



# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 10, October 2025**

# **A Distributed Ledger-Based Secure e-Voting Architecture to Achieve Trust, Transparency, and Verifiability in Electronic Elections**

**Punam Saykar, Prof. S. C. Puranik**

ME Student, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahilyanagar,  
Maharashtra, Savitribai Phule Pune University, Pune, India

Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahilyanagar,  
Maharashtra, Savitribai Phule Pune University, Pune, India

**ABSTRACT:** In the present digital era, ensuring the integrity and transparency of election systems has become a major challenge. The proposed project, titled “e-Voting Scheme Using Blockchain”, introduces a secure, transparent, and tamper-proof voting framework developed using Java technology with a customized blockchain environment. This system aims to overcome the limitations of traditional voting methods such as vote tampering, duplication, and unauthorized access by leveraging the decentralized and immutable nature of blockchain. The blockchain framework is designed to securely record each vote as a unique transaction, making it impossible to modify or delete any vote once it is added to the chain. In this project, the e-voting process is implemented as a web-based application where each voter (user) can securely log in, verify their identity, and cast a single vote. The system includes different modules such as the User/Voter, Admin, Candidate Management, and Blockchain Security System. The Admin is responsible for adding candidates, managing voter data, and monitoring the voting process, while the blockchain ensures transparency and tamper-resistance of all votes. A built-in authentication system validates real users and prevents fake or multiple voting attempts. The proposed scheme not only secures vote integrity but also promotes easy accessibility and trust among voters. This blockchain-based e-voting model significantly enhances the voting process by providing a decentralized environment that ensures anonymity, security, and traceability without exposing voter identity. The system can be used to conduct elections at different levels—academic, organizational, or even governmental—by maintaining the core principles of confidentiality and verifiability. Overall, the proposed solution demonstrates how blockchain technology can revolutionize the voting process in the era of digital governance.

**KEYWORDS:** Custom Blockchain Technology, Secure e-Voting System, Immutable Distributed Ledger, Consensus Mechanism, Two-Step Authentication, Cryptographic Hashing, Java Web Application, Smart Authentication System, Decentralization, Transparency, Voter Verification, etc.

## **I. INTRODUCTION**

Electronic voting has emerged as an efficient solution to replace manual paper-based systems that often suffer from security loopholes, human errors, and logistical complexities. However, most e-voting systems today are still vulnerable to manipulation, unauthorized access, and lack of transparency. To address these challenges, this project introduces a blockchain-based e-voting scheme that integrates cryptographic security and distributed data management for a secure and verifiable election process. Blockchain's decentralized structure ensures that each vote is recorded in an immutable ledger, visible to authorized participants but impossible to alter or forge.

The main objective of the project is to develop a Java-based web application that enables voters to cast their votes remotely and securely using a custom blockchain framework. The system's architecture involves four main entities: the Admin, responsible for managing elections and candidates; the Voter/User, who securely logs in and casts a vote; the Blockchain Network, which ensures the integrity of recorded votes; and the Authentication Module, which verifies voter identity to prevent duplication or fraudulent activity. Every vote cast is treated as a separate block added to the blockchain, ensuring both transparency and confidentiality.

This system also emphasizes accessibility, allowing voters to participate from any location through secure online verification and encryption techniques. The proposed blockchain model ensures that one voter can vote only once, and every transaction is traceable without compromising anonymity. The integration of smart authentication and distributed ledger technologies ensures that the system remains tamper-proof, trustworthy, and auditable, thus addressing long-standing issues of fraud, transparency, and efficiency in traditional voting systems.

### **PROBLEM STATEMENT**

The existing voting systems often face challenges such as voter fraud, duplicate voting, lack of transparency, and centralized control. Manual counting and database-based systems are prone to errors and tampering. Hence, there is a need for a secure, transparent, and tamper-proof e-Voting system that ensures voter privacy and maintains the integrity of the election process in the new age of digitization to cast votes from any discreet place.

## **II. LITERATURE SURVEY**

**S. Majumder et al. (2024), “ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain and Zero Knowledge Property”.** This paper introduces an advanced blockchain-based e-voting framework called ECC-EXONUM-eVoting that integrates Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKP) to enhance voter privacy and vote authenticity. The authors propose a signature-based verification mechanism where each vote is digitally signed using ECC keys and stored securely on the Exonum blockchain platform. The system ensures that no third party, including administrators, can link a voter to their vote, thereby preserving voter anonymity while maintaining transparency. The Zero-Knowledge Proof technique further validates votes without revealing any private data. The research demonstrates that ECC-EXONUM-eVoting achieves strong resistance against tampering, replay, and Sybil attacks, making it an ideal solution for secure and verifiable digital elections. Experimental analysis shows that the scheme outperforms conventional blockchain voting models in terms of computational efficiency, data integrity, and low latency, proving its suitability for large-scale public elections.

**X. Wang et al. (2023), “Application of Data Storage Management System in Blockchain-Based Technology”.** In this study, Wang and colleagues explore the role of data storage optimization in blockchain-based systems, emphasizing how effective storage management enhances system scalability and performance in applications such as e-voting. The authors design a distributed data storage model that ensures secure, efficient, and tamper-proof management of sensitive data blocks. They propose a layered architecture that integrates blockchain’s immutable ledger with off-chain storage to reduce blockchain size while maintaining traceability and data integrity. The paper highlights how this hybrid storage approach supports real-time access, fast transaction processing, and reliable data backup, making it highly relevant for digital voting systems that handle large-scale user data. Their experiments demonstrate that the proposed storage management system significantly improves data retrieval time and network throughput while maintaining high security, thus serving as a key foundation for decentralized and transparent e-governance platforms like blockchain-based e-voting.

**K. M. et al. (2024), “Design and Implementation of Secured E-Voting System”.** This paper focuses on developing a secure and efficient electronic voting system that ensures authenticity, integrity, and transparency through blockchain integration. The proposed system architecture uses cryptographic hashing and digital signatures to authenticate voters and prevent double voting. The researchers implement an end-to-end verifiable voting mechanism where every cast vote is stored as a unique transaction in the blockchain ledger, ensuring immutability and traceability. The system design includes modules for voter registration, candidate management, and result generation, all controlled by a secure access mechanism. The authors validate the system through a practical implementation using smart contracts that automatically count and verify votes. Their results show reduced system latency, higher voter privacy, and resilience to common cyber threats such as vote manipulation and data breaches. The paper concludes that blockchain-based design provides an efficient alternative to conventional centralized e-voting systems.

**R. Ramyadevi and V. Priya (2024), “Blockchain-Powered E-Voting System: A Secure and Transparent Solution with Three-Tiered OTP Security Mechanism”.** Ramyadevi and Priya propose a blockchain-powered e-voting model that emphasizes strong multi-level authentication and transparency. The system introduces a three-tiered One-Time Password (OTP) security mechanism that verifies voter identity at different stages of the voting process to prevent unauthorized access and identity theft. The blockchain ensures that each vote is permanently recorded in an immutable

ledger accessible to authorized parties for verification. The authors discuss how this design guarantees anonymity while ensuring that no single entity can alter or delete votes. Their experimental model, implemented using Ethereum smart contracts, exhibits enhanced user authentication accuracy and improved voting reliability compared to traditional systems. The proposed model demonstrates a significant reduction in fraudulent activities and enhances voter confidence by combining the immutability of blockchain with a dynamic authentication process that supports transparent and tamper-proof digital elections.

**M. R. P and M. T. (2025), “Secure E-Voting with Blockchain: Enhancing AES and RSA Encryption with Face Authentication Technology”.** This paper presents a hybrid e-voting framework that merges blockchain technology with advanced encryption and biometric authentication to achieve superior security and user verification. The authors employ AES and RSA encryption algorithms to secure vote data during transmission and storage, ensuring confidentiality and protection against unauthorized decryption. Additionally, a facial recognition module is integrated into the authentication process, ensuring that only legitimate voters can access and cast their votes. The blockchain ledger serves as the backend for immutable vote storage and transparent tallying. The study highlights that this combination of cryptography and biometrics provides robust protection against identity spoofing, vote duplication, and data tampering. Experimental results show the proposed system achieves high recognition accuracy, faster encryption performance, and enhanced voter privacy. The authors conclude that combining blockchain with encryption and face authentication establishes a highly secure and practical digital voting infrastructure for future democratic processes.

### **III. SYSTEM OVERVIEW**

The e-voting system architecture is designed with modular components to ensure a smooth, secure, and verifiable voting process. The system begins with voter registration, where each voter’s identity is verified and securely stored in the blockchain-based ledger. Once registered, the voter can log in through the web application, verify their credentials, and cast a vote. The Admin module manages the overall election process—adding candidates, managing voters, and monitoring the blockchain ledger for all voting transactions. Each vote is converted into a unique digital transaction, encrypted, and stored in the blockchain, ensuring that the data cannot be changed later.

The Blockchain Security System is the backbone of this project. It ensures that once a vote is cast, it becomes part of a distributed ledger that all authorized nodes can verify but none can alter. The blockchain also maintains voter anonymity while allowing verification of the voting count and process integrity. The system’s decentralized structure makes it nearly impossible for hackers or insiders to manipulate the outcome. Moreover, the use of smart authentication prevents multiple voting and guarantees that only verified users can participate in the election.

In summary, the system overview reflects a complete digital transformation of the voting process with a focus on security, transparency, and accessibility. The combination of Java-based web application development and blockchain technology provides a highly secure environment for digital voting. This system ensures that each vote is authentic, traceable, and counted accurately, leading to a trustworthy and tamper-proof election process that can be applied in various organizational and governmental elections.

### **IV. PROPOSED SYSTEM**

The proposed e-voting system using blockchain technology aims to solve the issues of vote tampering, unauthorized access, and lack of transparency found in traditional systems. In this project, the voting process is implemented as a web-based Java application that uses a custom blockchain framework for secure data management. The system includes several main modules: User/Voter, Admin, Candidate Management, and Blockchain Security System. The Admin manages the election by adding candidates and verifying voter registrations, while voters can log in securely and cast their votes online. Each vote is stored as an encrypted block within the blockchain, ensuring it cannot be altered or deleted.

The blockchain framework ensures decentralization, where each transaction (vote) is verified by multiple nodes before being recorded permanently in the ledger. This prevents any single authority from controlling or tampering with voting data. The system also includes an authentication module that verifies each voter’s identity before allowing them to vote, ensuring that one voter can vote only once. The authentication mechanism uses encryption and digital signatures to

validate each user. If an unauthorized or fake voter attempts to access the system, the blockchain's validation mechanism immediately rejects the attempt, ensuring strong security.

Overall, the proposed system provides an efficient, secure, and transparent voting environment that encourages trust and participation. By integrating blockchain with Java-based web technologies, this system creates a decentralized election network where data is immutable, audit trails are verifiable, and results are transparent. This design enhances the credibility of elections and eliminates the need for manual supervision, providing a modern and fair voting experience.

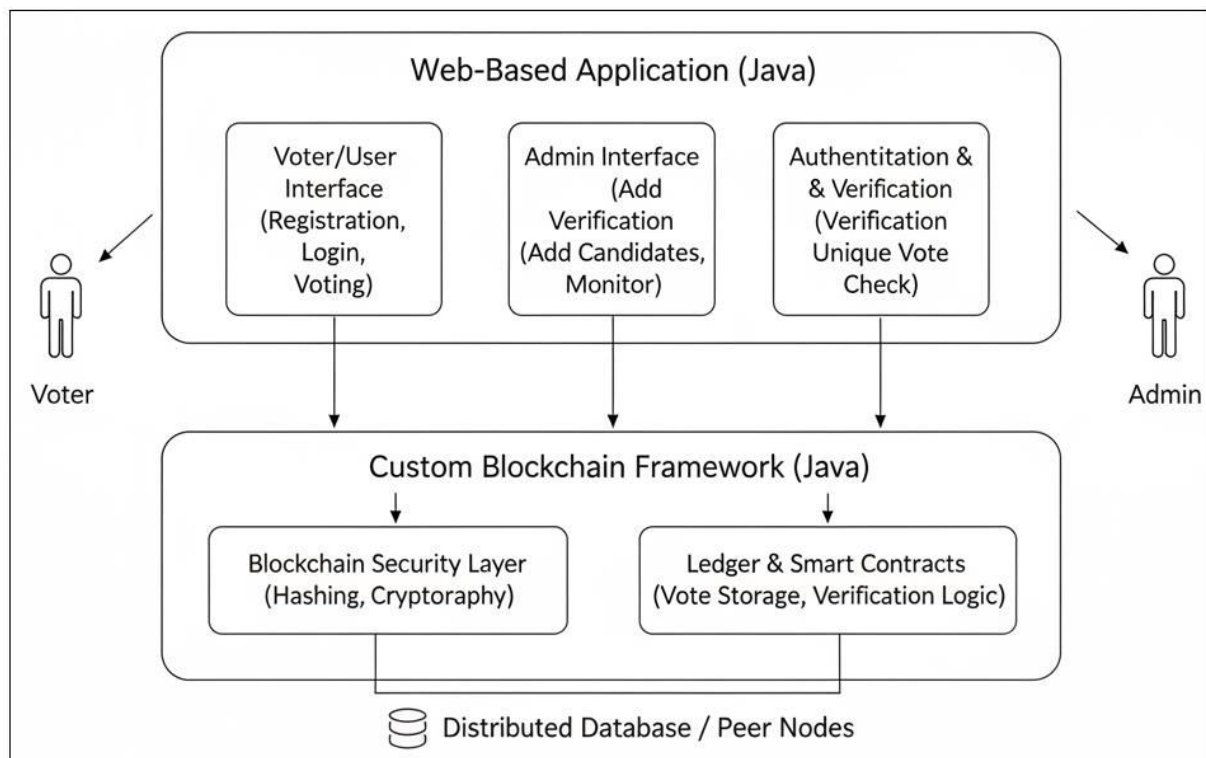


Fig.1: System Architecture Design

## V. CONCLUSION

The proposed e-Voting system using blockchain technology provides a secure, transparent, and tamper-proof framework for conducting digital elections. By integrating blockchain's immutability with advanced authentication and verification mechanisms, the system ensures that only legitimate voters can participate and each voter casts exactly one vote. The modular architecture, including the Admin, Voter, Blockchain, Authentication, and Result Generation modules, allows efficient management of election processes, real-time monitoring, and accurate vote tallying, while maintaining data integrity and voter privacy.

The use of cryptographic techniques, multi-step authentication, and blockchain-based storage significantly enhances the system's security against unauthorized access, vote manipulation, and fraudulent activities. The automatic result generation module ensures transparency and verifiability, reducing human intervention and the possibility of errors. This approach addresses many limitations of traditional paper-based voting systems, providing a modern solution suitable for digital elections in diverse environments.

**VI. ACKNOWLEDGEMENT**

I would like to sincerely thank the researchers and publishers for making their valuable resources available. I am also grateful to my guide for their constant support and guidance, and to the reviewers for their insightful suggestions. Finally, I thank the college authorities for providing the necessary infrastructure and support throughout the course of this project.

**REFERENCES**

1. S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das and Y. Park, "ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain and Zero Knowledge Property," in IEEE Open Journal of the Communications Society, vol. 5, pp. 583-598, 2024, doi: 10.1109/OJCOMS.2023.3348468
2. X. Wang et al., "Application of data storage management system in blockchain-based technology," 2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 2023, pp. 1437-1440, doi: 10.1109/EEBDA56825.2023.10090564.
3. K. M, B. S, D. B. K, D. V. G and G. S. M, "Design and Implementation of Secured E-Voting System," 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), Coimbatore, India, 2024, pp. 879-883, doi: 10.1109/ICC-ROBINS60238.2024.10533907.
4. R. Ramyadevi and V. Priya, "Block Chain-Powered E-Voting System: A Secure and Transparent Solution with Three-Tiered OTP Security Mechanism," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 728-731, doi: 10.1109/IC2PCT60090.2024.10486507.
5. M. R. P and M. T, "Secure E-Voting with Blockchain: Enhancing AES and RSA Encryption with Face Authentication Technology," 2025 5th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2025, pp. 1306-1312, doi: 10.1109/ICPCSN65854.2025.11035902.
6. K. J. Thakkar, N. Patel, C. Patel, and K. Shah, "Privacy-Preserving E-voting System through Blockchain Technology," 2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES), pp. 1–6, 2021, doi: 10.1109/TRIBES52498.2021.9751618.
7. G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," IEEE Access, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.
8. M. S. Farooq, U. Iftikhar, and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," IEEE Access, vol. 10, pp. 59959–59969, 2022, doi: 10.1109/ACCESS.2022.3180168.
9. E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan, and P. A. Sunarya, "Using Blockchain Data Security Management for E-Voting Systems," 2020 8th International Conference on Cyber and IT Service Management (CITSM), pp. 1–4, 2020, doi: 10.1109/CITSM50537.2020.9268847.
10. M. Kamran, M. H. Nasir, M. Imran, and J.-S. Yang, "Study on E-Voting Systems: A Blockchain Based Approach," 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), pp. 1–4, 2021, doi: 10.1109/ICCE-Asia53811.2021.9641914.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details