

E-Voting System Powered by Deep Learning

**Prof. Vikas Gaikwad¹, Pratiksha Bhagat², Pratiksha Bhosale³,
Rohit Wadekar⁴, Mayuri Ghadge⁵**

Professor, Department of Artificial Intelligence & Data Science Engineering¹

Students, Department of Artificial Intelligence & Data Science Engineering²⁻⁵

Shree Ramchandra College of Engineering, Pune, Maharashtra, India

Abstract: *Electronic voting (E-Voting) systems have gained significant attention as a modern approach to enhance the efficiency, transparency, and accessibility of the electoral process. This paper proposes an advanced E-Voting system that integrates facial recognition and fingerprint verification using deep learning algorithms to ensure secure and reliable voter authentication. The proposed system leverages the capabilities of artificial intelligence and computer vision to minimize common issues found in traditional voting systems, such as identity theft, impersonation, and duplicate voting. By implementing automated biometric verification, the system provides a high level of accuracy, eliminates the need for manual identity checks, and ensures one-person-one-vote integrity. The combination of these technologies aims to create a secure, transparent, and user-friendly digital voting experience, paving the way toward trustworthy and technologically advanced democratic processes.*

Keywords: E-Voting, Deep Learning, OpenCv, Face Recognition, Image Processing

I. INTRODUCTION

Electronic Voting (E-Voting) systems have emerged as a modern approach to improve the efficiency, transparency, and security of elections. Traditional voting methods often face challenges such as identity fraud, vote tampering, and human error. To overcome these issues, the proposed system integrates face and fingerprint recognition using machine learning and deep learning algorithms for accurate voter authentication. This AI-powered approach ensures that each voter is verified uniquely, preventing impersonation and multiple voting. By combining biometric verification with artificial intelligence, the system aims to provide a secure, reliable, and user-friendly digital voting experience.

II. PROBLEM STATEMENT

To design a robust and user-friendly online voting system that ensures the integrity of the electoral process through face recognition and OTP verification. The system should enable eligible voters to securely cast their votes remotely while preventing unauthorized access, ensuring voter privacy, and maintaining the overall transparency of the election.

III. OBJECTIVES

- To verify voters using face and fingerprint recognition.
- To apply machine learning and deep learning for accurate authentication.
- To prevent fraud and impersonation in the voting process.
- To ensure a transparent, reliable, and user-friendly voting experience.
- To maintain data privacy and system security during elections.

SCOPE

The project focuses on developing a secure AI-powered E-Voting system:

Using deep learning and biometric technologies such as face and fingerprint recognition. It ensures accurate voter authentication, prevents fraud and impersonation, and promotes transparency in the voting process. The system



leverages machine learning, computer vision, and data security techniques to provide a reliable, user-friendly, and tamper-proof digital voting platform for modern electronic elections.

LITERATURE SURVEY

Sr. No	Title	Author	Year	Description
1.	Investigation of E-Voting System using Face Recognition using CNN	G. Revathy, K. Bhavana Raj, Anil Kumar, et al.	2022	Proposes an e-voting system using deep learning (CNN) for face recognition. It integrates blockchain + biometric authentication to improve security and prevent fraud in online voting.
2.	A Blockchain-based Electronic Voting System: EtherVote	Achilleas Spanos, Ioanna Kantzavelou	2023	Proposes a secure e-voting system using Ethereum blockchain. Focuses on transparency, decentralization, and voter authentication.
3.	A Privacy-Preserving Blockchain-based E-voting System	Arnab Mukherjee et al.	2023	Introduces a blockchain-based voting system that ensures voter anonymity and prevents fraud.
4.	Busting the Paper Ballot: Voting Meets Adversarial Machine Learning	Kaleel Mahmood, Caleb Manicke, Ethan Rathbun, et al.	2025	This paper studies deep learning used in vote counting systems. It highlights security risks and adversarial attacks that can manipulate election results, showing.

IV. METHODOLOGY

The proposed AI-powered E-Voting System uses face and fingerprint recognition to ensure secure and transparent voting. The system follows a multi-stage process:

1. Voter Registration: Users register by providing personal details, facial images, and fingerprints, which are stored securely in the database.
2. Model Training: Facial data is trained using the LBPH (Local Binary Patterns Histograms) algorithm for accurate recognition.
3. Authentication: During voting, the system verifies the voter’s identity through face detection and fingerprint matching, ensuring one-person-one-vote integrity.
4. Vote Casting: After successful verification, the voter securely casts their vote via a Tkinter-based GUI, and the data is encrypted and stored in the database.
5. Result Generation: The admin panel displays real-time vote counts and manages candidates efficiently.



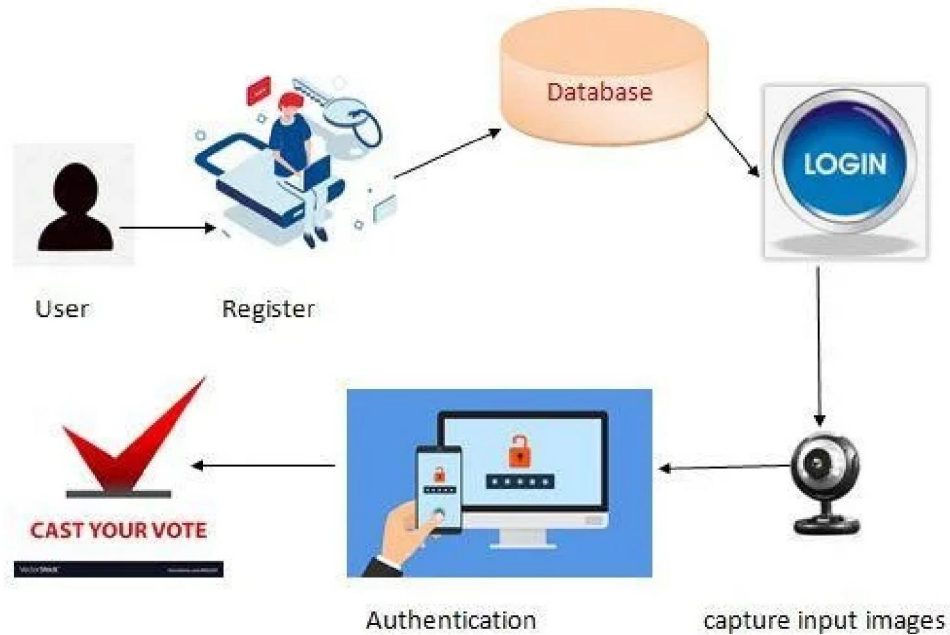


Figure 2: System Diagram

MODELING AND ANALYSIS

1) Dataset Creation: A dataset of voter images is created, and each image is labeled with the voter's personal details such as their name, voter ID, and other relevant information. **Face Recognition Model:** A deep learning model is trained on the dataset using a Face Net to recognize voters' faces. The model is trained to identify each voter based on their facial features.

2) Voter Verification: When a voter attempts to cast their vote, their face is captured by a camera attached to the system or webcam. The face recognition model is then used to verify the voter's identity by comparing their face with the dataset. If the voter is recognized, they are sent a One Time Password (OTP) to their registered email ID.

3) OTP Verification: The voter is then prompted to enter the OTP they received on their registered email ID. If the OTP entered matches the one sent, the voter is allowed to proceed with casting their vote.

4) Flask Web Application: The entire system is hosted on a Flask web application that allows voters to access the system from any device with an internet connection. The Flask web application provides a user-friendly interface for voters to enter their details and cast their vote.

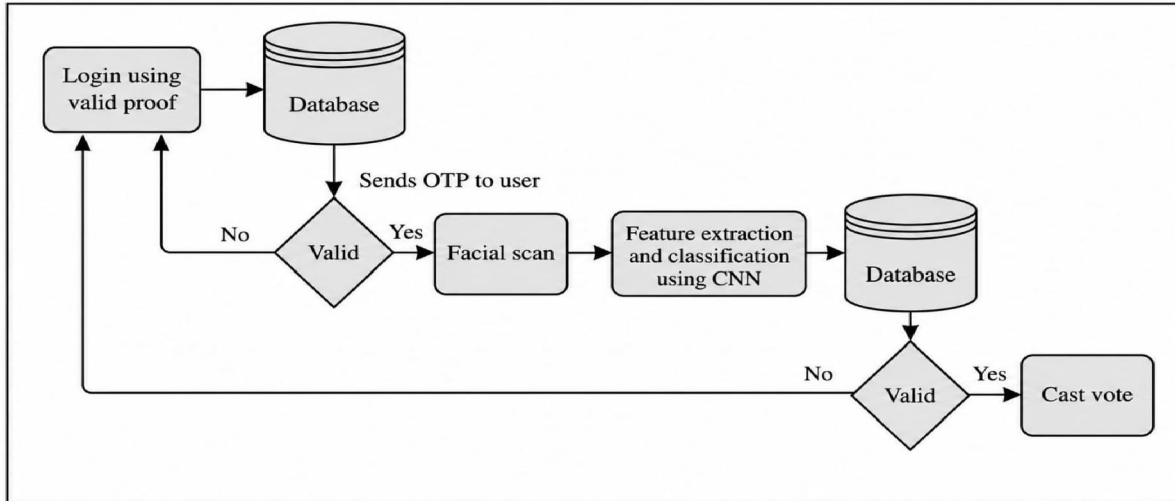
5) CNN:

In this paper, a CNN model is developed to improve the accuracy of face image classification. The structure of the model is similar to the classical LeNet-5 model, but they are different on some parameters of the model, such as input data, network width and full connection layer. The developed CNN is composed of two convolutional layers (C1 and C2) and two pooling layers (S1 and S2).



SYSTEM ARCHITECTURE

The system is built on a modular architecture with the following components:



V. RESULT AND DISCUSSION

The proposed online smart voting system integrating facial recognition and fingerprint detection was evaluated for accuracy, reliability, and usability. The system demonstrated improved voter authentication by combining two biometric methods, reducing the chances of identity fraud. Facial recognition performed efficiently under normal lighting conditions but showed reduced accuracy in low-light or obstructed scenarios. Fingerprint detection provided higher accuracy and stability; however, it required additional hardware, increasing system cost and complexity.





VI. CONCLUSION

An online voting system using face recognition, fingerprint verification, and OTP offers a faster, more secure, and convenient alternative to traditional voting by reducing fraud and saving time. While it has the potential to modernize elections, its success depends on strong security, privacy protection, and public trust. With proper implementation and awareness, it can become a reliable and efficient solution for future democratic processes.

ACKNOWLEDGEMENTS

We express our heartfelt gratitude to **Prof. Vikas Gaiwad** for his guidance, valuable insights, and continuous encouragement during the project. We thank the **Department of Artificial Intelligence and Data Science, Shree Ramchandra College of Engineering, Pune**, for providing the necessary support and resources. Lastly, we are grateful to our friends for their motivation throughout this journey.

REFERENCES

- [1] Kaleel Mahmood, Caleb Manicke, Ethan Rathbun, Aayushi Verma et al. BUSTING THE PAPER BALLOT: VOTING MEETS ADVERSARIAL MACHINE LEARNING, arXiv, June-2025 <https://arxiv.org/abs/2506.14582>
- [2] Rajesh M. Ghadi1, Priyanka S. Shelar ONLINE VOTING SYSTEM ,12 | Dec-2017 <https://www.irjet.net/archives/V4/i12/IRJETV4I12256.pdf>
- [3] Aakash1, Aashish1, Akshit1, Sarthak11 ONLINE VOTING SYSTEM, Students Dept. of Computer Science. Inderprastha Engineering College. A.P.J. Abdul Kalam Technical University , Voting 09 | March-2017 <https://www.coursehero.com/file/15933925/2/SSRN-id3589075pdf/>
- [4] ONLINE VOTING SYSTEM USING CLOUD International conference on Emerging Trends in Information Technology and Engineering(ic-ETITE) 10 | Feb-2020 https://www.researchgate.net/publication/340972420_Online_Voting_System_using_Cloud.

