Proceedings of the 5th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA-2026)
DVD Part Number: CFP26K58-DVD; ISBN: 979-8-3315-6199-4

AI-Driven Cryptographically Auditable Cloud-Based E-Voting System

1st S. Jeevitha
Assistant Professor
Department of Cyber Security
Mahendra Engineering
College(Autonomous),
Namakkal, India.
sjeevitha813@gmail.com

2nd N. Harishwar
UG Student
Department of Cyber Security
Mahendra Engineering
College(Autonomous),
Namakkal, India
harishwarn06@gmail.com

3rd S. DineshKumar
UG Student
Department of Cyber Security
Mahendra Engineering
College(Autonomous),
Namakkal, Inida
dineshkumar9092a@gmail.com

4th B. Gopinath
UG Student
Department of Cyber Security
Mahendra Engineering
College(Autonomous),
Namakkal, India
gopinath4851@gmail.com

5th J. Dineshwar
UG Student
Department of Cyber Security
Mahendra Engineering
College(Autonomous),
Namakkal, TamilNadu.
vigneshdinesh@gmail.com

ABSTRACT - Secure, transparent, and auditable digital elections cannot be done without advanced cloud-based e-voting systems. Traditional voting and legacy electronic voting systems, however, are frequently vulnerable to security breaches, lack of auditability, are centralised and prone to fraud. To overcome these obstacles, the proposed AI E-Voting System is designed to adopt a multi-layered security approach, which will improve the integrity, reliability, and confidence of the voting process. The AI E-Voting System proposed includes multiple layers of security to ensure the election process is secure and trustworthy. Voter authentication is done in the initial stage with Multi-Factor Authentication (MFA), requiring the voter to put in their credentials and an extra verification factor to ensure that the voter is not being registered by an imposter. Once authenticated, the voter eligibility will be checked by a Domain-Specific Language (DSL) that will predefine rules based on the attributes like Department, Age, Designation, authorized voter groups, etc. and only voters who meet those criteria will be allowed to vote in a particular election. Eligibility verification is followed by vote recording using the a SHA-256-based cryptographic hash-chaining mechanism that generates a tamper-evident and independently verifiable audit trail for recorded votes. In addition, an AI-based Behavioural Analytics (AIBA) module constantly monitors users' interaction patterns with the machine, such as mouse movements, the intervals between clicks and the timing of user actions, to identify and block automated and fraudulent voting in real time. Experimental assessment proves higher voter authentication, genuine eligibility verification, effective counter fraud, greater vote integrity and high scale up with low operational cost and near zero latency. The proposed system is a safe, efficient and reliable solution for the electronic voting system in modern institutional applications.

Keywords: Cloud Security, Election Integrity, Voter Authentication, Data Privacy, Fraud Prevention, Trust Management, Secure Access Control, Digital Democracy, System Reliability.

I. INTRODUCTION

Blockchain technology plays a pivotal role in the evolution of secure and transparent electronic voting systems, offering a layer of integrity and tamper resistance to data storage that is crucial for trust. By providing a layer of transparency and tamper resistance to data storage, blockchain technology has emerged as a fundamental building block for developing secure and transparent electronic voting systems, ensuring a level of trust in the voting process. It can be used to facilitate a distributed verification system that fosters trust and decreases reliance on a centralized authority. Blockchain could be well suited for current secure voting applications due to these properties [1]. Additionally, decentralized electronic voting systems provide enhanced security measures such as the absence of single points of failure and the ability to validate voting records peer-to-peer. This enhances transparency and offers auditable mechanisms of all voting transactions. They also solve significant problems in the conventional centralized voting systems [2].

Smart Contract-Based Voting Systems: They add automation to the voting process by running predetermined conditions. These contracts ensure that only valid conditions are counted and increase system reliability and decrease any operational errors. This helps to optimize the process of conducting elections and ensures uniformity [3]. Incorporating multimodal authentication and optimized contract execution methods, advanced e-voting blockchain systems boost the security of voter verification and system efficiency. All of these techniques guarantee that only voting individuals are allowed to vote and that the voting process is scalable in large-scale elections. They also help to enhance the processing speed and secure the handling of votes [4]. In e-voting, AI technologies are being adopted to enhance authentication and prevent fraudulent activities on the fly. The intelligent models analyze user interaction patterns and detect anomalies and thwart unauthorized access [5].

A. Objectives

- To create a secure e-voting system based on cloud computing technology based on Multi Factor Authentication for secure user logins.
- To make sure that only eligible voters can vote, following a rule-based Domain-Specific Language approach.
- To ensure the integrity of votes and that the votes are not tampered with, via SHA-256 hash chaining.
- To identifies fraudulent and machine voting in real-time through artificial intelligence (AI) based behaviour pattern analysis.

B. Contributions

This paper proposes an e-voting system which has authentication, eligibility checking and fraud detection all in one system. It enhances the security and trust of electronic voting through the use of AI and cryptography. The system is efficient and expandable, and appropriate for institutional elections.

C. The organization of the paper

The paper is organised as follows. The related works and the existing problems of e-voting systems are explained in section 2. The proposed system design and working are discussed in section 3. The result and discussion have been included in the Section 4 and Future scope and conclusion are included in the Section 5 respectively.

II. RELATED WORK

The author [6] discussed the fusion of Artificial Intelligence (AI) and Blockchain Technology (BT) for enhancing the security of an e-voting network. The proposed framework uses pattern recognition, anomaly detection, and machine learning (ML) algorithms to detect any malicious activities in the voting network. Combining Blockchain with AI creates a powerful alliance for securing data immutability and transparency, along with better threat detection and risk assessment. The system enhances security in case of cyber-attacks and manipulation of votes. In [7] a secure authentication system is proposed with the use of AI Facial Recognition (FR) for voter verification. The model is based on deep learning (DL), Convolutional Neural Networks (CNNs) and biometric feature extraction techniques for verifying voter identities. To mitigate impersonation and identity fraud, multi-factor authentication mechanisms are needed. The system uses fingerprint and facial biometrics to verify voters and the blockchain technology for decentralized and tamper-proof vote storage in [8].

Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) are applied to analyse the sequential biometric patterns at the same time increasing the accuracy of the authentication process over time. In [9] a novel block chain-based voting platform using AI (Artificial Intelligence) is presented for secure and transparent voting. The framework has real-time verification, smart contracts (SCs), and AI-based verification systems to ensure the authenticity of voting transactions. The blockchain keeps voting data secure and unalterable, and AI constantly checks the system's integrity. A blockchain-based e-voting system, which combines voter authentication by using Face Recognition (FR), is presented in [10]. The architecture that is proposed includes image processing, deep neural networks (DNNs), and DLT for securing the election process. Facial biometric verification ensures that no multiple voting and no unauthorized access is made. This blockchain and FR partnership contributes to a more reliable and trustworthy electoral process.

TABLE 1: COMPARATIVE ANALYSIS AI-ENABLED BLOCKCHAIN-BASED E-VOTING SYSTEM

Ref.	Method	Security Features	Advantages	Limitations
[11]	Decentralized Biometrically Secured E-Voting Framework	Biometric voter authentication, hybrid encryption, decentralized vote storage	Ensures strong voter verification and data confidentiality	Higher computational complexity due to encryption processes
[12]	Privacy-Preserving Scalable Blockchain E-Voting System	Privacy preservation, tamper-proof records, scalable architecture	Supports large-scale elections with enhanced transparency	Network and transaction delays may affect efficiency
[13]	AI-Powered Security and Privacy Framework for E-Governance	Intelligent threat detection, privacy protection, anomaly monitoring	Improves security through adaptive AI-based analysis	Not specifically optimized for e-voting environments
[14]	Blockchain-Based Voting System	Immutable ledger, decentralized verification, secure vote recording	Provides transparency, integrity, and auditability	Limited support for advanced voter authentication
[15]	AI-Powered Security and Privacy Framework for Multimedia and Multimodal Data	Intrusion detection, privacy preservation, secure data processing	Enhances security monitoring and data protection	Requires significant computational resources

Table 1 presents a comparative of AI- and blockchain-enabled e-voting security frameworks. The reviewed studies focus on improving election security through techniques such

as biometric authentication, privacy-preserving mechanisms, decentralized vote storage, and intelligent threat detection. Most approaches enhance transparency, voter verification, and protection against tampering, while also addressing privacy concerns. However, challenges such as computational overhead, scalability issues, and increased system complexity remain important considerations for practical deployment in large-scale electronic voting environments.

III. PROPOSED METHODOLOGY

The proposed AI E-Voting System will have a multi-layered security architecture to secure, transparent and reliable digital elections. Voter authentication is done by Multi-Factor Authentication (MFA), and Voter Eligibility is done by a custom Domain-Specific Language (DSL) based on the election criteria in a predefined manner. After being validated, votes are safely stored according to a hash-chaining system, with SHA-256 cryptography, thus generating an audit trail, which is unchangeable and not vulnerable to tampering. AI-Based Behavioural Analytics module (AIBA) keeps an eye on users' interaction patterns and automatically identifies and prevents fraudulent or automated voting throughout the process.

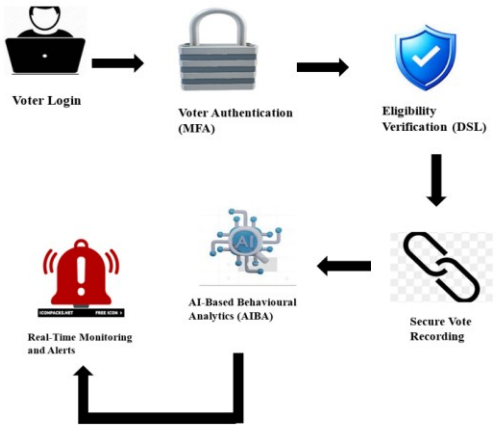


Figure 1: AI-Driven Secure E-Voting System Architecture

The proposed of secure e-voting system is shown in Figure 1, which is based on artificial intelligence. The platform will initially allow voters to log into the site via secure login process and then via Multifactor Authentication (MFA) to verify the voter's identity. It then checks the eligibility with a decentralized security layer (DSL) before approving submission of votes. Once verified, votes are securely recorded and protected through mechanisms based on blockchain in order to guarantee the integrity and transparency of the process. Additionally, AI Based Behavioural Analytics (AIBA) is used to continuously monitor voting activities and the real-time monitoring and alert module will be used to detect suspicious activity and provide security alerts to ensure a secure electoral environment.

A. Multi-Factor Authentication (MFA)

To ensure the identity of voters prior to access on the voting platform, Multi-Factor Authentication (MFA) is used. The voter enters his or her login information and has a further verification step to ensure that there is no unauthorized access. This process will increase the security of the accounts and make sure only the rightful ones so that only a valid user can cast their vote. MFA highly diminishes the likelihood of ID theft and the possibility of being cast a ballot by somebody you never recognized.

$$PV = Verify(P, H) \quad (1)$$

The voter's password entered is compared with the stored hashed password to ensure the voter's identity in equation (1).

$$OV = (OTP_u = OTP_s) \quad (2)$$

The OTP entered by the user is checked against a system-generated OTP to carry out second factor authentication in equation (2)

$$AS = PV + OV \quad (3)$$

In equation (3), the authentication score is based on the results of password verification, combined with the OTP validation result.

$$AA = \begin{cases} 1, & AS = 2 \\ 0, & AS < 2 \end{cases} \quad (4)$$

Access will be denied if any of the authentication factors failed or will be denied if they are met in equation (4).

B. Domain-Specific Language (DSL) Verification

Once authenticated, voter eligibility checks are performed with a Domain-Specific Language (DSL) custom written. The DSL is based on some pre-defined rules based on the department, age, designation and authorized voter groups. Voters that meet specific requirements are only allowed to use the ballot. This mechanism allows for voter verification with accuracy and based on rules.

$$R_s = \sum_{i=1}^{n} w_i \, r_i \quad (5)$$

DSL checks several eligibility criteria and assigns a voters' rule-matching score that is a cumulative total of how they match the rules in equation (5).

$$C_e = \frac{M_r}{T_r} \quad (6)$$

Eligibility confidence is computed as the ratio between number of matched rules (M_r) and number of total rules (T_r) in equation (6).

$$E_v = \begin{cases} 1, & C_e \geq \theta \\ 0, & C_e < \theta \end{cases} \quad (7)$$

The voter is made eligible just if the voter's eligibility confidence is greater than the set threshold (θ) in equation (7).

$$V_a = V_u \cap V_l \quad (8)$$

The system checks if the user (V_u) is in the list of approved voters (V_l) in the DSL rules in equation (8).

C. SHA-256 Hash Chaining

If a voter is found to be eligible the votes are stored securely using a SHA-256 hash-chaining mechanism. Every vote is secured by a cryptographic chain to the previous vote, making it tamper-resistant and unalterable for one to trace back the voting process. This will help to ensure the integrity of the votes and helps to prevent unauthorised changes in voting records. The audit trail can also be used to verify independently and ensure the transparency of elections.

$$H_0 = SHA256(B_0) \quad (9)$$

The equation (9) represents the creation of first hash in the chain. Voter ID, Timestamp, or Vote Metadata is passed through the SHA-256 to get the first hash value H_i.

$$H_i = SHA256(H_{i-1} \;||\; B_i) \quad (10)$$

In equation (10), B_i is concatenated (||) with the previous one H_{i-1}. Then a new hash H_i is created using the SHA-256 function.

$$V_i^{secure} = SHA256(V_i \;||\; T_i \;||\; H_{i-1}) \quad (11)$$

V_i is combined with the previous hash $H_{i-1}$and timestamp T_i. It ties the vote in with the time and history of the chain of votes, so that if the vote or time changes, then the hash chain is broken in equation (11).

D. AI-Based Behavioural Analytics (AIBA)

The AI-Based Behavioural Analytics (AIBA) module, which is a real-time voter interaction analysis module, tracks voter interaction patterns throughout the voting process. It observes the movement of the mouse, the interval between the pressing of keys and the timing behaviour to detect suspicious or automated behaviour. Real-time detection of any abnormal behaviour and flagging it up as a possible fraud attempt. This method would further boost the security of the election as it will stop bot voting and fraudulent voting.

The AIBA model uses only features of behavioral interaction and does not use the figures of constituency-level elections such as name of the candidate, political party, total votes received, or percentage of votes received. For each voting session, collected behavioral features are represented in the following ways:

$$X_i = \{M_i, C_i, K_i, T_i, N_i, R_i\} \quad (12)$$

where Equation (12) M_i denotes mouse movement characteristics, C_i represents click interval patterns, K_i denotes keystroke timing, T_i represents typing behavior, N_i denotes navigation sequences, and R_i represents response and interaction timing. These features are analysed by the AIBA model to distinguish normal human voting behaviour from anomalous or automated interaction patterns.

$$K_f = \frac{1}{n}\sum_{i=1}^{n}(t_{release_i} - t_{press_i}) \quad (13)$$

The equation (13) determines the mean duration of the keystrokes in this formula. Measures the amount of time between key press/key release events. This pattern is then used by the AI system to detect if typing activity is by a true user or a bot.

$$M_v = \frac{\Delta x + \Delta y}{\Delta t} \quad (14)$$

The equation (14) calculates the speed of mice in terms of changes in its x and $y$coordinates over time.

$$B_d = \sqrt{(K_f - \mu_k)^2 + (M_v - \mu_m)^2} \quad (15)$$

The equation (15) quantifies the deviation of the users' activity from the normal user behaviour. It makes a comparison between the value of the keystroke and mouse movements at the moment and the average (μ_k, μ_m).

$$P_f = \sigma(w_1 K_f + w_2 M_v + w_3 T_b) \quad (16)$$

The equation (16) computes the chance of fraudulent activity. Combined with weights (w_1, w_2, w_3) are keystroke dynamics (K_f), mouse velocity (M_v) and timing behaviour (T_b).

IV. Result and Discussion

The results of the experiment highlight that the proposed AI E-Voting System has greatly improved the security and reliability of the voting process. This is an effective way to enhance voter authentication and ensure that only authorized users can gain access to and use the system. The eligibility verification system properly weeds out voters by following set organisation rules, which decreases invalid voting. The votes are kept in secure and tamper-proof boxes, which ensure that the voting process is transparent and reliable. AI-based monitoring is also able to effectively identify fraudulent and unusual voting patterns in real time. The system's performance is efficient, scalable, and has a low latency, while it has a good security performance which is appropriate for the institutional e-voting applications. In this process, there are two distinct data sources being used for the experiments. The data concerning elections are utilized for processing the election information and the eligibility rules, while the behavioural interaction data are used solely for the training and evaluation of AIBA module. The separation of the data helps to avoid the situation when the election outcomes are used for any behavioural attributes and ensures that the behavioural analytics model is created based on real features of interactions with users.

A. Dataset Description

i. Election Dataset

The dataset that pertains to elections consists of many components such as constituency information, candidate name, party information, total votes, and vote percentage. In the suggested approach, these components are not used for training the AI-Based Behavioral Analytics (AIBA) module, but are utilized for election information management and for enabling eligibility processing.

ii. Behavioural Interaction Dataset for AIBA

An exclusive dataset of behavioural interaction is utilized for creating and testing the AI-Based Behavioural Analytics (AIBA) module. The features included in this dataset pertain to user–system interaction variables, including mouse motion tracks, speed of cursor movement, click rates, timing of keystrokes, speed of typing, duration of the login, path followed in voting, and the time taken to submit the votes. Data pertaining to users is harvested from the voting-session interaction controlled for differentiating authentic human users from those working on scripted interactions.

B. Comparison Table

TABLE 2: EVALUATION OF MFA-BASED VOTER AUTHENTICATION

Evaluation Metric	Proposed MFA (%)
Authentication Success Rate	98.9
OTP Verification Success Rate	99.2
Password Verification Success Rate	99.4
False Acceptance Rate	0.6
False Rejection Rate	0.8

The performance of the proposed multi-factor authentication process based on password and OTP is shown in Table 2. The authentication was successful at the rate of 98.9%, where the OTP and the password had verification successes of 99.2% and 99.4%, respectively, while the false acceptance and rejection were 0.6% and 0.8%, respectively.

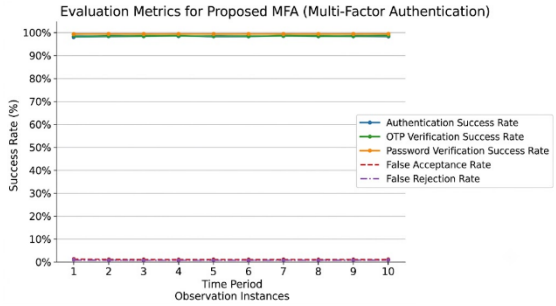


Figure 3. Evaluation Metrics of the Proposed MFA-Based Voter Authentication

The performance of the MFA technique is depicted in the illustration shown in Figure 3 with various parameter values. All success rates such as for authentication, OTP and password verification are high, and failure rates are very low. This means that the MFA mechanism is stable, trustworthy and secured for use in the voter authentication process.

TABLE 3: BEHAVIOURAL VERIFICATION PERFORMANCE COMPARISON

Method	Behavioural Verification Rate (%)
CNN	87.9
RNN	91.2
DNN	94.3
Proposed AIBA	98.6

Table 3 Represents the models' Behavioral verification performance. The CNN, RNN and DNN models used so far, obtained the verification rates of 87.9%, 91.2% and 94.3% respectively. The proposed AIBA framework recorded the highest verification rate of 98.6% which guarantees that only authorized and eligible voters are to vote in Elections. The findings suggest that the voters' validation accuracy and reliability have been enhanced.

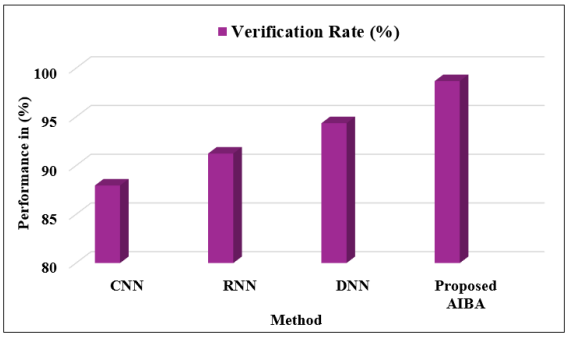


Figure 4: Behavioural Verification Performance

The effectiveness of various models to validate voter eligibility prior to voting is shown in Figure 4. The Behavioural verification performance gradually approaches the voter validation rules defined, showing that the approaches evaluated perform better. The proposed AIBA framework has the greatest verification power since it correctly assesses voters' attributes and qualification criteria. This is an improvement to ensure fair and reliable elections, and ensure that only those allowed by the law participate in the electoral process.

TABLE 4: FRAUD DETECTION PERFORMANCE COMPARISON

Method	Fraud Detection Rate (%)
CNN	89.5
RNN	92.3
DNN	95.6
Proposed AIBA	99.1

The comparative performance between the suggested AI-Based Behavioural Analytics (AIBA) algorithm and other methods such as CNN, RNN, and DNN for detecting any fraudulent behavioural activities is shown in Table 4. The suggested AIBA algorithm shows the maximum performance with a fraud detection rate of 99.1%, while CNN has a 89.5% fraud detection rate, RNN has 92.3%, and DNN has 95.6%.

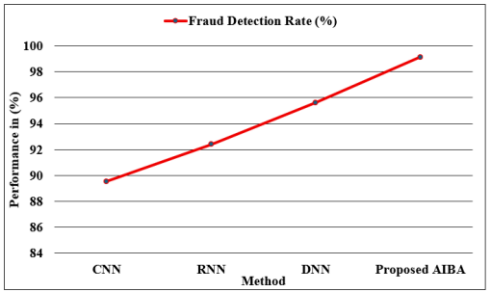


Figure 5: Fraud Detection Performance

In Figure 5, the models' ability to detect suspicious voting behaviour and abnormal voting is shown. The continuous improvement of the performance trend from the traditional deep learning methods to the proposed method is presented. AIBA's real-time analysis of voter behaviour helps to differentiate between genuine voters and potential fraudsters. Therefore, the suggested approach can be utilized to ensure better safeguards against election manipulation and further increase the overall electoral trust.

TABLE 5: SHA-256 HASH-CHAIN INTEGRITY EVALUATION

Tampering Scenario	**Records Tested**	**Tampering Detected (%)**	**Integrity Verification (%)**
Original Untampered Records	1000	0.0	100.0
Vote Data Modification	1000	99.8	99.9
Vote Record Deletion	1000	99.6	99.8
Vote Record Insertion	1000	99.7	99.9
Previous Hash Modification	1000	100.0	100.0

The efficiency of the SHA-256 hash-chain-based vote-recording approach was discussed in Table 5 through a comparison of different types of attacks. The outcomes of this evaluation prove that the alteration of vote data, deletion of records, addition of records, and changes to past hashes could be successfully identified thanks to the hash-chain verification technology. Consequently, one may conclude that the proposed solution ensures the creation of a reliable tamper-proof system of verifying votes.

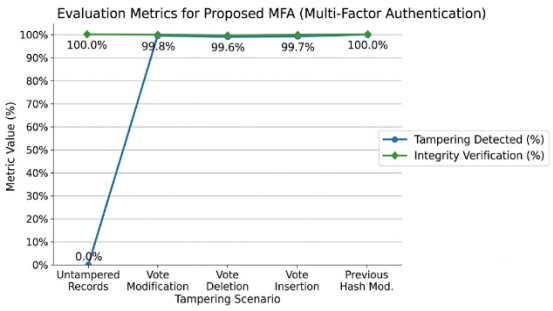


Figure 6. SHA-256 Hash-Chain Tampering Detection and Integrity Verification

The performance of the SHA-256 hash-chain mechanism has been depicted in Figure 6 under various tampering scenarios. Nearly all cases have been identified accurately by the system as an efficient integrity verification process.

V. CONCLUSION

Finally, the proposed AI E-Voting System offers a secure, transparent, and efficient voting system for digital elections in the cloud. It incorporates Multi-Factor Authentication (MFA), Domain-Specific Language (DSL) based verification, SHA-256 hash chaining and AI-Based Behavioural Analytics (AIBA) into the voting process to boost the security at each stage. The authentication module verifies the identity of the voters to grant access to the voting platform with several identity verification factors. Later, the voter eligibility is verified using the DSL verification mechanism based on a set of pre-defined voters' eligibility conditions, thus making sure that only the eligible voters can vote. Votes are recorded using the SHA-256 hash chaining method which provides a secure method of recording votes and ensures an audit trail of the votes to maintain vote integrity and transparency. In addition, the AIBA module tracks users' behaviour patterns in real-time, detecting any suspicious activity and blocking fraudulent voting attempts. Results of the experiments reveal high level of authentication Rate 98.9%, high level of eligibility verification 98.6%, effective fraud detection 99.1% and secure voter integrity 99.3%. The proposed system is its excellent scalability, low operational costs and near zero latency, which enables it to be used in large-scale institutional elections. The framework will address the security and trust issues associated with traditional voting methods, making them more credible and trusted. Overall, the AI E-Voting System is a powerful and secure solution for contemporary electronic voting systems, ensuring a reliable and transparent way to vote in the digital future.

REFERENCE

[1] Ainur, Jumagaliyeva, Muratova Gulzhan, Tulegulov Amandos, Rystygulova Venera, Serimbetov Bulat, Yersultanova Zauresh, And Shegetayeva Aizhan. "The Impact of Blockchain and Artificial Intelligence Technologies in Network Security For E-Voting." International Journal of Electrical and Computer Engineering (Ijece) 14, No. 6 (2024): 6723-6733.

[2] Sarkar, Moumita, Prabhat Das, And Sajal Saha. "Decentralized Electronic Voting Using Blockchain: State-Of-The-Art, Limitations, And Research Directions."

Devare, Manoj Himmatrao, Sambhav Rahul Choudhary, Prasad Nagambar Jambukar, And Anita Manoj Devare. "Blockchain-Based Smart Contracts for Decentralized E-Voting System." In Bridging Technology and Development for Sustainable Innovation and Geopolitical Dynamics, Pp. 119-168. Igi Global Scientific Publishing, 2025.

[3] Pachorkar, Pravin R., Sivaram Ponnusamy, And Ankita Karale. "A Secure and Intelligent Blockchain-Based E-Voting System Using Multimodal Voter Authentication and Smart Contract Optimization." In 2025 International Conference qon Future Technologies (Icft), Pp. 1-7. Ieee, 2025.

[4] Devi, V. Seedha, S. Kaavya, B. Deepika, D. Jayashree, And L. Nithikaa. "Ai-Driven Voter Authentication and Fraud Detection System." International Journal of Computer Technology and Electronics Communication 9, No. 3 (2026): 1008-1017.

[5] Jumagaliyeva, Ainur, Elmira Abdykerimova, Asset Turkmenbayev, Bulat Serimbetov, Gulzhan Muratova, Zauresh Yersultanova, And Zhomart Zhiyembayev. "Identifying Patterns and Mechanisms of Ai Integration in Blockchain For E-Voting Network Security." Eastern-European Journal Of Enterprise Technologies 130, No. 2 (2024).

[6] Pasha, Xhesika, And Hamid Jahankhani. "Securing E-Voting Authentication: A Framework Integrating Ai-Based Facial Recognition." In Navigating the Intersection of Artificial Intelligence, Security, And

Ethical Governance: Sentinels of Cyberspace, Pp. 19-46. Cham: Springer Nature Switzerland, 2024.

[7] Paul, Anthony Lawrence. "Next-Generation E-Voting: Enhancing Privacy, Trust, And Authentication Through Biometrics and Blockchain Technology."

[8] Varshini, P. Arasi. "Secure And Unified Ai-Blockchain Voting System with Real-Time Verification." International Journal Of Engineering & Extended Technologies Research (Ijeetr) 8, No. 2 (2026): 3746-3754.

[9] Preiya, V. Sathya, V. D. Kumar, R. Vijay, And N. Kirubakaran. "Blockchain-Based E-Voting System with Face Recognition." Fusion: Practice & Applications 12, No. 1 (2023).

[10] Nahid, Nausheen, And P. Rajarajeswari. "A Decentralized and Biometrically Secured E-Voting Framework Using Hybrid Encryption." International Journal of Engineering & Extended Technologies Research (Ijeetr) 8, No. 2 (2026): 883-896.

[11] Sahoo, Susant Kumar, And Mrs Ankita Singh Baghel. "Blockchain-Based Secure E-Voting System with Privacy-Preserving and Scalable Architecture." Quantum Pulse: Journal Of Ai, Data Science & Systems Engineering (Qp-Aidse) 2, No. 1 (2026).

[12] Breja, Manvi. "Ai-Powered Security and Privacy Frameworks for Multimedia and Multimodal E-Governance Data: Challenges, Techniques, And Applications." In Multimedia and Multimodal Intelligence for Sustainable Development, Pp. 275-293. Crc Press, 2026.

[13] Chirchi, Vanajaroselin, S. Visalini, And S. Balasubramaniam. "Blockchain-Based Voting System." In Ai Based Advancements in Biometrics and Its Applications, Pp. 219-237. Crc Press, 2024.

[14] Breja, Manvi. "Ai-Powered Security and Privacy Frameworks for Multimedia and Multimodal E-Governance Data: Challenges, Techniques, And Applications." In Multimedia and Multimodal Intelligence for Sustainable Development, Pp. 275-293. Crc Press, 2026.