International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

A Blockchain-Enabled Secure and Transparent Voting Management System

Seva Pradeep[1], Porapu Sai Manaswi[1], Battula Venkata Siva[1], Konthala Lakshmi Prashanth[1], and Dalli Chaitanya Reddy[1]

Anil Neerukonda Institute of Technology and Sciences, India

Abstract. In this project, a voting system is offered in a decentralised blockchain system to enhance the security, transparency and reliability of democratic elections. In the absence of trust-based systems, and in the presence of cryptographic protection, a vote is stored as a verifiable blockchain transaction, and there is no central point of failure. Smart contracts ensure that voter registration, eligibility checks, casting of votes, and live tallying are automated, and cryptography makes a voter anonymous. The integration of blockchain can be used to develop electoral systems which are highly integrated, precise, and efficient as compared to ordinary e-voting systems, and this is a critical facet which could develop credible, open, and efficient electoral frameworks.

Keywords: Smart Contracts · Cryptography · Decentralization · E-Voting · Blockchain

1 Introduction

1.1 Problems with Traditional and Centralized Electronic Voting Systems

Voting systems need to be transparent and reliable to conduct democratic elections. Voting via paper is slow to count, prone to human error, subject to ballot fraud and costly. Electronic alternatives are generally based on centralized design, leading to insider threats, single points of failure, and poor verifiability. Such systems require unquestioning faith in election authorities, making them susceptible to manipulation, data breaches, and denial of service attacks. The absence of transparent auditing undermines confidence in popular institutions of democracy.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

1.2 Blockchain and Smart Contracts as Decentralized Electoral Trust-Enabling Technologies

By eliminating the requirement of a central authority, blockchain ensures that votes cannot be manipulated without the conformity of the network. Cryptographic hashing and digital signatures provide integrity and non-repudiation. Smart contracts automatically implement the rules of elections, including registration, eligibility verification, voting, and counting, minimising human oversight and eliminating bias and inaccuracies without compromising the entire system.

1.3 Objectives of the Proposed Blockchain Voting System

The suggested framework will be a blend of smart contracts, decentralisation, and cryptography to offer a secure, transparent and convenient tool to vote. It allows longitudinal auditing of the votes without loss of voter anonymity and substitutes an intermediary trust with cryptography certification, which is a viable answer to the basic dilemmas of integrity, transparency, and dependability in modern day elections.

2 Literature Review

Mobile-based platforms and biometrics have been mentioned in the topic of blockchain voting, smart contracts, and privacy. E-governance was explored using mobile blockchain voting, with proposed challenges of scale and security of devices [1]. The integration of biometrics enhanced the elimination of impersonation, but template protection is also a challenge [2]. Digital identity authentication was improved with systems and blockchain but created issues of control and privacy [3]. Smart contract tallying was also achieved but at a price, and transaction time in public blockchain is limiting [4]. Layered engineering of architecture encryption enhanced both security and integrity, but needs optimisation of scaling [5,6]. End-to-end decentralised systems were tamper-resistant, but weakened throughput capacities [7], and hybrid designs provided the optimal transaction cost–transparency trade-offs [8]. The more general literature has focused on digital preparedness and infrastructure readiness [9]. AI-assisted palmprint recognition enhanced accuracy at the expense of increased computational complexity [10], and OTP multi-factor authentication enhanced verification while network stability [11] is vital to it. Zero-knowledge proofs came in handy in the trade-off between voter anonymity and voter auditability [12]. Combining biometrics and blockchain reduced centralised reliance despite the interrelationship of scaled fraud detection using deep hybrid learning [13]. This approach has been proven cost effective [14], and a governmental prototype proved electoral viability with proposed scalability and biometric integration enhancements [15].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

3 Methodology

3.1 Overview of the Proposed Methodology

The system employs a secure, modular, layered architecture that includes cryptographic and biometric authentication as well as blockchain-based data integrity. It relies on a Python fingerprint microservice, a MongoDB database, and a Node.js backend, communicating via RESTful APIs between clients and servers. The backend performs authentication, encryption, and eligibility checks prior to data storage. AES-256-CBC encrypted votes preserve confidentiality and tamper-evidence even in the event of a breach.

3.2 Backend Server

Written in Node.js and Express, the backend controls registration, authentication, election configuration, candidate organisation, and vote tallying using RESTful interfaces. It implements role-based access control, ensures eligibility prior to vote submissions, liaises with the biometric microservice, and encrypts all voting-related data before storage.

3.3 Biometric Authentication Module

Fingerprint template matching and authentication responses are handled by a specialised Python microservice separated from vote processing logic, providing enhanced security, modularity, and scalability. It verifies the identity of the voter and authorises them to vote, removing any chance of impersonation and unauthorised access.

3.4 Data Security and Encryption

Encryption of votes using AES-256-CBC with a unique Initialisation Vector (IV) ensures the confidentiality of votes, since only ciphertext with IVs is stored while raw data remains protected. Eligibility verification and elimination of duplication of voting are also implemented by system checks.

3.5 Database Management

MongoDB stores hash keys, biometric data, election data, and encrypted votes in structured collections. Isolation is ensured because only authenticated backend services can access data. The data is backed up and indexed to prevent tampering.

4 System Architecture

The architecture contains a secure, modular, three-layer design comprising the Client Layer, Application Layer, and Data Layer, providing separation of concerns, scalability, and efficient processing of the electoral process.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

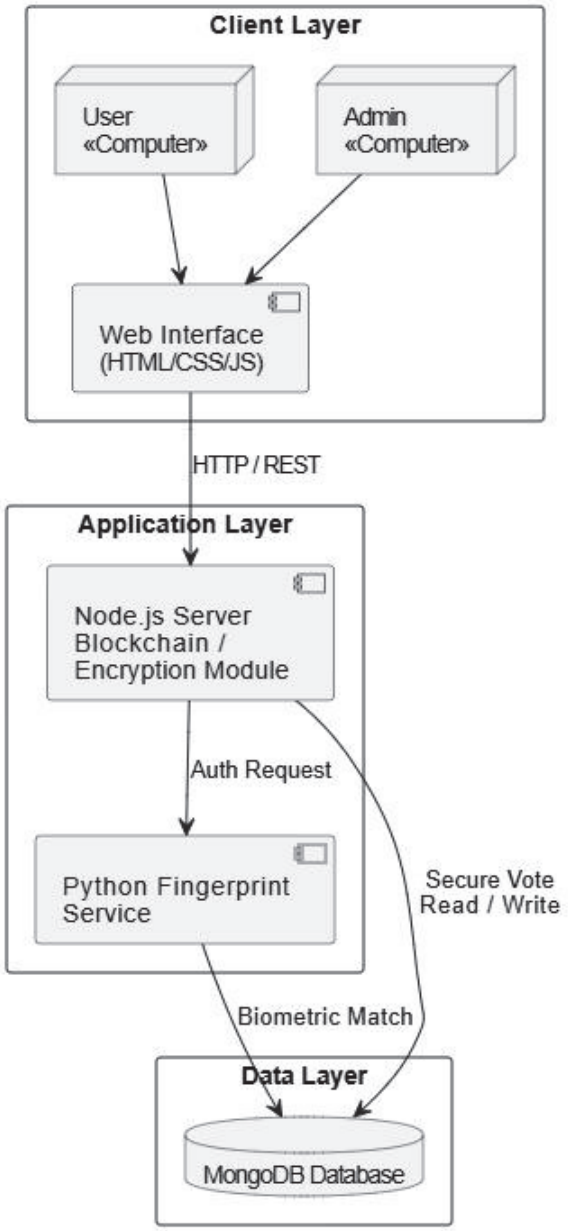

Fig. 1. Three-Layer System Architecture Diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Client Layer. Written in HTML/CSS/JavaScript, the interface supports two roles: Voter and Administrator. Voters handle registration, authentication, and vote casting; administrators manage elections, candidates, and eligibility. Role-based access control, HTTPS/REST APIs, session tokens, and input sanitisation protect communication and thwart unauthorised access.

Application Layer. The processing layer is driven by three main components. The Node.js Server handles authentication, access control, eligibility verification, vote encryption, and database communication. The Encryption Module uses AES-256 to encrypt votes and calculate cryptographic hash values, where any unauthorised modification is detectable through hash mismatch. The Python Fingerprint Service provides independent biometric template matching, returning access/denial responses with security isolation and modularity.

Data Layer. MongoDB offers scalable, durable document storage of hashed credentials, biometric templates, encrypted votes, cryptographic hashes, vote blocks, and audit logs. All information is encrypted and hashed prior to storage and is only accessible to authenticated backend services. Indexing and data backup ensure data reliability and tamper-proofing.

5 Experiments

The decentralised e-voting system was experimentally evaluated to assess its precision in authentication, scalability, API performance, duplicate vote prevention, and cryptographic integrity. All tests were conducted on the deployed system and results were reported from direct execution.

5.1 Precision of Biometric Authentication

The fingerprint authentication module was tested on five real fingerprint samples using ORB keypoint extraction and RANSAC-based matching. During enrollment, each fingerprint generated between 955 and 976 keypoints, well above the minimum reliability threshold. All genuine match confidence scores achieved a perfect value of 1.0000, as shown in Table 1.

Table 1. Biometric Enrollment and Genuine Match Results.

Subject ID	ORB Keypoints	Genuine Confidence Score
S1	972	1.0000
S2	964	1.0000
S3	955	1.0000
S4	976	1.0000
S5	968	1.0000

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Cross-subject impostor testing was also conducted. The highest number of impostor matches recorded was 6, far below the acceptance threshold of 50, indicating zero unauthorised acceptances.

5.2 Large-Scale Evaluation

Scalability was assessed on 100 subjects from the SOCOFing dataset. The system completed 100 legitimate tests and 500 impostor tests in 9.2 seconds. Table 2 shows that the False Accept Rate (FAR) and False Reject Rate (FRR) were both equal to 0.0000%.

Table 2. Large-Scale Authentication Results.

Metric	ult
Total Subjects	100
Genuine Tests	100
Impostor Tests	500
Execution Time	9.2 sec
False Accept Rate (FAR)	0.0000%
False Reject Rate (FRR)	0.0000%

5.3 REST API Performance

REST response times were measured for all Node.js backend endpoints to evaluate system performance. The results are summarised in Table 3. All endpoints achieved response times below 40 ms, indicating the responsiveness of the system under sequential access.

Table 3. REST API Response Time Analysis.

Endpoint	Mean Response Time (ms)
User Registration	16.8
User Login	21.5
Vote Casting	28.3
Candidate Retrieval	34.2
Election Status Check	19.7

5.4 Duplicate Vote Prevention and Vote Encryption

Duplicate vote testing included parallel and serial attack sequences. VoterID and electionID compound indexing on MongoDB was able to avert concurrent

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

submissions within 400 ms. Every vote was ciphered with AES-256-CBC using a 16-byte unique IV, where semantic security is guaranteed and duplication of ciphertext cannot be achieved even when the same vote choices are made. Unifor- mity and tamper resistance were also enforced with three-node hash validation.

5.5 Confusion Matrix Analysis

The large-scale test with 100 genuine trials and 500 impostor trials was used to construct the confusion matrix shown in Table 4. No false rejections or false acceptances were observed.

Table 4. Biometric Authentication Confusion Matrix.

	Predicted Genuine	**Predicted Impostor**
Actual Genuine	100 (TP)	0 (FN)
Actual Impostor	0 (FP)	500 (TN)

The biometric performance indicators are calculated as follows:

$$\text{FAR} = \frac{FP}{FP + TN} = \frac{0}{0 + 500} = 0.0000\% \quad (1)$$

$$\text{FRR} = \frac{FN}{FN + TP} = \frac{0}{0 + 100} = 0.0000\% \quad (2)$$

The result of $FP = 0$ and $FN = 0$ confirms that both FAR and FRR are 0.0000%, demonstrating that genuine and impostor samples can be separated correctly using ORB and RANSAC matching.

5.6 Security Analysis

Upon security checks, duplicate voting, impersonation, replay attacks, and data tampering were all prevented. AES-256-CBC encryption using unique IVs, MongoDB-based storage, and blockchain hash validation provided confidentiality and in- tegrity throughout.

6 Future Work

Future additions involve biometric authentication based on multiple modalities, blockchain scalability at Layer 2, database separation, and smart contract op- timisation to lower latency and costs. Voting interfaces in multiple languages can boost voter turnout. Mobile voting, accessibility features, and cloud inte- gration are also planned. Before mass adoption is achieved, practices require practical testing via pilot elections, security audits, and adjustment of dedicated regulations.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

7 Conclusion

This paper has suggested a decentralised blockchain-based voting system which includes smart contracts, cryptographic encryption, and biometric authentication to offer transparency, immutability, and tamper-resistance without centralisation. Smart contracts automate the electoral operations, and encryption and hashing ensure data integrity. The performance evaluation demonstrates the system's effectiveness in withstanding fraud and manipulation. Its construct can be scaled to institutional and national elections. Despite limitations in scalability and regulatory compliance, the system offers a strong baseline upon which future studies and practical applications can build toward better achievements of electoral integrity through democracy.

References

1. Android Blockchain E-Voting System: A Comprehensive Overview. (2022).
2. Pandiararajan, P., Kumarasamy, M.: Online voting using blockchain-based joint biometric identification. (2023).
3. Shadab, M., et al.: Blockchain-based e-voting with the use of Aadhaar card authentication. In: Proceedings of the 3rd ICPCSN, 2023. https://doi.org/10.1109/ICPCSN58827.2023.00207
4. Kumar, R., et al.: Smart contract deploying cryptographically guarded decentralized e-voting based on blockchain. In: Proceedings of the 13th Confluence, 2023. https://doi.org/10.1109/Confluence56041.2023.10048871
5. Verma, G., et al.: Secure e-voting with blockchain. In: Proceedings of the 2nd ICCSEA, 2022. https://doi.org/10.1109/ICCSEA54677.2022.9936073
6. Faruk, M.J.H., et al.: Bie-Vote: Biometric blockchain-based secure voting system. (2022).
7. Pavuluri, G., et al.: Block-Voter: DApp end-to-end Ethereum e-voting. In: Proceedings of the 19th ICICCS, 2025.
8. Gochhi, S.K., et al.: A review and comparative analysis of blockchain-based e-voting systems. (2023).
9. Khanpara, P., et al.: The opportunities and challenges of e-voting based on blockchain. (2022).
10. Sujatha, P., et al.: Palmprint voting system based on blockchain and AI. (2025). https://doi.org/10.1109/10986302.2025.10986302
11. Ramyadevi, R., et al.: Blockchain e-voting using three-layer OTP security system. (2023).
12. Liu, Z., et al.: DBE-voting: Privacy-auditable blockchain e-voting. In: Proceedings of IEEE ICC, 2023. https://doi.org/10.1109/ICC45041.2023.10279692
13. Waniya, J.S., et al.: BDT: Biometric-authenticated decentralized blockchain voting. (2023).
14. Base, M.A., et al.: E-voting through deep hybrid learning using blockchain. (2023).
15. Tandon, S., et al.: E-Matdaan: Decentralized blockchain e-voting. In: Electronic Learning Communities, 2022.