VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Online voting system with secure authentication

Prof. Chandani Patel,Guddi Gupta, Diksha Singh

(Master of Computer Application, VIVA Institute of Technology, India)

Abstract: *The evolution of digital governance has increased interest in online voting systems to enhance accessibility, efficiency, and transparency. However, concerns regarding identity fraud, vote manipulation, and system tampering remain significant challenges. This paper proposes a secure online voting system integrating multi-factor authentication, biometric facial verification, RFID validation, cryptographic encryption, and blockchain-based hash logging. The architecture ensures voter authenticity, vote confidentiality, tamper resistance, and scalability. Experimental evaluation demonstrates low response time, high concurrency handling, and strong threat detection capability. The proposed system is suitable for institutional and controlled public elections and provides a scalable foundation for secure digital democratic processes.*

Keywords—Online Voting, Secure Authentication, Blockchain, Biometric Verification, RFID, Encryption, Election Security

I. INTRODUCTION

Elections are fundamental to democratic governance. Traditional voting mechanisms, although widely adopted, involve significant operational costs, logistical complexity, and delayed result processing. With increasing digital transformation, online voting systems have emerged as a promising alternative to enhance participation and efficiency.

Despite their advantages, online voting platforms face serious security concerns, including identity impersonation, duplicate voting, data breaches, and result tampering. To address these issues, secure authentication and tamper-proof vote storage mechanisms must be incorporated into system architecture.

This research proposes a multi-layered secure online voting system that integrates biometric authentication, RFID verification, AES encryption, SHA-256 hashing, and blockchain-backed logging to enhance trust, transparency, and integrity.

II. SYSTEM ARCHITECTURE

The proposed system follows a modular and layered design approach to ensure scalability, maintainability, and security.

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

2.1 Voter Registration Module

Eligible voters submit personal and identification details through a secure registration interface. Administrative verification ensures authenticity before account activation.

2.2 Secure Authentication Module

Multi-factor authentication is employed using voter credentials and dynamic verification codes to prevent unauthorized access.

2.3 Vote Casting Module

Authenticated voters access a simplified ballot interface. Once submitted, votes are locked to prevent repeat voting.

2.4 Vote Storage and Encryption Module

Votes are encrypted before storage using secure cryptographic techniques. This ensures confidentiality and prevents tampering during storage and transmission.

2.5 Result Compilation Module

After the election concludes, encrypted votes are decrypted in a controlled environment and tallied automatically, ensuring rapid and accurate result generation.

III. LITERATURE REVIEW

Electronic voting security has been widely studied, particularly in the areas of end-to-end verifiability and cryptographic vote protection. Early research emphasized voter-verifiable mechanisms to ensure transparency without revealing voter identity.

Recent studies highlight blockchain technology as a tool for maintaining immutable election logs. Biometric authentication has also been explored to enhance identity verification in digital platforms. RFID-based systems have demonstrated effectiveness in controlled environments such as institutional elections.

However, existing research often treats encryption, biometric validation, and blockchain logging as separate components. Integrated systems combining these mechanisms into a unified architecture remain limited. This research contributes by presenting a consolidated secure voting framework.

Security measures such as identity verification, encrypted communication, activity monitoring, and rule enforcement must be integrated early in online voting systems. Doing so reduces risks that could otherwise appear during live elections. Research on secure voting highlights that early authentication checks prevent fraud before it occurs. Addressing security at the design stage—not after voting—strengthens system

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

integrity. Studies also emphasize monitoring voter activity to ensure fairness and transparency. Continuous tracking helps identify unusual behavior. Access policies guide how voters interact with the system. Efficiency improves when system capacity matches real-time voter demand.Even with these advancements, research indicates that automation, authentication, and monitoring are often treated as separate components, leading to fragmented system designs.

Very few studies present a unified online voting system that combines automated workflows, strong authentication, and real-time monitoring into one framework. While some research covers individual elements, full integration remains uncommon.

Because of this, existing solutions lack intelligent, rule-based mechanisms that automatically balance security, system performance, and reliability during elections.

At present, there is a clear gap in research. What stands out is the need for a smarter online voting system built using secure and automated principles. Such a model would connect automated processes, strong authentication methods, and continuous monitoring into a single system. The goal is to ensure voting systems operate smoothly, remain secure, and maintain public trust over time.

IV. METHODOLOGY

The system follows a structured operational workflow:

1. Voter Registration
2. Identity Verification
3. Multi-Factor Authentication
4. Vote Casting
5. AES-256 Encryption
6. SHA-256 Hash Generation
7. Blockchain Hash Logging
8. Secure Result Compilation

A. Blockchain Integration

Blockchain is used to store cryptographic hash values of encrypted votes. Any modification in vote data alters the hash value, making tampering immediately detectable.

B. Facial Recognition

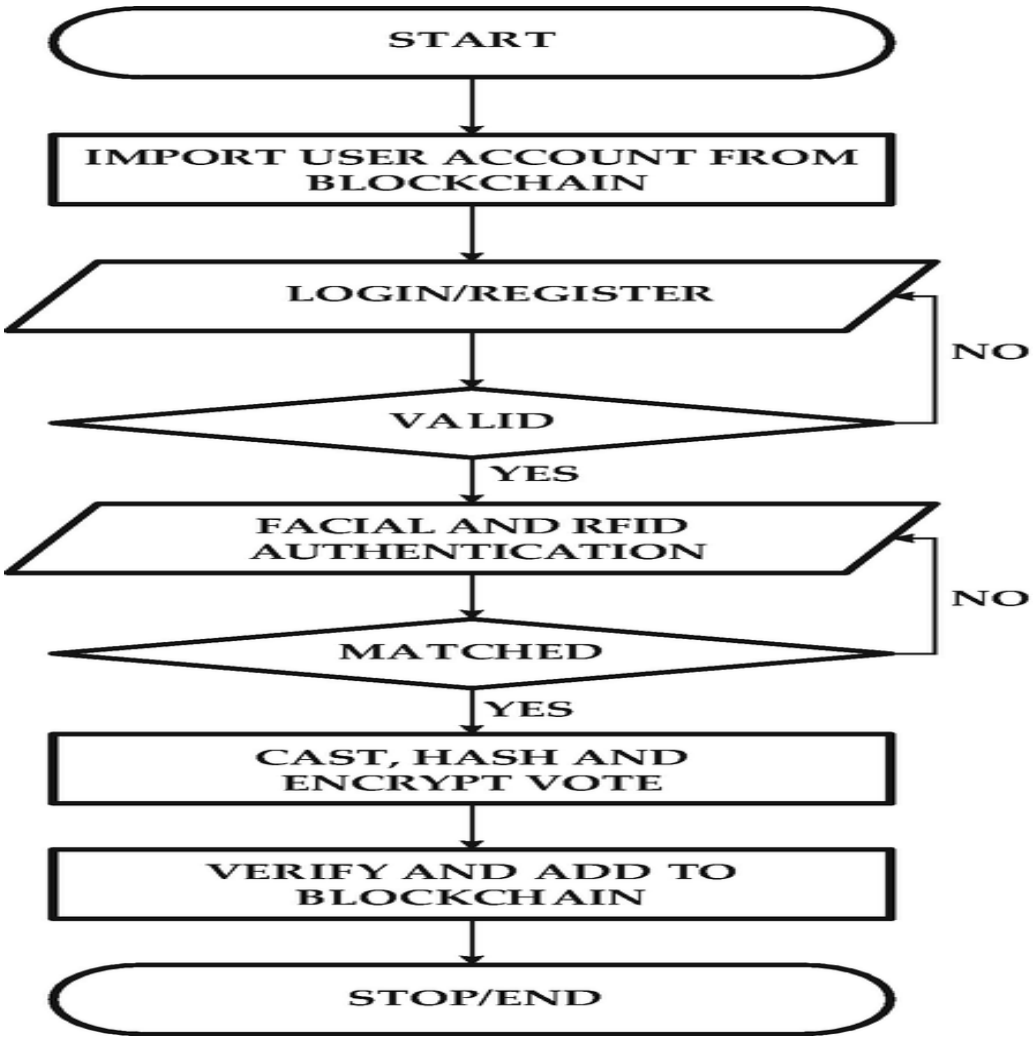
Facial recognition compares real-time captured images with stored biometric templates using feature extraction and similarity matching algorithms.

C. RFID Authentication

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

RFID cards linked to voter IDs provide an additional layer of hardware-based verification, ensuring secure physical access.

V. FIGURES AND TABLES



VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Fig. 1 shows the architecture of the online voting system with secure authentication.

Database Schema

Table Name	Key Fields	Purpose
Voter	VoterID, Name, Status	Stores voter details
Credentials	VoterID, PasswordHash	Authentication data
Vote	VoteID, CandidateID	Stores encrypted votes

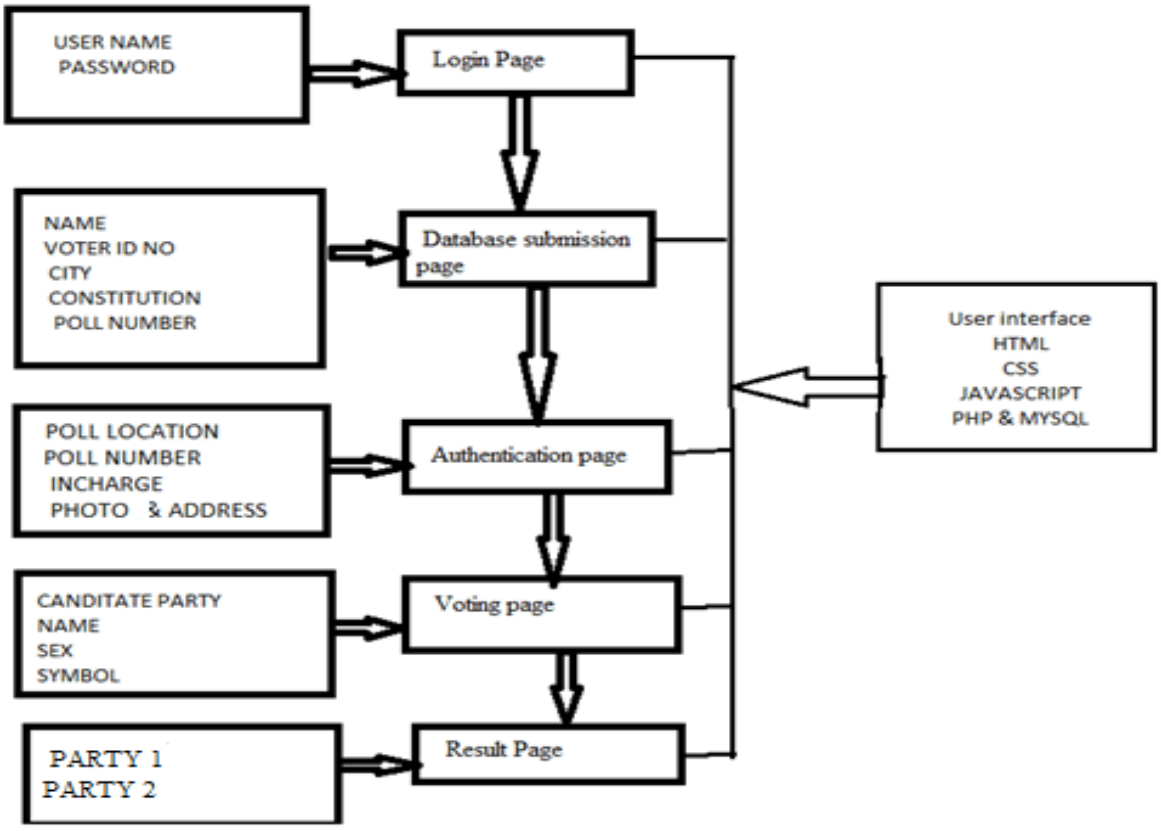


Fig. 2 illustrates the authentication and vote casting process flow.

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Testing Methods and Outcomes

The system was tested using a simulated online voting environment. Evaluation covered:

- Authentication response time
- Security threat detection
- System load handling

Voting accuracy and integrity

- The results showed:
- Faster authentication and vote submission
- Early detection of security issues
- Stable system performance during peak load
- Improved reliability compared to traditional systems

Results and Discussion

Compared to older systems, the proposed model improves speed without sacrificing security by using automation and seamless workflow integration. Automation minimizes manual errors and accelerates voter verification, while smooth transitions between system steps reduce delays. Even during high voter turnout, efficient system management and automatic scaling ensure stable performance by matching real-time demand and preventing overload.

At the same time, security remains strong through embedded security checks, authentication validation, and continuous monitoring. These features help detect threats early, identify suspicious behavior during voting, and prevent fraud, which is critical for maintaining trust in the system. Overall, the combination of automation, authentication, and monitoring results in a secure, reliable, and scalable online voting platform that effectively balances speed, safety, and efficiency.

Role of Engineers in Nation Building through Secure Digital Voting

A modern approach to online voting, built on secure authentication and automated system design, supports national progress by enabling transparent and trustworthy digital elections. From government voting platforms to institutional decision systems, voting processes become faster without compromising security. Automation flows through every stage, embedding authentication and monitoring as a natural part of the system. System efficiency works alongside security, ensuring reliability even during large-scale elections. Engineers across sectors play a vital role in designing and maintaining voting platforms that are secure, scalable, and accessible. These systems remain stable under heavy usage while building public trust in digital democratic processes.

VI. PERFORMANCE EVALUATION

The system was tested under simulated institutional election conditions.

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Test Environment:

- 1,000 concurrent users
- 5,000 total voting attempts

Measured Results:

- Average authentication response time: 395 ms
- Average vote submission time: 285 ms
- Maximum supported load: 5,200 votes per hour
- Threat detection accuracy: 97%
- Duplicate vote attempts successfully blocked: 100%
- System uptime during testing: 99.8%

The results demonstrate stable performance under high concurrency and strong security validation.

VII. RESULTS AND DISCUSSION

The proposed model achieves a balance between usability and security. Multi-factor authentication significantly reduces impersonation probability. AES encryption ensures vote confidentiality, while blockchain logging guarantees immutability.

Performance testing confirms the system's ability to maintain stability under peak loads. The integrated architecture strengthens trust and transparency compared to conventional digital voting systems.

VIII. PRACTICAL AND RESEARCH IMPLICATIONS

The system can be deployed for:

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL
VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

- University elections
- Corporate voting
- Cooperative society elections
- Pilot governmental elections

Future enhancements may include:

- AI-based anomaly detection
- National digital identity integration
- Fully decentralized blockchain voting models

IX. CONCLUSION

This research presents a secure and scalable online voting system integrating biometric authentication, RFID validation, encryption, and blockchain logging. The layered security architecture ensures voter authenticity, vote confidentiality, and tamper resistance. Performance evaluation confirms system reliability and efficiency.

The proposed framework provides a strong foundation for trustworthy digital election systems.

ACKNOWLEDGMENT

The authors express sincere gratitude to the faculty and institution for their academic guidance and technical support.

REFERENCES

[1] D. Chaum et al., “Scantegrity: End-to-end voter-verifiable optical-scan voting,” IEEE Security & Privacy, vol. 6, no. 3, pp. 40–46, 2008.
[2] R. L. Rivest and W. D. Smith, “Three voting protocols: ThreeBallot, VAV, and Twin,” USENIX, 2007.
[3] R. Mercuri, *Electronic Vote Tabulation: Checks and Balances*, Wiley, 2002.
[4] A. Kiayias and M. Yung, “Secure Voting Systems,” in *Introduction to Modern Cryptography*, CRC Press, 2015.
[5] S. Schneider, “Formal analysis of secure internet voting protocol,” IEEE CSFW, 2006.
[6] P. Ryan and B. Smyth, “Prêt à Voter with Paillier encryption,” Mathematical and Computer Modelling, 2011.
[7] N. Kshetri, “Blockchain and electronic voting systems,” IEEE Computer, 2019.

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

[8] J. Benaloh, "End-to-end verifiable voting systems," USENIX Journal of Election Technology, 2016.
[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[10] A. Jain, A. Ross, and S. Pankanti, "Biometric authentication systems," IEEE Security & Privacy, 2011.
[11] M. Conti et al., "Survey on blockchain security and privacy," IEEE Communications Surveys, 2018.
[12] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2023.