IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

Online Voting with Security

Jyoti Dattu Gardhe[1] and Pratibha D. Lagad[2]
[1,2]Department of IT Engineering,
[1,2]Adsul Technical Campus, Chas, India
pratibhalagad2@gmail.com1, jyotigardhe6@gmail.com2

Abstract: *Traditional paper-based and centralized electronic voting systems are increasingly vulnerable to security breaches, lack of transparency, and administrative manipulation. This paper proposes a robust, end-to-end verifiable online voting framework designed to maximize voter privacy while ensuring absolute data integrity. By integrating Blockchain technology for an immutable audit trail and Paillier Homomorphic Encryption, the system allows for the tallying of votes without ever decrypting individual ballots, thereby guaranteeing voter anonymity.*
To address identity theft, the framework incorporates Multi-Factor Biometric Authentication and Zero-Knowledge Proofs (ZKP) for eligibility verification. The proposed architecture is evaluated against common cyber threats, including Sybil attacks and DDoS attempts. Preliminary results and simulations demonstrate that the system maintains high throughput and low latency, making it a scalable solution for national-level elections. This research provides a blueprint for a "trustless" electoral process where the public can independently verify the results without compromising the secrecy of the ballot.

Keywords: OnlineVoting,Security,Authentication,Encry,EVoting,WebApplication,OTPVerification,Cryptography,DataPrivacy,Vote Integrity Access Control

I. INTRODUCTION

1.1 Background: Democratic integrity relies on the sanctity of the vote. Traditionally, paper-based systems provided a physical "chain of custody" that was easy for the public to understand. However, as global populations grow and digital transformation accelerates, paper systems face challenges in accessibility, speed of counting, and the logistics of remote voting.

1.2 The Problem: The Security Paradox

Current electronic voting (e-voting) systems often rely on centralized servers. This creates a "black box" environment where voters must blindly trust the software vendors and government IT administrators. Centralized systems are vulnerable to:

Single Points of Failure: A single hack can compromise millions of ballots.

Lack of Transparency: Voters cannot verify if their vote was actually counted as cast without compromising their anonymity.

Data Manipulation: Database administrators could theoretically alter tallies without leaving a visible trace.

1.3 Proposed Solution : This paper introduces an End-to-End Verifiable (E2E-V) online voting system that leverages a decentralized architecture. By combining Blockchain for immutability and Asymmetric Cryptography for privacy, we create a system where the "chain of custody" is mathematical rather than physical. This ensures that even if an attacker gains access to a portion of the network, the integrity of the election remains intact.

1.4 Objectives : The primary goal of this framework is to satisfy four critical pillars:

Authentication: Ensuring "one person, one vote" via secure digital ID.

Privacy: Separating the voter's identity from the ballot.

Integrity: Preventing any unauthorized alteration of recorded votes.

Verifiability: Providing a public "Receipt" system where any citizen can audit the results.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

II.PROBLEM STATEMENT

- Duplicate and fake voting in unsecured systems.
- Lack of proper voter identity verification.
- Possibility of data tampering and hacking attacks.
- Lack of transparency in vote counting and result declaration.
- Time-consuming manual voting and counting process.
- High cost and manpower required in traditional elections.
- Human errors during vote counting.
- Difficulty for remote voters to participate in elections.
- Delay in publishing accurate results.

III.OBJECTIVE

- To provide a secure and reliable online voting platform for voters.
- To ensure the principle of "one person, one vote" through proper authentication.
- To maintain voter privacy and data confidentiality using encryption techniques.
- To prevent fake voting and vote tampering with strong security measures.
- To provide fast, accurate, and transparent result generation.
- To enable voters to cast their vote from any location using the internet.
- To reduce the time, cost, and manpower required in traditional voting systems.
- To store votes in a secure database with restricted admin access.
- To build a system that is easy to use for voters and administrators.

IV.PROPOSED SYSTEM

• The proposed system is a web-based secure online voting application designed to allow voters to cast their votes remotely using the internet while maintaining high security and transparency.

• In this system, voters first register by providing valid details such as voter ID, email, and mobile number. During login, the system performs OTP (One Time Password) verification to ensure that only authorized users can access the voting portal. This guarantees the principle of one person, one vote.

After successful authentication, the voter is directed to the voting dashboard, where the list of candidates along with their details is displayed. The voter selects their preferred candidate and submits the vote.

Before storing, the vote is processed using encryption techniques (such as AES/RSA) to maintain confidentiality and integrity. The encrypted vote is then securely stored in the database so that it cannot be modified or accessed by unauthorized users.

The system includes an admin panel where the administrator can:

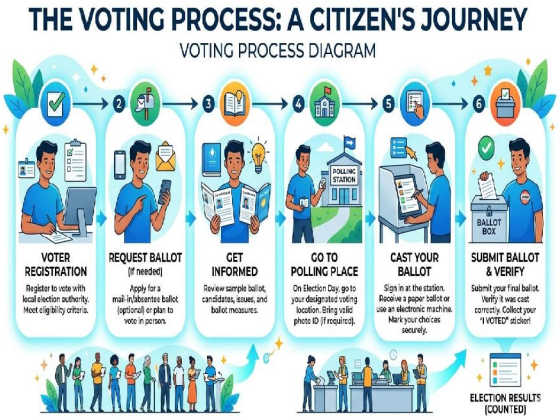
• Create and manage elections
• Add or remove candidates
• Monitor voter activity
• Control election start and end time
• View and publish results after the election ends

The result generation process is automated and accurate, providing fast and transparent results without manual counting.

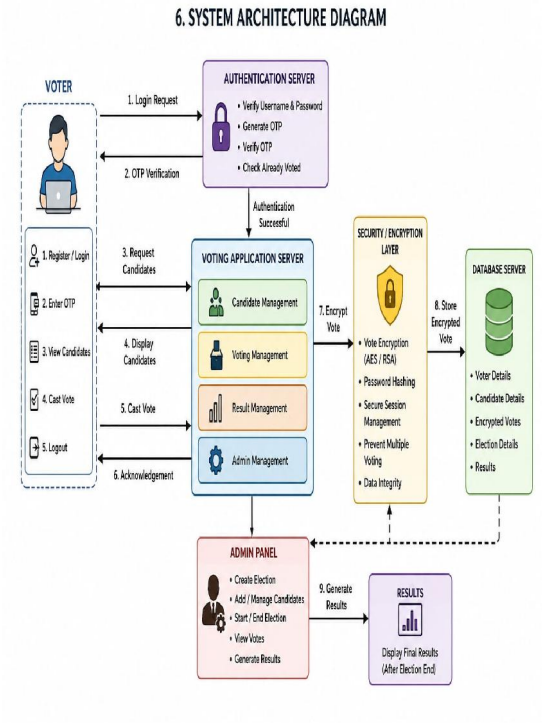
This proposed system reduces the problems of traditional voting such as fake voting, vote tampering, long queues, and high operational cost, while ensuring security, privacy, and reliability.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

V.VOTING SYSTEM



VI. SYSTEM ARCHITECTURE DIAGRAM



VII. MODULES ARCHITECTURE DIAGRAM

The system architecture of the Secure Online Voting System consists of multiple interconnected components that work together to provide a safe and reliable voting environment.

Main Components:

- Voter (User Interface)
- Authentication Server
- Voting Application Server

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

• Security/Encryption Layer
• Database Server
• Admin Panel

Working Flow:

Voter → Authentication (Login + OTP) → Voting Page → Encryption Layer → Database → Admin → Result

You should draw this block diagram showing the above flow using Word, PowerPoint, or draw.io and insert it here.

VIII. MODULES DESCRIPTION

The system is divided into different modules for proper functioning and security.

8.1 Voter Module

This module is used by the voters to participate in the election process.

Functions:

- New voter registration with valid details
- Login using username and password
- OTP verification for identity confirmation
- Viewing the list of candidates with their information
- Casting vote securely
- Restricting voters from voting more than once
- Logout after voting
- This module ensures that the voting process is simple and user-friendly for voters.

8.2 Authentication Module

This module verifies the identity of users before allowing access to the system.

Functions:

- Username and password verification
- OTP generation and validation
- Checking whether the voter is already voted or not
- Session management after successful login
- Blocking unauthorized access
- This module ensures the principle of one person, one vote.

8.3 Security Module

This module is responsible for maintaining data privacy and system security.

Functions:

- Encrypting votes before storing in database (AES/RSA)
- Password hashing for secure storage
- Secure session handling
- Preventing vote tampering
- Protecting against unauthorized database access
- Ensuring confidentiality and integrity of voting data

8.4 Admin Module

This module is used by the administrator to manage the entire election process.

Functions:

- Creating new elections
- Adding, updating, and removing candidates
- Monitoring voter participation
- Starting and ending the election
- Viewing encrypted votes

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

- Generating and publishing final results

8.5 Database Module

This module stores all the data required for the voting system in a secure manner.

Stores:

- Voter registration details
- Candidate information
- Encrypted votes
- Election details and status
- Result data
- The database is protected with restricted access and security mechanisms to prevent data leakage.

IX. SECURITY MECHANISMS

- Role-based access control for Admin and Voter
- CAPTCHA to prevent bot and automated attacks
- SSL/HTTPS protocol for secure data transmission
- Time-stamped voting logs for audit tracking
- Database access control and firewall protection
- Intrusion detection and prevention mechanisms
- Regular data backup and recovery mechanism
- Digital signature for vote authenticity
- Protection against SQL Injection and XSS attacks
- Secure API communication between modules
- Account lockout after multiple failed login attempts
- Encryption of sensitive user data in database
- Secure server configuration and patch management
- Audit trail for monitoring system activities

X. WORKING METHODOLOGY

1.Voter registers and receives a unique voter ID.
2. Voter eligibility and identity are verified by the authority.
3. Voter logs in using voter ID and password.
4. OTP is sent to the registered mobile number/email.
5. After OTP verification, a secure session is created.
6. System checks whether the voter has already voted.
7. Candidate list is fetched securely from the database.
8. Voter selects the candidate and reviews the choice.
9. Voter confirms the vote before final submission.
10. Vote is encrypted and stored securely in the database.
11. System records date and time of voting for audit tracking.
12. Confirmation message is displayed after successful vote casting.
13. Back navigation and re-voting are restricted after submission.
14. Admin dashboard monitors overall voting progress (without revealing votes).
15. Encrypted votes remain locked until the election ends.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

XI. ADVANTAGES

1. Secure, transparent, and tamper-proof voting process
2. Prevents duplicate and fake voting through strong authentication
3. Maintains voter privacy using encryption techniques
4. Saves time and reduces overall election cost
5. Provides fast and accurate result generation
6. Accessible from anywhere with an internet connection
7. Reduces manpower and paperwork compared to traditional voting
8. Eliminates long queues and manual counting errors
9. Easy-to-use interface for voters and administrators
10. Reliable data storage with restricted access control

XII. LIMITATIONS

1. Requires a stable internet connection to access the system
2. Security depends on proper system implementation and maintenance
3. Digital literacy is required for voters to use the system effectively
4. Risk of cyberattacks if security measures are weak
5. Dependence on servers and continuous power supply
6. Initial setup and development cost can be high
7. Possibility of technical issues or server downtime during voting
8. OTP delivery issues due to network problems

XIII. FUTURE SCOPE

- Integration with biometric authentication (fingerprint/face recognition) for stronger identity verification
- Use of blockchain technology to enhance transparency and tamper resistance
- Development of a mobile application for easier and wider access
- Multi-language support to make the system usable for diverse users
- Implementation of AI-based fraud detection to identify suspicious activities
- Cloud deployment for better scalability and availability
- Real-time result analytics and reporting dashboard
- Integration with government voter databases for automatic verification

XIV. CONCLUSION

The proposed online voting system with security provides a reliable, efficient, and transparent method for conducting elections in a digital environment. By implementing strong authentication mechanisms such as OTP verification, password hashing, and role-based access control, the system ensures that only authorized voters can participate and that the principle of one person, one vote is maintained.

The use of encryption techniques like AES/RSA secures the votes before storage, protecting voter privacy and preventing vote tampering. Secure database management and session handling further enhand accurate result generation with minimal human intervention.

Overall, the proposed system demonstrates how modern security technologies can be applied to create a trustworthy and user-friendly online voting platform suitable for institutions, organizations, and future large-scale elections.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

REFERENCES

[1] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-Resistant Electronic Elections," ACM Workshop on Privacy in the Electronic Society, 2005.
[2] D. Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Security & Privacy, vol. 2, no. 1, pp. 38–47, 2004.
[3] R. L. Rivest and W. D. Smith, "Three Voting Protocols: Three Ballot, VAV, and Twin," USENIX/ACCURATE Electronic Voting Technology Workshop, 2007.
[4] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.
[5] OWASP Foundation, "Web Application Security Guidelines." Available: https://owasp.org
[6] B. Adida, "Helios: Web-based Open-Audit Voting," USENIX Security Symposium, 2008.
[7] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)," FIPS PUB 186-4, 2013.
[8] K. Sampigethaya and R. Poovendran, "A Survey on Mix Networks and Their Secure Applications," Proceedings of the IEEE, vol. 94, no. 12, 2006.
[9] A. Kiayias and M. Yung, "Self-Tallying Elections and Perfect Ballot Secrecy," Public Key Cryptography (PKC), 2002.
[10] S. Schneier, Applied Cryptography, 2nd ed., Wiley, 1996