ONLINE VOTING SYSTEM WITH FACE RECOGNITION

P Sirisha [1] *G Subhash Reddy*[2], P Imam Shaheed[3], M Nawaz Basha[4], B Mohith Reddy[5]

[1]Assistant Professor, [2,3,4,5]UG Students, Aditya College of Engineering, Madanapalle – 517325, Andhra Pradesh, India.

Corresponding author: sirisha1236@gmail.com

Abstract: The project titled "Online Voting System with Face Recognition" is designed to provide a secure, reliable, and efficient method for conducting elections digitally. It eliminates the challenges of traditional voting systems such as impersonation, long queues, and logistical overhead by introducing face recognition for voter authentication. This system is developed using React.js for the front end, Spring Boot for the back end, and MySQL for the database. Python and OpenCV (LBPH algorithm) are integrated to perform real-time face recognition during both registration and voting. Voters register by providing personal details such as Voter ID or Aadhaar number, date of birth, and constituency, and must undergo live facial verification. During voting, users must log in and complete face authentication before accessing the ballot. This ensures one-person-one-vote integrity. The admin module allows authorized officials to add elections, candidates, voter lists, and publish results securely. For enhanced security, AES encryption is used for data transmission and SHA hashing protects user credentials. Keywords: Online Voting, Face Recognition Authentication, React JS Spring Boot, Advanced Encryption Standard, Secure Hashing Algorithm.

Keywords: Online Voting, Face Recognition Authentication, React JS Spring Boot, Advanced Encryption Standard, Secure Hashing Algorithm.

1. INTRODUCTION

In this system, voters can register online by providing their personal details such as Voter ID or Aadhaar number, date of birth, and constituency. During registration, the system captures and stores the voter's facial data using a camera. When a voter logs in to cast their vote, the system verifies their identity through real-time face recognition before allowing access to the voting page. This process ensures that only authorized voters can vote and that each person can vote only once. The system is developed using modern technologies such as React JS for the front-end, Spring Boot for the back-end, and MySQL for database management. Python and OpenCV are used to implement the face recognition functionality using the LBPH algorithm. Additionally, security techniques like AES encryption and SHA hashing are used to protect user data and ensure secure communication.

The primary objective of this project is to develop a secure and efficient Online Voting System that utilizes face recognition to verify voter identity and prevent electoral fraud. By integrating React JS, Spring Boot, Python with OpenCV (LBPH algorithm), and MySQL, the system ensures seamless interaction, robust back-end processing, and secure data storage. This system aims to allow registered voters to cast their votes remotely, only after successful real-time facial authentication, ensuring that each vote is legitimate and that a voter can vote only once. It also simplifies election management for administrators, enabling them to add elections, manage candidates, upload eligible voter lists, and publish results.

Voting is a fundamental right and a cornerstone of democratic societies, but traditional voting systems often face challenges such as voter impersonation, long waiting times, manual errors, and logistical complexities. These issues can affect the fairness and credibility of elections, leading to reduced voter turnout and mistrust in the democratic process. Additionally, many voters face difficulties reaching polling stations due to geographic or physical limitations, further limiting participation. To address this credibility of elections, leading to reduced voter turnout and mistrust in the democratic process. The system ensures voter authenticity through verification, making impersonation and multiple voting nearly impossible. The front-end is developed using React JS, offering an intuitive and responsive user interface for voters and administrators. The back-end utilizes Spring Boot to handle business logic and RESTful APIs, while MySQL manages data storage. Face recognition is implemented using Python and OpenCV's LBPH (Local Binary Pattern Histogram) algorithm, which captures and matches live facial images to registered voters during authentication Security is a critical aspect of the system, addressed by using AES encryption for secure data transmission and SHA hashing for protecting sensitive information like passwords. The platform supports election management by administrators, including candidate registration, voter list management, and result publication.

2. LITERATURE SURVEY

In this context, the integration of biometric authentication, particularly face recognition, has emerged as a promising

solution for enhancing the security of online voting systems. Face recognition technology leverages machine learning and deep learning algorithms to accurately identify and verify individuals based on their facial features. When combined with additional security mechanisms such as one-time passwords (OTP), cryptographic techniques, and blockchain, it significantly reduces the risk of fraudulent activities and ensures the integrity of the voting process. This literature survey focuses on analyzing existing research related to online voting systems that incorporate face recognition and other advanced security techniques. The study reviews various approaches, algorithms, and system architectures proposed by researchers, including methods based on Convolutional Neural Networks (CNN), Local Binary Pattern Histogram (LBPH), Support Vector Machines (SVM), and encryption models. It also examines different data sources used for voter authentication, such as facial image datasets, real-time webcam inputs, and government identity databases.

Singh, A., & Sharma, R., 2020, presented a comprehensive review on biometric authentication in e-voting systems [1]. The study analyzes various biometric techniques such as fingerprint, iris, and face recognition for voter verification. It highlights those biometric systems significantly reduce voter fraud and impersonation. However, concerns related to data privacy, storage security, and system reliability remain major challenges.

Sharma, K., & Kumar, P., 2019 proposed a secure online voting system using cryptographic techniques [2]. The system employs encryption algorithms to ensure confidentiality and integrity of votes during transmission. It effectively prevents unauthorized access and tampering, but key management and computational overhead are identified as limitations.

Chen, L., Zhang, Y., & Wang, J., 2021 developed a blockchain-based voting system integrated with biometric authentication [3]. The system uses blockchain to ensure transparency and immutability of voting records, while biometrics provide secure voter identification. Although the approach enhances trust and security, scalability and transaction latency pose significant challenges.

Patel, N., & Desai, S., 2018 designed a cloud-enabled online voting system using Spring Boot and MySQL [4]. The system allows remote voting with centralized data storage and efficient backend processing. While it improves accessibility and scalability, dependency on cloud infrastructure introduces risks related to data breaches and system downtime.

Gupta, S., Verma, R., & Singh, M. (2022 implemented a real-time face recognition system using the LBPH algorithm for secure voting [5]. The system provides efficient facial recognition with relatively low computational requirements. It performs well under controlled conditions; however, accuracy may decrease in cases of poor lighting or facial variations.

Jain, A., Ross, A., & Prabhakar, S. (2004 provided a foundational introduction to biometric recognition systems [6]. The study explains the principles, architectures, and performance metrics of biometric systems. It serves as a theoretical base for understanding modern biometric authentication, though it does not address recent advancements like deep learning-based recognition.

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003 presented an extensive survey on face recognition techniques [7]. The paper reviews traditional methods such as Eigenfaces, Fisher faces, and feature-based approaches. While it offers deep insights into early face recognition systems, it lacks coverage of modern deep learning techniques like CNNs.

III. PROPOSED METHODOLOGY

1. USER REGISTRATION

The system shall allow voters to register using valid credentials such as ID/Aadhaar number, date of birth, and constituency details. The system shall perform live face capture using a webcam and store the extracted facial features using the LBPH (Local Binary Pattern Histogram) algorithm.

2. USER LOGIN AND AUTHENTICATION

The system shall authenticate users through their registered credentials. The system shall verify the voter's identity using real-time face recognition before allowing access to the voting dashboard.

3. VOTING PROCESS

The system shall display available elections and candidates based on the voter's constituency.

The voter shall be able to cast a single vote per election.

Once a vote is cast, the system shall update the database securely and prevent re-voting by the same user.

4. ADMIN MODULE

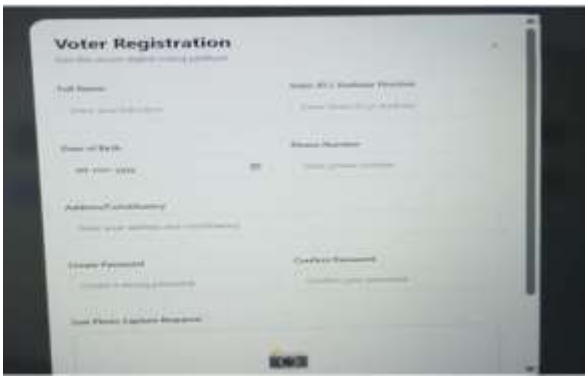
The admin shall be able to create and manage elections, candidates, and voter lists. · The admin shall be able to monitor voter participation and publish results after the election ends. · The admin shall have authority to verify and approve new voter registrations.

5. FACIAL RECOGNITION INTEGRATION

The system shall use Python and OpenCV to perform facial feature extraction and comparison using the LBPH algorithm. The system shall validate the live captured image against stored templates before granting voting access.

IV. RESULTS AND DISCUSSION

The voter registration interface of the Online Voting System with Face Recognition. This screen is used to create a new user account and initiate identity verification. The user is required to enter and confirm a password, ensuring basic account security through proper validation. The interface also indicates that live photo capture is mandatory for completing the registration process. After submitting the form, the system activates the camera to capture the user's facial image. The captured image is then processed to extract unique facial features and convert them into a secure digital representation. This data is stored in the database and later used for authentication during login and voting. Overall, the process ensures that each voter is uniquely registered and prevents unauthorized or duplicate access to the system. Perform live face capture registration Data and face template stored database.



The admin login interface of the Online Voting System with Face Recognition. This screen is used by the administrator to securely access the system dashboard and manage overall operations. The admin is required to enter a valid username and password, ensuring restricted access to authorized personnel only. Proper validation is performed to verify the entered credentials before granting access. Once authenticated, the admin can access functionalities such as managing voters, monitoring voting activities, and viewing results. The "Login as Admin" button initiates the authentication process, while the "Forgot your password?" option allows recovery of login credentials if needed. This login mechanism ensures that only authorized administrators can control and manage the system, thereby maintaining security and integrity of the voting process.

CONCLUSION

The "Online Voting System with Face Recognition" project successfully integrates advanced technologies to modernize the electoral process, making it more secure, efficient, and accessible. By eliminating the traditional challenges of voter impersonation, logistical overhead, and long queues, this system ensures a more transparent and trustworthy voting experience. The use of face recognition technology for both voter registration and voting authentication, paired with AES encryption and SHA hashing for data security, guarantees the integrity and confidentiality of the voting process. The system's cloud-based architecture provides scalability and remote access, making it suitable for large-scale elections and diverse demographic needs. The integration of a user-friendly interface with React JS and a robust backend powered by Spring Boot and MySQL ensures that the system is both reliable and easy to maintain. The use of the LBPH algorithm for facial recognition further strengthens the system's security b ensuring that only legitimate voters can cast their votes. This system not only enhances the voting experience by promoting ease of use accessibility but also strengthens public trust in the democratic process by leveraging cutting-edge technologies for transparency and security. The online voting system with face recognition provides a modern, secure, and efficient approach to conducting elections by integrating biometric authentication with digital such as voter impersonation, manual errors, and time-consuming result processing by implementing features like facial recognition for authentication, secure vote casting, and automated result generation, the system ensures accuracy, transparency, and reliability. However, its effectiveness depends on proper handling of challenges such as data privacy, biometric accuracy, and system security. With robust testing, validation, and continuous improvement, the system can serve as a practical solution for future digital voting needs. such as voter impersonation, manual errors, and time-consuming result processing. By implementing features like facial recognition for authentication, secure vote casting, and automated result generation, the system ensures accuracy, transparency, and reliability. However, its effectiveness depends on proper handling of challenges such as data privacy, biometric accuracy, and system security. With robust testing, validation, and continuous improvement, the system can serve as a practical solution for future digital voting needs. such as voter impersonation, manual errors, and time-consuming result processing. By implementing features like facial recognition for authentication, secure vote casting, and automated result generation, the system ensures accuracy, transparency, and reliability. However, its effectiveness depends on proper handling of challenges such as data privacy. The "Online Voting System with Face Recognition" has the potential for several future enhancements to further improve its functionality, security, and overall user experience. One key enhancement is the integration of multi-factor authentication (MFA), which would require voters to authenticate using additional methods, such as a One-Time Password (OTP) sent

to their registered mobile number or email. This added layer of security ensures that only the registered voter can cast their vote. Another important future development is the incorporation of block chain technology to ensure vote integrity. By utilizing a decentralized and immutable ledger, block chain guarantees that votes cannot be tampered with once cast, increasing transparency and trust in the electoral process. Additionally, it would allow for the creation of a transparent audit trail of each vote, ensuring accountability. Real-time monitoring and analytics can also be introduced for election administrators. A dashboard could be created to provide insights into voter participation, detect potential fraud, and identify any technical issues in real time, which would allow administrators to act quickly and efficiently. This To further enhance accessibility, the system could be expanded to support multiple languages, ensuring that voters from different linguistic backgrounds can easily engage with the system. This would foster greater inclusivity and ensure broader voter participation. Lastly, integrating more advanced biometric authentication, such as fingerprint or iris, alongside face recognition.

References

1. Singh and R. Sharma, “Biometric Authentication in E-Voting Systems: A Review,” International Journal of Computer Applications, vol. 175, no. 12, pp. 30–36, 2020.
2. K. Sharma and P. Kumar, “Secure Online Voting Using Cryptography,” in the IEEE International Conference on Information Security, pp. 45–50, 2019.
3. L. Chen, Y. Zhang, and J. Wang, “Blockchain-based Voting System with Biometrics Integration,” Journal of Network and Computer Applications, vol. 182, p. 103002, 2021.
4. N. Patel and S. Desai, “Cloud-enabled Online Voting System Using Spring Boot and MySQL,” International Journal of Advanced Computer Science and Applications, vol. 9, no. 7, pp. 287 294, 2018. [5]. S. Gupta, R. Verma, and M. Singh, “Real-time Face Recognition Using LBPH Algorithm for Secure Voting,” Procedia Computer Science, vol. 192, pp. 450–456, 2022. A. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
5. W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, “Face Recognition: A Literature Survey,” ACM Computing Surveys, vol. 35, no. 4, pp. 399–458, 2003.
6. S. Reddy and A. Kumar, “Real-Time Face Detection and Recognition Using OpenCV and LBPH for Voting Applications,” 2024.
7. S. Sridharan and M. Karthik, “Smart Voting System Using Facial Recognition and Aadhaar Based Authentication,” 2024.
8. H. Tan and A. Kumar, “Online Voting System with Face Recognition and One-Time Password Verification,” 2022.
9. J. Smith and L. Brown, “Biometric Security in E-Voting Systems: Challenges and Solutions,”2022.
10. M. Brown and J. Taylor, “Multi-Modal Biometric Voting System Using Face and Voice Recognition,” International Journal of Advanced Research in Computer Science, vol. 12, no. 4, pp. 101–107, 2021.
11. Y. Park and H. Lee, “Real-Time Distributed Online Voting System Using Edge Computing and Facial Recognition,” IEEE Access, vol. 11, pp. 45678–45689, 2023