SECURE VOTING SYSTEMS USING BLOCKCHAIN

Vijay Kumar Sharma[1], Mohit saini[2], Rohit kumar[3]
[1]Assistant professor,[2,3]Research scholar
[1,2,3,]Department of computer science
Arya college of engineering, Jaipur, Rajasthan

Abstract—In the ever-evolving digital landscape, cybersecurity threats are becoming increasingly complex, persistent, and sophisticated. From advanced persistent threats (APTs) to zero-day vulnerabilities and insider attacks, the arsenal of cyber adversaries continues to expand. Traditional cybersecurity measures, including rule-based and signature-based Intrusion Detection Systems (IDS), often fall short in detecting and mitigating these evolving threats. These conventional systems are heavily reliant on pre-defined rules and known attack signatures, making them ineffective against novel or previously unseen attack patterns. As cybercriminals employ more dynamic and adaptive strategies, there arises an urgent need for smarter, more agile security mechanisms capable of identifying subtle anomalies and adapting in real-time.

Artificial Intelligence (AI), encompassing machine learning, deep learning, and other intelligent computational techniques, is increasingly being recognized as a transformative force in the field of cybersecurity. AI-powered Intrusion Detection Systems introduce a paradigm shift by enabling systems to learn from historical data, identify complex patterns, and detect anomalies that deviate from normal behavior—even if those anomalies do not match any known signature. By leveraging vast amounts of network traffic data, AI models can be trained to distinguish between legitimate and malicious activities with remarkable accuracy. Unlike traditional IDS, which are often reactive in nature, AI-driven IDS possess the potential to be predictive, proactively identifying and neutralizing threats before significant damage occurs.

By providing a comprehensive overview of the current landscape, this paper aims to inform cybersecurity researchers, professionals, and policymakers about the transformative role AI is playing in reshaping IDS technologies. As cyber threats continue to evolve, so too must our defense mechanisms—and the integration of AI represents a crucial step toward building more robust, intelligent, and adaptive cybersecurity systems.

Keywords— Artificial Intelligence, Intrusion Detection System, Cybersecurity, Anomaly Detection, Machine Learning, Deep Learning, Threat Detection, AI Security, Network Monitoring, IDS Architectures.

1. Introduction

In the digital age, organizations and individuals are increasingly dependent on interconnected systems and networks for communication, commerce, and data storage. This growing reliance on digital infrastructure has led to a dramatic increase in the volume and complexity of cyber threats. Cybercriminals now employ sophisticated techniques, including advanced persistent

threats (APTs), polymorphic malware, zero-day exploits, and social engineering, to breach security defenses. In response to this evolving threat landscape, cybersecurity mechanisms must also evolve to be more intelligent, adaptable, and proactive.

Intrusion Detection Systems (IDS) are vital components in the cybersecurity ecosystem. Their primary function is to monitor network and system activities for malicious actions or policy violations. However, traditional IDS solutions, primarily based on static rules or known signatures, are becoming less effective. These systems often struggle with high false positive rates and fail to detect previously unknown or zero-day attacks. Moreover, as attackers use encrypted communications, stealth techniques, and multi-vector attacks, it becomes increasingly difficult for signature-based systems to keep up.

Artificial Intelligence (AI), with its ability to learn from data, identify hidden patterns, and adapt over time, presents a compelling solution to these challenges. AI-powered IDS systems leverage machine learning (ML), deep learning (DL), and other AI paradigms to not only detect known threats but also uncover anomalous behaviors that may indicate new or sophisticated attacks. These intelligent systems offer dynamic and context-aware detection, reducing false alarms and enhancing threat visibility across large and complex environments.

This section outlines the foundational concepts of IDS, explores the transformative impact of AI in this domain, and introduces the architecture of AI-driven IDS frameworks that are shaping the future of cyber defense.

2. What is an Intrusion Detection System?

An Intrusion Detection System (IDS) is a security solution designed to monitor and analyze computer systems or network traffic to detect signs of unauthorized access, misuse, or anomalies. IDS plays a crucial role in identifying potential security breaches in real-time and enabling rapid incident response.

Types of IDS

Host-Based Intrusion Detection System (HIDS):

HIDS operates at the individual host or device level. It monitors system logs, file integrity, and process behaviors to detect suspicious activities. HIDS is particularly useful for detecting insider threats and changes in critical system files.

Network-Based Intrusion Detection System (NIDS):

NIDS monitors and analyzes traffic across the entire network. It inspects packets as they traverse the network and looks for patterns indicative of attacks. NIDS is effective in detecting external threats, DDoS attacks, and malware propagation.

3. Detection Techniques

Signature-Based Detection:

This technique relies on predefined rules or patterns, known as signatures, to detect known threats. While efficient and fast, it is limited to recognizing only previously identified attack vectors and cannot detect new or modified threats.

Anomaly-Based Detection:

This method establishes a baseline of normal behavior and raises alerts when deviations from this baseline are detected. It is more suitable for detecting novel threats but can result in a higher number of false positives if not fine-tuned properly.

Advanced IDS systems often integrate both signature-based and anomaly-based methods to provide comprehensive coverage.

4. Role of AI in IDS

Artificial Intelligence enhances IDS by enabling systems to learn from data, make intelligent decisions, and improve over time without explicit human intervention. The integration of AI allows IDS to overcome the limitations of traditional approaches by providing adaptive, scalable, and accurate threat detection.

Key AI Techniques in IDS

Machine Learning (ML)

ML algorithms can classify network traffic as benign or malicious based on historical data. Commonly used ML techniques in IDS include:

Decision Trees: Provide a transparent and interpretable model for classification.

Support Vector Machines (SVM): Excellent for handling high-dimensional data.

K-Nearest Neighbors (KNN): Classifies traffic based on similarity to known examples.

Random Forests: Combines multiple decision trees to improve classification accuracy.

Deep Learning (DL)

DL models can capture complex, non-linear patterns in data, making them effective in detecting sophisticated threats. Popular DL models include:

Convolutional Neural Networks (CNNs): Useful in extracting spatial features from traffic data or logs.

Recurrent Neural Networks (RNNs): Well-suited for sequential data analysis, such as monitoring time-series events.

Long Short-Term Memory (LSTM): A type of RNN that excels at learning long-term dependencies, making it ideal for identifying persistent threat patterns over time.

Unsupervised Learning

Techniques like clustering and dimensionality reduction can discover hidden structures in unlabeled data. This is particularly useful for identifying zero-day attacks or unknown threat behaviors.

Reinforcement Learning (RL)

RL models learn optimal strategies for intrusion detection through trial-and-error and reward-based feedback mechanisms. This dynamic approach allows the IDS to adapt and improve its accuracy over time.

Through these AI techniques, IDS becomes more resilient, flexible, and capable of managing large-scale, complex datasets with minimal human oversight.

5. AI-Based IDS Architecture

An effective AI-based IDS is designed with a modular and layered architecture to support data collection, processing, learning, and decision-making. The general architecture typically includes the following key components:

1. Data Collection Layer

This layer gathers raw data from various sources, including:

Network traffic logs (e.g., TCP/IP packets)

System event logs

Application logs

Host-based monitoring tools

Data can be collected in real-time or at scheduled intervals, depending on the system's requirements.

2. Preprocessing Layer

Before feeding the data into AI models, preprocessing is essential to ensure data quality and consistency. This includes:

Data cleaning to remove noise or irrelevant information.

Feature extraction and selection to identify the most informative attributes.

Normalization or standardization to ensure uniformity in scale.

Handling missing values and transforming categorical variables if needed.

This step significantly impacts the model's performance and accuracy.

3. Model Training and Learning Layer

In this stage, AI models are trained using historical datasets containing labeled instances of normal and malicious activity. Depending on the selected approach, models may be:

Supervised: Using labeled datasets.

Unsupervised: Learning from unstructured or unlabeled data.

Semi-supervised or hybrid: Combining both to enhance learning in environments with limited labeled data.

This layer is responsible for building intelligent models capable of recognizing known patterns and detecting new anomalies.

4. Detection Engine

This core component applies the trained model to real-time or incoming data to classify it as normal or suspicious. The detection engine uses:

Classification algorithms (for binary or multi-class classification)

Clustering techniques (for anomaly detection)

Scoring mechanisms (to rank threat severity)

In modern systems, detection is continuous and adaptive, with models periodically retrained to incorporate the latest threat intelligence.

5. Alerting and Response Layer

Once a threat is detected, this layer:

Generates alerts for security teams with relevant details (IP, port, timestamp, etc.).

Initiates automated response mechanisms (e.g., blocking IPs, isolating endpoints).

Logs incidents for future analysis and forensic investigations.

Integration with Security Information and Event Management (SIEM) tools or orchestration platforms enhances the response efficiency.

Recent examples

The integration of Artificial Intelligence into Intrusion Detection Systems has moved beyond theoretical models and academic prototypes into practical, real-world deployments. Several case studies and implementations highlight the effectiveness of AI-based IDS in detecting and responding to modern cyber threats across diverse environments.

One notable contribution in this area comes from the Canadian Institute for Cybersecurity, which developed the CICIDS2017 dataset—a comprehensive and realistic dataset designed specifically to train, evaluate, and benchmark AI-driven intrusion detection models. Unlike earlier datasets that often lacked diversity and real-world complexity, CICIDS2017 simulates genuine network traffic, combining both benign and malicious activity over multiple days. It includes various attack scenarios such as Distributed Denial of Service (DDoS), brute-force attacks, botnet communications, port scans, and web-based intrusions, thereby providing a rich environment for training AI models.

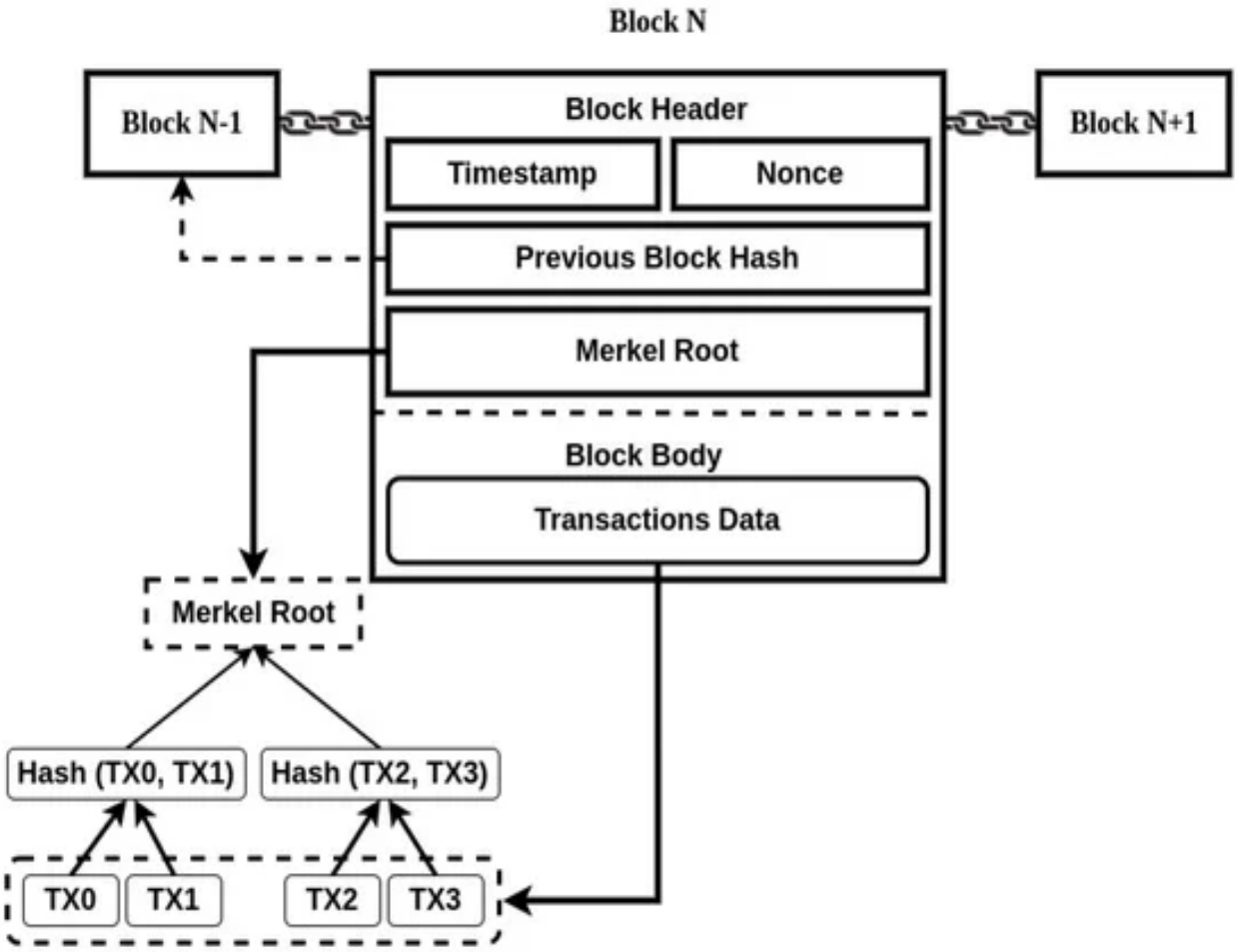
In a significant case study, a Deep Neural Network (DNN) was trained using the CICIDS2017 dataset to evaluate its capability in real-time intrusion detection. The results were impressive—the model achieved over 98% accuracy in detecting and classifying malicious traffic, with high precision and low false positive rates. This performance underscores the strength of deep learning architectures in capturing complex patterns and correlations within high-dimensional data that traditional IDS might overlook. The model was particularly effective in identifying previously unseen variants of DDoS and brute-force attacks, demonstrating AI's ability to generalize beyond the training data. Moreover, its deployment in a simulated enterprise environment showed that the system could analyze and respond to threats in real-time, significantly improving the organization's threat visibility and incident response efficiency.

Another compelling example of AI in action is IBM's QRadar Advisor with Watson, a commercial Security Information and Event Management (SIEM) solution that integrates cognitive AI capabilities for advanced threat detection and investigation. Watson, IBM's AI platform, processes massive volumes of structured and unstructured security data—including

threat intelligence feeds, attack patterns, vulnerability databases, and even natural language sources such as blogs and whitepapers—to provide contextual insights during incident analysis.

When integrated with QRadar, Watson acts as a virtual security analyst. Upon detecting a suspicious event, QRadar triggers Watson to automatically investigate the incident. Watson correlates the alert with historical attack data, identifies relationships among indicators of compromise (IOCs), and evaluates the potential impact based on past incidents and global threat intelligence. This drastically reduces the time security teams spend on manual correlation and triage, enabling them to focus on high-priority threats. In production environments, organizations have reported that QRadar Advisor has cut incident investigation times by up to 60%, allowing for faster containment and mitigation.

These real-world implementations demonstrate the tangible benefits of AI in IDS: from increasing detection accuracy and reducing false positives, to accelerating incident response and scaling security operations. As the volume and sophistication of cyber threats continue to grow, such intelligent systems are not just enhancements—they are becoming essential components of modern cybersecurity infrastructure.



6. Opportunities and Benefits

Advantages of AI-Based Intrusion Detection Systems

The integration of Artificial Intelligence into Intrusion Detection Systems offers a wide range of advantages that significantly enhance their performance, efficiency, and adaptability in the face of growing cyber threats. Below are the key benefits, explained in detail:

1. Real-Time Threat Detection

AI-powered IDS are capable of identifying malicious activity as it happens, enabling organizations to respond immediately. Traditional IDS may experience delays due to the need for manual analysis or reliance on signature updates. In contrast, AI models—especially those employing deep learning and streaming analytics—can process and analyze large volumes of data in real time. This capability is essential in preventing attacks such as ransomware or data exfiltration, where even a few seconds can mean the difference between containment and catastrophe. Real-time detection ensures that suspicious activity is flagged and addressed before significant damage occurs.

2. Reduced False Positives

One of the major limitations of traditional IDS solutions is their high false positive rate, which can overwhelm security analysts with alerts that turn out to be harmless. AI-based IDS can intelligently distinguish between genuine threats and benign anomalies by learning from historical patterns and behavioral baselines. Machine learning algorithms improve over time, refining their understanding of normal vs. abnormal activity. This dramatically reduces noise in the alert system, allowing analysts to focus on real threats. In practice, AI has been shown to cut false positives by more than 50% in many environments, increasing the overall efficiency of security operations.

3. Scalability

In today's digital world, networks generate massive volumes of traffic from countless connected devices, cloud infrastructures, and distributed endpoints. AI-based IDS are inherently scalable and well-suited for handling such large datasets. They can process data from thousands of endpoints simultaneously and analyze millions of packets per second without performance degradation. Cloud-based AI solutions can also scale elastically based on demand, ensuring consistent monitoring across growing IT ecosystems. This makes AI-IDS especially valuable for large enterprises and service providers.

4. Adaptive Learning

Unlike static rule-based systems, AI-based IDS continuously learn and evolve. Using techniques like online learning and reinforcement learning, these systems can dynamically update their

models to reflect the latest threat landscape. When new forms of attacks are observed—such as novel variants of malware or evolving phishing tactics—AI can incorporate this knowledge into its detection logic without manual intervention. This adaptive capability ensures the IDS remains effective even in rapidly changing environments where threats evolve faster than traditional update cycles can handle.

5. Automation and Reduced Analyst Workload

AI introduces a high degree of automation into the intrusion detection process, significantly reducing the burden on cybersecurity teams. Tasks such as log analysis, anomaly correlation, threat prioritization, and even initial incident response can be handled autonomously. AI can also generate detailed reports and recommendations, allowing human analysts to focus on strategic decision-making and response planning. This not only saves time but also helps address the global shortage of skilled cybersecurity professionals by optimizing existing resources.

6. Predictive Capability

One of the most powerful aspects of AI-based IDS is their predictive ability. By analyzing historical attack data, user behavior, system activity, and global threat intelligence, AI can identify emerging trends and predict potential future attacks. Predictive models can forecast the likelihood of certain attack vectors being used against a particular system or user group, allowing organizations to proactively strengthen defenses. For example, if an AI system detects precursors to a ransomware attack—such as lateral movement or privilege escalation—it can alert teams or initiate automated countermeasures before the full attack is executed.

7. Challenges

While Artificial Intelligence significantly enhances the capabilities of Intrusion Detection Systems, it also introduces a new set of challenges and limitations that must be addressed for successful implementation and operation. These challenges span technical, operational, and ethical dimensions, impacting the overall effectiveness and trustworthiness of AI-based security solutions.

1. Data Quality and Availability

AI models are highly dependent on the quality and quantity of the data used for training and validation. In cybersecurity, obtaining rich, diverse, and well-labeled datasets is often difficult. Many datasets are synthetic or simulated, lacking the nuances of real-world traffic. Additionally, real intrusion data is often sparse or imbalanced, with a disproportionately low number of attack instances compared to normal traffic. This imbalance can cause the AI model to become biased, leading to poor detection performance, especially for rare or emerging threats. Furthermore, the lack of standardized datasets for benchmarking hinders consistent evaluation and comparison across different AI approaches.

2. High Resource Consumption

Advanced AI techniques, particularly deep learning models, require significant computational resources for training and deployment. These models may demand high-performance GPUs, large memory allocations, and extended processing times—resources that may not be readily available in all organizations. During inference (i.e., real-time detection), the need to process vast amounts of network traffic and system logs can strain system performance, potentially leading to delays or missed detections. This resource intensity poses a challenge for smaller enterprises or environments with limited IT infrastructure, making it difficult to adopt and sustain AI-based IDS solutions.

3. Vulnerability to Adversarial Attacks

AI models themselves can become targets of sophisticated adversarial attacks. Malicious actors can craft inputs—known as adversarial examples—that subtly manipulate traffic data to bypass detection without appearing suspicious. These carefully constructed data points exploit the weaknesses in the model's learning process, causing misclassification. For example, a slightly modified packet pattern might fool an AI model into classifying malicious traffic as benign. The susceptibility of AI to such manipulation represents a critical security risk and requires the development of robust and resilient models capable of withstanding adversarial interference.

4. Lack of Interpretability and Explainability

Many AI models, particularly deep learning systems like Convolutional Neural Networks (CNNs) or Long Short-Term Memory networks (LSTMs), operate as black boxes. They can provide highly accurate results but offer little to no insight into how a decision was reached. This lack of interpretability creates challenges for cybersecurity professionals who need to understand, verify, and trust the system's alerts. Without clear explanations, it becomes difficult to audit model decisions, troubleshoot errors, or meet compliance requirements. In critical sectors such as finance or healthcare, regulatory standards may demand transparent reasoning, which current AI models often fail to deliver.

5. Integration with Legacy Systems

Integrating modern AI-based IDS into existing security infrastructures—especially legacy systems—can be complex and resource-intensive. Legacy systems may lack the APIs, processing power, or architectural flexibility needed to support AI analytics. This often necessitates significant modifications or even complete system overhauls, increasing the cost and time required for deployment. Additionally, compatibility issues can arise when attempting to synchronize data flows between old and new components, leading to gaps in visibility and reduced effectiveness of the IDS.

6. Privacy and Ethical Concerns

AI-based IDS often require access to extensive network traffic, system logs, user behavior data, and even sensitive content to detect anomalies effectively. This deep level of monitoring raises significant privacy concerns, especially in environments with strict data protection regulations such as the General Data Protection Regulation (GDPR) or HIPAA. The indiscriminate collection and analysis of data can lead to the unintentional exposure of private or confidential information. Moreover, ethical concerns arise when AI decisions affect individuals, such as flagging specific users as suspicious based on learned patterns, which may reflect underlying biases in the data.

References

1. Singh, A., & Chatterjee, K. (2018, September). SecEVS: secure electronic voting system using blockchain technology. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 863-867). IEEE.
2. Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019, April). A comparitive analysis on e-voting system using blockchain. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-4). IEEE.
3. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.
4. Kumar, D. D., Chandini, D. V., Reddy, D., Bhattacharyya, D., & Kim, T. H. (2020). Secure electronic voting system using blockchain technology. International Journal of Smart Home, 14(2), 31-38.
5. Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., & Namratha, M. (2020, July). E-voting systems using blockchain: An exploratory literature survey. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 890-895). IEEE.
6. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. ACM Computing Surveys (CSUR), 54(3), 1-28.
7. Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M. H. (2018). Platform-independent secure blockchain-based voting system. In Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21 (pp. 369-386). Springer International Publishing.
8. Daraghmi, E., Hamoudi, A., & Abu Helou, M. (2024). Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine. Future Internet, 16(11), 388.
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. Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. IEEE Access, 10, 59959-59969.

11. Cheema, M. A., Ashraf, N., Aftab, A., Qureshi, H. K., Kazim, M., & Azar, A. T. (2020, November). Machine learning with blockchain for secure e-voting system. In 2020 first international conference of smart systems and emerging technologies (SMARTTECH) (pp. 177-182). IEEE.
12. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 01-09.
13. Sudharsan, B., MP, N. K., & Alagappan, M. (2019, October). Secured electronic voting system using the concepts of blockchain. In 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0675-0681). IEEE.
14. Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. Journal of King Saud University-Computer and Information Sciences, 34(9), 6855-6871.
15. Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), 53-62.
16. Pawade, D., Sakhapara, A., Badgujar, A., Adepu, D., & Andrade, M. (2020). Secure online voting system using biometric and blockchain. In Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1 (pp. 93-110). Springer Singapore.
17. Anitha, V., Caro, O. J. M., Sudharsan, R., Yoganandan, S., & Vimal, M. (2023). Transparent voting system using blockchain. Measurement: Sensors, 25, 100620.
18. Adiputra, C. K., Hjort, R., & Sato, H. (2018, October). A proposal of blockchain-based electronic voting system. In 2018 second world conference on smart trends in systems, security and sustainability (WorldS4) (pp. 22-27). IEEE.
19. Teja, K., Shravani, M. B., Simha, C. Y., & Kounte, M. R. (2019, April). Secured voting through Blockchain technology. In 2019 3rd international conference on trends in electronics and informatics (ICOEI) (pp. 1416-1419). IEEE.
20. Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M., & Almusali, M. (2023). Privacy-preserving e-voting system supporting score voting using blockchain. Applied Sciences, 13(2), 1096.