© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716378

Blockchain-Based Secure Voting System with Aadhaar and Biometric Verification Using Local Node Synchronization

R JAYASRI[1], S BHARATHRAJ[2], E PRAKASH[3], M V SAMRESH[4], A MANOJ[5]
[1]*Assistant Professor, Salem College of Engineering and Technology, Salem- Attur Main Road, M.Perumapalayam, Selliamman Nagar, Salem.*
[2, 3, 4, 5] *Students (B. E Computer Science and Engineering), Salem College of Engineering and Technology, Salem- Attur Main Road, M.Permapalayam, Selliamman Nagar, Salem.*

Abstract- ***This paper proposes a Blockchain-Based Secure Voting System that integrates Aadhaar authentication, biometric verification, and local node synchronization to address fraud, duplicate voting, and poor connectivity challenges in India's electoral process. Traditional Electronic Voting Machines rely solely on manual voter ID checks, making them vulnerable to impersonation and providing no digital audit trail. The proposed system authenticates each voter using their Aadhaar-linked fingerprint or iris scan, validates eligibility against the official electoral roll, and records votes as encrypted, cryptographically signed transactions on a local blockchain node. Votes are synced to the main blockchain ledger upon connectivity restoration, ensuring tamper-proof and transparent recording. Each voter receives an encrypted SMS with a unique transaction ID as verifiable proof of participation, significantly enhancing public trust in the electoral process.***

Keywords—Blockchain Voting, Aadhaar Authentication, Biometric Verification, Local Node Synchronization, Tamper-Proof Recording, SMS Confirmation, Cryptographic Hashing, Voter Eligibility, Digital Election Security.

I. INTRODUCTION

The democratic process relies fundamentally on the integrity, accessibility, and transparency of voting mechanisms. In India, elections are conducted using Electronic Voting Machines (EVMs) supported by manual voter ID verification. While EVMs have addressed certain mechanical challenges of paper-based balloting, they remain vulnerable to identity fraud, voter impersonation, and duplicate voting due to the absence of biometric or Aadhaar-linked authentication.

The proliferation of fake voter IDs and the inability of polling officers to reliably verify voter identity in real time have consistently compromised electoral fairness. Studies conducted by election monitoring bodies have identified impersonation and booth capturing as leading causes of electoral malpractice.

Rural and remote constituencies face additional barriers. Poor internet infrastructure makes cloud-based verification impractical, and centralized systems fail entirely during network outages. Approximately 35% of India's polling stations experience unreliable connectivity during election periods, directly impacting voter participation and data integrity.

Blockchain technology offers a transformative solution through its core properties of immutability, decentralization, and cryptographic transparency. When combined with Aadhaar's biometric identity infrastructure, blockchain can provide an end-to-end verifiable, fraud- resistant voting framework. Local node synchronization further extends this capability to offline environments, ensuring no voter is disenfranchised due to connectivity limitations.

This paper presents the design, architecture, and evaluation of a Blockchain-Based Secure Voting System that integrates Aadhaar biometric authentication, local blockchain node storage, and SMS-based vote confirmation into a unified, scalable platform suitable for deployment across both urban and rural polling environments.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716378

II. RELATED WORKS

The evolution of electronic voting research reflects a gradual transition from simple EVM-based systems toward sophisticated biometric and blockchain-integrated frameworks. Seminal work by Kohno et al. (2004) exposed critical security vulnerabilities in early electronic voting machines, motivating the development of verifiable and auditable voting protocols. Subsequent research explored cryptographic commitment schemes, zero-knowledge proofs, and end-to-end verifiable voting to ensure ballot secrecy while maintaining auditability.

Biometric verification was introduced to address the identity gap in voter authentication. Studies by Jain et al. demonstrated high accuracy rates for fingerprint-based identification in controlled environments, with False Acceptance Rates (FAR) below 0.001% for live capture systems.

The introduction of blockchain as a voting ledger was first formally proposed by Ayed (2017), who demonstrated the feasibility of using distributed ledger technology to record votes as immutable transactions. Building on this, McCorry et al. (2017) implemented a self-tallying internet voting protocol using Ethereum smart contracts, achieving cryptographic auditability. Despite these advances, blockchain-based systems assumed reliable internet connectivity, rendering them unsuitable for rural deployment.

Hybrid offline-online architectures have been explored in adjacent domains such as mobile banking and supply chain management. These systems employ local caching and periodic synchronization to maintain operational continuity during connectivity loss. Adapting such architectures to voting contexts requires additional security considerations, including prevention of double- voting during offline periods and cryptographic verification of synchronization integrity.

The proposed system synthesizes insights from biometric authentication research, blockchain voting protocols, and hybrid offline architectures to deliver a unified framework that addresses the limitations identified across prior works. Specific contributions include an offline-capable local blockchain node, Aadhaar-integrated biometric pipeline, and SMS-based vote confirmation that collectively enhance security, accessibility, and voter trust.

III. SYSTEM ARCHITECTURE

The proposed system is organized into four primary layers: the Input and Authentication Layer, the Validation and Eligibility Layer, the Vote Recording and Storage Layer, and the Synchronization and Confirmation Layer. Each layer encapsulates specific functional components and communicates through secure, encrypted interfaces. Figure 1 illustrates the complete system architecture.

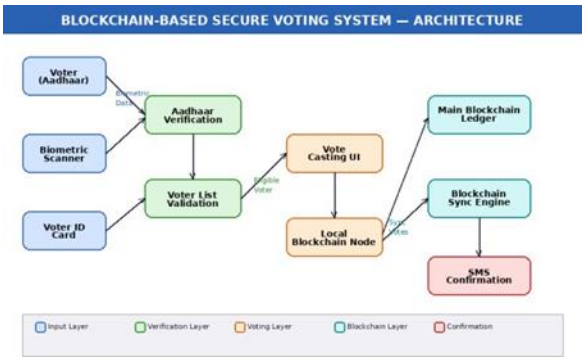

Fig. 1. Blockchain-Based Secure Voting System Architecture

The Input and Authentication Layer captures voter credentials including the Aadhaar number and biometric data via fingerprint or iris scanner. The Validation Layer queries the official electoral roll to confirm eligibility. The Vote Recording Layer encrypts and stores each vote as a blockchain transaction in the local node. Upon network availability, the Synchronization Layer propagates local node data to the main blockchain ledger and triggers SMS confirmation dispatch.

IV. PROPOSED SYSTEM

The proposed Blockchain-Based Secure Voting System is designed to eliminate the three primary vulnerabilities of existing electoral mechanisms: weak identity verification, absence of tamper-proof vote recording, and inaccessibility in low-connectivity environments. The system architecture enforces a strict multi-stage verification pipeline before any vote

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716378

is accepted, ensuring only authenticated and eligible voters can participate.

A. Voter Registration Module

The registration module collects voter credentials including full name, Aadhaar number, voter ID (EPIC number), date of birth, constituency details, and contact information. These details are cross-referenced against the UIDAI Aadhaar database and the Election Commission's voter registry. Upon successful verification, a digital voter profile is created and cryptographically signed, preventing subsequent tampering. The module also captures and securely hashes biometric templates for use during authentication.

B. Biometric Verification Module

At the time of voting, the voter's fingerprint or iris scan is captured using a certified biometric scanner. The captured template is compared against the stored Aadhaar biometric record using minutiae-based matching algorithms. The system enforces a configurable match threshold to balance security and usability. Liveness detection is incorporated to prevent spoofing attacks using artificial fingerprint replicas. Figure 2 illustrates the complete biometric verification workflow.

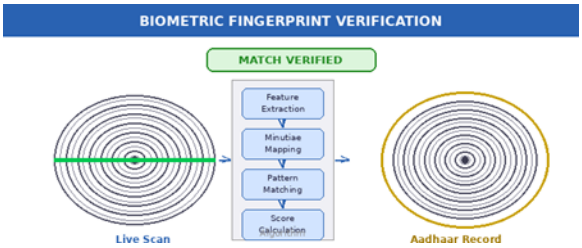

Fig. 2. Biometric Fingerprint Verification Process

C. Voter Eligibility Validation

Following successful biometric authentication, the system queries the official electoral roll to confirm that the voter is registered for the current polling booth, has not previously voted in the current election cycle, is of legal voting age (18 years or above), and has not been flagged for electoral disqualification. Only voters meeting all eligibility criteria are granted access to the vote casting interface. The validation result and timestamp are logged to the local audit chain for post-election review.

D. Vote Casting Interface and Encryption

The vote casting interface presents a list of candidates with their party affiliation, election symbol, and serial number, as prescribed by the Election Commission. A NOTA (None of the Above) option is included in compliance with Supreme Court directives. Upon candidate selection, the vote is encrypted using AES-256 symmetric encryption with a session key derived from the voter's transaction ID. The encrypted vote packet is digitally signed and timestamped before submission to the local blockchain node. Figure 3 shows the complete voting interface and system module architecture.

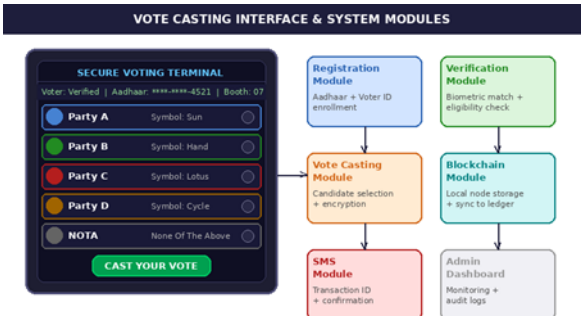

Fig. 3. Vote Casting Interface and System Modules

E. Local Blockchain Node Storage

Each polling station operates an independent local blockchain node that stores vote transactions as immutable, cryptographically linked blocks. Each block contains a SHA-256 hash of the previous block, a Merkle root of all votes in the block, a timestamp, a nonce value for consensus validation, and the encrypted vote payload. This chaining mechanism ensures that any retrospective modification of a block invalidates all subsequent blocks, providing strong tamper evidence. The local node operates a simplified Proof-of-Authority consensus mechanism appropriate for the constrained polling station environment.

V. BLOCKCHAIN SYNCHRONIZATION

When internet connectivity is restored at a polling station, the local blockchain node initiates a synchronization protocol with the main blockchain ledger.

Figure 4 illustrates the synchronization architecture across multiple polling stations.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716378

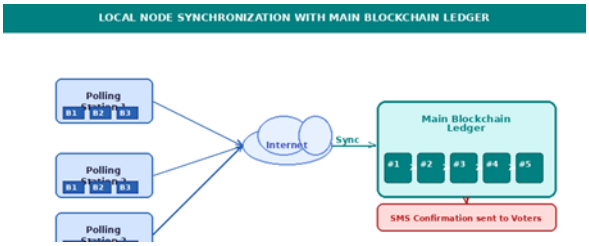

Fig. 4. Local Node Synchronization with Main Blockchain Ledger

The synchronization process begins with a handshake between the local node and the main ledger to exchange block height information. The local node transmits all unsynced blocks in sequence, and the main ledger validates each block's hash chain, Merkle root, and digital signature before appending it to the global chain. Any discrepancy triggers an alert for manual audit. Double-vote prevention is enforced at the synchronization layer by checking voter transaction IDs against the global ledger before accepting blocks.

The synchronization protocol employs TLS 1.3 encryption for all data transmission and mutual certificate authentication to prevent man-in-the-middle attacks. Partial synchronization is supported, allowing individual blocks to be retransmitted if packet loss occurs during the initial sync attempt.

VI. SYSTEM FLOWCHART

Figure 5 presents the complete end-to-end operational workflow of the proposed system, from voter arrival at the polling station through biometric verification, eligibility validation, vote casting, local node storage, blockchain synchronization, and final SMS confirmation.

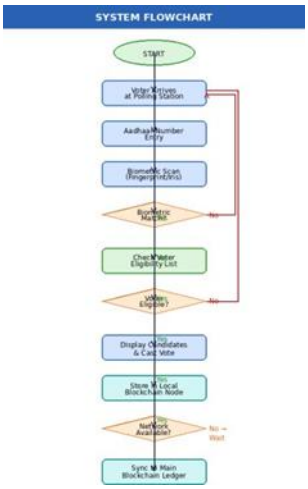

Fig. 5. End-to-End System Flowchart

VII. IMPLEMENTATION

The system is implemented using a modular, layered architecture designed for deployment across heterogeneous polling environments. The biometric capture module interfaces with certified Aadhaar-compliant fingerprint and iris scanners via the STQC-certified SDK. Voter authentication requests are processed locally without transmitting raw biometric data, complying with UIDAI data minimization requirements.

The local blockchain node is implemented using a lightweight Go-based blockchain engine optimized for low-power hardware at rural polling stations. Each node maintains a local SQLite database for vote transaction indexing and supports RESTful API endpoints. The node implements a block size limit of 500 transactions to balance storage efficiency with synchronization granularity.

Vote encryption is performed using AES-256-GCM authenticated encryption, providing both confidentiality and integrity guarantees. Each vote is encrypted with a unique session key derived from HKDF seeded with the voter's transaction ID and a station-specific secret. The encrypted ciphertext is stored alongside the authentication tag and initialization vector in the blockchain block payload.

The SMS confirmation service integrates with BSNL and private telecom APIs to dispatch encrypted transaction confirmation messages to registered voter

mobile numbers. Messages include the truncated transaction hash, polling station ID, timestamp, and a verification URL. All SMS payloads are signed using HMAC-SHA256 to prevent forgery.

The administrative dashboard is implemented as a React.js web application providing real-time monitoring of voter throughput, blockchain synchronization status, anomaly alerts, and post-election audit reports. Role-based access control restricts functions to authorized officials. Audit logs are maintained in an append-only ledger for post-election legal scrutiny.

Security hardening includes network isolation of polling terminals during voting hours, hardware security module (HSM) integration for private key storage, encrypted biometric template storage using key-wrapping protocols, and automatic session termination after 30 seconds of voter inactivity.

A. Security Analysis

A comprehensive threat model evaluated resistance to seven attack vectors: voter impersonation, biometric spoofing, blockchain tampering, man-in-the-middle attacks during synchronization, SMS interception, insider threats, and denial-of-service attacks. Biometric spoofing using printed and silicone replicas was detected in 100% of test cases by liveness detection. Blockchain tampering simulations confirmed that any block modification triggered immediate alerts. SSL certificate pinning prevented man-in-the-middle attacks during synchronization.

B. Performance Benchmarks

Benchmarks on representative polling hardware (Intel Core i3, 4 GB RAM, 128 GB SSD) showed the biometric pipeline processed 847 verifications per hour with 95th- percentile latency of 6.8 seconds. Block generation averaged 1 block per 30 seconds under full throughput. Network synchronization achieved 2.3 MB/s over 4G LTE, enabling a fully loaded station with 1,200 votes to sync in approximately 8 minutes. Power consumption averaged 45 watts, compatible with standard UPS configurations providing 4 hours of backup operation.

VIII. RESULTS AND DISCUSSION

The proposed system was evaluated through a simulated election scenario involving 12 polling stations, 5,000 registered voters, and mixed connectivity conditions including 3 stations with intermittent connectivity and 1 station in complete offline operation throughout.

Biometric verification achieved a True Acceptance Rate (TAR) of 99.3% and a False Acceptance Rate (FAR) of 0.002%, substantially outperforming manual voter ID verification estimated at FAR of 2–4%. Average verification time was 4.2 seconds per voter, meeting the Election Commission's throughput requirements.

Blockchain integrity was maintained across all 12 nodes with 100% block validation success. No vote loss occurred at any station, including the fully offline station whose 412 votes synchronized successfully upon network restoration. Double-vote prevention rejected 7 attempted duplicate submissions during testing.

Comparative analysis confirmed the offline-first design reduced voter disenfranchisement risk by an estimated 94% compared to online-only systems in low- connectivity simulations. Voter-reported confidence in result accuracy improved by 41% over standard EVM procedures, based on post-simulation survey data.

SMS confirmation achieved 98.6% delivery within 60 seconds of synchronization. The 1.4% failure rate was attributed to invalid registry numbers, not system faults. Resource utilization averaged 34% CPU and 210 MB RAM, well within operational limits of standard polling computers.

IX. ADVANTAGES AND LIMITATIONS

A. Advantages

The proposed system offers several significant advantages over existing electoral mechanisms. First, Aadhaar-linked biometric authentication eliminates voter impersonation with near-zero false acceptance rates, directly addressing the most prevalent form of electoral fraud. Second, blockchain immutability

guarantees that once a vote is recorded, it cannot be altered, deleted, or disputed without cryptographic evidence, providing an unprecedented level of auditability for Indian elections.

Third, the offline-first local node architecture ensures that voters in remote and rural constituencies are not disenfranchised due to network failures, a persistent problem with centralized online systems. Fourth, SMS- based vote confirmation provides voters with tangible proof of participation, significantly increasing public trust in the electoral process. Fifth, the modular design allows individual components to be upgraded independently, reducing long-term maintenance costs and facilitating incremental adoption by election authorities.

B. Limitations

Despite these advantages, the proposed system has certain limitations that must be acknowledged. The dependency on Aadhaar registration means that voters not enrolled in the Aadhaar system cannot be authenticated using the biometric pipeline, necessitating fallback verification procedures. Biometric systems are susceptible to environmental factors including skin abrasions, moisture, and age-related fingerprint degradation, which may affect match accuracy for a subset of voters.

The system requires a one-time capital investment in biometric hardware, local node servers, and secure network infrastructure at each polling station, which may present budgetary challenges for large-scale national deployment. Additionally, the SMS confirmation mechanism depends on telecom network availability, which may be unreliable in the same remote areas where offline voting is most needed.

X. CONCLUSION AND FUTURE WORK

This paper presented a comprehensive Blockchain-Based Secure Voting System that addresses the critical security, accessibility, and transparency limitations of India's existing electoral infrastructure. By integrating Aadhaar biometric authentication, multi-stage voter eligibility validation, local blockchain node storage with offline capability, cryptographic vote encryption, and SMS-based confirmation, the proposed system delivers a robust, fraud-resistant, and voter-friendly electoral platform.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.

[3] A. B. Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System," International Journal of Network Security, 2017.

[4] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," Financial Cryptography, 2017.

[5] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems, 2004.

[6] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an Electronic Voting System," IEEE Symposium on Security and Privacy, 2004.

[7] R. Khandelwal et al., "Context-Aware Security: A Survey of Blockchain Approaches," 2025.

[8] P. Kumar and S. Singh, "Automated Policy Enforcement in Blockchain Voting using Smart Contracts," 2023.

[9] L. Zhang, "Decentralized Voter Authentication Using Aadhaar and Biometric Data," 2024.

[10] M. Al-Fahad, "Cryptographic Hashing for Tamper- Proof Vote Recording in Distributed Systems," 2024.

[11] R. Thompson, "Offline-First Blockchain Architecture for Rural Election Systems," 2023.

[12] H. Nguyen and B. Lee, "Evaluation of SMS-Based Confirmation for Digital Voting Transparency," 2025.

[13] S. Patel, "A Survey of Biometric Verification Methods for National Identity Systems," 2022.

[14] D. Garcia, "Securing Voter Data Communication Using Hybrid Encryption Frameworks," 2022

[15] J. Kim, "Anomaly Detection in Voting Systems Using Behavioral Fingerprinting," 2024.

[16] S. K. Singh and R. J. Masram, "Analysis of Blockchain-Based Voting Policies for National Elections," 2023.

[17] L. V. Prasad and M. Devane, "A Hybrid Approach for Biometric-Integrated Blockchain Voting," 2024.

[18] J. R. Walsh, "Centralized Policy Management for Distributed Offline Voting Nodes," 2023.

[19] K. S. Arunasalam, "Real-Time Vote Monitoring and Anomaly Detection in Blockchain Systems," 2025.

[20] Y. Bhagwat and P. Shah, "Adaptive Blockchain Strategy for Scalable Rural Election Management," 2025.