Secure voting system using face recognition and fingerprint authentication

Alampally Shailu, Sarasam Spandana, Jarpula Yamunabai, K Madhuravani

Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women

B,tech students, Department of information Technolgy , Bhoj Reddy Engineering College for Women

ABSTRACT

A secure and transparent voting system is essential for maintaining trust in elections. Traditional voting methods often encounter challenges such as identity fraud, duplicate voting, and manual errors, which negatively impact the fairness and efficiency of the process. To address these limitations, this project proposes a Secure Voting System using Face Recognition and Fingerprint Authentication.

The system utilizes advanced biometric technologies along with OTP-based email verification to provide strong and reliable user authentication. It is designed with two main modules: an admin module for managing voters, candidates, and election results, and a user module for voter registration and voting. Users are required to register with personal and biometric details and must complete multi-level verification before being permitted to vote. During the voting process, the system verifies the user's identity through face recognition, fingerprint scanning, and OTP authentication. This multi-layered security approach ensures that only authorized individuals can cast their votes, effectively preventing duplication and impersonation while improving overall accuracy and security.

In conclusion, the proposed system enhances transparency, reduces human errors, and ensures a secure, reliable, and tamper-proof voting process.

Keywords:Secure Voting System; Face Recognition;Fingerprint Authentication; OTP Verification; Biometric Security; Digital Voting

OBJECTIVE

The main objective of this project is to develop a secure and reliable voting system using face recognition and fingerprint authentication. The system aims to ensure accurate voter identification through multi-level authentication, including biometric verification and OTP-based email validation. It is designed to prevent issues such as duplicate voting and identity fraud,

thereby improving the fairness of the election process. Additionally, the system provides a user-friendly platform for voter registration and voting, while enabling administrators to efficiently manage voters, candidates, and election results. Another important objective is to ensure the security and privacy of voter data, reduce manual errors, and minimize human intervention. Overall, the system aims to enhance transparency, accuracy, and trust in the voting process.

NEED FOR STUDY

The need for this study arises from the limitations and challenges associated with traditional voting systems, such as identity fraud, duplicate voting, manual errors, and lack of transparency. These issues can compromise the integrity and reliability of the election process. With the increasing use of digital technologies, there is a strong demand for a more secure, efficient, and trustworthy voting mechanism. This study focuses on developing a system that uses advanced biometric authentication methods like face recognition and fingerprint verification, along with OTP-based validation, to ensure accurate voter identification. It also aims to reduce human intervention, improve efficiency, and provide real-time result management. By addressing security and transparency concerns, this study contributes to building a reliable and tamper-proof voting system that enhances public trust in democratic processes.

EXISTING SYSTEM

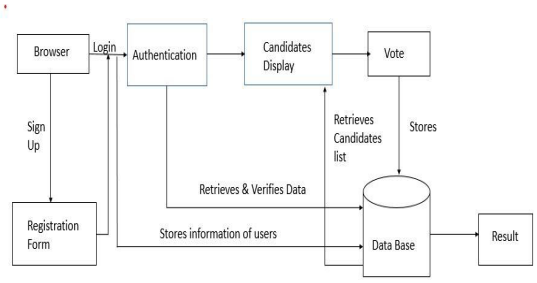
The existing voting system is mostly based on traditional methods such as paper ballots or basic electronic voting machines. These systems rely on manual verification of voter identity, which can lead to errors and delays. There is a risk of duplicate voting, impersonation, and lack of proper authentication mechanisms. Additionally, result processing is time-consuming and may lack real-time transparency. The system also requires significant human effort for management and monitoring. Overall, the existing system is less secure, less efficient, and more prone to fraud compared to modern digital solutions.

DISADVANTAGES

1. Prone to identity fraud and duplicate voting
2. Weak verification methods with no advanced authentication
3. High chances of human errors due to manual processes

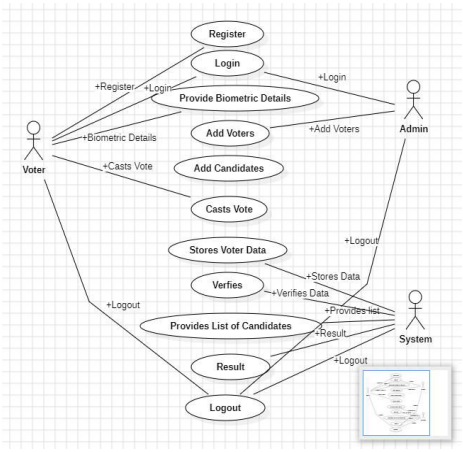
4. Time-consuming voting and result calculation
5. Lack of real-time transparency and monitoring
6. Requires more manpower and operational effort
7. Less secure and vulnerable to manipulation

SYSTEM ARCHITECTURE

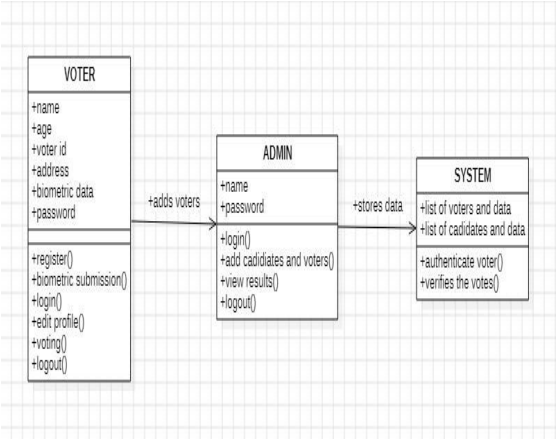


UML DIAGRAM

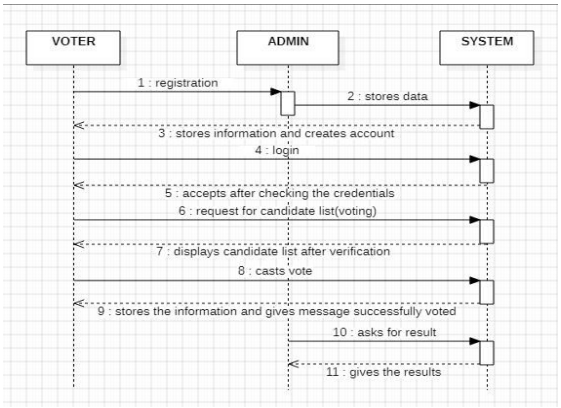
USE CASE DIAGRAM



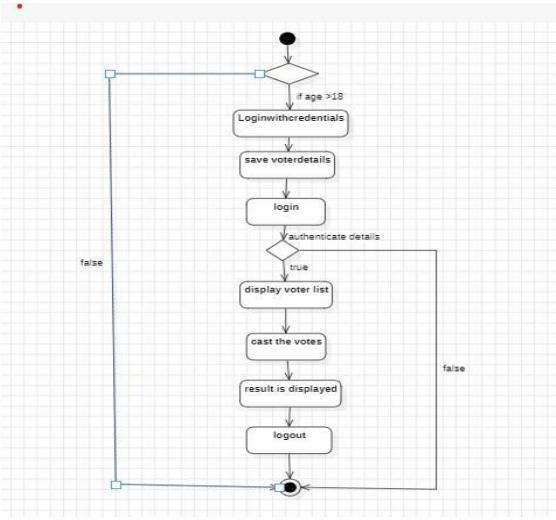
CLASS DIAGRAM



SEQUENCE DIAGRAM



ACTIVITY DIAGRAM



SYSTEM REQUIREMENTS

3.3.1 SoftwareRequirements

Backend: Django

Frontend: HTML,CSS,JavaScript

Data base : SQLite

Editor: VisualStudioCode

3.3.2 HardwareRequirements

Processor:Anyprocessormorethani3

RAM:8 GB

HardDisk:512GB

Web cam : For facial recognition

MODULE DESCRIPTION

A module is a functional unit of a program, and a complete system is composed of multiple independently developed modules. Each module performs a specific task and contributes to the overall functionality of the system. The following are the key modules of the proposed voting system:

- **User-Module**

  This module manages user registration and login processes. Users provide details such as name, mobile number, email, Aadhaar number, address, and password. It also handles user roles, such as voter and admin, and controls access based on these roles.

- **Biometric Authentication Module**

  This module verifies user identity using face recognition and fingerprint authentication. It ensures that only authorized and genuine users can proceed with the voting process.

- **OTP Verification Module**

  This module adds an extra layer of security by sending a One-Time Password (OTP) to the user's registered email. Access to the voting system is granted only after successful OTP verification.

- **Voter Management Module**

  This module maintains detailed records of voters, including their personal and biometric information. The admin can view, update, and manage voter details and verify their eligibility.

- **Candidate & Party Management Module**

  This module allows the admin to add, update, and manage information related to candidates and political parties. It ensures that accurate candidate details are available during the voting process.

- **Voting-Module**

  This module enables authenticated users to cast their votes securely. It ensures that each voter can vote only

once and stores the voting data safely in the database.

- **Result Dashboard Module**
  This module provides a centralized interface for the admin to monitor and manage voters, candidates, and election results. It displays real-time results and system information efficiently.

CHALLENGES&RISKS

The development and implementation of a secure voting system using face recognition and fingerprint authentication involve several challenges and risks. One of the major challenges is ensuring the accuracy and reliability of biometric authentication. Factors such as poor image quality, changes in facial appearance, or fingerprint damage can lead to false rejections or incorrect identification, affecting the user experience. Additionally, integrating multiple authentication methods like biometrics and OTP increases system complexity and requires careful synchronization to maintain smooth operation.

Another significant challenge is maintaining data security and privacy. The system stores sensitive information such as personal details, Aadhaar numbers, and biometric data, which makes it a potential target for cyberattacks. Any data breach could lead to misuse of personal information and loss of user trust. Therefore, strong encryption and secure storage mechanisms are essential.

Scalability is also a concern, especially during large-scale elections where the system must handle a high number of users simultaneously. Poor system performance or server overload can lead to delays and affect the voting process. Furthermore, ensuring continuous system availability and preventing downtime is critical, as any interruption during voting can disrupt the election process.

There are also operational risks, such as user resistance to new technology, lack of technical awareness, and difficulties in using biometric devices. Environmental conditions, hardware failures, or network issues may impact the system's functionality. Moreover, implementing such a system must comply with legal and regulatory requirements related to data protection and digital voting.

Overall, while the proposed system enhances security and transparency, careful planning, robust system design, and proper risk management strategies

are necessary to address these challenges effectively.

PROPOSED SYSTEM

The proposed Secure Voting System uses face recognition, fingerprint authentication, and OTP verification to ensure a highly secure voting process. It provides separate modules for admin and users, where the admin can manage voters, candidates, and results. Users can register with personal and biometric details and securely log in to vote. The system verifies identity through multiple authentication steps before allowing voting. It prevents duplicate and unauthorized voting while maintaining accurate records. Overall, it offers a reliable, transparent, and efficient digital voting solution.

ADVANTAGES

. 1. Provides high security using face recognition, fingerprint, and OTP verification

2. Prevents duplicate and unauthorized voting

3. Ensures accurate and tamper-proof record maintenance

4.Reduces human errors by automating the process

5. Saves time with faster voting and result generation

6. Enables easy management of voters, candidates, and results by admin

7. Increases transparency and trust in the voting system.

CONCLUSION

Using real-time voter data and multi-level authentication, the proposed Secure Voting System ensures a highly secure and efficient voting process, improving accuracy and eliminating manual errors. The system performs effectively even under high user load, as all modules—including user registration, biometric authentication, OTP verification, voting, and result management—are fully integrated and work seamlessly together. With automated OTP verification and secure data handling, the system ensures safe and reliable communication during the voting process.

Both web-based accessibility and a user-friendly interface make the system suitable for different environments, including small-scale and large-scale elections. Due to its scalability, reliability, and strong security features, this system is recommended as a modern solution for conducting elections digitally. In the future, integration with blockchain technology and mobile applications can

further enhance transparency and accessibility. The long-term objective is to provide a fully secure, transparent, and automated voting system that can be accessed from anywhere while maintaining the integrity of the electoral process.

FUTURE ENHANCEMENT

The Secure Voting System can be improved in the future by developing a mobile application so users can easily access voting services from their smartphones. Artificial Intelligence can be used to enhance face recognition accuracy and detect fraudulent activities more effectively. Integration with GPS and location-based services can help in identifying voter regions and managing constituency-based voting efficiently. The system can also include automated notifications and reminders for election schedules and voter participation. Adding support for multiple regional languages will make the system more user-friendly and accessible to a wider population. Advanced security technologies like blockchain can be implemented to ensure tamper-proof voting records and increased transparency. Finally, integrating the system with national election databases can improve coordination, scalability, and reliability for conducting large-scale elections.

REFERENCE

[1] A. I. Qureshi, M. Mandhare, R. Shekih, T. C. Parsutkar, and S. Adgulwar, “Online Voting System using Face Recognition and Fraud Detection,” *International Journal of Engineering Research & Technology (IJERT)*, Vol. 14, Issue 12, 2025.

[2] K. Patidar and S. Jain, “Decentralized E-Voting Portal Using Blockchain,” *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, doi: 10.1109/ICCCNT45670.2019.8944899.

[3R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, and M. A. Rahman, “Biometrically Secured Electronic Voting Machine,” *IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2017, doi: 10.1109/R10-HTC.2017.8288944.

[4] N. Bhuvaneswary, C. V. Reddy, C. Aravind, and K. H. Prasad, “Smart Voting Machine using Fingerprint Sensor and Face Recognition,” *International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, doi: 10.1109/ICAAIC53929.2022.9793210.

[5] M. Kandan, K. D. Devi, K. D. N. Sri, N. Ramya, and N. K. Vamsi, “Smart Voting System using Face Detection and

Recognition Algorithms," *ICISSGT*, 2021, doi: 10.1109/ICISSGT52025.2021.9604702.

[6] OpenCV Documentation, Available at: https://opencv.org/

[7] Python Software Foundation, Python Documentation, Available at: https://docs.python.org/

[8] MySQL Official Documentation, Available at: https://www.mysql.com/

[9] Election Commission of India, Available at: https://eci.gov.in/