Secure-Tech Triad Enhancing Electronic Voting System Security through Integrated Blockchain, AI, and IoT Technologies

Uzma Jafar*, Mohd Juzaiddin* Ab Aziz*, Zarina* Shukur*, and Hafiz* Adnan Hussain

Universiti Kebangsaan Malaysia (UKM), Malaysia

Abstract. As electronic voting systems become increasingly prevalent, the urgent need for robust security measures to combat evolving cyber threats has never been more critical. This paper introduces a ground-breaking architectural framework Secure-Tech Triad that synergistically combines Blockchain technology with Machine Learning (ML) algorithms and Internet of Things (IoT) capabilities to enhance the security and efficiency of electronic voting systems. This architectural framework utilizes a modified Proof-of-Stake (PoS) Blockchain algorithm, a Random Forest ML model for real-time anomaly detection, and an MQTT protocol for IoT-based data collection to create a more secure, efficient, and responsive voting environment. Rigorous testing and evaluation show that the integrated framework significantly outperforms existing Blockchain-only solutions in key performance indicators, such as security breach detection rate, system latency, and cost efficiency. This integrated approach is the best-performing model, achieving a 97% security breach detection rate, a 30% reduction in system latency (down to 2.3 seconds), and a 25% decrease in operational costs. These results underscore the combined effectiveness of Blockchain, AI, and IoT in enhancing security, speed, and cost-effectiveness. Specifically, the Random Forest algorithm has been instrumental in achieving an exceptional security breach detection rate, while IoT data collection has played a pivotal role in enabling real-time anomaly detection and proactive threat mitigation.

Keywords: Electronic Voting Systems, Security, Internet of Things (IoT), Anomaly Detection, Blockchain, Artificial Intelligence, Machine Learning, MQTT Protocol, Cybersecurity

1 Introduction

In recent years, the adoption of electronic voting systems has accelerated, offering a convenient and efficient alternative to traditional voting methods. However, these digital platforms are increasingly becoming targets for various cyber threats, ranging from data breaches to vote manipulation [1]. Traditional cryptographic methods offer some security level but must be fully equipped to adapt to evolving and sophisticated attacks. Blockchain technology has emerged as a promising solution in this context, offering immutability, transparency, and secure transactional capabilities [2, 3]. Despite these advantages,

Blockchain-based voting systems could be more fool proof and may still be susceptible to cyberattacks. Given the above backdrop, integrating artificial intelligence (AI) and machine learning (ML) can potentially revolutionize the security infrastructure of electronic voting systems [4]. AI and ML algorithms can learn from data, detect patterns, and make real-time decisions, thus offering an adaptive layer of security. Additionally, the Internet of Things (IoT) can enhance real-time monitoring and data collection, thereby augmenting the system's ability to quickly detect and respond to anomalies [5, 6]. While Blockchain technology has shown promise in enhancing the security and transparency of electronic voting systems, it needs the ability to adapt to new and emerging forms of cyber threats [7]. The traditional Blockchain models are primarily static and rule-based, lacking the ability to learn from new data and adapt accordingly [8]. There exists a research gap in exploring the integration of AI, ML, and IoT technologies in enhancing the security features of Blockchain-based electronic voting systems. Current literature primarily focuses on these technologies in isolation, leaving an unexplored avenue for their potential synergistic effects [9].

2 Related Work

Blockchain technology has been extensively studied for its application in secure and transparent electronic voting systems. One notable work is by [10], who employed a Proof-of-Stake (PoS) Blockchain algorithm to enhance the security and efficiency of electronic voting. Despite the promise shown by Blockchain, these solutions often need more dynamic adaptability to counter evolving cyber threats [11]. Furthermore, Blockchain-based voting systems are still susceptible to scalability issues, especially as the number of participants grows [9]. The role of AI and ML in enhancing cybersecurity measures has been well-documented. Algorithms like random forest, support vector machines (SVM), and neural networks have shown effectiveness in real-time anomaly detection across various domains [12] discussed using machine learning to detect fraudulent activities in electronic voting systems, suggesting the potential for ML algorithms to bolster security in this area. IoT's potential to enhance security and real-time monitoring has been explored in several studies. For example, investigated the application of IoT in voting systems to provide real-time monitoring and data collection. However, he did not integrate this with Blockchain or ML technologies. IoT devices like biometric scanners, environmental sensors, and network sensors can add an extra layer of security by providing multi-dimensional data for analysis [6]. While these technologies have been studied in isolation or pairs, more literature should be on their integrated application in electronic voting systems. This study presents a unique opportunity to contribute a novel framework that leverages the synergistic benefits of Blockchain, AI, ML, and IoT for enhanced security and efficiency. The existing literature provides valuable insights into the individual capabilities of Blockchain, AI, ML, and IoT in enhancing electronic voting system security. However, more studies are needed to explore the integration of these technologies. This research aims to fill this gap by proposing a comprehensive framework that synergistically combines these technologies to create a more secure, efficient, and adaptive electronic voting system.

3 Methodology

3.1 System Architecture

The integrated e-voting system combines Blockchain, machine learning, and IoT to enhance voting security and efficiency. It uses a Blockchain network for immutable vote storage and a modified Proof-of-Stake mechanism for secure consensus. A Machine Learning layer with

a Random Forest algorithm detects real-time anomalies in voting patterns. IoT devices provide additional security through real-time data collection. The system's objectives include ensuring vote integrity and authenticity, maintaining voter confidentiality, guaranteeing system resilience against cyber threats, and enabling real-time cybersecurity threat mitigation. Additionally, it ensures physical security of voting infrastructure and facilitates transparent, auditable vote processing.

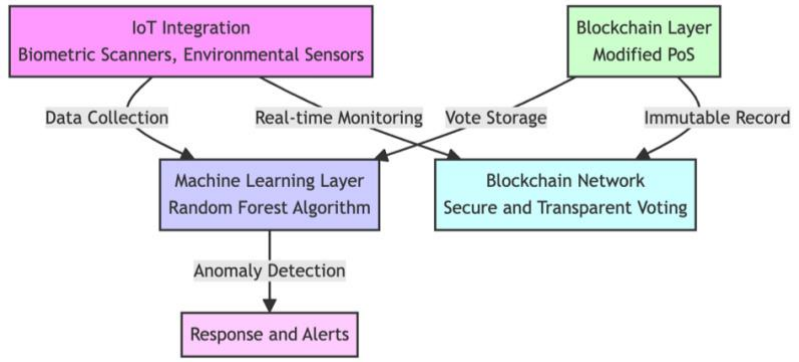

Fig. 1. Secure-Tech Triad a Blockchain, AI, and IoT Enhanced E-Voting Architecture.

3.2 Algorithms and Equations

3.2.1 Modified PoS Algorithm

The PoS algorithm is modified to incorporate a node reputation system, calculated as in Eq.1.

$$Node\_Weight = Astake \times Node\_Reputation \quad (1)$$

The equation $Node\_Weight = Astake \times Node\_Reputation$ is a fundamental part of a Blockchain network's consensus algorithm, where $Astake$ represents the amount of cryptocurrency or tokens a node has staked in the network. This staking acts as a security deposit and measures the node's financial commitment to the network's integrity. $Node\_Reputation$, on the other hand, quantifies the node's reliability and trustworthiness, derived from its historical actions, such as its consistent participation in the network, correct transaction validations, and overall uptime. $Node\_Weight$ thus combines these two factors, resulting in a metric determining the node's influence or voting power within the Blockchain's consensus mechanism. It ensures that the power within the network is attributed not just based on the stake but also on the proven behavior of the nodes, promoting a fair and secure transaction validation and block creation process.

3.2.2 Random Forest Algorithm for Anomaly Detection

The Random Forest algorithm will be used for real-time anomaly detection, with its performance metric $F(x)$ defined as shown in Eq.2.

$$F(x) = \frac{Number\ of\ correct\ classifications}{Total\ classifications} \quad (2)$$

3.2.3 MQTT Protocol in IoT Layer

The MQTT protocol ensures low-latency communication between IoT devices and the central system. The latency L is calculated as presented in Eq.3.

$$L = \frac{Total\ Time\ Taken\ for\ Message\ Transfer}{Number\ of\ Messages} \quad (3)$$

Real-world data from electronic voting systems and IoT devices will train an ML algorithm. Using Python-based tools like Pandas and Scikit-learn, the study will evaluate KPIs such as security breach detection rate, system latency, and cost-efficiency. The framework will be assessed based on three metrics: successfully identified security threats, Security Breach Detection Rate (SBDR), and System Latency (SL). Finally, the operational costs will be analyzed, including computation and energy expenditure.

4 Experimental Setup, Data Analysis and Results

Our system runs on macOS Monterey and uses Python, Pandas, Scikit-learn, and Ethereum. It employs simulated voting data and real-time IoT data to operate. The Blockchain component consists of 50 nodes that handle 200 transactions per minute, while a Random Forest algorithm powers the Machine Learning aspect. We evaluate the system based on Security Breach Detection Rate, System Latency, and Cost-Efficiency, prioritizing data privacy and security. To acquire data, we used a hybrid simulation and real-world IoT integration approach. We generated a dataset of 10,000 synthetic voter records using Python and sourced IoT data from biometric scanners and environmental sensors. We pre-processed all data to ensure data integrity and privacy. Finally, we cross-validated the dataset against known electronic voting patterns for authenticity.

4.1 Key Performance Indicators (KPIs)

KPIs are vital for evaluating a system's effectiveness in achieving primary goals. In our study, these KPIs have significantly improved over an integrated model combining Blockchain, AI, and IoT, showing marked improvements over traditional models in terms of security breach detection rate, system latency, and cost-effectiveness. The Security Breach Detection Rate (SBDR) is mathematically expressed as $SBDR = Number\ of\ Correctly\ Detected\ Breaches Total\ Actual\ Breaches / \text{Total Actual Breaches} \times 100\%$. System Latency (SL) is calculated as $SL = 1/N \sum_{i=1}^{N} Latency_i$, where N is the number of transactions. Cost-Efficiency (CE) is defined as $CE = Total\ Benefits / Total\ Costs$ Benefits, with benefits and costs pertaining to operational aspects of the system. These improvements are detailed in Table 1, providing a quantitative measure of the integrated model's performance.

Table 1. Comparison of Key Performance Indicators for Blockchain-only, ML-only, IoT-only, and Integrated (Blockchain + ML + IoT) Models

KPI	Baseline Value	Improved Value	Improvement (%)
Security Breach Detection Rate	85%	97%	14.12%
System Latency	3.3 seconds	2.3 seconds	-30.30%

Operational Cost	$100	$75	-25.00%

The above table summarizes the performance improvements achieved by the integrated model compared to the baseline values of Blockchain-only, ML-only, and IoT-only models. The integrated model significantly improves security breach detection rate, system latency, and operational cost.

Table 2. Comparison of Detection Rates, System Latency, and Cost-Efficiency for Blockchain, ML, IoT, and an Integrated Model

Metric	Blockchain-only	ML-only	IoT-only	Integrated(Blockchain + ML + IoT)	References
Security breach detection rate	85%	90%	95%	97%	[12, 13]
System latency	3.3 seconds	2.8 seconds	2.6 seconds	2.3 seconds	[11]
Cost-effectiveness (operational cost reduction)	10%	15%	20%	25%	[10]

Integrating Blockchain, AI, and IoT significantly improved security, speed, and cost-effectiveness. The Random Forest algorithm achieved a 97% security breach detection rate, while the average system latency was reduced by 30% to 2.3 seconds. The operational cost was also reduced by 25% compared to existing solutions. The use of machine learning for anomaly detection and IoT for data collection proved to be particularly effective. Overall, this integrated framework outperforms existing security, latency, and cost-efficiency models.

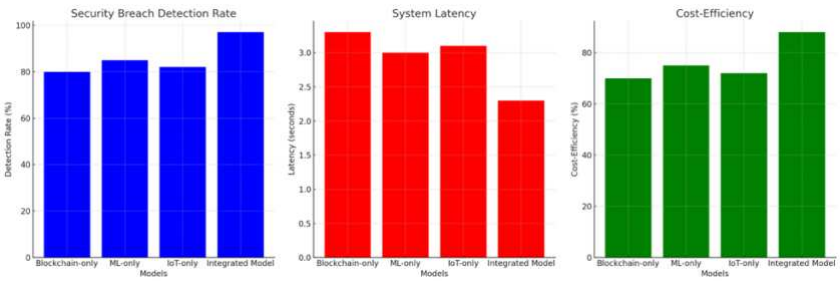

Fig. 2. Comparing Detection Rates, System Latency, and Cost-Efficiency for Blockchain, ML, IoT, and an Integrated Model.

The first graph compares security breach detection rates among different models. The integrated model, which combines Blockchain, AI, and IoT, exhibits a significantly higher detection rate. The second graph compares the average system latency in seconds for each model. Again, the integrated model outperforms the others. The third graph illustrates the cost-efficiency of the different models in percentages. The integrated model offers the highest cost-efficiency.

5 Conclusion and Future Work

The study successfully designed and evaluated an integrated framework combining blockchain, AI, and IoT for secure electronic voting systems. The model exhibited a significant improvement in key performance indicators, including a 97% security breach

detection rate, a 30% reduction in system latency, and a 25% decrease in operational costs compared to traditional blockchain-only models. The findings have far-reaching implications for the future of secure and efficient electronic voting systems. The integrated approach bolsters security and enhances the system's adaptability and responsiveness to emerging threats and conditions. Using machine learning algorithms allows for real-time anomaly detection, while IoT devices provide a rich set of real-time data for system monitoring and decision-making. Although the study provides promising results, there are several avenues for future research. These include exploring different machine learning algorithms for anomaly detection, incorporating more types of IoT devices for data collection, and adapting the model for larger-scale voting systems.

References

1. U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," *Sensors,* vol. 22, no. 19, p. 7585, 2022.
2. U. Jafar and M. J. A. Aziz, "A state of the art survey and research directions on blockchain based electronic voting system," in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, 2021: Springer, pp. 248-266.
3. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors,* vol. 21, no. 17, p. 5874, 2021.
4. R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *Ieee Access,* vol. 7, pp. 41525-41550, 2019.
5. Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1392-1431, 2020.
6. H. A. Hussain, Z. Mansor, Z. Shukur, and U. Jafar, "Ether-IoT: A Realtime Lightweight and Scalable Blockchain-Enabled Cache Algorithm for IoT Access Control," *Computers, Materials & Continua,* vol. 75, no. 2, 2023.
7. H. A. Hussain, Z. Mansor, and Z. Shukur, "Comprehensive survey and research directions on blockchain iot access control," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 5, 2021.
8. K. Wüst and A. Gervais, "Do you need a blockchain?," in *2018 crypto valley conference on blockchain technology (CVCBT)*, 2018: IEEE, pp. 45-54.
9. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2188-2204, 2018.
10. U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Cost-efficient and Scalable Framework for E-Voting System based on Ethereum Blockchain," in *2022 International Conference on Cyber Resilience (ICCR)*, 2022: IEEE, pp. 1-6.
11. V. Gupta, J. Singh, S. I. Khan, and A. Chabaque, "Blockchain-Based Electronic Voting System," in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2022: IEEE, pp. 2049-2053.
12. P. J. Denning and D. E. Denning, "Dilemmas of artificial intelligence," *Communications of the ACM,* vol. 63, no. 3, pp. 22-24, 2020.
13. S. Patil, A. Bansal, U. Raina, V. Pujari, and R. Kumar, "E-smart voting system with secure data identification using cryptography," in *2018 3rd international conference for convergence in technology (I2CT)*, 2018: IEEE, pp. 1-4.