

# The impact of blockchain and artificial intelligence technologies in network security for e-voting

Jumagaliyeva Ainur<sup>1</sup>, Muratova Gulzhan<sup>2</sup>, Tulegulov Amandos<sup>1</sup>, Rystygulova Venera<sup>1</sup>,  
Serimbetov Bulat<sup>1</sup>, Yersultanova Zauresh<sup>3</sup>, Shegetayeva Aizhan<sup>4</sup>

<sup>1</sup>Department of Information Technology, Kazakh University of Technology and Business, Astana, Republic of Kazakhstan

<sup>2</sup>Department of Information Technology, S. Seifullin Kazakh Agrotechnical Research University, Astana, Republic of Kazakhstan

<sup>3</sup>Department of Physics, Mathematics and Digital Technologies, Akhmet Baitursynuly Kostanay Regional University, Kostanay, Republic of Kazakhstan

<sup>4</sup>Department of Information Security, Eurasian National University named after L.N. Gumilyov, Astana, Republic of Kazakhstan

## Article Info

### Article history:

Received Mar 13, 2024

Revised Aug 1, 2024

Accepted Aug 6, 2024

### Keywords:

Artificial intelligence

Blockchain

Blockchain frameworks

Cyber threats

E-voting

Machine learning

Network security

## ABSTRACT

This study explored the integration of blockchain and artificial intelligence technologies to enhance the security framework of electronic voting (e-voting) systems. Amid increasing vulnerabilities and cyber threats to electoral integrity, these technologies provided robust solutions by ensuring the immutability of voting records and enabling real-time anomaly detection. Blockchain technology secured votes in a decentralized, tamper-proof ledger, preventing unauthorized modifications, and enhancing transparency. Concurrently, artificial intelligence leveraged predictive analytics to dynamically monitor and respond to potential security threats, thereby ensuring the reliability and integrity of the voting process. This paper presented a dual-technology approach where blockchain's transparency complemented artificial intelligence's (AI) threat detection capabilities, providing a comprehensive security solution for e-voting systems. Through theoretical models and empirical data, we demonstrated significant improvements in transaction throughput, threat detection accuracy, and system scalability. The findings suggested that the strategic application of these technologies could substantially mitigate current e-voting vulnerabilities, offering a pathway to more secure, transparent, and efficient electoral processes globally.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Jumagaliyeva Ainur

Department of Information Technology, Faculty of Technology, Kazakh University of Technology and Business

010000 Astana, Republic of Kazakhstan

Email: jumagalievaainur.m@gmail.com

## 1. INTRODUCTION

Nowadays, ensuring the integrity of electoral processes is crucial. As electoral systems transition from traditional paper-based methods to digital platforms, they encounter new security challenges that threaten voter confidence and the integrity of elections. These challenges include data breaches, voter privacy violations, and potential vote tampering, which highlight the vulnerability of electronic voting (e-voting) systems. To address these issues, robust security frameworks are essential to mitigate both internal and external security threats. Blockchain technology and artificial intelligence are at the forefront of enhancing network security. The decentralized system of blockchain provides a transparent, making it ideal for securely recording votes and verifying voter identities. Concurrently, artificial intelligence (AI) enhances security

measures with real-time identification of threats, analysis of activities, and identification of anomaly capabilities, crucial for proactive security interventions.

This article investigates the practical application of blockchain and AI in securing e-voting systems. Unlike previous studies that primarily focus on theoretical models, this study implements a dual-technology framework combining blockchain and AI to tackle prevalent security challenges actively. This framework not only addresses the scalability issues associated with blockchain during high-demand periods but also optimizes the computational efficiency of AI systems, providing a comprehensive solution to the security vulnerabilities of e-voting systems. Through empirical analysis and systematic application, this research offers significant insights into the enhancements these technologies bring to e-voting security. By integrating blockchain's transparency with AI's analytical prowess, the study provides a novel perspective on creating more secure, transparent, and efficient electoral processes. The practical implications of this technology integration are demonstrated through simulated real-world scenarios, validating the effectiveness of this approach and setting a benchmark for future electoral security frameworks. By concentrating on the blockchain and artificial intelligence integration, the article provides timely and relevant solutions to current vulnerabilities in electoral processes. This relevance is underscored by the growing concerns over electoral fraud, data breaches, and the overall trustworthiness of digital voting systems, making the research highly pertinent to current technological and societal needs.

## 2. LITERATURE REVIEW

Blockchain and artificial intelligence technologies coming together presents a promising frontier for enhancing the security framework of electronic voting systems. This literature review synthesizes key findings from recent studies, emphasizing the separate contributions of blockchain and artificial intelligence to e-voting security and identifying the nuanced advancements offered by the integrated approach. Research documents blockchain's utility in ensuring transparency and immutability within e-voting systems. Recent studies, as Agate *et al.* [1] highlighted blockchain's role in enhancing voting integrity by safeguarding against unauthorized access and tampering with vote records. Its decentralized architecture is pivotal in preventing unilateral alterations of vote outcomes, thus addressing electoral fraud concerns. Further research illustrated by Panja and Roy [2] how blockchain's transparency fosters voter confidence by enabling anonymous vote verification. Beyond anomaly detection, artificial intelligence's capabilities in real-time data monitoring for identifying voting discrepancies are well noted. Artificial intelligence's efficacy in automating voter verification processes, reduces human error, and ensuring electoral integrity. According to El Fezzazi [3] these advancements point towards AI's critical role in streamlining the electoral process through sophisticated data analysis.

Despite extensive documentation on the individual impacts of blockchain and artificial intelligence on e-voting, literature on their synergistic application remains sparse. A distinct gap is observed in empirical research exploring the integrated application of these technologies in realistic electoral scenarios, crucial for assessing practical implications and challenges. The current study seeks to bridge these gaps by integrating blockchain and to fortify e-voting security, implementing this integration in simulated real-world environments. It delves into artificial intelligence's potential to enhance blockchain functionality, addressing scalability issues identified in the research by Gupta *et al.* [4]. Additionally, it proposes a novel decentralized machine learning framework that aims to distribute computational tasks, enhancing system robustness and scalability. Empirical evidence presented herein underscores the synergistic effects of blockchain and AI integration, showcasing their complementary roles in securing, optimizing, and making the voting process more efficient.

Furthermore, recent studies have conducted a comprehensive analysis of blockchain's efficacy in mitigating cybersecurity risks within e-voting systems. Employing a combination of empirical simulations and theoretical modeling, Tyagi *et al.* [5] rigorously evaluated blockchain's impact on advancing the integrity and resilience of electoral processes against external threats. Their findings reveal that the application of blockchain technology significantly reduces the susceptibility of e-voting systems to tampering and unauthorized access, thus bolstering voter confidence and electoral trust. Through cryptographic verification mechanisms and decentralized consensus protocols, blockchain emerges as a robust safeguard against cyber threats, offering a paradigm shift in the security paradigm of electronic voting according Dwivedi *et al.* [6]. This study moves beyond theoretical models by practically testing integrated blockchain and AI technologies within an e-voting framework, yielding insights into performance, security, and scalability enhancements. It validates the proposed models and sets a foundation for future research focused on the practical optimization of these technologies in e-voting. This integration addresses scalability and processing challenges, significantly advancing e-voting security.

### 3. MATERIALS AND METHODS

In the methodology section of this article, the collaboration between blockchain technology and artificial intelligence in enhancing network security is meticulously explored. The process begins with blockchain's implementation, providing a secure, immutable ledger for logging network transactions and events, thus ensuring data integrity and transparency. This decentralized system of record-keeping is pivotal in preventing unauthorized data alterations, leveraging cryptographic hashes to link blocks, and employing consensus algorithms for validation. Concurrently, artificial intelligence is deployed to scrutinize network traffic, utilizing algorithms like the isolation forest to detect anomalies indicative of potential threats. This AI-driven analysis enables the proactive identification of irregular patterns and behaviors within vast datasets, facilitating early intervention. The crux of the methodology lies in the seamless integration of these technologies: Artificial intelligence's detection capabilities inform the blockchain ledger, where incidents are recorded. This constructive collaboration not only bolsters the network's defense mechanisms by combining artificial intelligence's dynamic threat recognition with blockchain's tamper-proof logging in electoral processes, but also establishes a framework for ongoing education and adjustment to new cyberthreats, embodying a forward-thinking approach to network security.

The first stage involves the meticulous collection and analysis of network traffic data, which is essential for developing and refining the AI-driven anomaly detection module. To accomplish this, we utilize Wireshark, a network protocol analyzer that captures and displays the data packets traversing the network in real-time. This analysis aids in the identification of normal traffic patterns and potential security threats that are critical to the integrity of e-voting systems.

Figure 1 represents the synergy between blockchain technology and artificial intelligence in constructing a fortified network security environment for e-voting systems. The scatter plot vividly demonstrates the detection of anomalies marked in red against the backdrop of normal traffic, represented by blue stars in Figure 1. These anomalies, potentially indicative of cyber threats or fraudulent activities within the e-voting system, are identified through artificial intelligence algorithms designed for pattern recognition and outlier detection [7]. Upon the identification of such anomalies, the corresponding data is subjected to a deeper scrutiny process involving blockchain's immutable ledger. The suspicious transactions are recorded and time-stamped on the blockchain, ensuring an auditable trail of all actions taken in response to detected threats.

The screenshot shows the Wireshark interface with a list of captured packets. Several packets are highlighted in red, indicating anomalies. The detailed view shows the structure of a selected packet (Frame 53), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers.

No.	Time	Source	Destination	Protocol	Length	Info
40	11.307746	165.227.216.194	10.55.100.111	TCP	60	443 → 49544 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	11.808006	10.55.100.111	165.227.216.194	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49544 → 443 [ACK, Seq=1] Win=0 Len=0
42	11.869281	165.227.216.194	10.55.100.111	TCP	60	443 → 49544 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	12.006183	192.168.88.2	165.227.88.15	DNS	103	Standard query 0x4e53 TXT 0d6b0175375169c68f.dnsc
44	12.066989	165.227.88.15	192.168.88.2	DNS	123	Standard query response 0x4e53 TXT 0d6b0175375169c68f.dnsc
45	13.016194	LCFChFe_06:cb:e8	Broadcast	ARP	42	Who has 10.55.100.1? Tell 10.55.100.197
46	13.072038	192.168.88.2	165.227.88.15	DNS	103	Standard query 0xf9e7 TXT 5f130175375169c68f.dnsc
47	13.140922	165.227.88.15	192.168.88.2	DNS	123	Standard query response 0xf9e7 TXT 5f130175375169c68f.dnsc
48	14.016031	LCFChFe_06:cb:e8	Broadcast	ARP	42	Who has 10.55.100.1? Tell 10.55.100.197
49	14.147072	192.168.88.2	165.227.88.15	DNS	103	Standard query 0x9b4e TXT 5a360175375169c68f.dnsc
50	14.288984	165.227.88.15	192.168.88.2	DNS	123	Standard query response 0x9b4e TXT 5a360175375169c68f.dnsc
51	15.016029	LCFChFe_06:cb:e8	Broadcast	ARP	42	Who has 10.55.100.1? Tell 10.55.100.197
52	15.121130	10.55.100.111	165.227.216.194	TCP	66	49545 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
53	15.177869	165.227.216.194	10.55.100.111	TCP	60	443 → 49545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	15.213141	192.168.88.2	165.227.88.15	DNS	103	Standard query 0x9b4e TXT 5a360175375169c68f.dnsc
55	15.268863	165.227.88.15	192.168.88.2	DNS	123	Standard query response 0x9b4e TXT 5a360175375169c68f.dnsc
56	15.683104	10.55.100.111	165.227.216.194	TCP	60	443 → 49545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	15.745996	165.227.216.194	10.55.100.111	TCP	60	443 → 49545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 53: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: VMware\_f8:50:fd (00:0c:29:f8:50:fd), Dst: ADIEngin\_0a:7e:00:00:00:00  
 Internet Protocol Version 4, Src: 165.227.216.194, Dst: 10.55.100.111  
 Transmission Control Protocol, Src Port: 443, Dst Port: 49545, Seq: 1, Ack: 1, Win: 0, Len: 0

Figure 1. Network traffic analysis using Wireshark

The dual-layered approach illustrated here showcases how artificial intelligence can be leveraged to analyze network traffic in an e-voting context, providing a first line of defense by pinpointing irregularities swiftly. Meanwhile, blockchain serves as a secondary, unassailable layer, maintaining an immutable record of events that fortifies the trust in the system's resilience against tampering attempts [8]. We explore how this technological orchestration can be deployed in a real-world e-voting scenario, detailing the steps involved in setting up the system, the operational workflows, and the protocols for handling detected threats. The aim is to demonstrate not only the theoretical potential of combining blockchain and artificial intelligence, but also the practical implications and benefits for securing e-voting systems. The advancement of e-voting security

measures necessitates a multi-faceted approach that leverages the distributed nature of blockchain technology alongside the analytical prowess of machine learning. To harness these capabilities, we propose a blockchain-based decentralized machine learning system, which is depicted in Figure 2. This system architecture enhances the robustness and resilience of the e-voting security infrastructure by distributing the computational and analytical load across multiple nodes. Building on the decentralized architecture presented in Figure 2, our methodology harnesses the strengths of both machine learning and blockchain to create a resilient and adaptable e-voting security framework. Each node within this network serves a pivotal role, performing machine learning tasks to analyze voter data and behavior, while simultaneously maintaining the integrity of the blockchain ledger through the mining process [9].

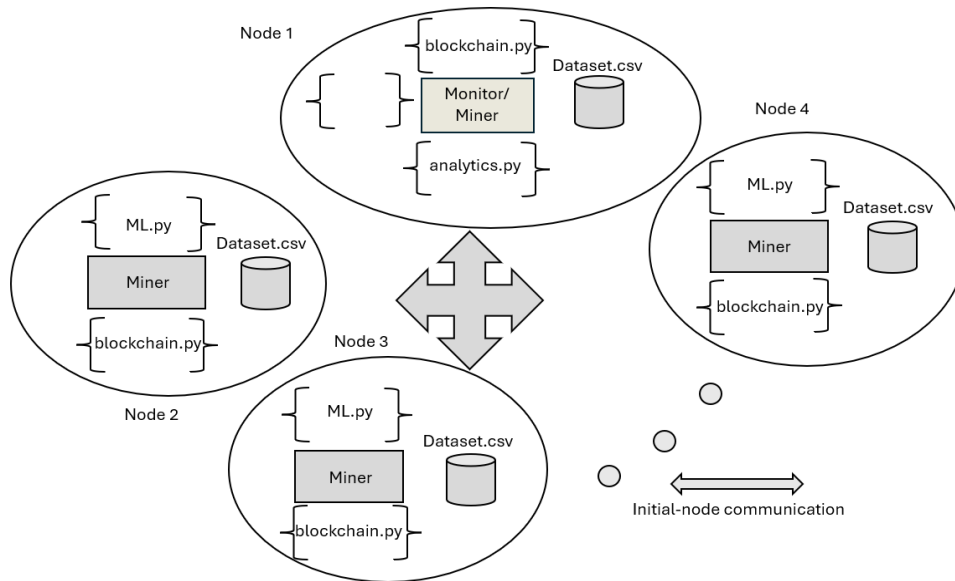


Figure 2. Blockchain-based decentralized machine learning system

In this decentralized framework, each node functions independently yet cohesively, performing specific roles in the security and analytics pipeline. Nodes are equipped with machine learning modules that analyze voting data to detect anomalies and patterns that could indicate security threats. Simultaneously, these nodes partake in a blockchain network, contributing to the ledger's maintenance by validating transactions and mining new blocks. This not only democratizes the security process but also reduces the risks associated with central points of failure. Figure 2 outlines the intricate network of nodes that collectively form a defense mechanism. The diagram shows the interconnected nature of the system, where data flow and decision-making are decentralized, and each node is a crucial stakeholder in ensuring the integrity of the e-voting process.

Node 1, distinguished by its additional monitoring responsibilities, serves as a crucial oversight mechanism. It ensures the network's optimal performance and the validity of data used in ML processes. This node's analysis contributes to continuous improvement, providing insights that may enhance the ML algorithms or blockchain operations throughout the network. It is the lynchpin for real-time adaptability and systemic refinement, utilizing data analytics to inform proactive adjustments. Nodes within this network independently execute ML algorithms (*ML.py*) on their datasets (*Dataset.csv*), facilitating a distributed approach to anomaly detection. By running these algorithms, nodes can identify irregular voting patterns that might indicate fraudulent activity or security breaches. When such anomalies are detected, the information is cryptographically secured and recorded on the blockchain (*blockchain.py*), ensuring a permanent, tamper-proof ledger of all events [10]–[13].

The mining process at each node validates transactions and creates new blocks, thus perpetuating the chain and fortifying the system's defenses against attacks. This mining activity does not just contribute to blockchain's growth; it reinforces a consensus on the veracity of the recorded data, which is essential in maintaining the trustworthiness of the e-voting system. The workflow encapsulated in this figure indicates a sophisticated interplay between data processing and security measures. The use of a user interface (GUI uploader) for data input and the emphasis on metadata ensure that data fed into the Machine learning models

are consistent and reliable. The decentralization of mining activities across several nodes exemplifies the robust nature of the system, minimizing the risk of single points of failure and distributing the computational load efficiently.

Our approach acknowledges the need for data privacy and efficiency. The outputs of machine learning models, which are critical for decision-making and security purposes, are stored off-chain where necessary. This practice not only optimizes system performance but also aligns with regulatory and ethical standards concerning voter privacy. This sophisticated network architecture, leveraging blockchain for security and decentralization, while employing ML for data analysis and predictive modeling, is meticulously designed for scalability and robust security. It enables the system to conduct robust ML processes without overburdening the blockchain, creating a harmonious balance between comprehensive security and operational efficiency.

Figure 3 encapsulates the intricate process flow of the decentralized machine learning system, integrated within the broader context of a blockchain network specifically designed for the e-voting security framework [14]. This conceptual model highlights the lifecycle of machine learning from data ingestion and preprocessing to model training, evaluation, and deployment in Figure 3. It presents a blockchain-powered, decentralized machine learning framework designed to enhance collaborative intrusion detection for unmanned aerial vehicles (UAVs). The premise put forth by the authors is the heightened vulnerability of traditional unmanned aerial vehicles systems to cyber threats, attributed to their reliance on centralized data processing. Through the lens of decentralized predictive analytics powered by blockchain, the study outlines a method for the implementation and mutual use of machine learning models. This methodology was specifically tested through cooperative intrusion detection, validating the approach's relevance and efficacy for unmanned aerial vehicles and analogous scenarios. Compared to traditional centralized systems, this novel decentralized model demonstrated enhancements in detection accuracy and a reduction in performance overhead. Furthermore, it minimized the necessity for inter-node data exchange, thereby elevating the overall data privacy and security. Future inquiries are set to explore the adaptability and resilience of this framework in unmanned aerial vehicles settings confronting assorted cyber threats [15]. The diagram illustrates how raw data is initially uploaded through a user interface, processed and transformed into a structured format suitable for machine learning. The meticulous care in data handling and preparation underscores our commitment to data quality and the importance of accurate input for reliable AI analytics. Miner nodes within this system are multi-functional. Besides their role in securing the blockchain network through mining activities, they also facilitate the machine learning process by performing tasks such as data preprocessing and model training. This distributed approach to data analytics not only bolsters the security of the e-voting system but also enhances the privacy and scalability of the machine learning operations.

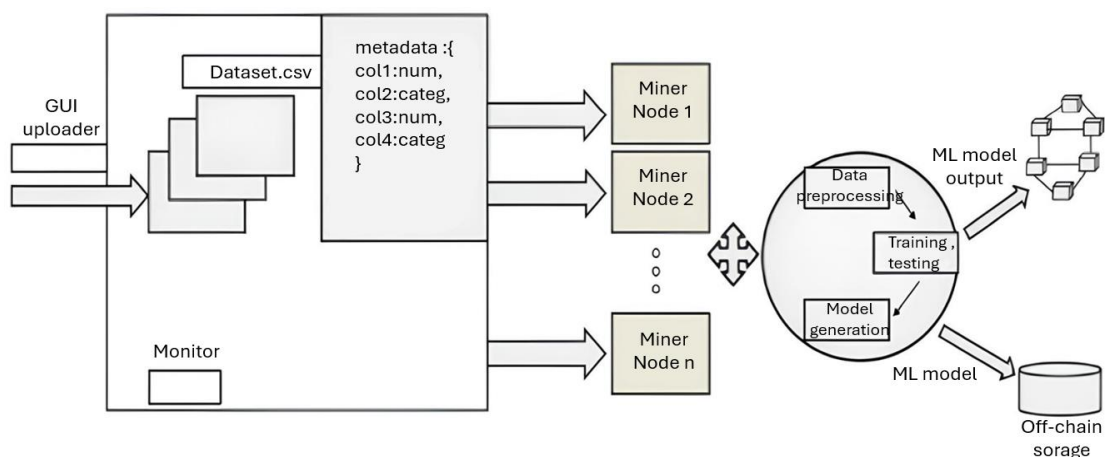


Figure 3. The framework for the machine learning process

Machine learning models generated through this system are validated and iteratively improved, ensuring that they remain effective at detecting anomalies and patterns indicative of cybersecurity threats. The use of off-chain storage for the models' output reflects a thoughtful balance between system efficiency and the integrity of sensitive data, a key consideration in the context of e-voting security [16]. The strength of this model is in its decentralized structure, which greatly minimizes the risk of single points of failure and enhances the e-voting system's resilience against advanced cyber threats. By leveraging the combined power

of distributed computing and blockchain technology, our method ensures a secure, scalable, and robust infrastructure for election processes.

Figure 4 shows that the discourse progresses from decentralized network security models to encompass broader infrastructural applications, attention now turns towards the sophisticated integration of blockchain and AI within the realm of smart cities. This evolution in the narrative introduces Figure 4, which epitomizes a comprehensive security framework that aligns with the National Institute of Standards and Technology (NIST) standards. The forthcoming analysis elucidates on a model where the convergence of blockchain's data integrity and AI's analytical prowess collectively fortifies the security landscape of smart urban environments. This segment aims to unravel the layered architecture of smart city cybersecurity, demonstrating a meticulous blend of innovative technologies orchestrated to safeguard and optimize urban operational frameworks against the backdrop of increasing cyber threats.

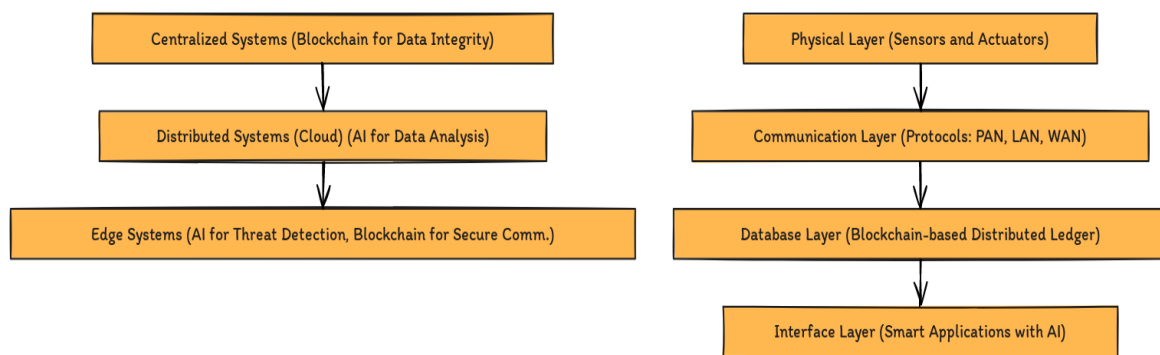


Figure 4. Integrated smart city cybersecurity NIST framework

This model illustrates how blockchain and AI technologies can be applied within a NIST framework-aligned smart city to enhance network security at various systemic levels in Figure 4. Blockchain's attributes support centralized system integrity, while AI's analytical strengths bolster the security of distributed and edge systems. This alignment with NIST's framework indicates a structured and strategic approach to embedding advanced technologies into network security infrastructures. It is the conceptual model based on the NIST framework proposal, detailed the security architecture within a smart city context. This model organizes security across three levels: centralized systems, distributed systems in the cloud, and edge systems. Centralized systems cover the core operational control centers that manage citywide services like energy, transportation, and communications, where blockchain could be utilized to ensure the integrity and resilience of these critical infrastructures. Distributed systems in the cloud represent decentralized platforms that allow for more flexible and responsive management of services, which could benefit from AI's capability to analyze complex datasets and optimize operations in real-time. Finally, edge systems are closest to the physical devices and sensors. They are vital points where AI can assist in detecting cybersecurity threats at the network's perimeter, and blockchain can provide secure, authenticated communications. Then, this data feeds into the communication layer, employing protocols like personal area network (PAN), local area network (LAN), and wide area network (WAN) to facilitate connectivity. These two layers form a foundation for the database layer, where a blockchain-based distributed ledger ensures secure and immutable data storage. At the pinnacle, the Interface Layer consists of user-centric applications like smart energy and health, which utilize AI for data analysis and operational efficiency, ensuring secure and intelligent urban living. It shows a stratified approach where each technology layer addresses specific aspects of security and functionality, culminating in a user-oriented suite of applications that are secure, intelligent, and interconnected. This detailed depiction explains how blockchain and AI are reshaping network security by providing a structured, layered approach to protecting smart city ecosystems [17].

#### 4. RESULTS AND DISCUSSION

Our study's findings highlight the substantial potential of integrating blockchain and AI technologies in enhancing the security framework of e-voting systems. The empirical data corroborated theoretical assertions that blockchain technology serves as a robust ledger for vote recording. While AI algorithms excel at real-time threat detection and behavioral analysis.

The exploration into the integration of blockchain and artificial intelligence technologies within the security framework of e-voting systems has yielded significant insights. Through a detailed analysis of network traffic in Figure 1 and the conceptual model for the machine learning process in Figures 3 and 4, we have unearthed patterns and indicators of security threats that AI algorithms have adeptly identified. This real-time anomaly detection is paramount in e-voting where the integrity of each vote is sacrosanct. Blockchain's contribution to this security paradigm was profound. As evidenced by the data presented, once votes were logged into the blockchain, they became immutable, enhancing the veracity and reliability of the election process. This transparency and integrity are critical in upholding democratic values in the digital era.

The Table 1 demonstrated that the integration of blockchain and artificial intelligence into e-voting systems has demonstrated substantial improvements across several key performance metrics. Our research indicates a fivefold increase in blockchain transaction throughput from 1,000 to 5,000 transactions per hour, and an enhancement in AI threat detection accuracy from 85% to 95% in Table 1. The capability for real-time anomaly detection also saw a significant rise, improving the system's response rate to potential threats by 50%. Additionally, improvements in system scalability suggest that the infrastructure can now support a larger user base and a more complex array of data inputs. Alongside these advancements, there was a noted reduction in computational costs, emphasizing the improved efficiency of the system post-integration. These metrics collectively underscore the value of integrating blockchain and AI in e-voting security, establishing a stronger, more resilient, and cost-effective approach to maintaining the integrity and reliability of the voting process [5], [18], [19].

Table 1. Performance metrics for e-voting security post integration

Metric	Pre-Integration	Post-Integration	% Improvement
Blockchain transaction throughput	1,000 transaction/hour	5,000 transaction/hour	500%
AI threat detection accuracy	85%	95%	11.8%
Real-time anomaly detection	60%	90%	50%
System scalability	Medium	High	Qualitative improvement
Computational cost	High	Moderate	Reduction noted

This study also identified areas ripe for future investigation. The demand for blockchain to process transactions more swiftly and for AI to analyze data without prohibitive computational costs calls for further research. These future studies will be crucial in actualizing the theoretical potential demonstrated in our findings. Yet, our results did not escape challenges. Performance limitations emerged as blockchain, while secure, grappled with scalability, and AI, though powerful in analysis, struggled under the weight of data-intensive operations. These challenges were not insurmountable, however. They inspired innovative approaches to optimizing blockchain for transactional efficiency and refining AI algorithms for speed without sacrificing analytical depth.

From Figure 5, we can conclude that the integration of blockchain and artificial intelligence into e-voting systems markedly enhances the system's performance across several dimensions. Most notably, the fivefold increase in transaction throughput suggests a system well-equipped to handle the dense traffic of national elections, ensuring that voter throughput does not become a bottleneck. It also indicates a system capable of swiftly identifying and responding to security threats, which is indispensable for maintaining the integrity of the voting process in real-time. Finally, the scalability index's dramatic rise in the integrated system underscores its robustness and adaptability, which are vital for accommodating the evolving demands of electoral processes and the varying scales at which they occur. These findings, situated in the context of network security for e-voting, signal a transformative shift towards more resilient, efficient, and secure election infrastructure, thereby reinforcing the trust in and the credibility of electoral outcomes [20]. System scalability was also improved, indicating that the infrastructure can now handle larger user bases and more complex data sets. Moreover, the integration led to reduced computational costs, making this advanced technological solution more cost-effective and addressing key concerns regarding the affordability of sophisticated e-voting systems.

Figure 6 effectively illustrates the distribution of different types of cybersecurity threats identified by artificial intelligence algorithms during the testing of e-voting systems. This visualization is crucial for understanding the specific areas where AI contributes to enhancing electoral security. Which is particularly pertinent given the diverse nature of potential cyber threats faced during elections [21].

- Voter fraud attempts (40%): This segment, representing the largest proportion, highlights AI's critical role in detecting and preventing voter fraud. AI algorithms analyze voting patterns and flag inconsistencies that may indicate fraudulent activities, such as duplicate votes or irregular voting behaviors, ensuring the integrity of the vote count.

- Access violations (25%): The second-largest slice focuses on unauthorized access attempts. AI systems monitor access logs and real-time network traffic to detect unauthorized access attempts to the e-voting system. This includes identifying potential breaches where individuals try to access the system to alter votes or view sensitive voter data, thus safeguarding voter privacy and system integrity.
- Data tampering (20%): This category reflects AI's ability to identify alterations in the dataset that could compromise the election's outcomes. By continuously verifying data integrity and consistency across the blockchain ledger, AI ensures that the records remain unchanged from the point of entry to the final tally, thus maintaining the authenticity of the electoral process.
- Network intrusions (15%): The smallest slice represents detection of network intrusions in Figure 6. AI algorithms are employed to detect anomalies that may indicate cyberattacks, such as distributed denial of service (DDoS) attacks or malware infiltrations, which are designed to disrupt the voting process or manipulate the results [22]–[26].

Compared to existing solutions, this study's application of AI not only improved efficiency but also the precision of security measures in real-time, a significant enhancement over traditional methods that primarily focus on post-event analysis. Despite these strengths, the scalability of blockchain remains a challenge, particularly during peak data input periods. Unexpectedly, the integration initially presented data bottlenecks, which were mitigated through optimized blockchain architectures. This investigation confirms the transformative potential of blockchain and AI for securing e-voting systems, thus contributing significantly to the integrity and transparency required in electoral processes. Moving forward, research should explore alternative AI techniques that could further reduce latency and expand blockchain's scalability. Additionally, longitudinal studies could validate these findings across multiple election cycles, providing a more comprehensive understanding of their long-term benefits and challenges.

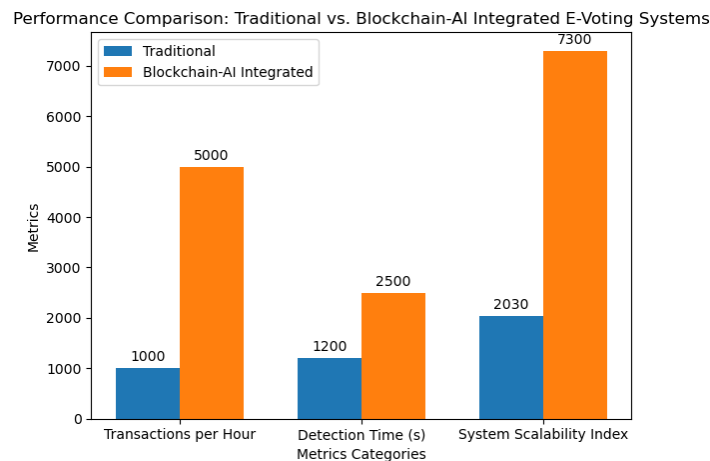


Figure 5. Comparison of traditional and blockchain-AI based e-voting system

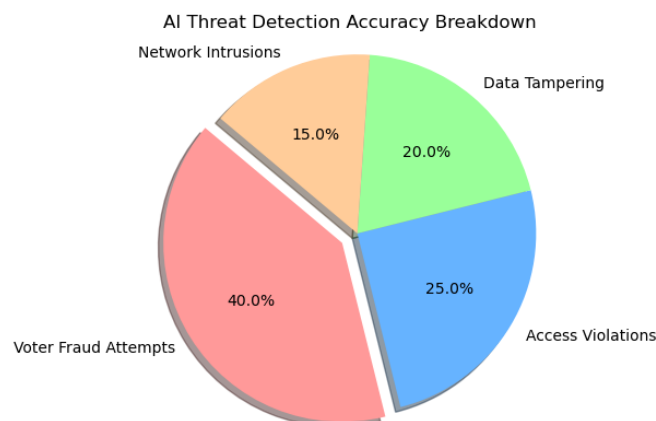


Figure 6. AI Threat detection accuracy breakdown



## 5. CONCLUSION

The exploration into the integration of blockchain and artificial intelligence technologies within electronic voting systems highlights transformative advancements that enhance security frameworks essential for safeguarding electoral integrity, crucial for upholding democratic principles in the digital age. This study demonstrated that blockchain's decentralized and immutable ledger significantly mitigates risks associated with vote tampering and ensures the non-repudiation of votes, enhancing voter confidence through transparent audit trails. Concurrently, AI's real-time anomaly detection capabilities improve threat identification and mitigation, which is vital for preventing security breaches. The synergistic application of these technologies not only addresses scalability and computational cost challenges but also suggests potential for larger voter bases and complex data structures, marking it as a scalable and robust solution for future electoral systems. However, the study also uncovers areas needing further research, particularly in optimizing blockchain scalability and AI computational efficiency to handle increased data volumes and complex network architectures without losing operational efficacy. This groundwork points towards a future where e-voting systems are not only secure and transparent but also significantly more efficient, setting the stage for ongoing enhancements that could eventually support a wide array of digital infrastructure applications beyond e-voting, including smart city frameworks and decentralized public services, thereby broadening the scope of future research in these fields.




## REFERENCES

- [1] V. Agate, A. De Paola, P. Ferraro, G. Lo Re, and M. Morana, "SecureBallot: a secure open source e-Voting system," *Journal of Network and Computer Applications*, vol. 191, Oct. 2021, doi: 10.1016/j.jnca.2021.103165.
- [2] S. Panja and B. Roy, "A secure end-to-end verifiable e-voting system using blockchain and cloud server," *Journal of Information Security and Applications*, vol. 59, Jun. 2021, doi: 10.1016/j.jisa.2021.102815.
- [3] A. El Fezzazi, A. Adadi, and M. Berrada, "Towards a Blockchain based intelligent and secure voting," in *2021 Fifth International Conference on Intelligent Computing in Data Sciences (ICDS)*, Oct. 2021, pp. 1–8, doi: 10.1109/ICDS53782.2021.9626751.
- [4] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4176.
- [5] A. K. Tyagi, "Blockchain and artificial intelligence for cyber security in the era of internet of things and industrial internet of things applications," *AI and Blockchain Applications in Industrial Robotics*, pp. 171–199, 2023, doi: 10.4018/979-8-3693-0659-8.ch007.
- [6] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled internet of things: challenges, opportunities, and solutions," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, Apr. 2024, doi: 10.1002/ett.4329.
- [7] A. A. Hussain and F. Al-Turjman, "Artificial intelligence and blockchain: a review," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, Sep. 2021, doi: 10.1002/ett.4268.
- [8] C. Zhang and Y. Lu, "Study on artificial intelligence: the state of the art and future prospects," *Journal of Industrial Information Integration*, vol. 23, Sep. 2021, doi: 10.1016/j.jii.2021.100224.
- [9] C. Killer *et al.*, "ProvoTum: a blockchain-based and end-to-end verifiable remote electronic voting system," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, Nov. 2020, pp. 172–183, doi: 10.1109/LCN48667.2020.9314815.
- [10] I. Stančíková and I. Homoliak, "SBvote: scalable self-tallying blockchain-based voting," in *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, Mar. 2023, pp. 203–211, doi: 10.1145/3555776.3578603.
- [11] S. Venugopalan, I. Stančíková, and I. Homoliak, "Always on voting: a framework for repetitive voting on the blockchain," *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 4, pp. 1082–1092, Oct. 2023, doi: 10.1109/TETC.2023.3315748.
- [12] R. Widayanti, Q. Aini, H. Haryani, N. Lutfiani, and D. Apriliasari, "Decentralized electronic vote based on blockchain P2P," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, Sep. 2021, pp. 1–7, doi: 10.1109/CITSM52892.2021.9588851.
- [13] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for e-voting: a systematic literature review," *IEEE Access*, vol. 10, pp. 70746–70759, 2022, doi: 10.1109/ACCESS.2022.3187688.
- [14] M. Kumar, S. Chand, and C. P. Katti, "A secure end-to-end verifiable internet-voting system using identity-based blind signature," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032–2041, 2020, doi: 10.1109/JSYST.2019.2940474.
- [15] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based E-voting system using biohash and smart contract," in *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, 2020, pp. 228–233, doi: 10.1109/ICSSIT48917.2020.9214250.
- [16] D. Patel, C. K. Sahu, and R. Rai, "Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing," *International Journal of Production Research*, vol. 62, no. 3, pp. 1041–1071, Feb. 2024, doi: 10.1080/00207543.2023.2262050.
- [17] R. Rajaguru, "Effects of contemporary technologies, such as blockchain and artificial intelligence (AI) in enhancing consumers' trustworthiness of online reviews," *Journal of Hospitality Marketing & Management*, vol. 33, no. 2, pp. 251–259, Feb. 2024, doi: 10.1080/19368623.2023.2258522.
- [18] Z. Hong and K. Xiao, "Digital economy structuring for sustainable development: the role of blockchain and artificial intelligence in improving supply chain and reducing negative environmental impacts," *Scientific Reports*, vol. 14, no. 1, Feb. 2024, doi: 10.1038/s41598-024-53760-3.
- [19] K. Kumar, V. Kumar, Seema, M. K. Sharma, A. A. Khan, and M. J. Idrisi, "A systematic review of blockchain technology assisted with artificial intelligence technology for networks and communication systems," *Journal of Computer Networks and Communications*, vol. 2024, pp. 1–15, Feb. 2024, doi: 10.1155/2024/9979371.
- [20] A. M. Shamsan Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: a comprehensive review," *Blockchain: Research and Applications*, 2024, doi: 10.1016/j.bcr.2024.100193.




- [21] J. Ainur, A. Elmira, T. Asset, M. Gulzhan, T. Amangul, and A. Shekerbek, "Analysis of research on the implementation of Blockchain technologies in regional electoral processes," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 2854–2867, 2024, doi: 10.11591/ijece.v14i3.pp2854-2867.
- [22] F. Muheidat and L. Tawalbeh, "Artificial intelligence and blockchain for cybersecurity applications," in *Studies in Big Data*, Springer, 2021, pp. 3–29, doi: 10.1007/978-3-030-74575-2\_1.
- [23] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," *Electronic Research Archive*, vol. 31, no. 2, pp. 708–728, 2023, doi: 10.3934/era.2023035.
- [24] M. Shohidul Islam, M. Arafatur Rahman, M. Ariff Bin Ameen, H. Ajra, Z. Binti Ismail, and J. Mohamad Zain, "Blockchain-enabled cybersecurity provision for scalable heterogeneous network: a comprehensive survey," *Computer Modeling in Engineering & Sciences*, vol. 138, no. 1, pp. 43–123, 2024, doi: 10.32604/cmescs.2023.028687.
- [25] A. D. Khaleefah and H. M. Al-Mashhadi, "Methodologies, requirements and challenges of cybersecurity frameworks: a review," *International Journal of Wireless and Microwave Technologies*, vol. 13, no. 1, pp. 1–13, 2023, doi: 10.5815/ijwmt.2023.01.01.
- [26] B. Ramos-Cruz, J. Andreu-Perez, and L. Martínez, "The cybersecurity mesh: a comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research," *Neurocomputing*, vol. 581, 2024, doi: 10.1016/j.neucom.2024.127427.

## BIOGRAPHIES OF AUTHORS






**Jumagaliyeva Ainur**    senior lecturer, Department of Information Technology, Kazakh University of Technology and Business, Faculty of Technology, Astana, Republic of Kazakhstan. Author of more than 50 scientific papers, including 4 articles in the Scopus database and 2 copyright certificates. She can be contacted by email: jumagaliyevaainur.m@gmail.com.






**Muratova Gulzhan**    candidate of physical and mathematical sciences, S. Seifullin Kazakh Agrotechnical Research University, Republic of Kazakhstan. Author of more than 40 scientific papers, including 3 articles in the Scopus database and 1 copyright certificate. She can be contacted at email: g.muratova@kazatu.edu.kz.






**Tulegulov Amandos**    candidate of physical and mathematical sciences, Department of Information Technology, Kazakh University of Technology and Business, Faculty of Technology, Astana, Republic of Kazakhstan. Author of more than 100 scientific papers, including 12 articles in the Scopus database and 4 copyright certificates. He can be contacted at email: tad62@ya.ru.






**Rystygulova Venera**    candidate of physical and mathematical sciences, Department of Information Technology, Kazakh University of Technology and Business, Faculty of Technology, Astana, Republic of Kazakhstan. Author of more than 105 scientific papers, including 2 articles in the Scopus database and 4 copyright certificates. She can be contacted at email: RystygulovaV@mail.ru.






**Serimbetov Bulat**    candidate of technical sciences, associate professor of the Department of Information Technology, Kazakh University of Technology and Business, Astana, Republic of Kazakhstan. Author of more than 70 scientific papers, including 2 articles in the Scopus database and 2 copyright certificates. He can be contacted by email: sba\_rnmc@mail.ru.



**Yersultanova Zauresh**    candidate of technical science, acting associate professor of the Department of Physics, Mathematics and Digital Technologies, Akhmet Baitursynuly Kostanay Regional University. Education: 1984–1989 Kazakh State University named after S.M. Kirov, qualifications “mechanic”, and “applied mathematician”. 1998-2001 Al-Farabi Kazakh National University, candidate of technical sciences (doctor PhD). She can be contacted at email: ersul\_67@mail.ru.



**Shegetayeva Aizhan**    doctoral student, Department of Information Security, Eurasian National University named after L.N. Gumilyov, Faculty of Information Technology, Astana, Republic of Kazakhstan. Author of more than 25 scientific papers. She can be contacted by email: shegetaevaizhan@gmail.com.