WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

E Vote: An Online Voting System A Secure and Transparent Online Voting System with Multiple Layers of Security

Mohammad Waseem[1], Gaurav Pandey[2], Dr. Vibha Srivastava[3]

[1]UG student of Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management, Uttar Pradesh, Lucknow
mw84762@gmail.com
[2]UG student of Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management, Uttar Pradesh, Lucknow
gp4012016@gmail.com
[3]Associate Professor of Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management, Uttar Pradesh, Lucknow
vibha@srmcem.ac.in

ABSTRACT :

Providing secure and transparent elections is a serious challenge in contemporary democracies. Traditionally employed voting technologies suffer from voter verification, data integrity, and result accuracy problems.

This article presents "E-Vote," an online voting system with layered security measures to enable secure and tamper-free elections. The system utilizes cutting-edge authentication processes such as facial recognition, OTP, and barcode-based voter ID checks to authenticate voter identities. Additionally, sensitive voter information are protected against breach by stringent encryption protocols.

With real-time monitoring, keen audit trails, and meticulous vote management, e-Vote minimizes fraud opportunities and ensures electoral integrity. This new system inspires faith in online voting and thus makes its contribution towards secure e-governance.

Keywords: e-voting, multi-level security, facial recognition, barcode verification processes, voter verification procedures, electoral integrity.

Introduction

In an era of fast-paced technological development and a growing demand for convenient civic engagement, E-Vote: An Online Voting System provides a safe and efficient method for online voting. Qualified voters can cast their votes in the comfort of their homes with the online system, while ensuring high security and transparency standards.

Our system uses facial recognition, barcode scanning, and one-time password (OTP) verification to protect the electoral process. Facial recognition only allows qualified individuals to vote, thereby eliminating fraudulent processes. Barcode scanning confirms voter identification against official documents, thereby eliminating forgery. OTP verification, which is sent to registered phone numbers, also offers an increased level of security, which confirms voter validity.

By integrating these technologies, E-Vote provides a tamper-proof environment, thereby ensuring voters a seamless and reliable digital electoral process. Not only does this revolution facilitate the ease of voting, but it also increases trust, transparency, and participation in democratic processes.

Literature Review

Chaum (2011) – Introduced an end-to-end verifiable (E2E) cryptographic voting system to ensure election integrity. The system enabled voters to verify their votes without compromising privacy. It laid the foundation for modern electronic voting security.

Estonia's I-Voting System (2014) – Estonia pioneered nationwide online voting, allowing citizens to vote remotely. Springall et al. (2014) identified security vulnerabilities, including risks of cyberattacks. Despite this, Estonia's system became a model for digital elections.

Zhao et al. (2015) – Explored multi-layer authentication methods to secure online voting systems. The study emphasized OTP-based authentication and voter ID verification for preventing impersonation. These measures enhanced election security and voter trust.

Kumar et al. (2017) – Proposed an SMS-based voting system for voters in remote areas. The system enabled casting votes via registered mobile numbers, ensuring accessibility. The study highlighted mobile verification as a secure alternative to physical polling stations.

Li & Wang (2018) – Investigated electronic voter registration systems to streamline the electoral process. Their study emphasized database management, identity verification, and secure record-keeping. The system significantly reduced manual errors in voter registration.

Zhou et al. (2019) – Analysed the impact of two-factor authentication (2FA) in online voting. The research concluded that combining passwords with SMS-based OTPs improved voter authentication. It ensured that only registered voters could participate.
Sharma et al. (2020) – Explored cloud-based voting infrastructure to enable large-scale elections. Their system provided secure data storage, easy scalability, and faster result processing. The study stressed the need for encrypted cloud storage to prevent data breaches.
Alam et al. (2021) – Introduced a QR code-based voting mechanism to enhance voter verification. Voters scanned a unique QR code linked to their identity before casting votes. This method improved security while minimizing the chances of vote duplication.
Singh et al. (2022) – Examined the role of secure web-based portals for online voting. Their system provided user-friendly interfaces, real-time vote tracking, and automated result generation. The research highlighted accessibility improvements for disabled and remote voters.

Importance of An Online Voting System

An internet-based voting system is essential in providing safe, transparent, and accessible elections in the modern era. With a combination of several layers of security such as facial recognition, OTP verification, and barcode-based voter ID validation, such systems increase the credibility and integrity of the electoral process.
In most jurisdictions, traditional voting methods are plagued by logistical problems, vote manipulation, and labour-intensive manual tabulation processes. Internet voting platforms bridge these problems by providing a smooth, efficient, and tamper-evident voting process. The system's real-time monitoring feature and its extensive audit trails give election authorities the ability to detect and correct irregularities in a prompt fashion.
Further, internet-based voting systems encourage participation by enabling distant voting, hence enabling citizens who are in far-flung or under-served areas to cast their votes. This technology is particularly crucial in big democracies, where dealing with tens of millions of voters can be challenging.
With the rise in digital development, the application of secure web-based voting systems makes the democratic process strong, transparent, and credible. The sophisticated systems enhance public confidence in elections, encouraging the establishment of secure e-governance worldwide.
Proposed System: E-Vote Architecture and Features

System Architecture

The suggested E-Vote system architecture is designed to ensure a secure, open, and efficient e-voting process. It consists of several components, each of which plays a vital role in maintaining electronic voting secure, confidential, and accessible.

Frontend (User Interface):

Frontend is the main interface where the voters can interact with the system. It offers the easy-to-use and accessible interface for casting votes. It is implemented using Django Templates, HTML, CSS, JavaScript, and Bootstrap, with the aim of ensuring ease and responsiveness. The system is developed to maximize usage across devices such as desktops, tablets, and smartphones, thus ensuring extensive accessibility.

Backend (Processing Engine):

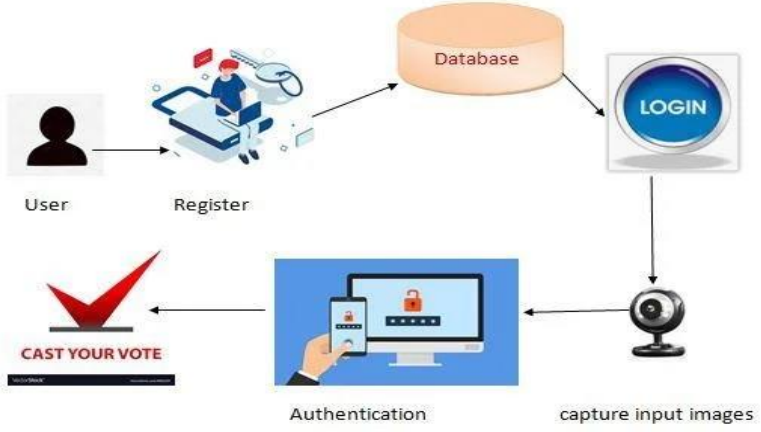
The backend serves as the processing unit, dealing with user authentication, encryption of votes, and secure communication between the frontend and database. It is responsible for the implementation of security measures, thereby preventing unauthorized access and ensuring system stability. The backend, which is developed using Django, is tasked with the management of the core functions of the voting system.

Database:

A secure database is a fundamental component of the E-Vote system, which ensures confidentiality and integrity of voters' information and vote records. The database stores encrypted votes, authentication logs, and audit trails to ensure an open and auditable election process. A relational database management system (RDBMS) (SQLite) is employed to store structured records, eliminating redundancy and ensuring conformity with one-person-one-vote legislation.

Security Layer:

Security is a critical element of the system, enforced by a variety of mechanisms like Django's native authentication and session handling for user security. Hashing algorithms in password security (e.g., RSA hashing). Encryption of votes end-to-end for confidentiality. Django Middleware for protection against malicious attacks using CSRF. Logging mechanisms for fraud detection and audit trail purposes.



Key Features

Multi-Factor Authentication (Aadhaar, voter card, OTP, and facial recognition).
Tamper-Proof Voting Process using encryption and blockchain (future scope).
Automated Vote Counting and Secure Storage to prevent fraud.
Real-Time Monitoring and Audit Logs for transparency.

Procedure / Methodology

The E-Vote system is implemented through a structured approach, ensuring security, transparency, and accessibility. The methodology follows a step-by-step process, integrating authentication, encryption, fraud prevention, and result declaration mechanisms.

1.Voter Registration

The registration process ensures that only legitimate voters can participate. It involves multi-layered verification to prevent fraudulent activities:

2.Aadhaar and Voter Card Verification:

The system verifies the voter's identity using government-issued Aadhaar and Voter ID cards.

3.Facial Recognition:

To enhance security, facial recognition technology is implemented (or planned for future enhancement) to ensure that each voter is unique and cannot register multiple times.

4.OTP Authentication:

An additional security layer is added through One-Time Password (OTP) verification via SMS. This prevents unauthorized access and ensures that the registered voter is actively participating.

5.Secure Login:

Voters log in using multi-factor authentication, ensuring that only verified individuals can access the system.

6.Vote Casting Process

Once registered and authenticated, voters can securely cast their votes through the system:

7.Dynamic Ballot Display: The system dynamically generates the digital ballot based on the ongoing election. The voter selects their preferred candidate.

8.Vote Encryption and Storage: Once a vote is cast, it is encrypted using cryptographic algorithms and securely stored in the backend database to prevent tampering.

9.Duplicate Vote Prevention: Each voter is assigned a unique voter ID, preventing them from voting multiple times.

10.Device and IP Tracking: The system tracks login activity based on device information and IP addresses. If anomalies are detected, security alerts are triggered.

11.Public Result Announcement: Once voting is completed, results are displayed on the admin dashboard, making the process fully transparent for stakeholders and the public.

Challenges in Online Voting System

- Security and Prevention of Fraud – Protection against hacking, phishing, and vote tampering is required. Election integrity necessitates the application of strong encryption, multi-factor authentication, and real-time fraud detection.
- Voter Accessibility and Digital Divide – Not all voters are connected to digital devices or the internet. Inclusion of them requires development of infrastructure, awareness campaigns, and other voting methods for excluded groups.
- System Reliability and Scalability – The system should be able to support large traffic volumes without crashing or slowing down, providing seamless voting processes. Load balancing, redundancy, and real-time monitoring are required to ensure stability.
- Public Trust and Legal Compliance – The majority of voters and officials can be suspicious of Internet voting due to concerns over openness and security. Compliance with voting law, conducting independent audits, and roll-out of public information campaigns are important to stimulate take-up.

Conclusion

The E-Vote system offers a secure, efficient, and transparent mechanism for running online elections. With the addition of multi-factor authentication, end-to-end encryption, and real-time monitoring, the system significantly minimizes risks associated with traditional voting practices, including voter fraud, unauthorized entry, and manipulation of results. Aadhaar and voter card authentication and OTP verification and facial recognition (a future enhancement) ensure only authenticated voters cast their votes, and secure audit logs and device/IP tracking prevent fraud.

Also, the automated count system improves efficiency by avoiding human error. Further, the integration of blockchain technology in future iterations of the system adds to the reliability by allowing for unmodifiable records of votes. Through the utilization of an easy-to-access digital ballot, offering encrypted storage of votes, and public proclamation of results, the platform adds to transparency and voter confidence.

In a nutshell, the E-Vote system seeks to modernize the electoral process by utilizing state-of-the-art security features and technology-based solutions. Its implementation has the potential to revolutionize both the accessibility and credibility of elections, thereby offering a scalable and tamper-evident digital voting system for future democratic processes.

Future Scope

- Advanced Security: Continuously enhance security against emerging threats.
- Blockchain Integration: Strengthen transparency with blockchain technology.
- AI and ML: Implement AI for real-time threat detection and fraud prevention.
- Biometric Verification: Expand biometric methods for identity verification.

REFERENCES

[1] Sherry Verma, Priyanka Tyagi, Assistant Professor Avinash Kumar Sharma, “encryption and authentication for improved voting accuracy”, © 2018 IJCRT | Volume 6, Issue 2 April 2018 | ISSN: 2320-2882.

[2] Ankit, Anand, Pallavi Divya,“An Efficient Online Voting System “, p. 2631 - 2634 Posted: 2019-08.

[3]. M A Imran, M S U Miah, H Rahman, May 2015, “Face Recognition using Eigenfaces,” in International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 5

[4] Rajesh, M. Ghadi, Priyanka S. Shelar, “user-friendly online voting system using Aadhaar card”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 12 | Dec-2017, p ISSN: 2395-0072

[5] Malwade Nikita, Patil Chetan, Chavan Suruchi, Prof. Raut S. Y, Secure Online Voting System Proposed By Biometrics, Vol. 3, Issue 5, May 2017.