



# 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 15, Special Issue 1, January 2026**

# Secure E-Voting System

Vighney Adurkar<sup>1</sup>, Nutan Acharekar<sup>2</sup>, Yash Bhingarde<sup>3</sup>, Bharat Bhakare<sup>4</sup>

Department of Information Technology Engineering, Indala College of Engineering, Mumbai, India<sup>1234</sup>

**ABSTRACT:** Electronic voting (E-voting) systems are transforming the traditional election process by enabling voters to cast their votes electronically through a secure web-based platform. Conventional voting systems suffer from several drawbacks such as long queues, high manpower requirements, paper wastage, vote rigging, delayed results, and human errors. This paper presents a detailed design and implementation of a secure and efficient online e-voting system using user authentication, database validation, and access control mechanisms. The proposed system ensures fairness, transparency, integrity, confidentiality, and availability of votes. It also prevents duplicate voting and reduces human intervention. The system is implemented using a secure web framework and a centralized relational database for storing voter, candidate, and election-related information.

**KEYWORDS:** E-Voting System, Online Voting, Security, Authentication, Database Validation, Access Control.

## I. INTRODUCTION

Voting plays a vital role in maintaining democracy in any nation. Traditional voting systems are mostly paper-based and require significant manpower, time, infrastructure, and financial resources. These systems also face challenges such as booth capturing, fake voting, proxy voting, ballot stuffing, counting errors, and delayed declaration of results. As technology advances, there is a growing demand for secure, fast, and cost-effective digital solutions for election management.

An online e-voting system allows voters to participate in elections using the internet from any authorized location. This increases voter participation, especially for students, working professionals, and citizens living in remote areas. However, security and trust are the main concerns in online voting systems. Challenges such as unauthorized access, identity manipulation, vote tampering, server attacks, and multiple voting must be addressed efficiently.

This paper proposes a secure and efficient online e-voting system based on strong user authentication, database verification, encryption techniques, and role-based access control. The proposed system minimizes human intervention, ensures accurate result processing, and enhances the credibility of the election process.

## II. SYSTEM MODEL AND ASSUMPTIONS

The proposed online e-voting system is designed using a client-server architecture and consists of the following major components:

1. Administrator Module
2. Voter Module
3. Candidate Module
4. Centralized Database Server
5. Web Application Interface

The administrator is responsible for managing elections, adding candidates, verifying voter records, monitoring voting activities, and generating final results. The voter module allows registered voters to log in, view candidate information, and cast their vote. The candidate module stores details of all contesting candidates. All system data is stored securely in a centralized database.

Assumptions of the system:

- Every voter possesses a valid and unique voter ID.
- Voters have access to internet-enabled devices such as mobile phones, laptops, or desktops.

- Each voter is allowed to vote only once.
- The server and database are protected using proper security mechanisms such as firewalls and authentication protocols.

The system uses role-based access control where the administrator and voters have separate privileges. This prevents unauthorized access and misuse of system functionalities.

### **III. PROPOSED E-VOTING SYSTEM**

The proposed system operates in three main phases: Registration Phase, Authentication Phase, and Voting Phase. A. Registration Phase

In the registration phase, the voter creates an account in the system by entering personal details such as full name, voter ID number, date of birth, email ID, mobile number, and address. The system validates the voter ID with the existing voter database to ensure that only eligible voters can register. If the voter ID is verified successfully, the user account is created and stored in the database. Duplicate voter registration is strictly prevented.

#### **B. Authentication Phase**

After successful registration, the voter logs into the system using a unique username and password. The entered credentials are verified with the stored database records. If the credentials match, the voter is authenticated and granted access to the voting dashboard. If invalid credentials are entered, access is denied and security alerts are generated. This ensures secure access to the voting system.

#### **C. Voting Phase**

After successful authentication, the voter is redirected to the voting page where the list of candidates along with their party names and symbols is displayed. The voter can carefully review the candidate details and cast one vote for the desired candidate. Once the vote is submitted, it is securely stored in the database.

The system automatically updates the voting status of that voter and prevents further voting from the same account. This ensures the principle of “One Person – One Vote.”

### **IV. SECURITY MECHANISMS**

Security is the most critical requirement of any online e-voting system. The following security mechanisms are implemented in the proposed system:

#### **1. User Authentication:**

Only verified and registered users can log into the system. Unique usernames and strong password policies ensure secure access.

#### **2. One-Time Voting Restriction:**

Each voter is strictly allowed to vote only once. The database maintains vote status flags to prevent duplicate voting.

#### **3. Data Encryption:**

Sensitive data such as passwords, voter credentials, and vote records are stored in encrypted format inside the database.

#### **4. Role-Based Access Control:**

The system strictly separates the privileges of administrators and voters. Voters can only cast votes, while administrators can manage elections and view aggregated results.

#### **5. Secure Database Management:**

The centralized database is protected using authentication credentials, firewall rules, and access permissions to avoid data leaks and tampering.

#### **6. Prevention of Unauthorized Access:**

Session management, automatic logout, and restricted URL access protect the system from unauthorized access.

**V. RESULT AND DISCUSSION**

The proposed online e-voting system was tested under various conditions using multiple user accounts and simulated elections. The system performed efficiently with fast login response time, secure vote casting, and accurate vote counting. The one-time voting restriction successfully prevented duplicate voting. All votes were securely stored in the database without any data loss or inconsistency.

The administrator was able to monitor voting activity in real-time and generate accurate election results instantly after the voting session ended. The system significantly reduced human effort, paper usage, and manual errors. Compared to traditional voting systems, the proposed system offered higher transparency, faster processing, and improved accessibility.

**VI. CONCLUSION**

This paper presented a detailed design and implementation of a secure and efficient online e-voting system without the use of external verification mechanisms. The proposed system ensures voter authenticity through strong authentication, database validation, and strict access control. It guarantees fair elections by enforcing one-time voting, data encryption, and secure result management.

The system reduces cost, manpower, and time required for conducting elections while improving voter participation and trust. In the future, the system can be further enhanced by integrating biometric authentication such as fingerprint or face recognition, blockchain-based vote storage, and advanced intrusion detection mechanisms to further strengthen security.

**REFERENCES**

1. Chaum, D., "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Security & Privacy, 2004.
2. Cetinkaya, O., "Analysis of Security Requirements for E-Voting Systems," IEEE Conference, 2008.
3. Shahzad, B., Crowcroft, J., "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," IEEE, 2019.
4. G. Neumann, "Security of Electronic Voting," ACM Conference, 2004.
5. A. Fujioka et al., "A Practical Secret Voting Scheme for Large Scale Elections," Advances in Cryptology, 1992.



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