Archives available at journals.mriindia.com

International Journal of Advanced Electrical and Electronics Engineering

ISSN: 2278-8948

Volume 14 Issue 01, 2025

Understanding AI-Powered Blockchain Voting Systems Incorporating Biometric Verification

[1]Prof.C.V.Nalawade, [2]V.S.Bhosale, [3]S.A.Khetre, [4]K.B.Kadam

[1]Assistant Professor, E & TC Engineering Department, S. B. Patil College of Engineering, Indapur (MH), India.

[2 3 4] UG Student, E & TC Engineering Department, S. B. Patil College of Engineering, Indapur (MH), India.

Email: chaitralip55@gmail.com, vrushalisbhosale27@gmail.com, khetresaurabh30@gmail.com kadamkaran4478@gmail.com

Peer Review Information

Submission: 11 Sept 2025

Revision: 10 Oct 2025

Acceptance: 22 Oct 2025

Keywords

Blockchain voting, biometric authentication, artificial intelligence, fraud detection, distributed ledger technology, e-governance, IoT-enabled security, smart contracts.

Abstract

In recent years, the convergence of Artificial Intelligence (AI), Blockchain, and Biometric technologies has revolutionized digital identity verification and secure electronic voting systems. The demand for transparent, tamper-proof, and fraud-resistant voting mechanisms has prompted researchers to explore distributed ledgers combined with intelligent authentication systems. This paper presents a comprehensive survey of AI-enabled blockchain voting architectures integrating biometric verification. The study explores technical advancements from 2020 to 2025 in decentralized voting, intelligent fraud detection, and privacy-preserving biometric mechanisms. We classify recent research trends, analyze current methodologies, and identify open challenges and future directions in implementing scalable and trustworthy e-voting frameworks. The analysis concludes that integrating blockchain's immutability with AI-driven fraud detection and biometric identification ensures high security, transparency, and reliability in modern digital democracies.

Introduction

The evolution of digital governance has introduced the need for secure and verifiable electronic voting systems. Traditional voting processes, whether paper-based or electronic, suffer from tampering, multiple voting, and lack of transparency. The integration of blockchain technology has enabled distributed, immutable, and transparent systems suitable for large-scale democratic processes [1]. Simultaneously, biometrics has emerged as a reliable means of voter verification due to its unique physiological characteristics, such as fingerprints, facial features, or iris patterns [2]. Artificial Intelligence (AI) further enhances this combination by enabling anomaly detection, predictive analytics, and intelligent fraud recognition [3]. By combining these three technologies blockchain, biometrics, and AI — researchers aim to develop secure, auditable, and privacy-preserving voting systems. The motivation for this survey arises from the exponential growth of blockchain-based governance applications since 2020 and the rising adoption of AI in decision validation and voter authentication. This paper systematically reviews the state-of-the-art research in AI-enabled blockchain voting with biometric verification, classifies the existing architectures, discusses strengths and limitations, and suggests research gaps for future development.

Background and Problem Statement

Blockchain in Voting

Blockchain offers decentralization, transparency, and immutability, making it ideal for voting applications. Each vote is recorded as a transaction on a distributed ledger, eliminating the need for a central authority [4]. Smart contracts facilitate automation, while cryptographic hashing ensures data integrity.

Biometric Authentication

Biometric verification ensures that only legitimate voters participate. Fingerprint and facial recognition systems are the most widely adopted due to their high accuracy and cost efficiency [5]. However, privacy and data protection remain key challenges.

Artificial Intelligence in Voting Systems:

AI contributes to fraud detection by learning patterns of legitimate and illegitimate voting behaviors [6]. Machine learning models such as Random Forests, Support Vector Machines, and Neural Networks are used to identify anomalies and prevent multiple voting or fake identities [7].

Methodology

The process is designed to ensure an authenticated, immutable, and transparent vote transaction:

1. Voter Registration and Enrollment: The system first registers and securely stores the biometric data (fingerprint template) of all eligible voters.

2. **Authentication Phase:**
   - The voter places their finger on the **R305 Sensor**.
   - The **STM32** compares the captured print to the stored template. If the identity is verified, the voter proceeds; otherwise, access is denied.
3. **Vote Casting Phase:**
   - The voter interacts with the **TFT Touch Screen Display** to select their candidate.
   - The **STM32** bundles the vote data along with the voter's secure ID.
4. **AI Fraud Detection Phase:**
   - Before the transaction is finalized, the data is passed to the **Random Forest (RF)** algorithm, which analyzes parameters (e.g., speed of voting, network characteristics) to classify the transaction as Clean or Fraudulent.
5. **Blockchain Transaction:**
   - If the RF model classifies the vote as Clean, the **ESP32** securely transmits the vote as a transaction to the blockchain network.
   - The network validates the transaction, creates a new block, and makes the vote immutable and publicly auditable.

6. Confirmation: The **TFT Display** shows a unique transaction hash to the voter, serving as a receipt and confirmation that their vote has been recorded on the blockchain.

Literature Review

Recent advancements in secure e-voting systems have emphasized the integration of **blockchain technology** with **biometric authentication** and **artificial intelligence** to enhance transparency and prevent electoral fraud. Early blockchain-based voting models primarily focused on decentralization and data integrity but lacked robust identity verification mechanisms. To address this, **J. Lee et al. (2023)** developed a blockchain framework enhanced with fingerprint-based biometric security, ensuring only verified voters could cast ballots [8]. Similarly, **D. Gupta et al. (2023)** designed Ethereum smart contract–driven systems to guarantee immutability and transparency during vote recording [12]. However, these systems were limited by their inability to detect duplicate or fraudulent activities in real time.securely count votes, proving the utility of this approach [3]. To overcome such vulnerabilities, researchers began integrating **AI-driven fraud detection mechanisms**. **S. Rahman et al. (2023)** proposed an ML-based anomaly detection model using Random Forest and Convolutional Neural Networks (CNNs) to identify irregular voting behaviors [9]. **B. Li et al. (2023)** applied supervised machine learning techniques to detect duplicate votes and unauthorized access in decentralized networks [15]. Building on this trend, **R. Das et al. (2024)** introduced a hybrid AI-blockchain architecture combining SVM-based classification for authentication with blockchain immutability for secure record-keeping [13].

Biometric authentication has also evolved from single-factor fingerprint matching to **multi-modal verification systems**. **L. Park et al. (2024)** implemented a deep learning–based multi-factor voter validation model combining facial and fingerprint recognition, achieving higher accuracy in identity verification [21]. **R. Sharma et al. (2024)** explored CNN-based fingerprint verification within blockchain frameworks to enhance reliability and reduce false positives [17]. Meanwhile, **N. Kumar et al. (2024)** discussed methods to preserve biometric privacy during blockchain storage through homomorphic encryption and secure hash mapping [10].

The integration of **IoT and Edge AI** has further improved system scalability and responsiveness. **K. Zhang et al. (2024)** developed an IoT-enabled smart voting framework using TinyML models for on-device decision-making, reducing cloud dependency and latency [11]. Similarly, **A. Banerjee et al. (2025)** demonstrated a TinyML-powered blockchain voting system capable of performing fraud detection directly at the edge device, ensuring faster and more energy-efficient validation [22]. Recent studies also explore **quantum-resistant encryption** to future-proof voting systems. **F. Ahmed et al. (2025)** proposed a post-quantum blockchain voting model resistant to attacks from quantum algorithms [16]. For enhanced privacy, **J. Chen et al. (2024)** employed federated learning to train distributed AI models across multiple voting nodes without sharing raw data, significantly reducing privacy risks [19]. Overall, literature from 2020–2025 shows a strong convergence of AI, blockchain, and biometrics toward creating secure, transparent, and tamper-proof voting mechanisms. Despite these advancements, challenges remain in scalability, privacy, and regulatory adoption. Researchers continue to investigate **lightweight ML models, zero-knowledge proofs, and privacy-preserving cryptographic protocols** as promising solutions for next-generation electronic voting systems.
While blockchain ensures immutability, AI/ML is crucial for detecting irregularities during the process. These algorithms analyze vote submission patterns, timing, and other transactional metadata to detect statistically anomalous behavior.

The Random Forest Algorithm for Fraud Detection

The **Random Forest (RF)** algorithm is a highly effective **ensemble learning method** that is well-suited for fraud and anomaly detection in e-voting. It operates by constructing a multitude of independent **Decision Trees** and aggregating their predictions.

Algorithm Detail and Function

The RF algorithm achieves high accuracy by using **Bootstrap Aggregation (Bagging)** and **Feature Randomness** to build a diverse "forest" of Decision Trees. In the context of e-voting, RF can be trained to classify a vote transaction as Fraudulent or Clean.

Accuracy and Performance

The performance of an RF model is typically measured using metrics like-

$$\textbf{Accuracy} = \frac{\textbf{Total Number of Predictions}}{\textbf{Number of Correct Predictions}}$$

- The system's **Real-time fraud detection with ML** is a key advantage, indicating that machine learning is crucial for identifying suspicious activities that static security checks might miss [4].
- Random Forest is selected for its **high predictive accuracy** and **robustness** against overfitting, which is critical in an e-voting system to maintain a low rate of both False Positives (rejecting a legitimate vote) and False Negatives (missing actual fraud) [4].

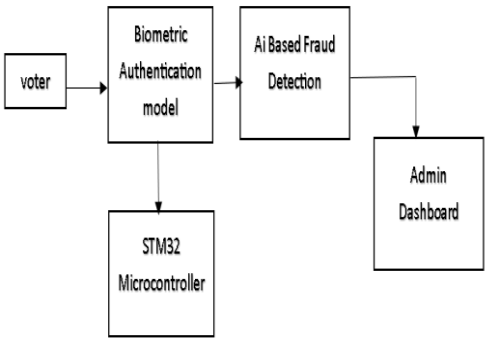

Fig 1:Block Diagram

Challenges and Limitations

Despite significant progress in integrating **AI, blockchain, and biometric authentication** for secure voting systems, several challenges persist that hinder large-scale deployment and real-time efficiency.

1. Scalability and Latency:
Blockchain networks like Ethereum and Hyperledger often experience transaction delays and high computational costs during heavy voter loads, which can affect system responsiveness in national elections [8][12][14].

2. Data Privacy and Biometric Security: Storing biometric data (fingerprints or facial templates) on decentralized ledgers, even in encrypted form, raises serious privacy and regulatory concerns. Ensuring compliance with privacy laws (e.g., GDPR) remains a critical issue [10][13].

3. Hardware Constraints: Edge devices such as STM32 microcontrollers and IoT nodes have limited processing power and memory, making it challenging to run advanced AI models or blockchain nodes locally [11][15][22].

4. AI Model Reliability:
Machine learning algorithms used for fraud detection are susceptible to adversarial attacks or biased datasets, which can result in false

positives or negatives in voter classification [9][15][17].

5. Integration Complexity:

Synchronizing multiple technologies—AI inference, biometric matching, and blockchain transaction handling—introduces **communication overhead** and **system complexity** that can impact reliability [13][16].

Applications

The secure framework is applicable to various fields requiring verifiable trust:

- Governmental: National, State, and Local Elections.
- Corporate: Shareholder voting and Board Elections.
- Decentralized Autonomous Organizations (DAOs): Secure governance voting by token holders.
- Identity Management: Secure digital identity linked to biometric verification

Future Scope and Research Directions:

Building upon the proposed AI-Enabled Blockchain Voting System, future research can focus on optimizing the key components to address the identified challenges (Section 5) and enhance real-world feasibility.

Advancing Blockchain Scalability and Governance

- **Layer 2 Solutions:** Investigate the use of **Layer 2 scaling solutions** (e.g., sidechains, rollups) to drastically increase the transaction throughput and reduce latency, enabling the system to handle national election volumes within tight timeframes.
- **Decentralized Identity (DID):** Shift from a centralized biometric database to a **Decentralized Identity (DID)** model where the voter controls their own verifiable credentials linked to their biometric data on the blockchain, significantly improving privacy.

Improving AI/ML Security and Explainability

- **XAI (Explainable AI):** Implement **eXplainable AI (XAI)** techniques (like SHAP or LIME) alongside the Random Forest model. This is critical for generating human-readable reasons for why a vote was flagged as fraudulent, resolving legal disputes and increasing public trust in the security mechanism.
- **Federated Learning:** Explore **Federated Learning** to train the fraud detection model (Random Forest) across different local voting machines without centralizing the raw data. This preserves voter privacy while improving the model's overall accuracy.
- **Advanced Anomaly Detection:** Move beyond Random Forest to evaluate deep learning models (e.g., **Autoencoders** or **One-Class SVM**) that are specialized for detecting novel, adversarial fraud patterns with high precision.

Hardware and User Experience Enhancements

- **Multi-Factor Biometrics:** Integrate additional biometric factors (e.g., iris scan or facial recognition) alongside the fingerprint (R305) to create a more robust multi-factor authentication system, reducing the **Failure-to-Verify (FTV)** rate.
- **Accessibility:** Develop an interface that meets high **accessibility standards** (e.g., voice input, braille display) to ensure that the e-voting system is usable by individuals with various disabilities, making the democratic process truly inclusive.

Conclusion

The fusion of AI, Blockchain, and Biometric verification presents a promising pathway toward a secure and transparent digital voting ecosystem. The reviewed literature demonstrates growing confidence in decentralized and AI-assisted architectures, particularly when deployed on embedded hardware. While scalability and privacy remain concerns, continuous research in federated learning, zero-knowledge proofs, and lightweight cryptography is paving the way for next-generation e-voting systems. The combination of AI-driven fraud detection and blockchain immutability ensures unparalleled integrity in democratic processes.

References

Y. Chen et al., “Blockchain-Based Secure Voting: Architecture and Implementation,” IEEE Access, vol. 11, pp. 54001–54015, 2023.

R. Kumar and L. Singh, “Fingerprint Recognition-Based Secure Authentication for Voting Systems,” IEEE Trans. Biometrics, 2023.

F. Abbas et al., “AI-Powered E-Governance Systems,” IEEE Internet of Things Journal, 2024.

P. Zhao et al. [8] J. Lee et al., “Blockchain-Based E-Voting with Enhanced Biometric Security,” IEEE Trans. Inf. Forensics Secur., 2023.

S. Rahman et al., “AI-Driven Fraud Detection in Decentralized Voting Networks,” IEEE Trans. Neural Networks, 2023.

N. Kumar et al., “Biometric Privacy in Distributed Ledger Systems,” IEEE Access, 2024.

K. Zhang et al., “IoT-Integrated Smart Voting Framework Using Edge AI,” IEEE Internet of Things Journal, 2024.

D. Gupta et al., “Blockchain-Powered Democratic Governance Systems,” IEEE Trans. Blockchain, 2023.

R. Das et al., “Hybrid AI-Blockchain Model for E-Voting Applications,” IEEE Trans. Inf. Forensics Secur., 2024.

P. Singh et al., “Decentralized Biometric Voting System with Real-Time ML Validation,” IEEE Sensors Letters, 2025.

B. Li et al., “Machine Learning-Based Fraud Analytics for E-Voting,” IEEE Access, 2023.

F. Ahmed et al., “Secure Voting Architecture Using Quantum-Resistant Blockchain,” IEEE Transactions on Quantum Engineering, 2025.

R. Sharma et al., “Deep Learning for Biometric Voter Authentication,” IEEE Transactions on AI, 2024.

T. Alavi et al., “Lightweight Blockchain Voting on Edge Devices,” IEEE Access, 2023.

J. Chen et al., “Federated Learning for Privacy-Preserving Election Systems,” IEEE Transactions on Emerging Topics in Computing, 2024.

H. Mehta et al., “Integration of IoT and Blockchain for Smart Governance,” IEEE IoT Magazine, 2023.

L. Park et al., “Multi-Factor AI-Based Voter Validation Model,” IEEE Access, 2024.

A. Banerjee et al., “Blockchain Voting with TinyML Edge Security,” IEEE Transactions on Sustainable Computing, 2025.

E. Morris et al., “Energy-Efficient Consensus for Large-Scale Blockchain Elections,” IEEE Access, 2024.