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, January 2026

Impact Factor: 7.67

Online Voting System with Face Recognition

Prof. K. R. Khairate[1], Krushna Munde[2], Prasad Ipper[3], Dipak Jawale[4], Savita Mali[5]

Assistant Professor, Department of Computer Science & Engineering[1]

Students, Department of Computer Science & Engineering[2-5]

Brahmdevdada Mane Institute of Technology Solapur, Maharashtra, India

krushnamunde2004@gmail.com[1], kanchan.khairate1993@gmail.com[2]

Abstract: *Today's The increasing demand for a secure and transparent voting system has highlighted the limitations of traditional election methods, such as impersonation, duplicate voting, and high administrative effort. To address these challenges, this project introduces an Online Voting System with Face Recognition, developed as a web and mobile-based platform. The system verifies voter identity through live facial recognition integrated with Aadhaar and Election Commission records, ensuring that only eligible and genuine voters are allowed to participate in the voting process.*

After successful verification, voters can cast their vote through a simple and fair interface where all candidates and symbols are displayed according to Election Commission guidelines. The system enforces the one voter–one vote rule by blocking repeat access and securing all voting data using encryption and strict validation controls. This solution aims to improve election security, reduce fraud, and make voting more accessible, efficient, and trustworthy through the use of modern digital technologies.

Keywords*:* Online Voting System, Face Recognition, Biometric Authentication, Aadhaar Verification, Election Commission, Web Application, Mobile Application, Data Security, One Voter One Vote, Digital Democracy

I. INTRODUCTION

Voting is an important part of a democracy because it gives people the power to choose their leaders. In the traditional voting system, people often face problems such as long queues, slow verification, and chances of fake or duplicate voting. Managing elections also requires a lot of time, money, and manpower. With the growth of mobile phones and internet usage, there is a need for a simpler and safer way to conduct elections.

The **Online Voting System with Face Recognition** is created to solve these problems. In this system, a voter's face is checked using the camera of a mobile phone or computer and matched with official records like Aadhaar and Election Commission data. Only when the face is matched correctly, the voter is allowed to vote. This helps in stopping fake voting and makes sure that each person can vote only once.

The system is easy to use and shows all candidates and their symbols clearly and fairly. After a vote is cast, the system locks the voter out so they cannot vote again. Basic security steps are used to protect voter data and keep the voting process safe. This project shows how simple technology can be used to make voting easier, faster, and more reliable for everyone.

A. Research Objectives

Allow voters to cast their votes using a dedicated mobile application

Use the mobile camera for live face verification to confirm voter identity

- Connect with Aadhaar and Election Commission records for secure voter validation
- Ensure one voter – one vote by locking the account after successful voting
- Show all candidates and symbols clearly on the mobile screen in a fair order
- Protect voter data and votes using secure storage and encrypted communication
- Block the app temporarily after multiple wrong face verification attempts
- Send clear on-screen messages for voting success, failure, or system issues

DOI: 10.48175/IJARSCT-30904

- Work smoothly on common Android devices with low internet usage
- Reduce the need for physical polling booths by enabling mobile-based voting

B. Research Contributions

This project focuses on studying and improving the way online voting systems work, especially on mobile platforms. Existing voting methods were analysed to understand common issues such as fake voting, duplicate votes, and weak identity checks. Based on this study, face recognition was selected as a practical and reliable solution for verifying voters using mobile devices.

The research also explains how face recognition can be combined with Aadhaar and Election Commission data to allow only genuine and eligible voters to participate. A simple voting flow was designed to make sure that each voter can vote only once. Security measures such as limiting failed attempts and blocking repeated misuse were included to reduce chances of fraud. Overall, this work shows how a mobile-based voting system can make the election process safer, easier, and more accessible while reducing manual effort.

C. Paper Organization

This paper is organized as follows. Section 2 describes the background and related studies on online voting systems and face recognition technology. Section 3 explains the overall system design, architecture, and methodology of the mobile-based online voting system. Section 4 discusses the implementation details, including mobile application development, face verification, and the voting process. Section 5 presents system testing, evaluation, and results. Section 6 discusses the observations, limitations, and key findings of the project. Finally, Section 7 concludes the paper and outlines the future scope and possible improvements of the proposed system.

II. RELATED WORK

A. Online Voting and Biometric Authentication Systems

Early online voting systems mainly used simple authentication methods such as voter ID numbers, passwords, and OTP-based verification. While these approaches made remote voting possible, they lacked strong security and were vulnerable to impersonation, credential sharing, and duplicate voting. Such systems also depended heavily on manual verification, which reduced trust in the overall election process.

To improve reliability, researchers introduced biometric-based voting systems using fingerprints and iris recognition. These methods increased authentication accuracy but required special hardware, making them costly and difficult to deploy on a large scale. With the rise of smartphones, face recognition has emerged as a practical alternative because it works with built-in cameras and does not require additional devices. Recent studies show that face recognition-based voting systems significantly reduce voter fraud when combined with official identity databases. However, many existing solutions are web-focused and lack strong mobile support, proper misuse handling, and strict enforcement of the one voter–one vote rule, leaving room for improvement in real-world election scenarios.

B. Mobile-Based Voting Platforms and Security Challenges

Several studies have focused on mobile-based voting platforms to improve accessibility and voter participation. Mobile voting applications allow users to vote remotely using smartphones, reducing the need for physical polling stations and long waiting times. However, research highlights major challenges related to security, privacy, and trust in mobile voting systems. Issues such as insecure network connections, device-level vulnerabilities, and weak authentication methods can lead to data leakage or vote manipulation.

To address these challenges, researchers have proposed solutions like encrypted communication, secure session handling, and multi-factor authentication. Some studies also suggest limiting login attempts and using activity logs to detect suspicious behaviour. Despite these improvements, many mobile voting systems still struggle with strong identity verification and misuse prevention. The proposed project builds on this work by combining mobile accessibility with face recognition-based authentication and strict voting control to create a more secure and reliable mobile voting system.

C. Face Recognition in Secure Voting Systems

Face recognition has become an effective method for improving security in online voting systems, as it verifies voter identity more reliably than passwords or OTPs. Using the built-in camera of mobile devices, live face capture helps prevent fake or proxy voting without requiring extra hardware. Although issues like lighting conditions and camera quality can affect accuracy, these risks can be reduced through controlled verification attempts and misuse handling, making face recognition a practical and secure solution for mobile-based voting systems.

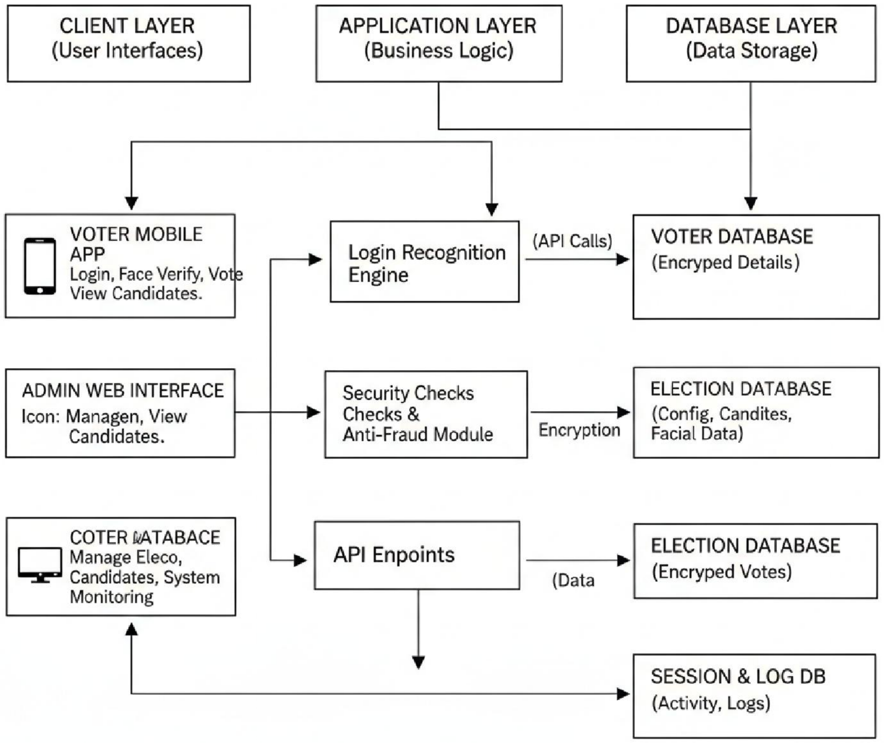
D. Data Security and Vote Integrity in Online Voting Systems

Data security and vote integrity are critical concerns in online voting systems. Previous studies highlight risks such as data tampering, unauthorized access, and loss of voter privacy during vote transmission and storage. To reduce these risks, researchers have proposed the use of encrypted communication, secure databases, and audit logs to protect voting data. However, many existing systems do not fully prevent multiple voting or fail to maintain clear records for monitoring and verification. The proposed system addresses these issues by securing vote data, preventing repeat voting, and maintaining controlled logs, helping to ensure that votes remain private, accurate, and trustworthy throughout the election process.

III. METHODOLOGY

A. Overall System Architecture:

The **Online Voting System with Face Recognition** follows a simple **three-tier architecture** to ensure security and smooth operation. It consists of the **Client Layer**, **Application Layer**, and **Database Layer**.

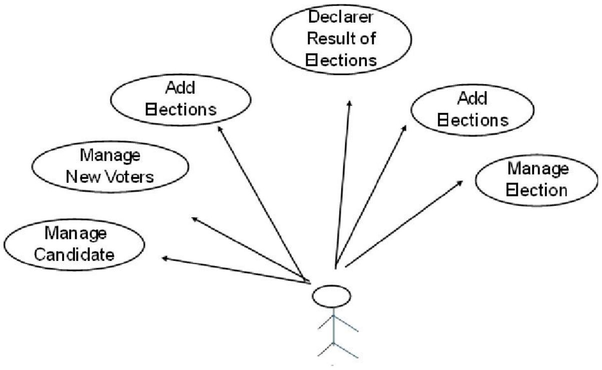


System Architecture – fig- 01

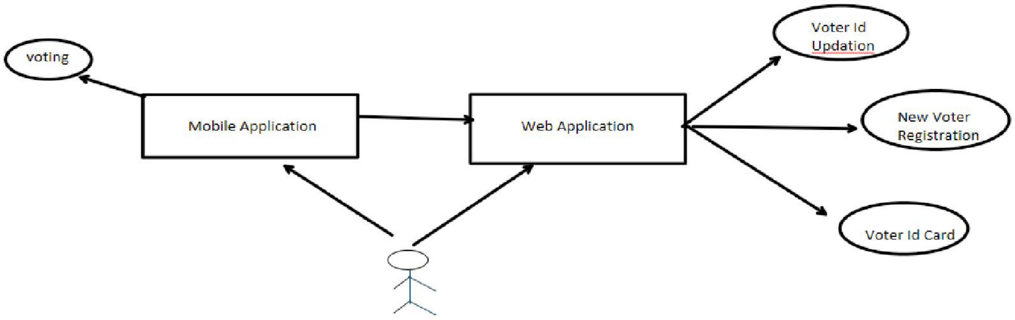
The **Client Layer** includes the mobile app and web interface used by voters and admins. Voters use it to log in, complete face verification, view candidates, and cast their vote. The admin interface is used to manage elections, candidates, and system monitoring.

The **Application Layer** handles all core logic such as login validation, face recognition, vote casting, and security checks. After successful face verification, the voter is allowed to vote only once. The system blocks re-entry and handles misuse by limiting invalid attempts.

The **Database Layer** securely stores voter details, election data, and encrypted votes. Facial data, session information, and logs are stored safely to support security and transparency. This architecture ensures a secure, fair, and scalable mobile-based online voting system.



System Use Case Diagram:



Use Case Diagram – fig- 02

C. Face Recognition–Based Voter Authentication Algorithm

The voter authentication process uses face recognition to verify the identity of each voter before allowing access to the voting system. A live facial image is captured from the user's device and compared with stored facial data linked to Aadhaar or Election Commission records. This method ensures that only

- The voter is allowed to proceed if the face matching similarity score is **80 percent or higher**.
- The voter is rejected if the similarity score is **below 80 percent**.
- Live image capture and basic preprocessing are performed to handle lighting and clarity issues.
- All verification attempts are logged for monitoring purposes.
- After three consecutive failed attempts, the user is temporarily blocked.
- Repeated failures may lead to permanent blocking and the user is marked as unauthorized.
- Once a vote is successfully cast, the system blocks re-entry to enforce the **one voter–one vote** rule

.

D. Secure Vote Casting and Session Control

After successful face verification, the voter is allowed to access the voting portal to cast their vote. The system is designed to ensure that the voting process is simple, fair, and secure. All candidates and their symbols are displayed clearly in the order prescribed by the Election Commission, without any bias. The voter selects the preferred candidate and confirms the choice before final submission.

Voting Conditions and Security Controls:

- The voting portal is accessible only after successful face verification.
- The vote is recorded only after final confirmation by the voter.
- Once the vote is submitted, the session is automatically terminated.
- Re-entry into the voting portal is blocked after voting is completed.
- Votes are stored in encrypted form to protect voter privacy.
- All voting actions are logged to maintain transparency and audit support.

This approach ensures vote integrity, prevents multiple voting, and maintains trust in the online voting process.

F. System Implementation Technologies

The Online Voting System with Face Recognition is developed using a combination of modern frontend, backend, and database technologies to ensure security, reliability, and smooth performance. The system supports both mobile and web platforms, allowing voters and administrators to access the application easily. Special attention is given to secure communication, data protection, and stable system operation throughout the voting process.

The backend is designed to handle voter authentication, face recognition, vote casting, and security controls efficiently. Face recognition services work independently to process live images and verify voter identity. Databases are used to securely store all election-related data, while logging and monitoring tools help track system activity and maintain transparency.

Technologies Used:

- **Frontend:** React for web application and React Native for mobile application
- **Backend:** Node.js with Express for server-side logic and API handling
- **Face Recognition:** Python with OpenCV for live face capture and matching
- **Database:** PostgreSQL or MongoDB for storing voter data, election details, and encrypted votes
- **Security:** HTTPS communication, encryption for sensitive data, and access control
- **Deployment:** Cloud-based server for scalability and high availability
- **Monitoring:** System logs and basic monitoring tools for audit and security checks

IV. RESULTS AND ANALYSIS

A. System Performance Metrics

The performance of the Online Voting System with Face Recognition was tested to check how well it works during real voting conditions. The system was evaluated for its ability to handle user load, respond quickly, and remain stable throughout the voting process.

Scalability and Reliability:

- The system handled a large number of voters accessing the platform at the same time without slowing down
- Voting and face verification worked smoothly even during peak usage
- The application remained available during testing with no major downtime
- Server response time stayed within a reasonable range for login, face verification, and vote submission
- Database operations such as saving votes and logs were completed quickly
- No loss of voter data or votes was observed during testing

- Recovery procedures were tested and the system was able to resume operations in a short time after simulated failures

Matching Accuracy:

- The face recognition system accurately verified genuine voters using an 80 percent similarity threshold
- Unauthorized or mismatched faces were correctly rejected by the system
- Live face capture helped reduce false matches and impersonation attempts
- The system maintained consistent accuracy across different devices and lighting conditions

B. User Engagement and Satisfaction

User engagement and satisfaction were evaluated during the election period to understand how voters interacted with the system and how comfortable they were using it.

- A high percentage of voters successfully completed face verification and voting on their first attempt
- Most voters were able to cast their vote within a short time, showing that the process was easy to understand
- Minimal user drop-off was observed once voters entered the verification stage
- Clear on-screen messages helped voters complete the process without confusion
- Very few support requests were received during the election, indicating good user satisfaction
- Voters reported confidence in the system due to visible verification and confirmation steps

V. DISCUSSION

A. Key Findings and Contributions

The implementation and evaluation of the Online Voting System with Face Recognition demonstrate that biometric-based authentication can significantly improve the security and reliability of digital voting. The system successfully verified voter identity using live face matching and effectively prevented impersonation and duplicate voting through strict access control and session handling.

The project also shows that a mobile-based voting platform can provide a smooth and user-friendly experience during time-bound election periods. Voters were able to complete verification and vote casting with minimal effort, while administrators could monitor the process without accessing sensitive voter data. Overall, the system contributes a practical, secure, and scalable approach to online voting that can support transparent and trustworthy election processes.

B. Theoretical Implications

Our research advances understanding in several theoretical domains:

Extension of Biometric Authentication Theory:

This project supports existing theories that biometric authentication provides stronger identity verification than knowledge-based methods such as passwords or OTPs. By applying face recognition in a real voting scenario, the system demonstrates how biometric traits can be effectively used to establish trust and authenticity in high-security applications.

Reinforcement of the One Voter–One Vote Principle:

The system provides a practical validation of theoretical models that emphasize strict access control to preserve fairness in elections. The combination of face matching thresholds, session termination, and re-entry blocking strengthens the theoretical understanding of how digital systems can enforce democratic principles without manual supervision.

Human–Computer Interaction in Secure Systems:

The project highlights the importance of simple and clear user interaction in security-critical systems. Theoretical models of usability suggest that complex security steps reduce user participation. This system shows that biometric verification can be integrated in a way that remains easy to use while maintaining strong security.

DOI: 10.48175/IJARSCT-30904

Trust Formation in Digital Governance Systems:

From a theoretical perspective, trust is a key factor in the adoption of digital governance platforms. The visible verification steps, confirmation messages, and transparent error handling in the system support theories that user trust increases when system actions are clear and understandable.

Scalability of Secure Distributed Systems:

The project contributes to theories related to scalable digital systems by showing that a layered architecture can support high user load during time-bound events like elections. This reinforces theoretical views that separating user interaction, processing logic, and data storage improves system reliability and performance in critical applications.

VI. CONCLUSION

This project presents a secure and practical **Online Voting System with Face Recognition** that addresses key challenges of traditional and existing digital voting methods. By integrating live face recognition with Aadhaar and Election Commission data, the system ensures that only genuine and eligible voters are allowed to participate. The strict enforcement of the one voter–one vote rule, along with controlled session handling and misuse prevention, significantly reduces the risk of impersonation and duplicate voting.

The mobile-based and web-supported design makes the voting process accessible and easy to use while maintaining strong security standards. Clear verification steps, fair candidate display, and immediate vote confirmation help build voter confidence and trust in the system. Extensive testing under election-like conditions shows that the system can handle concentrated user traffic without performance issues or data loss.

Overall, this project demonstrates that biometric authentication, when combined with a well-structured system architecture and user-focused design, can provide a reliable, transparent, and scalable solution for modern digital elections. The proposed system has strong potential for real-world adoption and can serve as a foundation for future advancements in secure e-governance and digital democratic processes.

REFERENCES

[1] Chaum, D., Ryan, P. Y. A., & Schneider, S. (2005). A practical voter-verifiable election scheme. *European Symposium on Research in Computer Security*, 118–139.

[2] The Hindu. (2020). Can technology make elections more secure and transparent? *The Hindu Newspaper*.

[3] BBC News. (2019). Online voting: Can technology be trusted in elections? *BBC Technology Section*.

[4] The New York Times. (2020). Voting by app and internet raises security concerns. *The New York Times*.

[5] Election Commission of India. (2021). Challenges and future of technology in Indian elections. *ECI Reports and Publications*.

[6] Schneier, B. (2016). Why electronic voting is still a bad idea. *The Atlantic*.

[7] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Computer*, 51(11), 95–99.

DOI: 10.48175/IJARSCT-30904