IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ELECTRONIC VOTING SYSTEM USING FACE RECOGNITION

[1]A. Lalitha Pavani, [2]Prof. B. Prajna, [3]B. Bhagyalakshmi, [4]B. Harika Priya, [5]B. Indira Priya Darshini, [6]B. Venkata Sitara

[1]Student, [2]Head of the Department, [3]Student, [4]Student, [5]Student, [6]Student

[1]Department of Computer Science and Systems Engineering,

[1]Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India

Abstract: Ensuring the integrity and security of electoral processes is paramount in democratic societies. Current Electronic Voting Machines (EVMs) have become prevalent in modern elections due to their efficiency and reliability. However, they still face challenges such as identity verification and security threats. This project proposes the development of an Electronic Voting System (EVS) integrated with facial recognition technology to address these issues. The EVS aims to enhance the existing EVM by providing a more secure, efficient, and accessible platform for voters. Leveraging facial recognition and iris detection technology, voters can authenticate their identity seamlessly and securely, mitigating impersonation and unauthorized access concerns. Furthermore, the EVS offers convenience to voters by eliminating the need for EVMs and reducing waiting times at polling stations.

Index Terms **- Electronic Voting Machines, Facial Recognition, Iris Detection, Electronic Voting System with Face Recognition.**

I. INTRODUCTION

The Electronic Voting System represents a paradigm shift in elections, promising greater efficiency, accessibility, and security. From Electronic Voting Machines (EVMs) to online voting platforms, the EVS encompasses a range of technologies tailored to meet the diverse needs and infrastructural realities of different electoral systems. One of the key advantages of the EVS is its potential to enhance the integrity and transparency of elections. The EVS promises greater inclusivity and accessibility in the electoral process. By offering alternative means of authentication and voting, such as facial recognition technology, Iris detection, and accessible interfaces for voters with disabilities, the EVS seeks to ensure that all eligible citizens can access their democratic right to vote without barriers. By harnessing the power of technology, the EVS can revolutionize how elections are conducted, making them more secure, accessible, and reflective of the diverse voices within society. However, realizing the full potential of the EVS requires a comprehensive approach that balances innovation with safeguards to uphold the principles of democracy and ensure the integrity of electoral processes.

II. REVIEW OF LITERATURE

Thorat, S. B., Nayak, S. K., & Dandale, J. P. [1] delve into facial recognition technology, specifically focusing on its scope within India. The authors highlight that a facial recognition system is a computer application designed to automatically identify or verify individuals from digital images or video frames sourced from video footage. This method involves comparing selected facial features from an image with those in a database to ascertain a person's identity. Facial recognition is primarily utilized in security

systems and holds significant importance for biometric authentication alongside fingerprint and iris recognition systems. While discussing the scope of facial recognition technology in India, the authors provide insights into its multifaceted implications within diverse sectors, including but not limited to national security measures and public surveillance infrastructure management at transportation facilities and commercial establishments.

Nawfal, J., & Mungur, A. [2] say exploration of the performance evaluation between Tiny Yolov3 and MobileNet SSDv1 sheds light on their respective strengths and weaknesses when applied to various practical contexts within computer vision tasks. They say that both Tiny Yolov3 and MobileNet SSDv1 are popular models for object detection in computer vision. They have been widely used in various applications, such as self-driving cars, surveillance systems, and augmented reality. However, the author points out several limitations of each model regarding performance evaluation. The limitation of Tiny Yolov3 lies in its trade-off between speed and accuracy. On the other hand, MobileNet SSDv1 is recognized for its efficiency in terms of speed and resource usage on mobile devices or edge computing platforms.

Wolchok, S., Wustrow, E., Halderman, J. A., Prasad, H. K., Kankipati, A., Sakhamuri, S. K., ... & Gonggrijp, R. [3] sought to uncover potential weaknesses in the EVMs by conducting an independent security evaluation due to widespread reports of election irregularities and concerns about the lack of public disclosure regarding the machines' design details. The study examines in detail the design and operation of Indian EVMs, highlighting their simplicity and minimal software-trusted computing base. Despite these advantages, the machines are susceptible to severe attacks compromising election results and violating ballot secrecy. Future studies must extend their scope beyond individual system evaluations to incorporate broader considerations related to electoral processes and safeguards against potential threats. One limitation of this research is its reliance on a single EVM obtained from an anonymous source for analysis. A broader sample size across various regions or states could provide a more representative assessment of the overall security landscape concerning Indian EVMs.

III. SYSTEM ARCHITECTURE

The "Electronic Voting System Using Facial Recognition" project follows a streamlined system architecture:

Frontend:
Developed with HTML, CSS, and potentially JavaScript for dynamic updates.

Backend:
Utilizes Django, a Python web framework, for rapid development, URL routing, ORM, and authentication.

Database:
Stores data using SQLite (development) or PostgreSQL (production) for voters, parties, and votes.

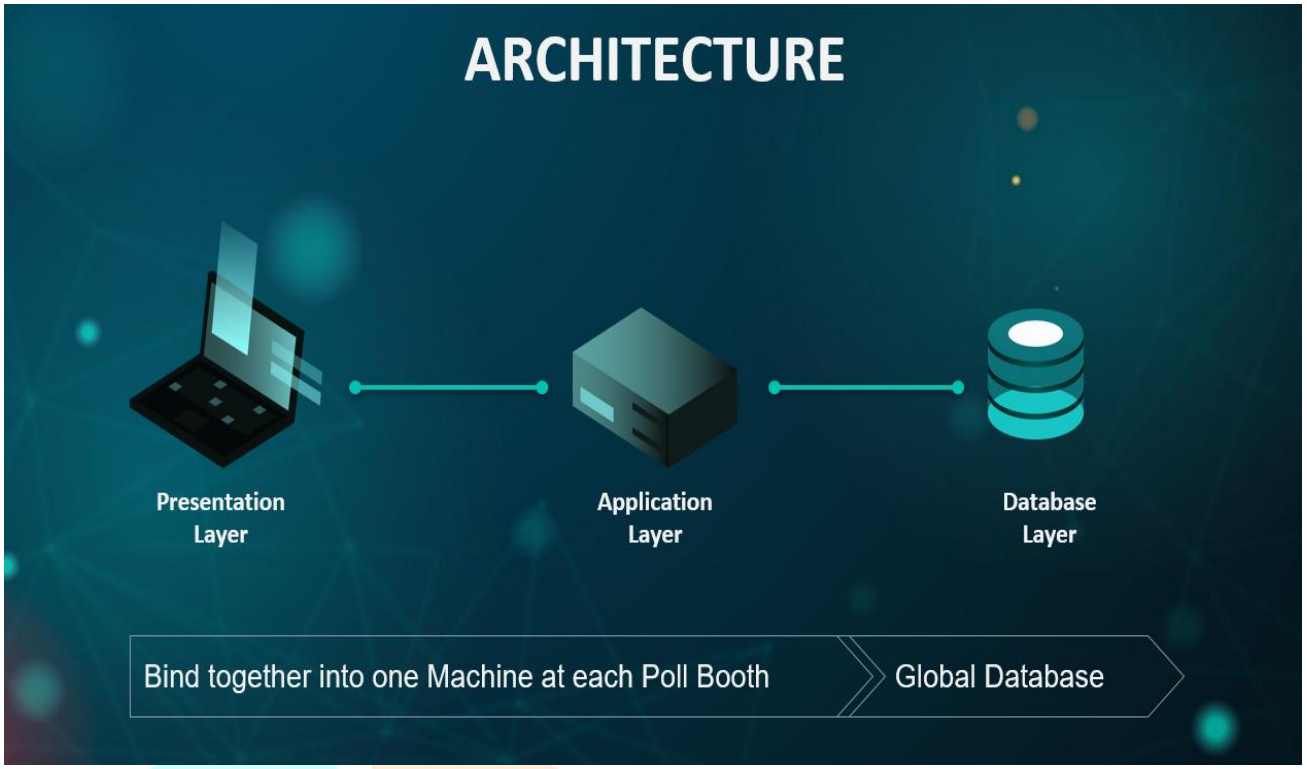
Computer Vision:
Employs OpenCV for real-time image and video analysis, person detection, mask detection, and face recognition.

SMS Notification:
Integrates Twilio API for sending SMS to voters on successful voting.

Asynchronous Execution:
It uses Python's threading module to execute tasks asynchronously, like sending SMS.

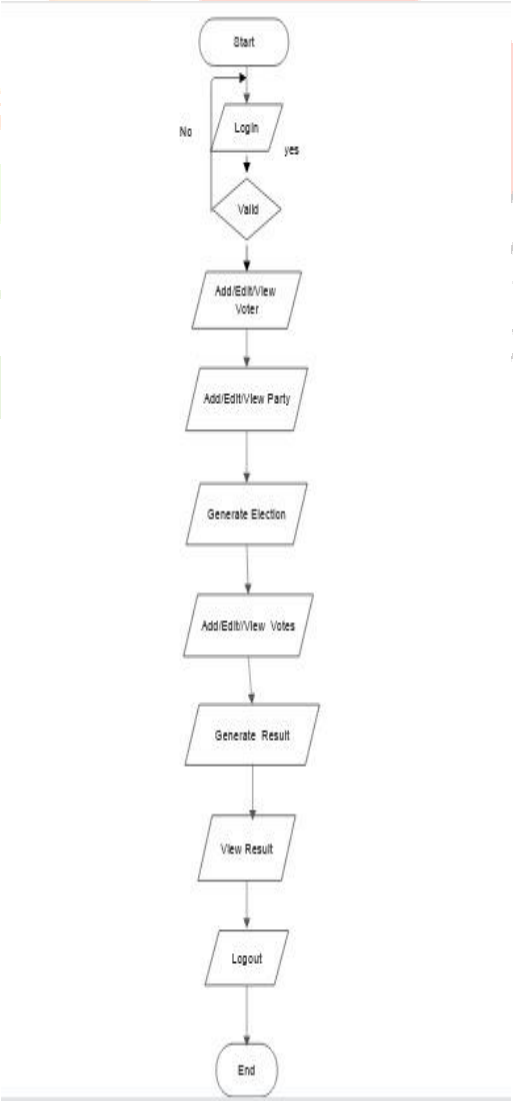
Deployment:
Deploys with Docker, Docker Compose, or Heroku for scalability and consistency.

This architecture ensures a secure and efficient electronic voting system, seamlessly integrating frontend and backend components with advanced features like facial recognition and Iris detection.



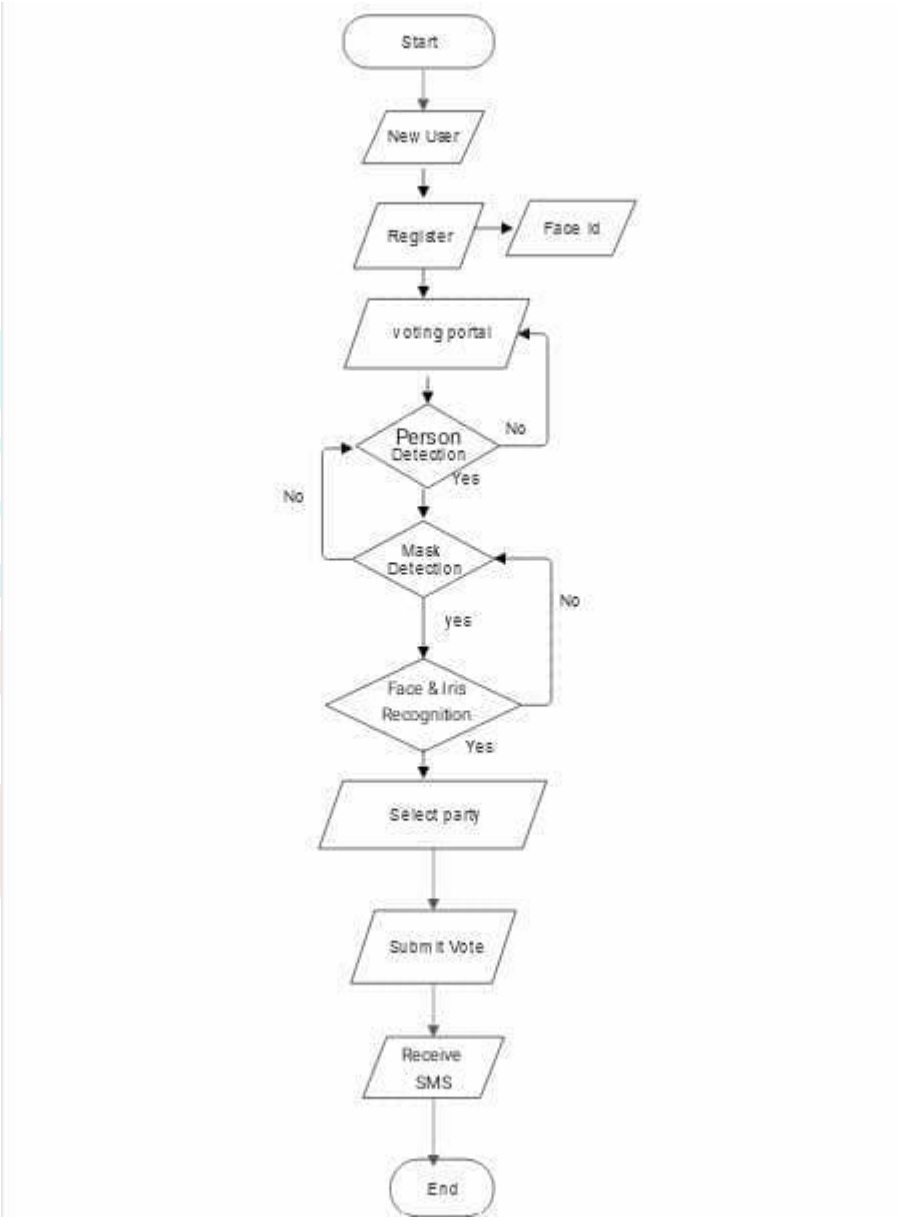
System Architecture

IV. METHODOLOGY



Flowchart of Admin

Description: The Electronic Voting System with Face Recognition begins with the Admin logging in using a secure username and password. Once authenticated, the Admin gains access to a dashboard, allowing them to perform critical functions. The first step involves managing voter details, enabling the Admin to add, edit, or view voter information. Subsequently, the Admin can handle party details, facilitating adding, editing, or viewing party-related data. The system also allows the Admin to manage vote details, where they can add, edit, or view information related to votes cast. Following these tasks, the Admin proceeds to the crucial phase of producing results, ensuring a transparent and efficient election process. This comprehensive flow chart empowers the Admin to oversee and control every aspect of the electronic voting system, contributing to a secure and accountable electoral environment.



Flowchart of Voter

Description: This flowchart describes that the voter must complete the registration process with the help of the Admin by providing the Epic number, Aadhar number, First Name, Last Name, Date of Birth, and Phone number. Voters can then go to the EVS Portal and begin voting by completing three phases. In the first phase, Person Detection, where more than one person cannot be allowed. Upon successful detection of the first phase, the system goes to the second phase, where mask detection is performed. On its successful completion, the system goes to the third phase, Face & Iris Recognition, where the face matches the face given at the time of registration, and the iris is matched. If the voter is voting for the first time, then the voter will be promoted to the Voting phase. The voter can vote for the preferred party. On successful voting, the SMS is received by the voter.

V. SYSTEM REQUIREMENTS

Software Requirements:

- Django
- Installation of Anaconda
- Jupyter NoteBook
- MongoDB
- Twilio

Hardware Requirements:

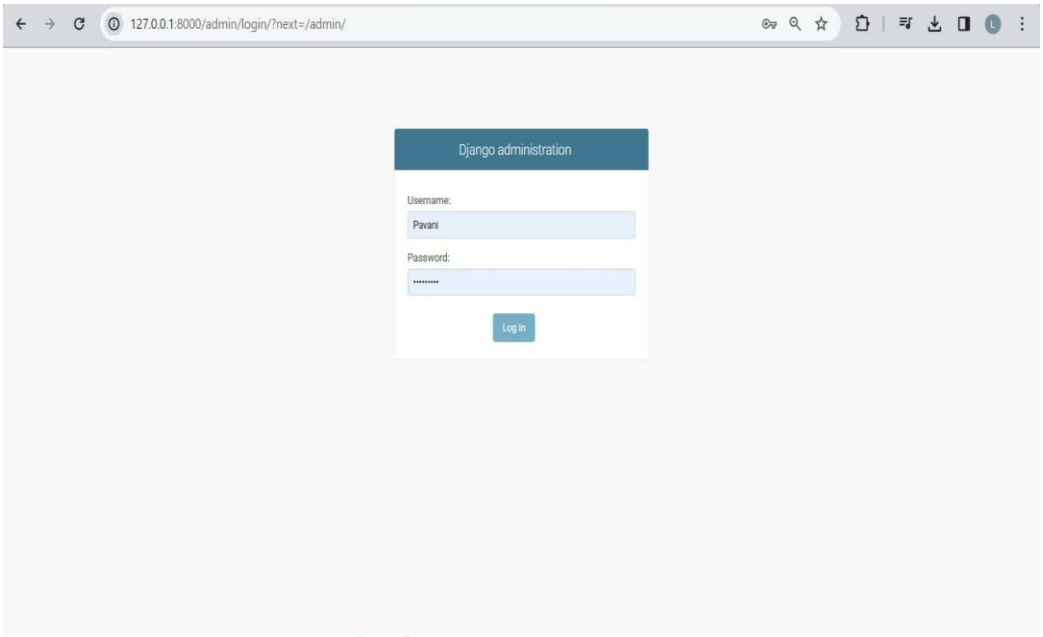
- CPU
- GPU
- RAM
- Storage

VI. IMPLEMENTATION

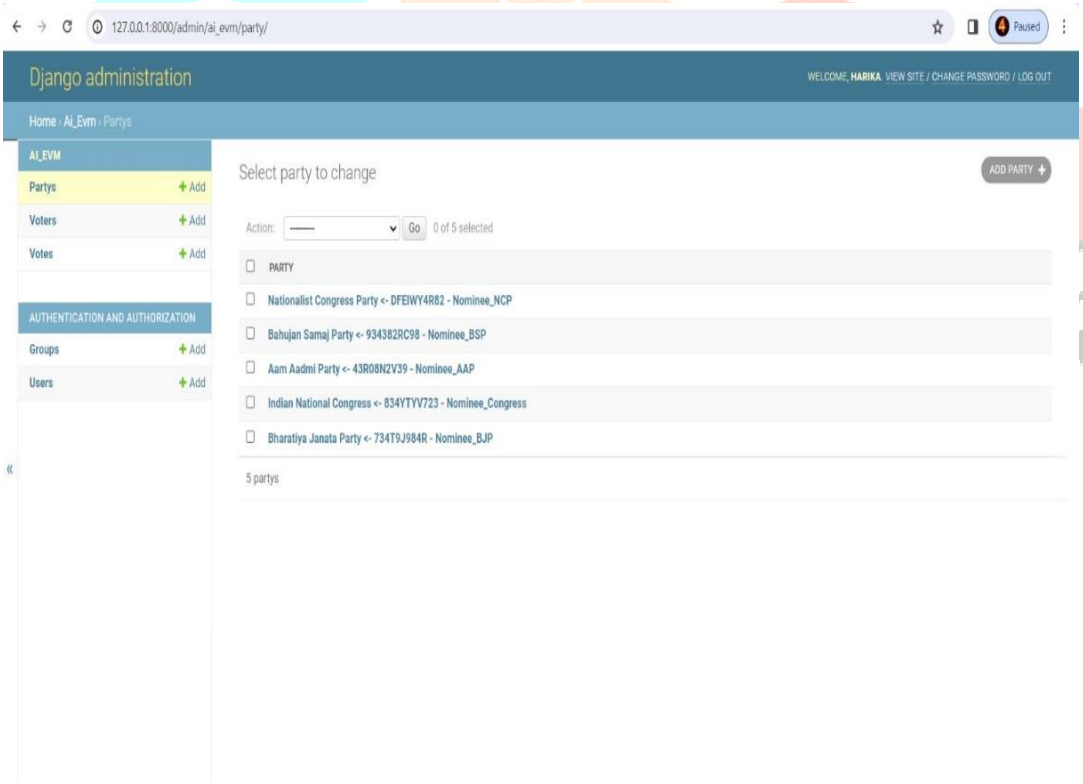
The implementation steps include:

1. Set up the environment using Anaconda Prompt and Jupyter Notebook.
2. Develop the web application with Django.
3. Integrate OpenCV, including the MobileNet SSD model, for person, mask, and face detection.
4. Implement Twilio API for SMS. This integration requires a Twilio account SID, authentication token, and phone number.
5. Threading is used to asynchronously execute tasks like sending SMS.
6. Incorporate JavaScript for enhanced user interfaces without full-page reloads.
7. Utilize HTML/CSS for web development.
8. Employ SQLite or PostgreSQL, supported by Django, for data storage.
9. Integrate dlib and face recognition for machine learning features.
10. Use NumPy, scipy, and Matplotlib for scientific computing and plotting.
11. Implement TensorFlow for machine learning capabilities.
12. Integrate Google for secure access.
13. Utilize requests for HTTP handling and working with APIs.
14. Incorporate pyOpenSSL for security and encryption.
15. Use python-dateutil for datetime extensions.
16. Implement PyHamcrest for testing match rules.
17. Utilize termcolor for ANSI color formatting.
18. Integrate Werkzeug for WSGI utility.
19. Leverage Twisted for event-driven networking.
20. Use zope.interface to define interfaces in Python.
21. Deploy the application for production using Docker, Docker Compose, or Heroku.

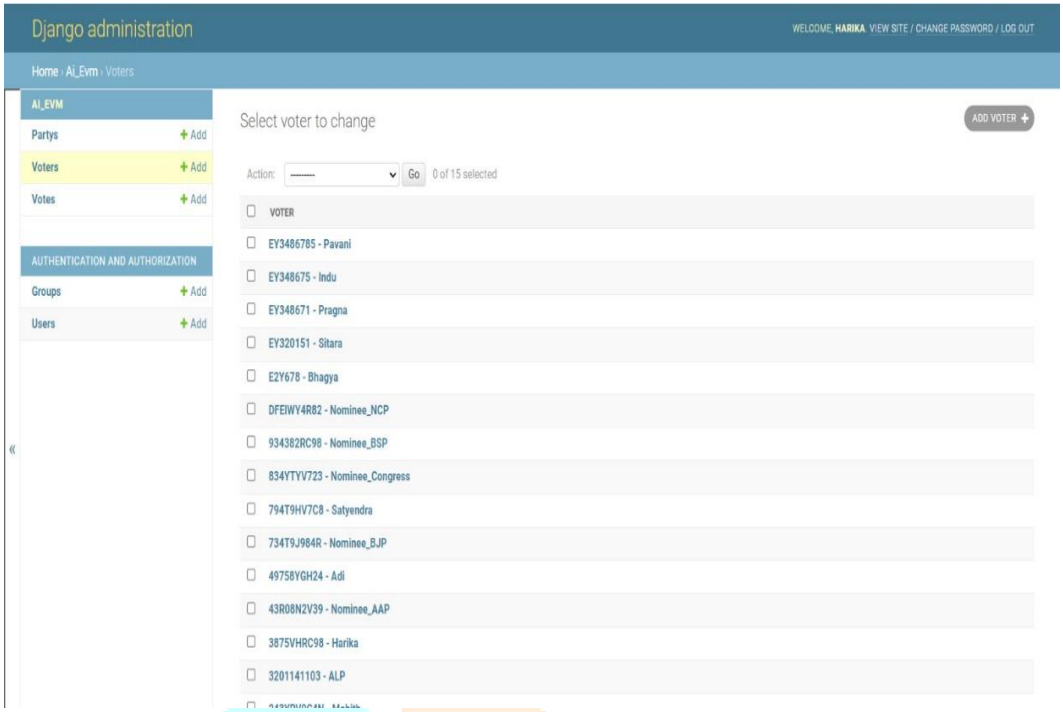
VII. OUTPUT



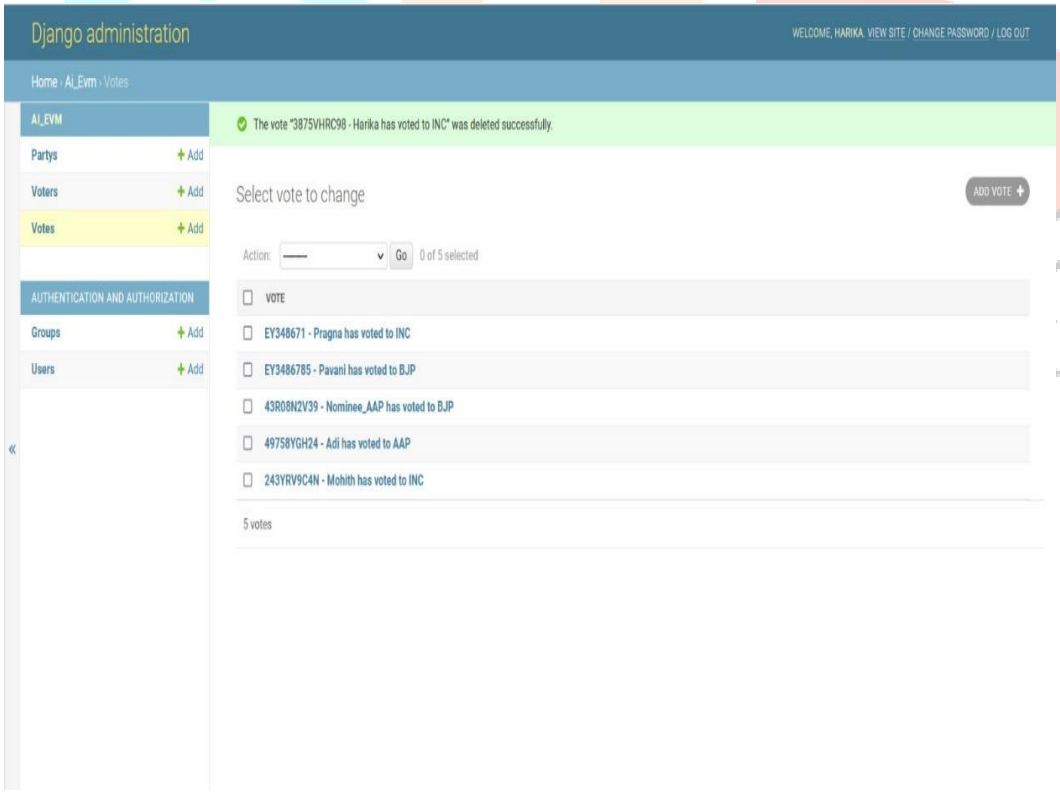
Admin Login Page



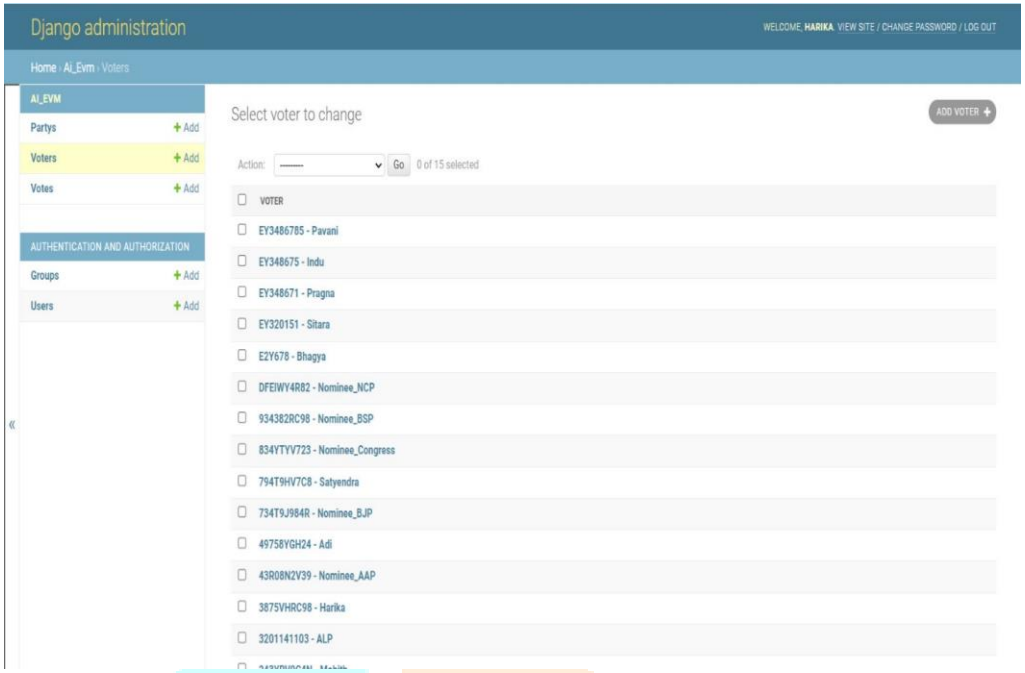
Edit/Delete Party Page



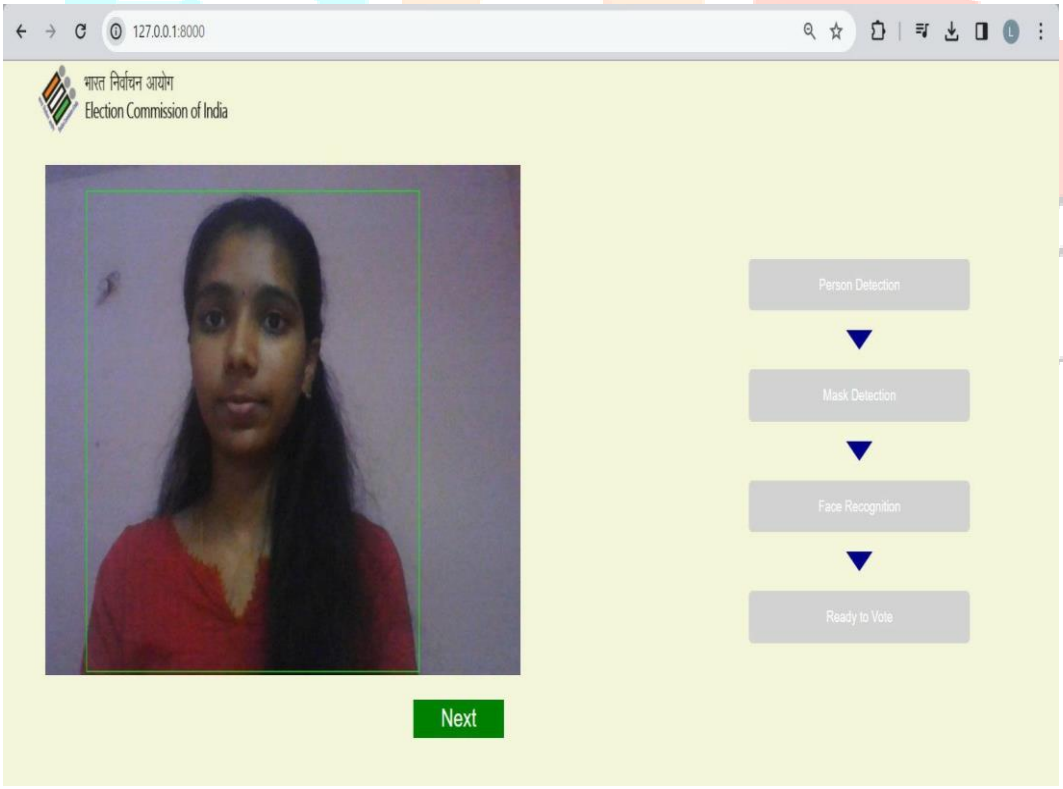
Edit/Delete Voters Page



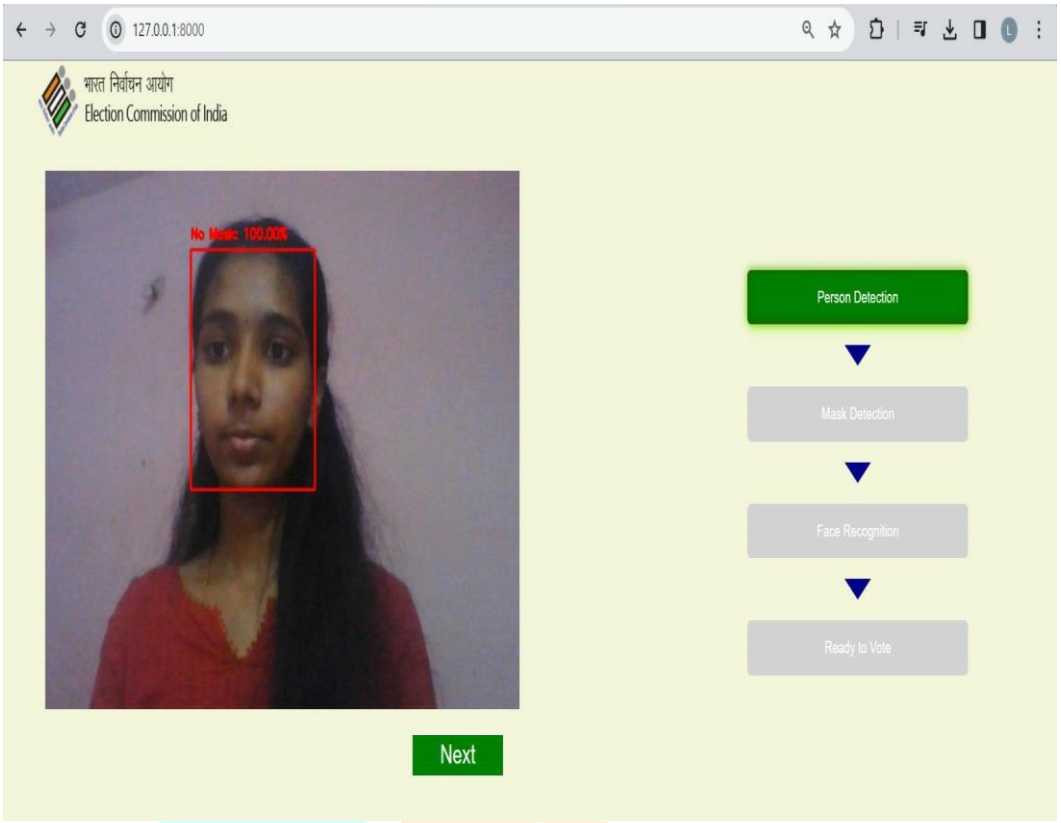
Edit/Delete Votes Page



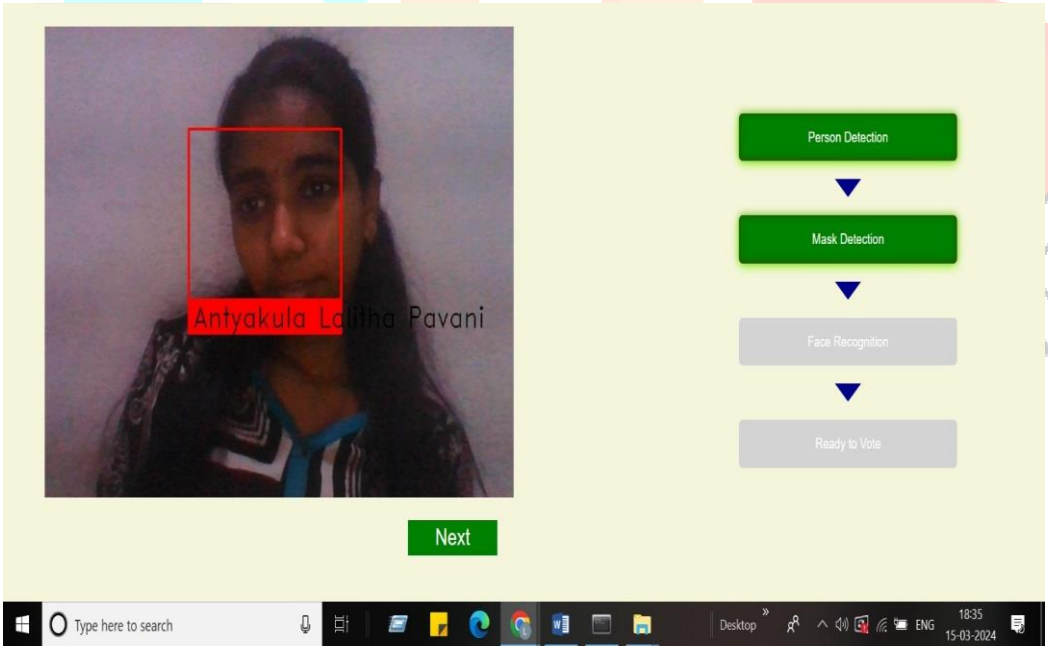
Admin Dashboard



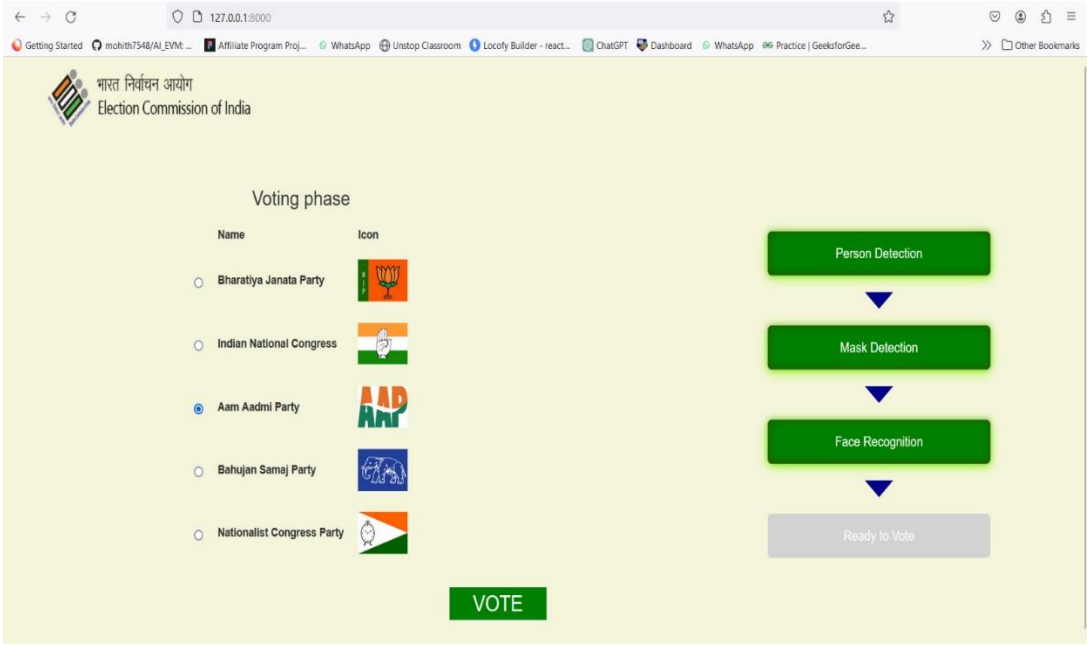
Phase-1: Person Detection



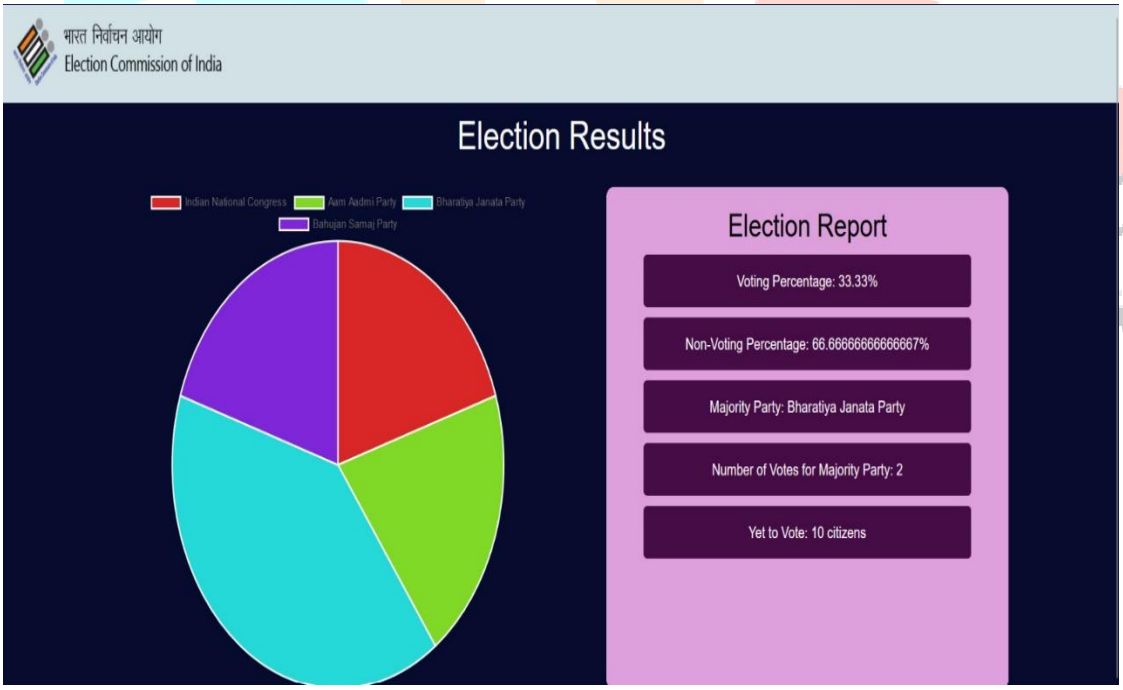
Phase-2: Mask Detection



Phase-3: Face Recognition



Voting Dashboard



Results Page

VIII. CONCLUSION & FUTURE WORK

In conclusion, the Electronic Voting System utilizing Face Recognition enhances the integrity and security of elections. It ensures accurate voter authentication, reducing the risk of fraudulent activities. The system's success in providing a transparent and efficient electoral process is evident. The future scope involves further advancements such as block-chain integration for added security, accessibility enhancements for diverse user groups, and continuous refinement of face recognition algorithms. Constant research and development can lead to a more robust, scalable, and inclusive Electronic Voting System, fostering trust in democratic processes globally.

IX. REFERENCES

[1] Thorat, S. B., Nayak, S. K., & Dandale, J. P. (2010). Facial recognition technology: An analysis with scope in India. arXiv preprint arXiv:1005.4263.

[2] Micha Nawfal, J., & Munugur, A. (2022, November). Performance Evaluation Betwwen TinyYolov3 and MobileNet SSDv1 for Object Detection. In 2022 4th International Conference on Emerging Trends in Electrical, Electronic and Communication Engineering (ELECOM) (pp. 1-6). IEEE.

[3] Wolchok, S., Wustrow, E., Halderman, J. A., Prasad, H. K., Kankipati, A., Sakhamuri, S. K., & Gonggrijp, R. (2010, October). Security analysis of India's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 1-14).