A Robust Online Voting System Based on Authorized Blockchain Infrastructure and Cryptograpic Trust Models

Ajay Rajas[1], Sherin Raj S S[2]
[1,2]*Department of Computer Science and Engineering, Sivaji College of Engineering and Technology, Tamil Nadu, India*
doi.org/10.64643/IJIRTV12I11-201418-459

***Abstract*—A blockchain based electronic voting (e-voting) system is attracting attention by the reason for enhancing transparency, security, efficiency and accessibility. From the recent years, e-voting and blockchain technologies were studied and developed significantly, which can ably reshape electoral systems globally. Countries like Switzerland, Russia, Estonia, America was experimentally implementing blockchain based e-voting systems. In this paper, we present a blockchain based e-voting system which ca ensure vote integrity through cryptographic signature and invariable ledger technologies. This system implements RSA-2048 digital signature for voter authentication, SHA-256 hashing for blockchain integrity, and B crypts for password security. It also contains Java Swing based desktop applications which have different portals for admin and voters. The system can prevent common attacks like double voting, unauthorized access, and ballot manipulation. In the system, each vote is cryptographically signed by the voter's private key and recorded in a proof of work blockchain with Merkle tree validation. This work can contribute to a practical implementation of blockchain technology for democratic process and addressing key challenges in e-voting security.**

***Index Terms*—Blockchain, electronic voting, RSA signatures, SHA-256, proof-of-work, Merkle trees, cryptographic security, digital democracy, Java Swing.**

I. INTRODUCTION

Voting plays an essential role in any democratic system by ensuring individuals to express their opinions by choose representatives. Traditional voting methods such as paper ballots and centralized electronic voting systems are facing several challenges, including vote manipulation, lack of transparency, high operational costs, and delayed result declaration. With the increasing use of digital technologies, online voting systems have emerged, but they often rely on centralized architectures that are exposed to security breaches and manipulation.

Blockchain technology grant a solution to these challenges by offering a decentralized, transparent, and immutable data storage mechanism. In an authorised blockchain environment, only verified participants are allowed to access and validate transactions, which making it suitable for secure voting applications. Cryptographic trust models are further enhancing system security by ensuring voter authentication, vote confidentiality, and data integrity. This project proposes a robust online voting system based on authorised blockchain infrastructure and cryptographic trust models. The system ensures secure vote casting, prevents duplication and manipulating, and provides transparent and verifiable election results. The proposed solution is particularly suitable for college, university, and organizational elections, where trust, security, and efficiency are essential.

II. RESEARCH CONTRIBUTION

This paper can be able to develop a secure electronic voting system using blockchain technology to ensure data integrity and transparency in voting. We tried to implement RSA-2048 digital signatures for strong voter authentication and non-repudiation. Using SHA-256 hashing and Merkle trees to guarantee immutability and efficient vote verification in system. Able to Design a desktop-based architecture which enabling secure voting even in low or no internet environment.

III. RESEARCH GAP

Current blockchain based e-voting systems were depending on fully distributed networks, it effects in

scalability and latency of the system. Systems requiring internet connectivity may affects in the deployment of the system in low resource environments. If system highly focus on security, it may affect the usability because of complex cryptographic methods. And there is lot of practical in balance to implement in real-world voting's.

IV. SYSTEM ARCHITECTURE

This system follows a layered architecture which based on a Model, Data Access, Services, Cryptography, Blockchain, and Presentation layers. The Model layer describes core entities like users, votes, elections, and blocks, meantime the Data Access layer manages SQLite database operations. The Service layer manages logic containing vote validation, authentication, and processing. The Cryptography layers in system applies RSA-2048 for digital signatures and SHA-256 for hashing. And the Blockchain layer ensures permanent vote storage using proof-of-work, and the Presentation layer provides a user-friendly interface for voters and admin.

Table:1 Algorithms Employed

Algorithm	Key Size	Purpose	Security Level
RSA	2048-bit	Digital signature	high
SHA-256	256-bit	Hashing	high
B Crypt	12 rounds	Password hashing	Very high
Secure Random	256-bit	Token generation	High

V. SECURITY ANALYSIS

The system makes sure secure voter authentication using BCrypt-based passwords and RSA-2048 digital signatures. The vote integrity is maintained through cryptographic hashing (SHA-256) and immutable blockchain storage, preventing manipulation. Mechanisms like unique vote IDs and validation checks prevent double voting and replay attacks. Voter privacy is preserved through data masking by hashing voter identities before storing them on the blockcha in.

The multi-layered security method provides strong resistance against unauthorized access and common cyber threats.

Table:2 Attack Resistance Analysis

Attack Vector	Defence Mechanism	Effectiveness
Double voting	DB uniqueness constraint + application validation	High
Vote tampering	Blockchain immutability + Merkle verification	Very High
Unauthorized access	BCrypt passwords + admin verification	High
SQL injection	Prepared Statement parameterization	Very High
Replay attack	Timestamp in signed data + unique Vote IDs	High

VI. IMPLEMENTATION

This system is implemented using Java 17 with a structured architecture separating logic, data handling, and user interface. In this system SQLite is used as the embedded database to store users, votes, and blockchain data with ACID compliance. Cryptographic operations were handled by Java's security libraries for the purpose of RSA-2048 digital signatures and SHA-256 hashing. The user interface is developed using Java Swing, it is providing separate portals for voters and administrators. In real-time vote visualization is achieved using JFreeChart, with background processes handling blockchain mining and data updates efficiently.

VII. MODULES

- User Authentication Module – Handles registration, login, and password recovery for voters and admins.
- Voter Registration Portal – GUI for new voters to create accounts, with email verification.
- Voting Module – Interface for authenticated voters to view candidates and cast votes.
- Admin Dashboard Module – Provides administrative functions: manage voters, candidates, elections, and view blockchain.

- Blockchain Core Module – Implements block, transaction, hashing, and proof-of-work.
- Network Module – Manages peer-to-peer communication and chain synchronization.
- Cryptography Module – Provides digital signatures, hashing, and encryption.
- Email Service Module – Sends password reset emails with secure tokens.
- Real-Time Results Module – Displays vote counts using dynamic charts.
- Blockchain Explorer Module – Allows browsing and verification of the blockchain.
- Database Module – Stores persistent data (voters, candidates, election settings)

VIII. DISCUSSION

The introduced system provides strong security and transparency through the integration of blockchain and cryptographic techniques. Its desktop-based architecture can be able to reduces dependency on the network connectivity and making it suitable for controlled environments. However, the lack of decentralised agreements limits scalability and fully decentralization in large-scale elections. Key management for RSA private keys will be a usability challenge for non-technical and old aged users. In future, improvements can focus on distributed deployment of the system, enhanced privacy techniques, and user-friendly key management solutions.

IX. RESULT

The Robust Online Voting System Based on Authorized Blockchain Infrastructure and Cryptographic Trust Model was successfully implemented and tested, demonstrating its ability to provide a secure, transparent, and efficient electronic voting process. The system allows verified users to cast votes, which are digitally signed and safely stored in a blockchain structure. Each vote is verified and recorded without data loss or data modification.

During testing, the system showed reliable performance with an average vote processing time less than 200 milliseconds. The blockchain mechanism ensured immutability, preventing any kind manipulation of stored votes. The use of cryptographic algorithms such as RSA-2048 and SHA-256 provided strong security for authentication and data integrity.

Also, the system prevented multiple voting and unauthorized access.

The user interface functioned smoothly, enabling both voters and administrators to interact with the system easily. Real-time vote visualization was achieved using charts, improving transparency and usability. Overall, the results confirm that the proposed system meets the objectives of security, accuracy, and efficiency in electronic voting.

X. CONCLUSION

The proposed a robust online voting system based on authorized blockchain infrastructure and cryptographic trust model demonstrates a secure and efficient blockchain-based electronic voting solution. By integrating RSA digital signatures and SHA-256 hashing, the system makes sure that strong authentication, integrity, and non-repudiation. The use of blockchain technology provides transparency and prevents vote manipulation through non-modifiable data storage. The desktop-based system implementation enables reliable operation even in low-connectivity or no network areas environments. However, in the current state it did not reach its full potential but also it can be able to provide and enhance trust and security in modern digital voting system.

REFERENCES

[1] H. O. Ohize, A. A. N. Abdalla, M. A. H. Ali, and S. M. Sani, “Blockchain for Securing Electronic Voting Systems: A Survey of Recent Advances,” *Cluster Computing*, 2025.

[2] Shaikh, M. A. Khan, S. A. Shah, and N. Javaid, “Blockchain-Enhanced Electoral Integrity: A Robust Model for Secure Voting,” *Scientific Reports*, 2025.

[3] F. H. Hadiprodjo, A. R. Pratama, B. A. Prabowo, and R. P. Sari, “Implementation of Blockchain-Based Electronic Voting System,” *Procedia Computer Science*, 2025.

[4] K. Rimba, R. W. Sari, and A. Nugroho, “Implementation of Blockchain Technology in E-Voting System,” *Teknika Journal*, 2025.

[5] S. El Kafhali, K. Salah, and M. A. Azizi, “Blockchain-Based Electronic Voting System:

Significance and Challenges," *Security and Communication Networks*, 2024.

[6] M. Sharp, J. Wilson, D. Patel, and R. Kumar, "Blockchain-Based E-Voting Mechanisms: A Survey and Comparative Study," *Blockchain: Research and Applications*, 2024.