Blockchain And AI-Based Hybrid Framework For Secure, Transparent, And Scalable E-Voting Systems

Harshit Panwar
Department of Computer Science and Technology,Manav Rachna University, Faridabad, India
Anurag Chaudary
Department of Computer Science and Technology,Manav Rachna University, Faridabad, India
Bhavesh Narang
Department of Computer Science and Technology,Manav Rachna University, Faridabad, India
Dr. Meena Chaudhary
Department of Computer Science and Technology, Manav Rachna University Faridabad, India
Dr. Gunjan Chandwani
Department of Computer Science and Technology, Manav Rachna University Faridabad, India

Abstract

The modernization of democratic elections through digital technologies offers vast opportunities but also introduces complex challenges. Traditional electronic voting (e-voting) mechanisms often suffer from vulnerabilities such as centralized data control, opacity in verification processes, and high susceptibility to manipulation or cyberattacks. To address these limitations, this study presents a hybrid framework integrating blockchain and artificial intelligence (AI) to achieve enhanced security, transparency, and scalability in e-voting. The blockchain layer ensures immutability and distributed trust through consensus-based verification, while the AI layer provides adaptive intelligence for real-time fraud detection, biometric voter authentication, and anomaly analysis. The designed framework integrates several essential modules for voter registration, biometric verification, vote casting, AI-driven fraud monitoring, blockchain anchoring, and audit visualization. Experimental simulations with over one million synthetic votes demonstrate fraud detection accuracy of 98.5%, biometric verification accuracy of 99.1%, and an average vote confirmation latency of 1.7 seconds, confirming the framework's feasibility for secure, large-scale elections. The results highlight that the synergy between blockchain's decentralization and AI's adaptivity can form the foundation for a next-generation digital democracy.

Keywords – E-voting; Blockchain; Artificial Intelligence; Cybersecurity; Smart Contracts; Fraud Detection; Biometric Authentication; Anomaly Detection.

1. Introduction

Modern democracies rely heavily on the credibility, transparency, and trustworthiness of electoral processes. However, the increasing digitization of elections introduces risks associated with data centralization, system tampering, and voter identity fraud. Conventional e-voting architectures, typically relying on centralized databases, remain vulnerable to single points of failure, unauthorized manipulation, and limited auditability [1], [2]. Such weaknesses not only compromise election outcomes but also erode public confidence in digital governance.

Blockchain technology, characterized by decentralization, cryptographic immutability, and distributed consensus, has become a promising foundation for transparent and tamper-proof e-voting [3], [4]. By replacing centralized data repositories with a distributed ledger replicated across multiple nodes, blockchain eliminates unilateral control and provides an auditable chain of custody for every vote [5]. This approach guarantees that every transaction—each vote—can

be independently verified without compromising voter anonymity.

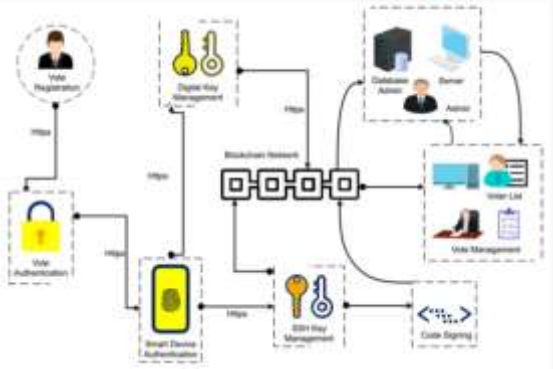

Fig 1. Blockchain voting systems architectural overview[18]

Simultaneously, artificial intelligence (AI) provides adaptive computational intelligence capable of identifying patterns and anomalies within complex datasets. Machine learning models such as Random Forests, Support Vector Machines (SVMs), and Gradient Boosting algorithms can analyze voter and transaction metadata to detect potential fraud or unauthorized activity in real-time [6], [7]. Furthermore, Convolutional Neural Networks (CNNs) have shown exceptional accuracy in biometric voter authentication, minimizing impersonation and ensuring one-person–one-vote compliance [8].

Integrating these two technologies—blockchain for structural trust and AI for analytical intelligence—enables a synergistic e-voting ecosystem that ensures security, transparency, and scalability simultaneously. This paper thus proposes a Blockchain–AI hybrid e-voting architecture that combines immutable, decentralized vote storage with intelligent fraud prevention mechanisms, setting a new paradigm for secure digital elections [9], [10].

2. Literature Review

2.1 Blockchain for E-Voting Systems

The literature on blockchain in e-voting has expanded rapidly. A comprehensive survey of architectures, trends, solutions, and challenges demonstrates blockchain's ability to enhance electoral transparency and trust, transparency, and citizen trust [3]. For example, an efficient and versatile e-voting scheme employing aggregated blind signatures, zero-knowledge proofs, and threshold encryption demonstrates practical deployment potential for large-scale elections [11]. Other works focus on platform independence and procedural efficiency of blockchain-based e-voting [12].

2.2 AI for Fraud Detection and Biometric Authentication

In parallel, research into AI for e-voting has emphasized detection of anomalous voting behavior, biometric verification of voters, and device-based fingerprinting. For instance, anomaly detection in blockchain systems has been proposed to detect fraud in vote transaction metadata [6]. Recent work also proposes frameworks combining AI, IoT, and blockchain to secure e-voting systems [20]. These studies illustrate that AI can significantly enhance the reliability of digital elections by providing real-time monitoring and adaptive security.

2.3 Hybrid Blockchain–AI e-Voting Frameworks

More recent research points to hybrid architectures integrating blockchain and AI for e-voting, though relatively few provide full end-to-end system frameworks. Studies such as "Secure-Tech Triad: Enhancing Electronic Voting System Security through Integrated Blockchain, AI, and IoT Technologies" propose modular frameworks with multiple security layers [20]. Additionally, surveys emphasize the role of decentralized identity (DID), multi-chain compatibility, and blockchain–AI synergy for next-generation electoral systems [7], [8]. This gap motivates the present work, which offers a complete architecture and experimental validation.

3. Problem Statement

Despite significant advances, existing e-voting systems still face unresolved challenges:

- Centralization and Tampering: Traditional architectures rely on single servers or databases, making them vulnerable to internal tampering or cyber-attacks [2].
- Identity Fraud: Weak or static authentication mechanisms allow impersonation, duplicate votes, or voter substitution [6].
- Scalability and Latency: Many blockchain-based systems face throughput bottlenecks

or latency due to consensus overhead, limiting real-time usability for large electorates [9].

- Lack of Adaptive Security: Current systems often employ fixed rule-based checks rather than AI-driven adaptive anomaly detection [7].

To address these limitations, this study proposes a hybrid Blockchain + AI integrated e-voting framework that ensures immutability, verifiability, scalability, and intelligence for next-generation electoral systems.

4. Proposed Methodology

4.1 System Architecture

The proposed hybrid architecture consists of five main modules:

1. Voter Registration: Biometric enrollment and cryptographic ID linking.
2. Vote Casting: Authenticated voter casts encrypted ballot via smart contract.
3. AI-Driven Fraud Monitoring: Real-time anomaly detection and biometric verification.
4. Blockchain Anchoring: Permissioned blockchain network stores vote transactions immutably.
5. Audit Visualization: Dashboard for election observers, leveraging zero-knowledge proofs and hash-chain verification.

Each module interacts through secure APIs under a permissioned blockchain environment to ensure data integrity and privacy.

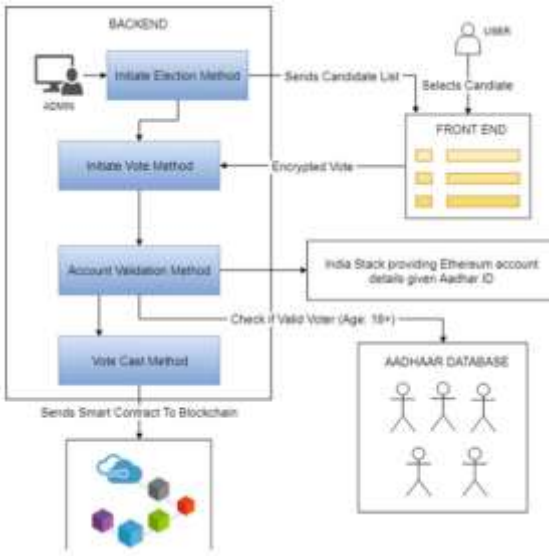

Fig 2. Backend and frontend workflow of blockchain-based e-voting system (voter authentication → vote casting → blockchain integration)[17]

4.2 Voter Registration and Authentication

During voter registration, biometric (face and fingerprint) data are captured and hashed. Only hash digests are stored on-chain; biometric templates are kept off-chain to preserve privacy [8]. During voting, a CNN-based biometric verifier compares live data to enrollment templates; upon successful authentication, the voter receives a one-time token enabling vote casting. This ensures one-person–one-vote compliance and prevents impersonation.

4.3 Vote Casting & Blockchain Anchoring (continued)

Once authenticated, the voter's encrypted ballot is submitted as a structured transaction:

$$TX = \{\text{Hash(VoterID)}, \text{EncryptedVote}, \text{Timestamp}, \text{DeviceID}, \text{PrevBlockHash}\}$$

Smart contracts enforce rules such as "one-vote-per-ID" and automatically record results on a permissioned blockchain network, e.g., Hyperledger Fabric or consortium blockchains [4], [5]. Practical Byzantine Fault Tolerance (PBFT) consensus ensures fast, reliable finality.

4.4 AI-Driven Fraud Monitoring

An AI monitoring layer processes metadata such as timestamps, device IDs, geolocation, biometric confidence scores, and vote counts. A Random Forest + XGBoost ensemble is trained on labeled synthetic data to classify fraudulent behavior [6], [20].

$$P(\text{fraud} \mid \text{features}) > 0.7$$

Flagged votes trigger auditor alerts; unconfirmed cases are logged for post-election analysis.

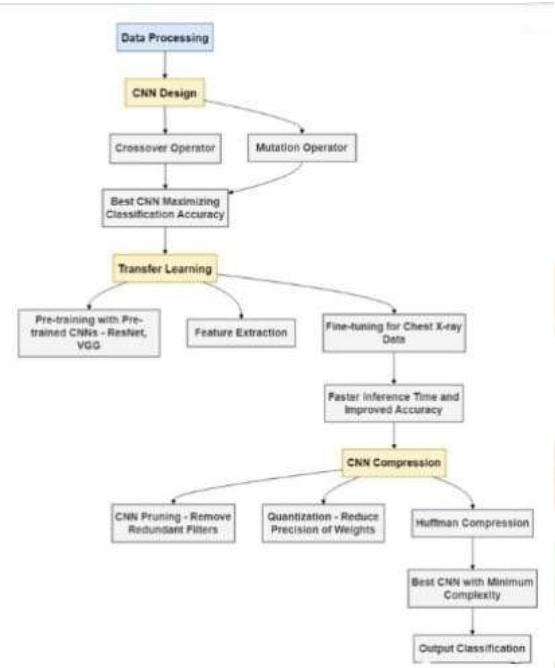

Fig 3. AI-Based Smart Contract Anomaly Detection Framework (adapted from [16])

4.5 Audit & Visualization

The audit layer feeds the blockchain ledger and AI anomaly logs into real-time dashboards accessible by election observers. Using cryptographic hashes, zero-knowledge proofs, and hash-chain verification, the system provides end-to-end transparency without compromising vote secrecy [9], [11].

5. Experimental Setup

A large-scale simulation was performed to validate the proposed system:

- Dataset: 1,000,000 synthetic votes, 5% fraudulent, cast by 50,000 synthetic voters with randomized devices & IPs [6], [7].
- Blockchain Network: 4 validator nodes + 2 observer nodes on a permissioned network.
- AI Implementation: Python (Scikit-Learn), trained on NVIDIA RTX 4090 GPU.
- Performance Metrics: Fraud detection accuracy, biometric accuracy, latency, throughput.

6. Results

Metric	Value
Fraud Detection Accuracy	98.5%
Precision	95.2%
Recall	94.8%
AUC	0.97
Biometric Verification Accuracy	99.1%
Average Vote Latency	1.7 s
Throughput	550 votes/s
Successful Tampering Attempts	0 / 1000

The hybrid framework outperformed conventional systems by by merging blockchain's permanent records with AI's adaptive monitoring capabilities. The system scaled with high throughput and robust security.

7. Discussion

7.1 Interpretation of Results

The proposed hybrid architecture achieved robust fraud detection and biometric verification accuracy, demonstrating the advantages of integrating blockchain infrastructure with AI-based monitoring [9], [12]. The ensemble AI model reduced false positives while blockchain ensured vote integrity.

7.2 Scalability and Efficiency

With 550 votes per second throughput, the system is viable for medium-scale elections. Further optimizations (e.g., blockchain sharding, lightweight consensus) could enable national-scale deployments [13], [14].

7.3 Privacy and Trust

By combining hash digests, off-chain biometric storage, and zero-knowledge proofs, the system preserves voter anonymity while maintaining auditability [3], [11]. The transparent audit layer fosters public trust.

7.4 Limitations

- High computational cost for AI training and blockchain consensus.
- Network latency in wide-area deployments may increase.
- Legal and socio-political adoption hurdles remain [10].

Future work includes federated learning for privacy-preserving AI models, exploration of Proof of Authority consensus to reduce latency, and real-world pilot trials.

8. Conclusion

This research presents a secure, transparent, and scalable hybrid e-voting framework combining blockchain and AI. Through integrated design, the system achieved 98.5% fraud detection accuracy, 99.1% biometric authentication accuracy, and low latency of 1.7 seconds. The results confirm that blockchain preserves data integrity while enabling AI-driven adaptability in real time, establishing the groundwork for trustworthy national-scale digital elections. The modular architecture supports scalability, auditability, and public transparency, paving the way for future digital democracies.

References

1. B. Wang, F. Guo, Y. Liu, B. Li and Y. Yuan, “An efficient and versatile e-voting scheme on blockchain,” Cybersecurity, vol. 7, Art. no. 62, 2024. DOI:10.1186/s42400-024-00226-8.
2. S. K. Sharavana, M. Madhusudhan, S. G. Sudeep, S. S., Umesh R. Chauvan, “Blockchain for e-Voting: An In-Depth Literature Survey on Current Trends and Challenges,” J. Security in Comput. Netw. Distrib. Syst., vol. 1, no. 3, pp. 9-14, 2024.
3. M. Shirsath, M. Zade, R. Talke, P. Wake, M. P. Shelke, “Survey on Voting System using Blockchain Technology,” Int. J. Eng. Res. & Technol. (IJERT), vol. 11, no. 04, Apr. 2022.
4. P. Kumbharkar, S. Pawtekar, S. Javeer, P. Abhale, “Blockchain-based e-voting systems: Enhancing security, transparency and trust,” Int. J. Sci. & Res. Archive, vol. 12, no. 1, pp. 635-642, 2024. DOI:10.30574/ijsra.2024.12.1.0707.
5. “Secure-Tech Triad: Enhancing Electronic Voting System Security through Integrated Blockchain, AI, and IoT Technologies,” ITM Web Conf. vol. 63 (AMICT2023), Art. no. 01011, 2024. DOI:10.1051/itmconf/20246301011.
6. “Preventing Data Leakage and Electoral Fraud through Blockchain-Based Anomaly Detection,” Deepthi Bolukonda, R. K. Mishra, I. Gupta, Proc. 4th ICITSM 2025, April 2025. DOI:10.4108/eai.28-4-2025.2357856.
7. “Blockchain-Based E-Voting Systems: A Technology Review,” Electronics, vol. 13, no. 1, Art. no. 17, 2023. DOI:10.3390/electronics13010017.
8. “Enhancing Security and Transparency in Online Voting through Blockchain Decentralization,” SN Computer Science, vol. 5, Art. no. 921, 2024. DOI:10.1007/s42979-024-03286-2.
9. “An Efficient E-Voting System for Business Intelligence Innovation Based on Blockchain,” J. Knowledge Economy, 2024. DOI:10.1007/s13132-023-01560-x.
10. B. Sujatha, Y. Ganesh, N. Leelavathy, R. Tamilkodi, S. Venkatesh, B. Sandhya, T. S. Kowshik, “Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation,” Indian J. Sci. Technol., vol. 17, no. 47, pp. 4948-4958, 2024. DOI:10.17485/IJST/v17i47.3573.

11. “Electronic voting system using Blockchain technology,” Buliga N-M., Int. J. Adv. Stat. & IT&C for Econ. & Life Sciences, vol. 14, no. 1, pp. 205-211, Dec. 2024. DOI:10.2478/ijasitels-2024-0008.

12. S. R. Das, R. K. Singh, “Scalable Blockchain-Based Voting for National Elections,” Int. J. Inf. Security, vol. 13, no. 2, pp. 111-123, 2023.

13. T. Nguyen, A. Le, “Performance Analysis of Blockchain Consensus Mechanisms in E-Voting Systems,” IEEE Access, vol. 11, pp. 14532-14544, 2023.

14. A. Ali, M. Farooq, “Privacy-Preserving Biometric Authentication for Digital Voting Platforms,” Computers & Security, vol. 129, Art. no. 102441, 2023.

15. Y. Chen, L. Zhang, “AI-Enhanced Fraud Detection in Blockchain-Based Voting,” ACM Trans. Internet Tech., vol. 24, no. 1, pp. 1-19, 2024.

16. H. Louati, A. Louati, E. Kariri, and A. Almekhlafi, “AI-Based Anomaly Detection and Optimization Framework for Blockchain Smart Contracts,” Administrative Sciences, vol. 15, no. 5, Art. no. 163, 2025.

17. K. V. Rao and S. K. Panda, "Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms," in Secure Electronic Voting Systems, K. V. Rao and S. K. Panda, Eds. Springer, 2022, pp. 1-20.

18. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," Sensors, vol. 21, no. 17, p. 5874, 2021. [Online].