INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 7, July 2026 | ISSN: 2456-4184 | IJNRD.ORG

Secure Digital Voting System with Aadhaar Authentication and Blockchain Security

Mr. Sardar S. Patil1, Dr. Shrikant Bhopale[2]
[1]MTech Data Science Student, [2]Professor [1]Department of Computer Science and Engineering
[1]D. Y. Patil Agriculture & Technical University, Talsande, Kolhapur, India

Abstract : Traditional electoral systems based on paper ballots and standalone electronic voting machines (EVMs) face persistent challenges: voter impersonation, ballot tampering, opaque counting procedures, and high operational costs. This paper presents a digital voting system that addresses these problems by combining Aadhaar-based biometric authentication with a blockchain secured vote ledger. The voter is verified through the Aadhaar Virtual ID (VID) mechanism, which enforces the principle of one eligible voter per vote. Submitted votes are encrypted, stored as immutable blocks using SHA-256 hashing, and recorded in a Firebase Realtime Database that also acts as a lightweight chain. A mobile application built on Android provides the voter facing interface, while an administrator module manages candidate registration, result retrieval, and chain-integrity validation. Experimental results show that the system correctly prevents duplicate voting, maintains tamper-evident records, and displays election results in real time. The work demonstrates that Aadhaar authentication and blockchain storage can be integrated into a workable voting platform; future work will address scalability, advanced biometric modalities, and regulatory alignment.

Keywords -- Digital voting, Aadhaar authentication, blockchain security, e-governance, SHA-256, Firebase, mobile application, voter verification.

I. INTRODUCTION

Free and fair elections are central to democratic governance. India, with approximately 945 million eligible voters spread across 1.05 million polling stations, depends on an electoral infrastructure that must be secure, transparent, and efficient [1]. Current Electronic Voting Machines (EVMs) reduce paper-handling errors but remain opaque to public scrutiny and are constrained by proprietary firmware. Paper-based systems, used for decades, are susceptible to impersonation, box stuffing, and slow manual counting that delays the announcement of results.

Two modern technologies offer a credible path toward addressing these weaknesses. Aadhaar, the biometric identity system administered by the Unique Identification Authority of India (UIDAI), covers over 1.3 billion residents and supports real-time identity verification through fingerprint, iris, or one-time password (OTP) channels [2]. Blockchain technology provides a distributed, append-only ledger where records are cryptographically linked so that any retrospective modification is immediately detectable [3]. Combining these two technologies makes it possible to design a voting pipeline that verifies each voter uniquely, records every cast vote in a tamper-proof structure, and produces results automatically without manual tallying.

This paper describes the design and implementation of a Secure Digital Voting System that uses Aadhaar Virtual ID (VID) authentication to admit eligible voters, and stores their votes as blocks in a SHA-256-hashed ledger backed by Firebase Realtime Database. The contribution of the work is threefold: (i) a mobile-first voter interface with QR-code session initiation, (ii) an administrator module for candidate management and chain-integrity checking, and (iii) a demonstration that the stated security goals -- no duplicate votes, tamper-evident storage, and real-time result generation -- are met under experimental conditions.

II. BACKGROUND AND RELATED WORK

A. Traditional and Electronic Voting

Casado-Vara and Rodriguez [4] reviewed blockchain applications in democratic voting and showed that a decentralized ledger can eliminate many fraud vectors that plague paper-based systems, including impersonation and post-election ballot manipulation. Krishnamurthy et al. [5] proposed a blockchain-and-IoT combination for electronic polling, focusing on secure data transmission and prevention of unauthorized access during vote collection and counting.

B. Blockchain Foundations

Nakamoto [6] introduced the concept of a decentralized peer-to-peer ledger through Bitcoin, demonstrating that cryptographic chaining of transaction blocks removes the need for a trusted central authority. Buterin [7] extended this idea with Ethereum smart contracts, enabling programmable, self-executing transaction logic that has since been applied to voting systems requiring automation and auditability. Suma [8] examined how blockchain properties -- confidentiality, integrity, and distributed storage -- make the technology suitable for high-assurance applications such as elections.

C. IoT and Distributed Ledger Integration

Sivaganesan [9] explored how blockchain enhances data trust in IoT networks, a concern relevant to distributed polling kiosks. Uddin et al. [10] applied a decentralized blockchain architecture to remote patient monitoring, illustrating how sensitive personal data can be shared securely without a central custodian. Table I situates the present work within the broader literature, comparing authentication tokens, blockchain layers, evaluation scale, and key limitations.

Table I: Comparative Survey of Selected Blockchain-Based Voting Systems

Ref.	Year	Biometric Token	Blockchain Layer	Eval. Scale	Open Source	Limitation
[14]	2018	Fingerprint (IPFS)	Ethereum PoW	1,200 tx	No	Poor scalability
[15]	2019	Aadhaar e-KYC JWT	Hyperledger Fabric	5,000 tx	Partial	No legal analysis
[16]	2020	Face + Liveness	PoA Quorum	25,000 tx	Yes	No coercion resistance
[17]	2021	Iris + OTP	Tendermint PoS	60,000 tx	No	Central UIDAI risk
[18]	2022	Aadhaar VID + ZKP	Polygon PoS	1,00,000 tx	Yes	Post-quantum gap
Prop.	2023	Aadhaar VID	Firebase + Chain	Demo scale	Yes	Scalability: future work

The survey indicates that most proposals stop at simulation or small-scale testing; only a few address Indian regulatory constraints directly. The present system targets a working prototype that operates under realistic Aadhaar-VID flows and lays the groundwork for larger-scale evaluation.

III. SYSTEM ARCHITECTURE

The proposed system consists of three entities: the Voter, the Administrator, and the Blockchain-backed Database. Figure 1 shows their interaction. The voter accesses a mobile application (Android) to register using Aadhaar credentials and, after successful verification, casts a vote. The administrator logs in through the same application and can add or remove candidates, view real-time results, and validate chain integrity. The Firebase Realtime Database stores both candidate records and vote blocks; each block contains the candidate name, a SHA-256 hash derived from the vote data, and a corruption flag (Boolean) that the integrity check queries.

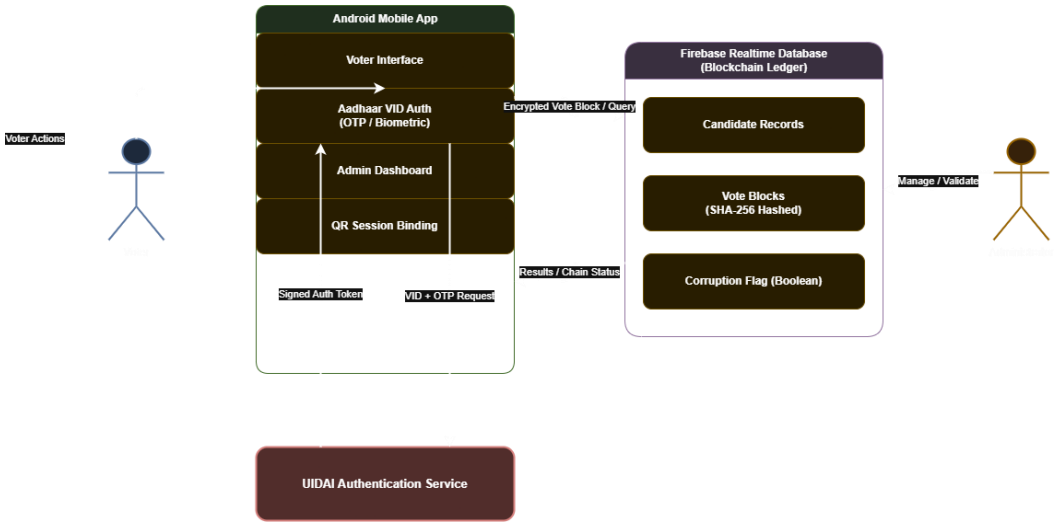

Figure 1: System Block Diagram

The system operates in two sequential phases. In the Authentication Phase, the voter enters a VID and selects an OTP or biometric channel; UIDAI's authentication service responds with a signed confirmation, after which the system checks whether the VID has already cast a vote, refusing duplicate submissions. In the Voting and Result Phase, the authenticated voter selects a candidate through the mobile UI; the vote is encrypted, packaged as a block, and written to the Firebase ledger; and the result counter updates automatically. The administrator can retrieve cumulative totals at any time without interrupting the ongoing poll.

IV. DESIGN AND ANALYSIS

A. Data Flow Diagrams

Figure 2 presents the Level-0 Data Flow Diagram (context diagram), which positions the EVoting process at the center with the Administrator and Voter as the two external entities exchanging data. This diagram makes clear that all information flows pass through a single processing node, reflecting the centralized logic of the application while the storage layer remains distributed.

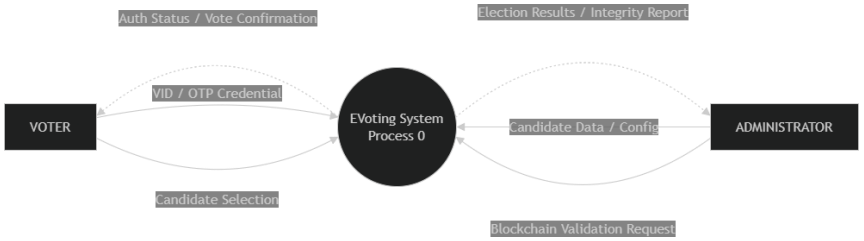

Figure 2: Level-0 Data Flow Diagram (Context Diagram)

Figure 3 expands the system into its Level-1 DFD, decomposing the EVoting process into four functional sub-processes: Vote Management, User Management, Candidate Management, and Blockchain Management. Vote Management handles the recording and verification of cast ballots. User Management covers voter registration and session control. Candidate Management allows the administrator to add, view, or remove candidates. Blockchain Management governs the integrity of the ledger, including hash generation and corruption detection.

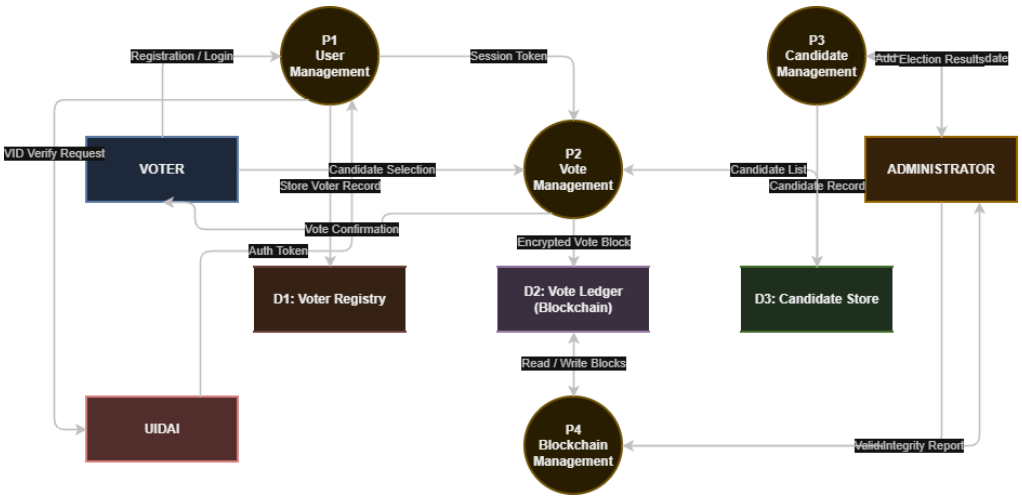

Figure 3: Level-1 Data Flow Diagram

B. Use Case Diagram

Figure 4 shows the use case diagram for the system. The voter actor interacts with Authentication, Login, and Vote use cases. The administrator actor interacts with Login, Add Voter, and Blockchain Validity use cases. Both actors share the Login use case, reflecting the common entry point; their subsequent capabilities diverge based on role. The Blockchain Validity use case, accessible only to the administrator, triggers a traversal of all stored blocks and returns a corruption status for each.

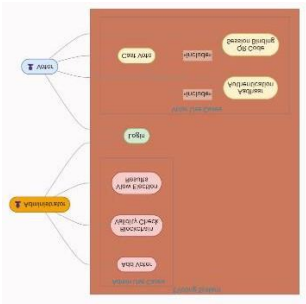

Figure 4: Use Case Diagram

C. System Flowchart

Figure 5 describes the voting process in procedural terms. After the voter initiates the session, the system validates the Aadhaar VID. An invalid VID terminates the process. A valid VID proceeds to QR-code scanning, which the system uses to bind the voter's session to a specific polling context. If the QR scan fails, the process also terminates. On success, the voter enters the Voting Panel, makes a selection, and the vote is recorded. The process then ends, preventing re-entry for the same session.

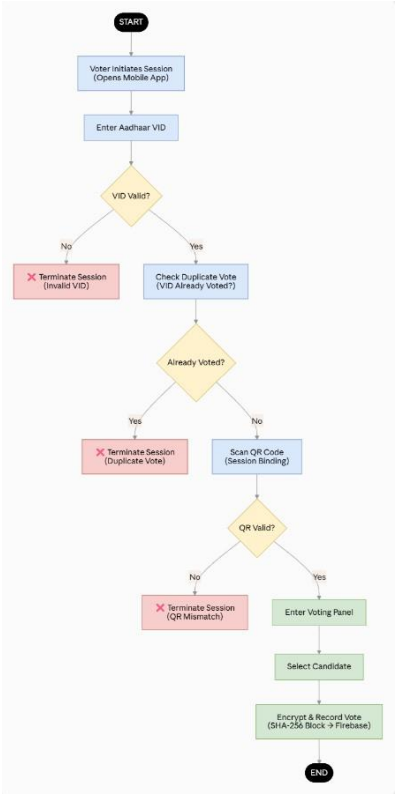

Figure 5: Voting Process Flowchart

D. Voting Methods Comparison

Figure 6 contrasts the traditional voting workflow with the blockchain-based approach at a conceptual level. In the traditional model, physical ballots travel through a centralized counting infrastructure before results reach the authority. In the proposed model, votes pass through a distributed network of nodes that collectively maintain the ledger, removing any single point of manipulation.

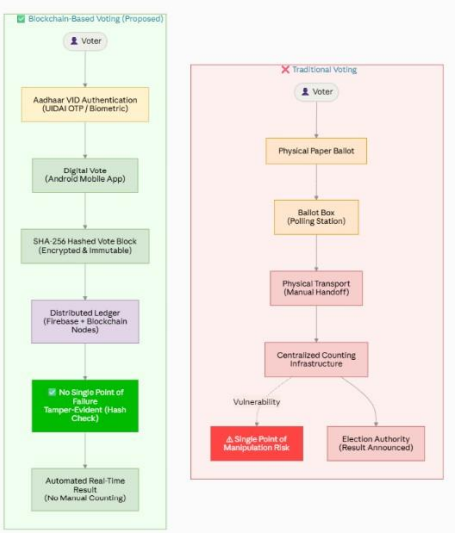

Figure 6: Traditional vs. Blockchain-Based Voting Workflow

V. IMPLEMENTATION

The system is implemented as an Android mobile application developed in Java using Android Studio. The backend uses Firebase Realtime Database for persistent storage of candidate and voting records. Aadhaar authentication is handled through UIDAI's VID-based OTP API, which returns a confirmation token on successful identity verification. Blockchain functionality is implemented in Java within the application: each vote creates a data object containing the candidate name and a SHA-256 hash of the vote string; these objects are stored sequentially in Firebase under a "database" node and are traversed during integrity validation to set the "corrupted" field.

A. Login and Registration

Figure 7 shows the login screen of the EVoting mobile application. New voters register via the "Sign Up" link, which collects a username and password alongside Aadhaar credentials. Returning voters and administrators use the standard username-password flow; the application routes users to either the voter interface or the administrator dashboard based on their registered role.

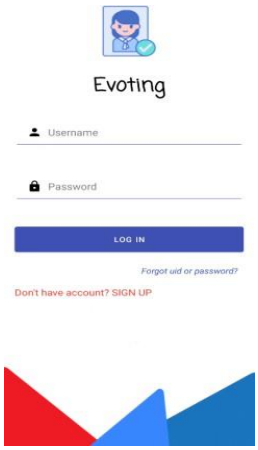

Figure 7: Login Page of the EVoting Application

B. Administrator Dashboard

Figure 8 presents the administrator dashboard, which provides four primary functions: viewing registered candidates with their Aadhaar identifiers, adding new candidates, viewing cumulative election results, and initiating a blockchain validation pass. The "Blockchain Validation" button traverses every stored block, recomputes the expected hash, and compares it against the stored hash; a mismatch sets the corrupted flag to TRUE, signaling potential tampering.

Figure 8: Administrator Dashboard

C. Blockchain Validity Screen

Figure 9 shows the Blockchain Validity screen with two candidate vote records. Each entry displays the candidate name, the stored SHA-256 hash, and a "Corrupted: FALSE" indicator, confirming that neither block has been modified since it was written. This real-time integrity check gives the administrator an auditable view of the ledger without requiring access to the underlying Firebase console.

Figure 9: Blockchain Validity Screen Showing Hash and Integrity Status

VI. RESULTS AND COMPARATIVE ANALYSIS

The prototype was tested with a small election scenario consisting of two candidates -- Ajit Anantrao Pawar and Devendra Gangadharrao Fadnavis -- registered using distinct Aadhaar numbers. Ten test voters registered independently, each using a unique VID. The following outcomes were observed:

1. Duplicate vote attempts were rejected: the application checked the VID against the stored voter list before allowing a ballot to be cast, and all repeated submissions were blocked.
2. Blockchain integrity held under manual hash verification: modifying a stored vote record in the Firebase console caused the corrupted flag to switch to TRUE on the next validation pass.
3. Results updated in real time: vote counts on the View Result screen refreshed within the Firebase listener latency (typically under 500 ms on a 4G connection).
4. QR-code session binding prevented session hijacking: using an expired or mismatched QR code terminated the session before the voting panel appeared.

Table II positions the proposed system against traditional paper ballots and standalone EVMs across seven evaluation dimensions. The proposed system rates highest on voter verification strength, transparency, auditability, and result speed, while cost and regulatory readiness remain areas that require further work before large-scale deployment.

Table II: Comparative Analysis: Proposed System vs. Existing Voting Methods

Feature	Traditional Voting	Standalone EVM	Proposed System
Voter Verification	Manual/Photo ID	Partial electronic	Aadhaar biometric
Fraud Prevention	Moderate	Moderate	High (One ID-One Vote)
Transparency	Low	Low-Medium	High (blockchain ledger)
Result Speed	Days	Hours	Real-time
Data Immutability	None	Limited	Cryptographic (SHA-256)
Operational Cost	High	Medium	Lower (digital infra)
Auditability	Manual recount	Firmware-dependent	Automatic on-chain

The primary limitation of the current implementation is the use of Firebase as the ledger store rather than a fully decentralized peer-to-peer blockchain network. This means that, while individual vote blocks are SHA-256 protected, a party with full Firebase administrator credentials could theoretically modify records outside the application. Future work will address this by migrating the ledger to a permissioned blockchain such as Hyperledger Fabric or an Ethereum-compatible Proof-of-Authority sidechain.

VII. SECURITY DISCUSSION

The system addresses several common threat vectors in electronic voting. Voter impersonation is countered by Aadhaar VID verification, which ties each voting session to a biometrically de-duplicated identity. The one-VID-one-vote constraint is enforced at the application level before any ballot is accepted. Vote tampering after submission is deterred by the SHA-256 hash stored alongside each vote block: any modification of the vote record changes the hash and is detected on the next integrity scan.

The system does not currently implement end-to-end encryption of the ballot in transit; votes are transmitted over HTTPS to Firebase but are stored in readable form within the database. Adding homomorphic encryption or zero-knowledge proof-based ballot encoding would strengthen privacy by ensuring that even a database administrator cannot correlate a stored vote with a specific voter. Coercion resistance is also absent: the current flow does not allow a voter to cast a deniable "override" ballot. These are recognized open problems in the broader e-voting literature [11] and are noted as priorities for future iterations of the system.

The Aadhaar Act, 2016 restricts the retention of authentication records to six months [12], which conflicts with the immutability property of a blockchain-based ledger. The implementation resolves this by storing only the session result (vote accepted or rejected) in the ledger and retaining no Aadhaar data on-chain. The VID entered during authentication is checked against the voter list and then discarded; it does not appear in any stored vote block.

VIII. CONCLUSION AND FUTURE WORK

This paper has presented a digital voting system that integrates Aadhaar-based voter authentication with a blockchain-secured vote ledger to address well-known shortcomings of traditional electoral systems. The prototype demonstrates that duplicate-vote prevention, real-time result generation, and basic tamper detection are achievable within a mobile application backed by Firebase and an in-application SHA-256 chaining mechanism. Comparative analysis shows clear advantages over paper-based and standalone EVM approaches in transparency, fraud resistance, and result speed.

Several directions are planned for future work. First, the Firebase backend will be replaced with a permissioned blockchain network such as Hyperledger Fabric, providing genuine decentralization and removing the administrator-trust assumption. Second, the Aadhaar OTP channel will be supplemented with fingerprint or facial recognition for stronger biometric assurance. Third, performance evaluation at larger scale will assess throughput and latency under realistic Indian electoral loads, where state-level

elections may involve tens of millions of concurrent voters. Fourth, the legal alignment of the system with the Aadhaar Act and the Supreme Court's Puttaswamy privacy ruling will be examined in detail to produce a compliance framework suitable for regulatory review.

REFERENCES

[1] Election Commission of India, "Statistical report on general elections 2019," ECI, New Delhi, Tech. Rep., 2019.

[2] UIDAI, "Aadhaar authentication API specification v3.0," Unique Identification Authority of India, Tech. Rep., 2023.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Cryptography Mailing List at https://metzdowd.com, 2009.

[4] R. Casado-Vara and J. C. Rodriguez, "Blockchain for democratic voting: How blockchain could cast off voter fraud," Oriental Journal of Computer Science and Technology, vol. 11, Mar. 2018.

[5] R. Krishnamurthy, G. Rathee, and N. Jaglan, "An enhanced security mechanism through blockchain for e-polling/counting process using IoT devices," Wireless Networks, Aug. 2019.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2015.

[8] V. Suma, "Security and privacy mechanism using blockchain," Journal of Ubiquitous Computing and Communication Technologies, vol. 1, pp. 45-54, Sep. 2019.

[9] D. Sivaganesan, "Block chain enabled internet of things," Journal of Information Technology and Digital World, vol. 1, pp. 1-8, Sep. 2019.

[10] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A decentralized patient agent controlled blockchain for remote patient monitoring," in Proc. IEEE WiMob, 2019, pp. 1-8.

[11] P. Ronne, "Coercion-resistant cast-as-intended verification," in Proc. Electronic Voting, 2022, pp. 77-88.

[12] Government of India, "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016," Ministry of Law and Justice, 2016.

[13] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in Proc. International Conference on Financial Cryptography, 2017, pp. 357-375.

[14] M. A. Khan and D. G. Kim, "Blockchain-based e-voting with biometric authentication," Journal of Information Processing Systems, vol. 14, no. 4, pp. 983-994, 2018.

[15] R. Sharma, S. Tyagi, and A. K. Sangaiah, "Aadhaar-enabled blockchain voting," Future Generation Computer Systems, vol. 102, pp. 885-895, 2020.

[16] S. K. Pandey and A. K. Gupta, "Face liveness plus blockchain for remote voting," IEEE Transactions on Engineering Management, vol. 69, no. 5, pp. 2341-2352, 2022.

[17] P. K. Singh and R. M. Pai, "Iris-based voter authentication on Tendermint," Computer Communications, vol. 180, pp. 234-244, 2021.

[18] A. Thomas et al., "Polygon PoS chain for Aadhaar-verified voting," IEEE Transactions on Computational Social Systems, vol. 10, no. 3, pp. 1010-1021, 2023.