and unauthorized access. Although blockchain increases transparency and trust, scalability and latency are also of serious problem especially during national elections of large scale.

6. MACHINE LEARNING-BASED FRAUD DETECTION APPROACHES

Fraud in IoT-enabled voting systems has been a matter that has attracted a lot of attention on machine learning (ML) methods because of their capability to detect complex and emerging patterns of attack. ML models categorize the voting behavior, network traffic, and device activity to find anomalies that could indicate a fraudulent activity.

When the labeled data is accessible, supervised learning algorithms, e.g. Support Vector Machines, Decision Trees, and Random Forests are typically employed. These are the models that are highly accurate in detection but they need large training data. Unsupervised methods of learning, such as clustering and anomaly detection models are useful in the detection of unknown fraud patterns in the absence of labeled data.

Deep learning methods also help to improve the detection performance by identifying non-linear connections of large data. Nonetheless, ML-based solutions have issues with privacy of data, interpretability of models, and cost of computation, particularly with low-power IoT devices.

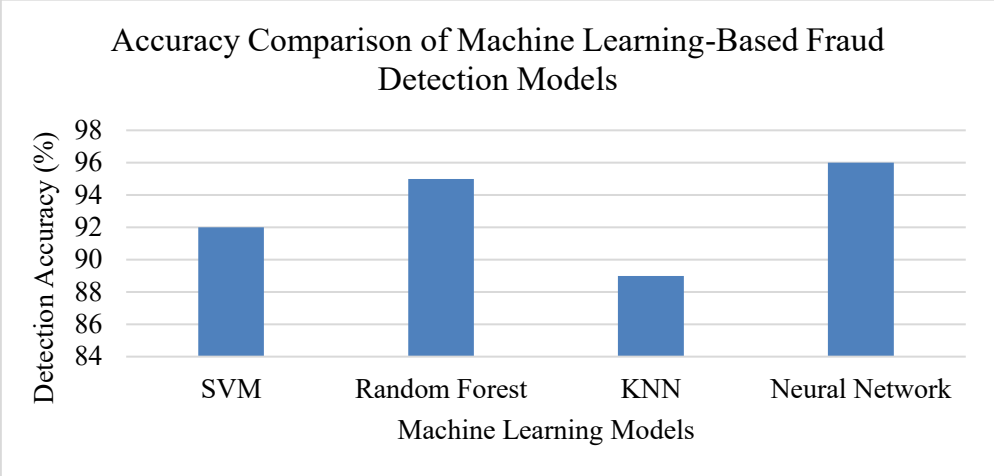

Figure 2: Comparative Performance Trends of Machine Learning-Based Fraud Detection Models in IoT-Enabled Voting Systems

Figure 2 shows a comparative analysis of the performance trends found in different machine learning algorithms utilized in fraud detection in IoT-based voting systems. Previous research suggests that ensemble learning and deep learning techniques, like Random Forest and Neural Networks, tend to exhibit greater effectiveness in detecting fraud compared to conventional algorithms such as SVM and KNN. This comparison is made based on the trends seen in past literature and not through direct experimentation.

7. HYBRID FRAUD DETECTION FRAMEWORKS AND PERFORMANCE EVALUATION

Hybrid fraud detection system combines cryptographic protection, blockchain systems and machine learning to leverage the strengths of multiple approaches. In such frameworks, cryptography provides secure communication, blockchain provides data integrity, and ML models are constantly monitoring the behavior of the system to identify anomalies.

The metrics used to gauge the performance of the fraud detection techniques are usually accuracy, precision, recall, latency of detection, and energy consumption. Hybrid solutions typically are more effective and resistant to detection than single-technique solutions, but can also incur moderate computational overhead.

Table 2: Comparison of Fraud Detection Techniques

Technique	Security Strength	Scalability	Computational Cost
Cryptographic methods	High	Medium	High
Machine learning models	Medium–High	High	Medium
Blockchain-based systems	Very High	Medium	High
Hybrid frameworks	Very High	High	Medium–High

Hybrid fraud detection models integrate cryptographic security, blockchain-based data integrity, and machine learning-based anomaly detection in order to increase the overall system robustness. With complementary advantages of these methods, hybrid models have better detection efficiency and are robust to different fraud cases.

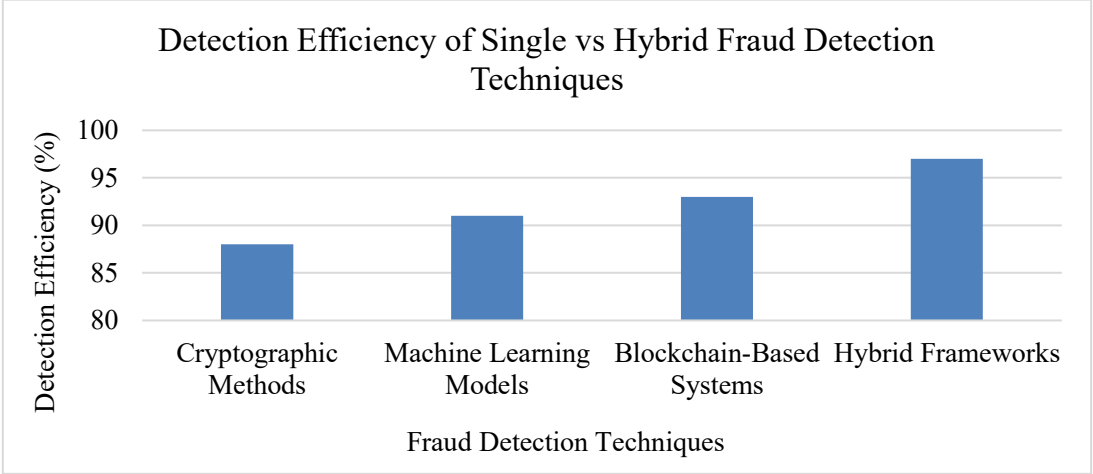

Figure 3: Comparative Detection Efficiency Trends of Fraud Detection Techniques in IoT-Enabled Voting Systems

Figure 3 depicts the detection efficiencies of the various fraud detection methodologies based on cryptography, machine learning, blockchain, and a combination of different approaches as reported by previous studies. It can be observed that the hybrid approach shows more robustness and improved detection efficiencies compared to other approaches since it combines different security features such as secure communication, anomaly detection, and decentralized data verification processes.

8. RESEARCH GAPS AND FUTURE DIRECTIONS

Although remarkable progress has been achieved in securing voting through IoT technology, there are still many research problems that need to be solved. Scalability and latency are still prevalent problems in existing voting mechanisms implemented using blockchain. The data used in machine learning techniques is required to be high quality and might produce false positive results and lack in interpretability.

In addition to security concerns, another major issue related to fraud detection is privacy preservation while performing real-time monitoring and voter identification. The majority of existing literature concentrates more on enhancing the security aspect without sufficient consideration being paid to light-weight implementations.

Further research can be directed towards creating scalable, efficient, and privacy-preserving hybrid solutions for the problem in question based on blockchain technology, federated learning, and cryptology techniques.

9. CONCLUSION

IoT based voting is a potential development in the current electoral systems since it enhances efficiency, accessibility, and real time monitoring but on the other hand, is very vulnerable to security threats and fraud in the system since it is distributed and interconnected. This review has explored significant fraud detection methodologies, such as cryptographic solutions, blockchain solutions, machine learning applications, and hybrid frameworks with the view that they are effective strategies in overcoming fraud threats such as voter impersonation, vote manipulation, and system disruption. Although cryptographic and blockchain are very secure and assure data integrity, their scaling capability and computational complexity is an issue, especially when it comes to large-scale elections. Machine learning solutions provide intelligent and adaptive methods of detecting fraud but have problems with data availability, privacy, and interpretability. The comparative analysis shows that hybrid fraud detection frameworks, using combination of various security mechanisms, have improved detection efficiency and robustness than single technique frameworks. All in all, the paper highlights the relevance of

scalable and privacy conscious and resource sensible hybrid architectures to ensure safe, transparent and credible IoT-enabled voting mechanisms in elections in the future. Future research directions must concentrate on developing lightweight, scalable, and privacy-friendly hybrid fraud detection systems for large-scale IoT-based voting systems.

REFERENCES

[1] Abubakar, J. A., Oluwatobi, A., & Ademola, O. F. (2024). Advancing Democratic Governance with AIoT-Enabled E-Voting: A Case Study of Covenant University's Departmental Associations in Alignment with SDG 16. In Artificial Intelligence of Things for Achieving Sustainable Development Goals (pp. 335-360). Cham: Springer Nature Switzerland.

[2] Al-Farouni, M. H., Dwivedi, J., Saravanan, T., Abduvahobkizi, I. Y., Pushpalatha, A., Karimov, B. N., & Sneha, N. (2025, November). Enhancing election security through a transparent and tamper-resistant eVoting system. 2025 International Conference on Intelligent Systems and Pioneering Innovations in Robotics and Electric Mobility (INSPIRE) (pp. 360–365). IEEE.

[3] Ashraf, N., & Ahmad, N. (2025). Personalized e-voting via blockchain on IoT-enabled social networks using graph theory in a distributed microservices cloud-fog infrastructure. International Journal of Advanced Computer Science and Applications. Advance online publication.

[4] Chinchamalatpure, S. V., Kapse, S. R., Balki, A. K., Rahangdale, V. A., Fulzele, V. K., & Telrandhe, S. (2024, February). Design of Blockchain-based Secured Election Voting System. In 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-7). IEEE.

[5] Dixit, A., Gupta, A. K., Kaur, G., Jain, M., Pandey, R. K., & Sharma, A. (2024, December). Enhancing Voting System Security and Accessibility through Biometric Authentication and IoT Integration. In 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N) (pp. 1460-1465). IEEE.

[6] Farooqi, A. H., Akhtar, S., Rahman, H., Sadiq, T., & Abbass, W. (2023). Enhancing network intrusion detection using an ensemble voting classifier for internet of things. Sensors, 24(1), Article 127.

[7] Galla, S., Malik, S. S., Nandyala, L. R., Koushik, B. S., Benarji, P. S. V., & Gangaprasad, G. (2025, September). Internet of Things based E-Ballot Voting System. In 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1025-1032). IEEE.

[8] Indrason, N., Baital, K., & Saha, G. (2025). Design and security analysis of SDN-based IoT-oriented blockchain protected e-voting system. IEEE Transactions on Mobile Computing. Advance online publication.

[9] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17), 5874.

[10] Jaisinghani, O. A., & Ramteke, P. L. (2024, November). Evaluating the Security Impact of Face Recognition and IoT-Enabled Blockchain on Electronic Voting Machines. In 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI) (pp. 1-6). IEEE.

[11] Kiran, A., Lavanya, C., Arunsai, D., Shalini, V., Koushik, P. S., & Koushik, A. V. (2025, May). Secure Biometric Voting System using Deep Learning and IOT. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-6). IEEE.

[12] Krishnamurthy, R., Rathee, G., & Jaglan, N. (2020). An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices. Wireless Networks, 26(4), 2391-2402.

[13] Ranganathan, C. S., Kabaleeswaran, S., Reddy, P. K. K., Selvarani, P., Srinivasan, C., & Rajarajan, S. J. (2024, November). Enhancing Voter Identity Verification Through Cloud Computing Enabled Biometric Authentication-Modern Voting. In 2024 International Conference on Smart Technologies for Sustainable Development Goals (ICSTSDG) (pp. 1-6). IEEE.

[14] Shaikh, A., Adhikari, N., Nazir, A., Shah, A. S., Baig, S., & Al Shihi, H. (2025). Blockchain-enhanced electoral integrity: A robust model for secure digital voting systems in Oman. F1000Research, 14, Article 223.
[15] Yasmin, M., Sharmila, S., Swathi, S., Sujitha, S., Renuka, G., & Thirisha, P. (2025, September). Secure IoT Voting System with Fingerprint Authentication and Real-Time Monitoring. In 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 1428-1435). IEEE.
[16] Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84–90.
[17] Benaloh, J. (1987). Verifiable secret-ballot elections. Yale University Department of Computer Science.