IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

WEB-BASED ELECTRONIC VOTING: SECURITY CHALLENGES AND A PROPOSED SECURE E-VOTING FRAMEWORK

[1]Vaishnavi Nandkishor Wakchaure, [2]Priyanka Vilas Jadhav, [3]Rajashri Narayan Jadhav

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor

[1]Department of Computer Science,

[1]S. S. G. M. College, Kopargaon, Maharashtra, India

Abstract: Electronic voting has become an important area of research due to the increasing use of digital technologies in election processes. A secure voting system must provide voter authentication, vote integrity, privacy, reliability and protection against unauthorized access. India currently uses Electronic Voting Machines (EVMs) with Voter Verifiable Paper Audit Trail (VVPAT), which is fundamentally different from Internet-based voting. This paper studies existing electronic and web-based voting approaches and identifies major security challenges associated with online voting. Based on these challenges, a secure web-based e-voting framework is proposed for controlled and institutional elections. The proposed framework includes authenticated voter access, role-based authorization, election management, candidate management, duplicate-vote prevention, secure database operations and automated result generation. Security measures such as password protection, parameterized database queries, session management, input validation and secure communication are considered. The proposed framework is evaluated conceptually against important security requirements including authentication, integrity, confidentiality, availability and non-duplication. The study concludes that web-based voting can improve accessibility and administrative efficiency for suitable controlled elections, but Internet-based voting introduces significant cybersecurity and privacy challenges. Therefore, further research is required in areas such as cryptographic verification, privacy preservation and end-to-end verifiable voting.

Index Terms - Electronic Voting, E-Voting, Web-Based Voting, Voting Security, Voter Authentication, Cybersecurity, Vote Integrity, Digital Elections.

I. INTRODUCTION

Voting is a fundamental component of a democratic system. It provides eligible citizens with the opportunity to participate in the selection of representatives. Therefore, an election system must maintain accuracy, fairness, reliability, security and voter confidence. Technological development has resulted in the use of electronic systems for several stages of election management. Electronic voting can reduce manual work, automate vote counting and improve the efficiency of election administration. However, introducing electronic and network-based technologies also creates new security challenges.

In India, elections are conducted using Electronic Voting Machines along with the Voter Verifiable Paper Audit Trail system. The Election Commission of India describes its EVM system as a standalone, non-networked system, with the Ballot Unit and Control Unit forming the primary components and VVPAT providing a paper-based verification mechanism.

A web-based voting system is different because it uses a network-connected application through which voters can access an election remotely or from an institutional environment. Such a system may provide advantages such as convenient access, automated processing and centralized election management. At the same time, it may be exposed to threats involving authentication, network communication, application vulnerabilities, database attacks and privacy.

Previous research has demonstrated both the potential and limitations of web-based voting. Helios, for example, is an open-source web-based electronic voting system designed with end-to-end verifiability. However, research has identified ballot-secrecy and replay-related vulnerabilities in Helios, demonstrating that verifiability alone does not eliminate all security problems.
Therefore, the objective of this research is to study the security requirements of web-based electronic voting and propose a secure framework suitable for controlled elections such as institutional, organizational and academic elections.

II. VOTING AND E-VOTING SYSTEMS

Traditional voting generally requires voters to visit designated polling locations, verify their eligibility and cast a physical ballot. Although this approach is well established, it requires significant administrative resources and physical infrastructure.

Electronic voting refers to the use of electronic technology to record, process or count votes. Electronic voting can exist in different forms, including electronic voting machines, polling-station electronic systems and Internet-based voting.

The major requirements of an electronic voting system include:

- **Authentication:** Only eligible voters should be allowed to participate.
- **Eligibility:** A voter should be permitted to vote only in elections for which they are authorized.
- **Uniqueness:** A voter should not be able to cast more than one valid vote in the same election.
- **Integrity:** Votes should not be modified or deleted without authorization.
- **Privacy:** The voter's choice should remain confidential.
- **Availability:** The voting service should remain accessible during the election.
- **Auditability:** Important election activities should be capable of being examined.
- **Accuracy:** The final result should correctly represent the recorded valid votes.

India's EVM/VVPAT model addresses these requirements through a combination of technology and election procedures. The ECI emphasizes that its EVMs are standalone systems and are not connected to external networks.

A web-based e-voting system introduces a different security model because the voting application, communication network, web server and database become part of the trusted computing environment.

III. EXISTING WEB-BASED E-VOTING APPROACHES

Several electronic voting systems have been proposed and studied internationally. One important research system is **Helios**, an open-source web-based voting system designed to provide end-to-end verifiability. Its objective is to allow appropriate participants to verify that election processing has been performed correctly.

However, research on Helios has identified security weaknesses. Cortier and Smyth demonstrated a vulnerability involving ballot secrecy in Helios in which ballot replay could compromise voter privacy.

Other research has also examined vulnerabilities associated with web browsers and web applications used in electronic voting. A security analysis of Helios reported that weaknesses in browser and web-security mechanisms could potentially affect sensitive information and election results.

These studies demonstrate an important research observation:

A web-based voting system cannot be considered secure merely because it provides user authentication or cryptographic verification. Security must be considered across the complete voting process.

The proposed research therefore focuses on multiple layers of security rather than relying on a single mechanism.

IV. SECURITY CHALLENGES IN E-VOTING

Web-based electronic voting introduces several security challenges.

4.1 Voter Authentication

The system must verify that a voter is a legitimate registered participant. Weak authentication can allow unauthorized users to gain access to voting functionality.

Secure authentication should use appropriate password protection and session management. OWASP identifies authentication as the process of verifying the identity of a user and recommends secure handling of authentication and session mechanisms.

4.2 Duplicate Voting

A voter should normally be able to cast only one valid vote in a particular election. The application should verify the voter's previous voting status before accepting a new vote.

4.3 Unauthorized Access

Administrative functions must be protected from ordinary voters. Role-based authorization can restrict access according to the user's assigned role.

4.4 SQL Injection

The voting database contains important election information and therefore can become a major attack target. SQL injection can occur when untrusted input is directly incorporated into database queries.

Parameterized queries and prepared statements are recommended defenses against SQL injection.

4.5 Session Attacks

A web voting application uses sessions to maintain authenticated users. If session identifiers are compromised, an attacker may be able to impersonate a legitimate user.

OWASP recommends secure session identifiers, session regeneration after authentication and appropriate session termination.

4.6 Vote Privacy

The system should prevent unauthorized parties from determining which candidate a particular voter selected. Maintaining voter identity and vote secrecy is one of the most difficult requirements in electronic voting.

4.7 Database Manipulation

Unauthorized modification of stored vote records can directly affect election results. Database permissions and application-level authorization must therefore be carefully controlled.

4.8 Denial of Service

An attacker may attempt to make the voting service unavailable. Availability is particularly important during the limited period in which an election is active.

4.9 Client-Side Security

In web-based voting, the voter's device and browser become part of the voting environment. Malware or compromised software may affect the user's interaction with the voting application.

These challenges demonstrate why secure web-based voting requires a combination of authentication, authorization, application security, database security and election-specific controls.

V. PROPOSED SECURE WEB-BASED E-VOTING FRAMEWORK

This research proposes a secure web-based e-voting framework intended primarily for controlled elections.

The framework consists of five major components:

1. **Authentication and User Management**
2. **Election Management**
3. **Voting Management**
4. **Security and Database Layer**
5. **Result Management**

5.1 Authentication and User Management

Users are registered in the system and assigned appropriate roles. Two major roles are considered:

- Administrator
- Voter

The administrator manages election-related activities, while the voter is permitted to participate in active elections.

The authentication process is:

User → Login → Credential Verification → Role Verification → Authorized Dashboard

5.2 Election Management

The administrator can create and manage elections.

An election may contain:

- Election name
- Start date
- End date
- Election status
- Candidate information
- Eligible voters

The election can have three basic states:

Upcoming → Active → Closed

Voting is permitted only during the active period.

5.3 Voting Management

The voter first authenticates with the system. The system then checks whether the voter is eligible and whether the selected election is active.

The voting process is:

Login → Select Election → View Candidates → Select Candidate → Confirm Vote → Validate → Record Vote

Before recording the vote, the system checks:

1. Is the voter authenticated?
2. Is the voter eligible?
3. Is the election active?
4. Has the voter already voted?
5. Is the selected candidate valid?

Only when all validations are successful is the vote accepted.

5.4 Database Layer

A relational database can be used to store election information.

Important entities include:

- User
- Voter
- Election
- Candidate
- Vote
- Result

A unique relationship between a voter and an election can be used to help prevent duplicate voting.

5.5 Result Management

After an election is closed, valid votes are counted candidate-wise.

The result process is:
Recorded Votes → Validation → Candidate-wise Counting → Result Generation

The system can automatically display the number of valid votes received by each candidate.

VI. SECURITY ANALYSIS

The proposed framework is analyzed according to important security properties.

Table 1

Security Requirement	Proposed Mechanism
Authentication	User credential verification
Authorization	Role-based access control
Duplicate prevention	Voter-election validation
Vote integrity	Controlled database operations
Database security	Parameterized queries
Session security	Secure session management
Input security	Input validation
Communication security	HTTPS
Auditability	Election and administrative logs
Availability	Server and application monitoring

6.1 Authentication Security

Only registered users should be permitted to access protected functions. Strong password storage and secure authentication practices should be used.

6.2 Authorization Security

The system should verify the user's role before providing access to administrative functions. A voter attempting to access an administrator function should receive an authorization failure.

6.3 Database Security

Parameterized queries should be used to reduce SQL injection risks. OWASP recommends prepared statements or parameterized queries as a primary defense against SQL injection.

6.4 Session Security

Sessions should use secure, unpredictable identifiers and should be terminated after logout or timeout.

6.5 Vote Integrity

Once a valid vote is recorded, unauthorized users should not be able to modify the vote record.

6.6 Privacy

Voter identity and vote selection should be separated as far as practical within the system design. A production-grade system would require stronger cryptographic techniques to provide robust ballot secrecy.

6.7 Limitations of the Security Model

The proposed framework improves application-level security but does not eliminate all threats associated with Internet voting. In particular, compromised client devices, advanced server attacks, coercion and sophisticated privacy attacks remain important research challenges.

VII. DISCUSSION AND FUTURE SCOPE

The proposed framework demonstrates how common web-security mechanisms can be combined with election-specific controls to develop a more secure web-based voting environment. Compared with traditional voting, a web-based system can reduce manual processing and provide faster result generation. It can also support controlled elections where participants are already registered within an institution or organization.

However, security must remain the primary consideration. Previous research on web-based voting systems demonstrates that vulnerabilities can exist even in systems designed with advanced verification mechanisms. Helios research has identified issues involving ballot secrecy and vote manipulation, highlighting the importance of continuous security analysis.

Future versions of the proposed framework can investigate:

- Multi-factor authentication.
- Digital signatures.
- End-to-end verifiable voting.
- Homomorphic encryption.
- Zero-knowledge proofs.
- Tamper-evident audit logs.
- Privacy-preserving vote storage.
- Independent security auditing.
- Penetration testing.
- Secure cloud deployment.

End-to-end verifiability is particularly important for future research because it can provide stronger evidence that votes were properly recorded and counted. Another important research direction is the development of privacy-preserving mechanisms that prevent election authorities or other parties from linking voters to their selected candidates.

Therefore, future work should move beyond basic database-based voting toward cryptographically verifiable and privacy-preserving electronic voting.

VIII. CONCLUSION

This paper examined electronic voting systems, existing web-based voting approaches and the security challenges associated with Internet-based elections. The study highlighted that electronic voting must address authentication, authorization, vote integrity, privacy, duplicate voting, database security and availability.

India's EVM/VVPAT system represents a different approach from Internet voting because the ECI's EVM architecture is standalone and non-networked. Therefore, a web-based voting framework should not be considered a direct replacement for India's current public election infrastructure.

A secure web-based e-voting framework was proposed for controlled elections. The framework combines voter authentication, role-based authorization, election management, duplicate-vote prevention, secure database operations, session management and automated result generation. The research also demonstrates that application-level security alone is insufficient for high-stakes Internet elections. Previous studies of systems such as Helios show that ballot privacy, verifiability and protection against sophisticated attacks remain challenging research problems.

The proposed framework can therefore serve as a foundation for further research into secure digital elections. Future work should focus particularly on cryptographic verification, voter privacy, end-to-end verifiability and independent security evaluation.

REFERENCES

[1] Election Commission of India, "EVM/VVPAT," Election Commission of India, Government of India.
[2] V. Cortier and B. Smyth, "Attacking and Fixing Helios: An Analysis of Ballot Secrecy," *Journal of Computer Security*, vol. 21, no. 1, pp. 89–148, 2013.
[3] M. Heiderich, T. Frosch, M. Niemietz and J. Schwenk, "The Bug that Made Me President: A Browser- and Web-Security Case Study on Helios Voting," International Conference on E-Voting and Identity, 2011.
[4] M. Meyer and B. Smyth, "Exploiting Re-Voting in the Helios Election System," *Information Processing Letters*, vol. 143, pp. 14–19, 2019.
[5] OWASP Foundation, "Authentication Cheat Sheet," OWASP Cheat Sheet Series.
[6] OWASP Foundation, "Session Management Cheat Sheet," OWASP Cheat Sheet Series.
[7] OWASP Foundation, "SQL Injection Prevention Cheat Sheet," OWASP Cheat Sheet Series.
[8] OWASP Foundation, "Database Security Cheat Sheet," OWASP Cheat Sheet Series.