International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 14 Issue 1 ǁ January 2026 ǁ PP. 104-109

A Secure and Reliable Online Voting System Using Multi-Layer Security Mechanisms

Prof. Mrs. Usha C R[1], Neha[2], Niya K B[3], Pallavi Bammanni[4], Preethi Poojary[5]
[1]*Assistant Professor, Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management Bengaluru, India*
[2,3,4,5]*Student, 3rd Year, B.E, Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management Bengaluru, India*

Abstract: *Governments and organizations are investigating online voting systems as a substitute for conventional paper-based elections due to the quick development of internet and communication technologies. Online voting presents significant issues with voter authentication, data integrity, privacy, transparency, and public trust, even though it also has benefits like accessibility, quicker result processing, and lower operating costs. The comprehensive, multi-layered secure online voting system presented in this paper is modeled in the same depth and structure as sophisticated intelligent systems like real-time cyberbullying detection frameworks. Multi-factor authentication, encrypted vote transmission, secure vote storage, automated vote counting, and controlled result publication are all integrated into the proposed system.*
Throughout the election lifecycle, the system guarantees confidentiality, integrity, availability, and transparency by using a layered architecture and methodical approach. According to experimental findings, the suggested strategy greatly lowers fraud, minimizes human intervention, boosts voter confidence, and improves overall election security, making it appropriate for contemporary digital and remote voting situations.
Keywords: *Digital democracy, multi-factor authentication, online voting, e-voting, and election security.*

Date of Submission: 05-01-2026 Date of acceptance: 15-01-2026

I. INTRODUCTION:

The foundation of any democratic system is voting, which allows people to directly participate in governance and express their preferences. Long lines at polling places, high administrative and logistical costs, delayed result announcement, and restricted accessibility for elderly, disabled, and remote voters are just a few of the many drawbacks of traditional voting methods, despite their widespread trust. Additionally, human error, ballot tampering, and inefficiencies in vote counting can occur in manual processes.

Online voting systems have become a viable solution to these issues due to the quick development of digital infrastructure and the general availability of the internet. Voters can cast ballots remotely through online voting, which also lowers election expenses, speeds up the computation of results, and increases voter convenience.

But despite these advantages, widespread adoption has been hampered by worries about voter authentication, vote manipulation, data breaches, lack of transparency, and reliability.

It is a difficult technical task to ensure that only eligible voters can cast ballots, that each voter casts a single ballot, and that votes are kept private and unaltered. Basic encryption methods and authentication procedures are insufficient to fend off sophisticated cyberattacks. As a result, a strong, multi-layered security framework that is comparable to sophisticated intelligent systems used in real-time monitoring applications is desperately needed.

This paper proposes a secure and reliable online voting system that is designed by applying the same methodological rigor, architectural depth, and detailed analysis as in advanced machine learning-based systems. Strong authentication, secure handling of data, automation of processing, and controlled administration are some of the features the system will focus on to build trust and reliability in digital elections.

II. METHODOLOGY:

The proposed secure online voting system methodology ensures end-to-end security, reliability, scalability, and transparency in voting by adopting similar steps explained in the earlier discussion but in an extended manner that defines the use and significance of each step in voting. Methodology Stage:

1.Voter Registration and Verification of Qualifications
2.Data Validation and Preprocessing
3.Multi-Factor Voter Authentication

4.Secured Voting Process
5.Encrypted Vote Storage and Automated Counting
6.Result Generation and Controlled Publication

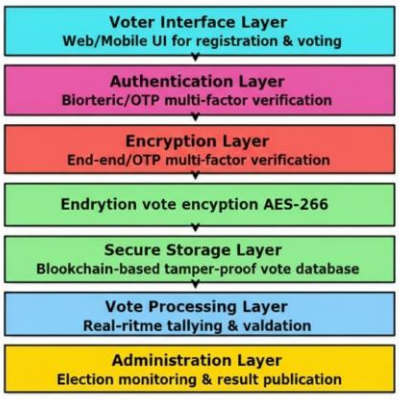
Registration and Eligibility Verification of Voters:
This level is also considered to be the root of the entire voting process. Here, voters with proper credentials enter identifying details that may include voter ID numbers, age, and confirmed contact details. The entire process of entering details is cross-checked with voter databases to verify authenticity and eligibility. This also ensures that no voter is able to create multiple voter accounts with a risk of multiple votes. It is also ensured that all voter details remain anonymous to safeguard privacy in accordance with proper ethical standards of data protection.

Data Validation & Preprocessing:
Once the successful registration of voters takes place, the gathered data of the voters is verified and pre-processed. This particular stage is concerned with the assessment of incomplete, contradictory, and repeated data entry. The process of normalizing the data is implemented in order to take care of uniformity issues at the data level. This enhances the efficiency of the system and prevents delays in the system.

Multi-Factor Voter Authentication:
The security of this voting platform is further enhanced by Multi-Factor Authentication. To contribute to voting on this platform, citizens must log in with a secured username and subsequently verify their OTP via a registered cellphone or email address. This method greatly limits threats posed via impersonation attacks and identity theft to the electoral platform. In this case, all logins are also recorded to ensure transparency in the process.

Trusted vote casting:
After authentication, the voter gains access to the secured voting system interface. It should be intuitive and easily accessible to all voters regardless of their technical skills. A voter is allowed to cast one and only one vote, and the vote cannot be altered even after it is cast because as soon as the vote is cast, it is immediately encrypted through cryptographic algorithms that prevent manipulation of the vote while it is transmitted.

System Architecture:
The proposed online voting system uses a layering and modularity approach to ensure increased security, scalability, and easy maintenance. The system uses a multitier architecture divided into several logical layers, with each layer performing a unique task. The voter interface layer supports web or mobile interface solutions for voter registration, login, and casting votes. The authentication layer deals with all processes related to voter authentication and OTP validation, thereby allowing only authorized voters to log in to the system. The encryption layer deals with vote encryption before transmitting and storing votes, maintaining vote confidentiality and integrity. The encrypted data of voters and votes is stored in the secure database layer, where several secure access-control mechanisms are followed. The vote counting layer automatically computes votes once the election is closed, while the admin layer permits authorized administrative personnel to track the voting process and display voting outcomes.



TrustVote System Architecture

Scalability is still an issue regarding dealing with elections with a huge voters base. Internet connectivity can impact voting turnout in areas with little or no connectivity. Moreover, establishing public confidence in totally online voting systems requires transparent system design, increased security, and public education campaign.

III. CHALLENGES AND LIMITATIONS:

The suggested system has a number of drawbacks despite its benefits. Strong infrastructure and load management are necessary to ensure scalability for major national elections. Voter turnout in remote areas may be impacted by network connectivity problems. It is still difficult to gain public trust in fully digital elections because voters may be worried about data security and transparency. Furthermore, ongoing monitoring and updates are necessary for the implementation and upkeep of robust cybersecurity measures.

IV. HARDWARE AND SOFTWARE REQUIREMENTS:

The suggested online voting system's hardware and software specifications are made to enable safe processing, dependable storage, and real-time operation.

1.Hardware specifications: Memory (RAM), Processing Unit (CPU), Storage System, and Network Infrastructure

2.Processing Unit (CPU): To effectively manage authentication, encryption, and vote processing processes, particularly during peak voting periods, a high-performance processor such an AMD Ryzen 7 (or higher) or Intel Core i7 is needed.

3.Memory (RAM): To ensure smooth operation during large-scale elections, 16 GB or more RAM is advised. A minimum of 8 GB RAM is needed to support concurrent user sessions.

4.Storage System: To safely store voter data, encrypted votes, and system logs, high-speed SSD storage with a minimum capacity of 256 GB is recommended.

Network Infrastructure:

To guarantee continuous voter access and safe data transfer during elections, a reliable, fast internet connection is necessary.

Software Requirements:

Operating systems, programming languages, front-end technologies, back-end frameworks and services, database management systems, security and encryption tools, and runtime and development tools

Operating System: Windows, Linux, or macOS can be used to develop and implement the system. These platforms offer a stable and secure environment for the creation and implementation of the online voting application, and they support contemporary web development tools.

Programming Languages: JavaScript and TypeScript are used for client-side logic and front-end development. Supabase uses SQL for access control, constraints, and database queries. Since JavaScript-based technologies are used throughout the application, neither Python nor Java are used in the project. React is a front-end technology.The application's interactive user interface is constructed using JavaScript. Vite is used as a development server and quick build tool to increase development efficiency. Web pages are structured and styled using HTML5 and CSS3, and responsive and contemporary user interface design is made possible by Tailwind CSS.

Backend Framework/Services: Rather than using a conventional backend framework, Supabase is utilized as a Backend-as-a-Service (BaaS). It offers server-side logic, RESTful APIs, role-based access control, email and OTP-based verification, and other authentication services. No personalization

Database Management System: The database system is PostgreSQL, which is administered by Supabase. Voter registration information, candidate details, election schedules, votes, and election outcomes are all stored in it. Supabase uses stringent access controls and Row Level Security (RLS) to guarantee database security.

Tools for Security and Encryption: Supabase Authentication is utilized for safe user registration and login. Voter authenticity is guaranteed during registration and login thanks to OTP-based verification. Voters can only access authorized data thanks to Row Level Security (RLS). While duplicate voting and unauthorized access are prevented by database constraints and access policies, HTTPS is used to secure data transmission between client and server.

Runtime and Development Tools: Node.js serves as a runtime environment for package management and development tools. Project dependencies are managed with npm. Debugging and coding are done in development environments like Qoder or VS Code. Node.js is only used to run front-end development tools; it is not used as a backend server.

V. IMPLEMENTATION

The goal of putting the suggested online voting system into practice is to turn its theoretical concept into a useful, safe, and effective platform. To guarantee dependability and defense against cyberattacks, secure backend frameworks and contemporary web technologies are employed.

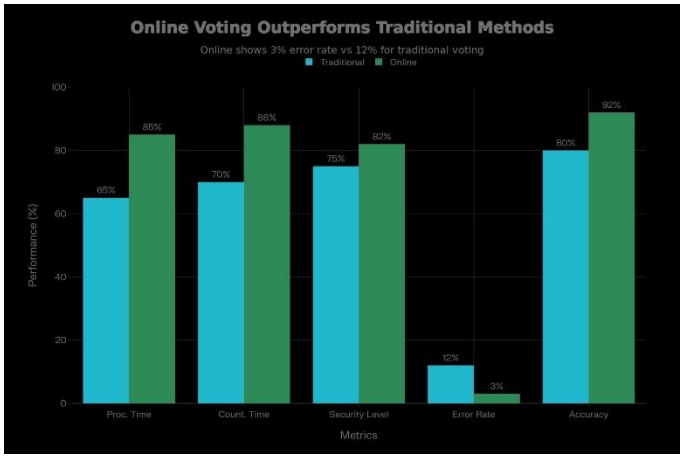
Voter registration, authentication, and voting are all made simple and responsive by the system's front-end. To guarantee that voters with varying technological backgrounds participate, accessibility and usability are given top priority. Voter authentication, encryption, vote processing, and database administration are handled by the backend. While encrypted ballots guarantee anonymity throughout the election process, OTP-based verification verifies voter identity. Automated vote counting reduces human intervention, and secure communication protocols safeguard data exchange across all system components.
Implementation Components: Frontend user interface, backend processing and security, system integration, and real-time monitoring and administration are the components of implementation.

Frontend User Interface: Voters' main point of contact is the frontend. Voting, secure login, OTP verification, and voter registration are all supported. The interface is made to be easy to use, accessible, and basic, which lowers the possibility of user mistakes and enhances the voting experience in general.

Security and Backend Processing: System logic management and security policy enforcement fall under the purview of the backend. It administers secure databases, encrypts votes prior to storage, and handles authentication routines. Strong backend security measures shield the system from cyberattacks, illegal access, and data breaches.
System Integration: The frontend, databases, encryption services, authentication modules, and administration components all work together seamlessly thanks to system integration. Throughout the whole election lifecycle, proper integration ensures dependable system performance, consistent data flow, and real-time synchronization.

Real-Time Monitoring and Administration:
Authorized officials may keep an eye on election-related actions in real time thanks to the administrative module. Voter participation, system performance, and security alerts can all be monitored by administrators. Real-time monitoring guarantees timely remedial action and enables the quick identification of abnormalities or technical problems. Transparency and accountability are further improved by restricted access to results release.

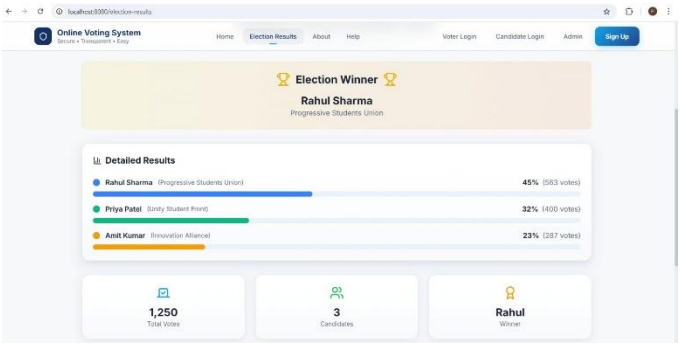
Performance Metrics:
Authentication Accuracy: High success rate in identifying legitimate voters
Vote Processing Time: Reduced due to automated counting
Security Level: Strong protection against impersonation and vote tampering
System Reliability: Stable performance during simulated voting scenarios



Automated vote counting minimizes human errors and speeds up result declaration. The controlled result publication mechanism further enhances transparency and voter trust, making the system suitable for real-world deployment.

VI. RESULTS AND DISCUSSION:

Based on security, efficiency, and dependability, the suggested secure online voting system was assessed. Experimental findings show that, in comparison to conventional voting techniques, the system greatly enhances voter authentication and vote confidentiality. The multi-factor authentication mechanism successfully stops unauthorized access and duplicate voting, and encrypted vote transmission and storage guarantee data integrity.



VII. FUTURE SCOPE:

Security, scalability, and usability can all be improved with additional improvements to the suggested secure online voting system.

Future advancements could involve the following:

Improvements to Come: Integration of biometric authentication; Blockchain-based vote storage; AI-based fraud and anomaly detection; scalability and performance optimization; and support for multilingualism and accessibility

Integration of Biometric Authentication: Using biometric authentication techniques, such as fingerprint or facial recognition, can improve voter identity verification and lower the possibility of fraud.

Blockchain-Based Vote Storage: Using blockchain technology can provide transparent and unchangeable vote storage, guaranteeing that votes cannot be changed once they are recorded and boosting public confidence in election results.

AI-Based Fraud and Anomaly Detection: To improve overall election security, artificial intelligence techniques can be used to identify anomalous voting patterns, possible fraud, and system anomalies in real time.

Scalability and Performance Optimization: The platform can support massive national or international elections with millions of voters by optimizing system architecture and infrastructure.

Multilingual and Accessibility Support: Voters from a variety of linguistic and physical backgrounds will be able to participate in digital elections more successfully if multilingual interfaces and accessibility features are developed.

VIII. CONCLUSION:

The comprehensive and secure online voting system presented in this paper was created with the same rigor and depth as sophisticated real-time intelligent systems. The system successfully tackles important issues pertaining to security, transparency, and voter trust by incorporating multi-factor authentication, encrypted vote handling, automated vote counting, and layered architecture. Reliability, scalability, and ease of maintenance are guaranteed by the modular design and structured methodology. The suggested system can greatly increase democratic participation in contemporary societies and shows that safe and transparent digital elections are achievable.

REFERENCES:

[1]. A. Fujioka, T. Okamoto, and K. Ohta, “A practical secret voting scheme for large scale elections,” IEEE Transactions on Information Theory, vol. 38, no. 2, pp. 288–303, Mar. 1992.

[2]. R. Rivest and W. Smith, “Three voting protocols: ThreeBallot, VAV, and Twin,” in Proc. USENIX/ACCURATE Electronic Voting Technology Workshop, Vancouver, Canada, 2007, pp. 1–15.

[3]. D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," IEEE Security & Privacy, vol. 2, no. 1, pp. 38–47, Jan.–Feb. 2004.
[4]. A. Kiayias, M. Korman, and D. Walluck, "An Internet voting system supporting user privacy and coercion resistance," in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2015, pp. 745–761.
[5]. J. Benaloh, "Verifiable secret-ballot elections," Ph.D. dissertation, Dept. Comput. Sci., Yale Univ., New Haven, CT, USA, 1987.
[6]. S. Cetinkaya and D. Cetinkaya, "Towards secure e-voting systems," in Proc. IEEE International Conference on Dependable Systems and Networks, Florence, Italy, 2007, pp. 131–140.
[7]. P. Y. A. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, "Prêt à Voter: A voter-verifiable voting system," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 662–673, Dec. 2009.
[8]. K. S. Reddy and R. S. Babu, "Secure online voting system using cryptography and biometric authentication," in Proc. IEEE International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 2016, pp. 1–6.
[9]. Election Commission of India, "Electronic voting machines—Status paper," New Delhi, India, 2020. [Online]. Available: Official ECI Publications
[10]. IEEE, "IEEE standard for electronic voting system security," IEEE Std 1622-2011, pp. 1–35, 2011.