SMART VOTING SYSTEM SUPPORT THROUGH FACE RECOGNITION

[1]R.SAI MANISH,[2]J.SAI BHARATH,[3]T.VINAY KUMAR,[4]M.DEEKSHITHA,[5]Mr. G. RAJ KUMAR
[1234] Students, [5] Assistant Professor
Department Of Information Technology
Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

In this paper a new authentication technique in online voting system using facial recognition of the voter is used. In India, currently there are two types of voting system in practice. They are secret Ballet paper and Electronic Voting Machines (EVM), but both of the process has some limitation or demerits. In India online voting has not been yet implemented. The current voting system is not safe and secure too. The voters need to go to distributed places like polling booths and stand in a long queue to cast their vote, because of these reasons most of the people misses their chance of voting. The voter who is not eligible can also cast its vote by fake means which may leads to many problems. That’s why in this project we have to propose a system or way for voting which is very effective or useful in voting. In our approach we have three level of security in voting process.

The first level is the verification of unique id number (UID), second level is the verification of election id number (EID) and third level is face recognition or face matching. The security level of our system is greatly improved by the new application method for each voter. The user authentication process of the system is improved by adding face recognition in an application which will identify whether the particular user is authenticated user or not.

I. INTRODUCTION

The Smart Voting System introduces a modern approach to elections by leveraging facial recognition technology to enhance security and accessibility. Addressing limitations of traditional methods like paper ballots and EVMs, this system proposes a three-tiered authentication process: verification of Unique ID (UID) and Election ID (EID), followed by facial recognition to ensure only registered and verified individuals can cast their votes. This innovation aims to reduce voter fraud, increase convenience by enabling remote voting, and streamline the election process, ultimately fostering greater participation and trust in the democratic process.

In a democratic society, fair and secure elections are essential to ensure the integrity of governance. However, traditional voting systems often face challenges such as voter impersonation, unauthorized access, and manual verification errors. To address these concerns, we propose a **"Smart Voting System Support through Face Recognition"**—a technologically advanced solution aimed at improving the accuracy, security, and efficiency of the voting process.

This system integrates **multi-level authentication** by verifying users through their **UID (Aadhar), Voter ID, and facial recognition** using the **Eigen Face algorithm**. By leveraging **Python, Django**, and **OpenCV**, along with deep learning frameworks such as **TensorFlow and Keras**, the system ensures that only authorized individuals can cast their votes. A **SQLite database** is used for storing user credentials and voting data securely.

The project also emphasizes user-friendliness and real-time identity verification, ensuring a seamless experience for voters while minimizing the risk of fraud. This solution has the potential to modernize the electoral process and pave the way for **secure digital voting** in the future.

Purpose of the Project

Now a day in India two types of method are used for voting. The first method is secret ballot paper, in which lots of paper are used and second method is EVM (electronic voting machine) which is used since 2003. we have to propose a method or way for online voting that is more secure than the existing system. In this proposed project face detection and recognition concept is used to identify the exact person. There are three levels of verification were used for the voters in our proposed system. The first one is Unique id number verification, second level of verification is election commission id or voter card number, if your election commission id number is correct then you have to go for third level of security which is the main security level where the system recognize the face of the real voter from the current database of face images given by the election commission. If the captured image is matched with the respective image of the voter in the database, then a voter can cast their vote in the election. as you have to know that in existing system is not much more secure because in existing system security level is only voter card so any one can give other person vote with voter card but here we proposed a way for voting which is more secure than existing system.

The current voting systems in India, which include secret ballot papers and Electronic Voting Machines (EVMs), have several limitations. These range from security concerns to voter inconvenience.

Online voting in India has not yet been implemented, and the existing systems are considered to be not entirely safe or secure. Voters often have to travel to polling booths and wait in long queues, which discourages many from voting. There's also the risk of ineligible individuals casting votes through fraudulent means.

To address these issues, a new voting system is proposed that uses facial recognition for voter authentication. This system aims to enhance security and make the voting process more efficient.

The proposed system uses a three-level security process. These levels are:

- Verification of the voter's unique ID number (UID).
- Verification of the voter's Election ID number (EID).
- Facial recognition to match the voter's face with the image in the election commission's database.

The system uses the Eigenface algorithm for facial recognition. This algorithm enhances the security of the voting process by ensuring that only authenticated users can vote.

Problem Statement

Cryptocurrency markets are characterized by extreme volatility and unpredictability, influenced by factors such as global economic shifts, market sentiment, and changing regulatory landscapes.This complexity makes accurate price forecasting a critical yet challenging task for traders, investors, and financial institutions seeking to make informed decisions and manage risks effectively.Traditional forecasting methods, like ARIMA and feedforward neural networks, often fall short in capturing the intricate and non-linear patterns present in cryptocurrency data.These approaches lack the capability to model sequential dependencies and respond to abrupt price changes, leading to inconsistent predictions and heightened financial uncertainties.

The lack of adaptive and robust forecasting models further exacerbates the problem, as the rapidly evolving nature of cryptocurrency markets demands solutions that can process and analyze large volumes of historical data effectively. Additionally, traditional systems face challenges in integrating realtime data and adjusting to shifting trends in the market, leading to delayed or suboptimal outcomes.This highlights the need for a modern forecasting approach that can handle temporal dependencies, non-linear patterns, and the dynamic nature of these markets, providing more accurate and timely insights to market participants.

EXISTING SYSTEM

Existing systems for cryptocurrency price forecasting are statistical models like ARIMA (AutoRegressive Integrated Moving Average) and machine learning approaches such as feedforward neural networks. ARIMA models focus on making the data stationary and use past values and errors to predict future prices, making them useful for stable and linear patterns.Feedforward neural networks, on the other hand, process historical data as individual inputs and utilize layered transformations to make predictions.These systems have been widely used for various financial forecasting tasks, leveraging historical price data to provide insights into market trends.Despite their foundational role, they are limited in their ability to address the unique characteristics of cryptocurrency markets.

Disadvantages of existing system:

ARIMA models are constrained by their assumption of data stationarity and linear relationships, which makes them unsuitable for capturing the complex, non-linear dependencies in cryptocurrency price data. They also require extensive manual feature engineering and preprocessing, increasing their implementation complexity. Similarly, feedforward neural networks fail to capture temporal dependencies as they treat each input independently, which is a significant drawback when working with sequential time-series data. Both approaches are less effective in handling the high volatility, sudden price spikes, and dynamic factors that characterize cryptocurrency markets, leading to unreliable predictions and limiting their practical applicability.

PROPOSED SYSTEM

The proposed system leverages Long Short-Term Memory (LSTM) neural networks, a specialized type of deep learning model designed for sequential data, to address the challenges of cryptocurrency price forecasting.Unlike traditional methods, LSTM models can effectively capture temporal dependencies and non-linear patterns in time-series data.By processing sequences of historical cryptocurrency prices, the model learns to identify trends and predict future values with higher accuracy.The system incorporates advanced data preprocessing techniques, such as handling missing values and normalizing input data, ensuring that the model receives clean and meaningful input.This robust approach allows the LSTM model to adapt to the volatile nature of cryptocurrency markets, providing more reliable forecasts.

Additionally, the proposed system automates feature extraction, eliminating the need for extensive manual intervention and enabling it to identify subtle patterns in the data that traditional methods may overlook.The model’s performance is validated using metrics like Mean Absolute Error (MAE), Mean Squared Error (MSE), and accuracy, demonstrating its effectiveness in improving prediction reliability.Visualizations of actual versus predicted prices and loss curves provide insights into the model’s behavior and its ability to generalize across datasets.By addressing the limitations of existing systems, this solution offers a powerful tool for traders, investors, and financial institutions to make better-informed decisions in the highly dynamic cryptocurrency market.

Advantages of proposed system:

The proposed system offers significant improvements over traditional forecasting models by utilizing Long Short-Term Memory (LSTM) neural networks, which excel at handling sequential data. One of the key advantages of using LSTM is its ability to capture temporal dependencies, which is crucial for time-series forecasting in volatile markets like cryptocurrency.LSTM models automatically learn from the historical price data, identifying patterns and trends that would be difficult for traditional models to recognize.This allows the system to produce more accurate and reliable predictions, even under the dynamic conditions of the cryptocurrency market.Moreover, LSTM's ability to process long sequences of data helps in understanding the complex, non-linear relationships that influence price movements over time.

Additionally, the proposed system reduces the need for manual intervention and extensive feature engineering, as the LSTM model automatically extracts features from the input data. This makes the model not only more efficient but also adaptable to changing market conditions.The system’s ability to handle missing data and integrate real-time information ensures that predictions remain robust, even in the face of incomplete or fluctuating inputs.With evaluation metrics like Mean Absolute Error (MAE) and Mean Squared Error (MSE), the system's performance is easily quantifiable, giving traders, investors, and financial institutions a trustworthy tool for making informed decisions and managing risks in an unpredictable market.

Scope of the Project

This project encompasses the end-to-end development of a time-series forecasting system for cryptocurrency prices, focusing on a single trading pair (e.g., XRP/USDT).It includes data acquisition and preprocessing handling missing values, converting timestamps, and normalizing price series— followed by the extraction of fixed-length windows for model input.The core of the work is the design, training, and evaluation of an LSTM neural network that learns temporal dependencies in historical price data.Performance is assessed using metrics such as MAE, MSE, and a custom accuracy measure, with visualizations of training/validation loss and actual versus predicted price curves provided for comprehensive analysis.

Beyond the immediate implementation, the project’s scope extends to exploring model scalability and adaptability.While the current work addresses a single cryptocurrency pair, the framework is designed to support multiple assets and additional features such as technical indicators, sentiment scores, or on-chain metrics in future iterations.Limitations include reliance on historical price data without real-time sentiment or order-book integration, and the absence of a live trading module.Nonetheless, the modular architecture allows for easy incorporation of new data sources, hyperparameter tuning strategies, and deployment pipelines, laying the groundwork for more sophisticated, production-ready forecasting solutions.

II. LITERATURE SURVEY

Time-Series Forecasting of Cryptocurrency Prices Using Deep Learning

In recent years, the evolution of secure and efficient voting mechanisms has been a critical focus in both technological and democratic landscapes. Traditional voting systems, including ballot-based and electronic voting machines (EVMs), have long been criticized for vulnerabilities such as vote tampering, impersonation, and logistical challenges in ensuring wide voter participation. The need for physical presence at polling booths has further contributed to decreased voter turnout, especially in rural and remote areas.

To address these challenges, biometric authentication methods have emerged as a viable solution. Among these, facial recognition stands out due to its non-intrusive nature and high accuracy in real- time identification. Techniques such as the Eigen Face algorithm, Principal Component Analysis (PCA), and convolutional neural networks (CNNs) have been explored extensively in literature for facial feature extraction and comparison. These algorithms work by analyzing unique facial characteristics and matching them against stored datasets, enabling accurate identification of legitimate voters.

Several studies indicate that deep learning models outperform traditional methods in recognizing facial features under varying lighting conditions, facial expressions, and angles. When integrated with smart voting systems, these models can ensure that only registered voters can participate, thereby preventing fraud such as multiple voting or identity theft. In countries like India, where electoral participation is vast and diverse, implementing such a system could significantly improve election credibility, accessibility, and efficiency. The application of deep learning in voting not only enhances security but also opens pathways for remote voting through online platforms, reducing the need for voters to physically travel to designated polling locations.

III. SYSTEM DESIGN

SYSTEM ARCHITECTURE

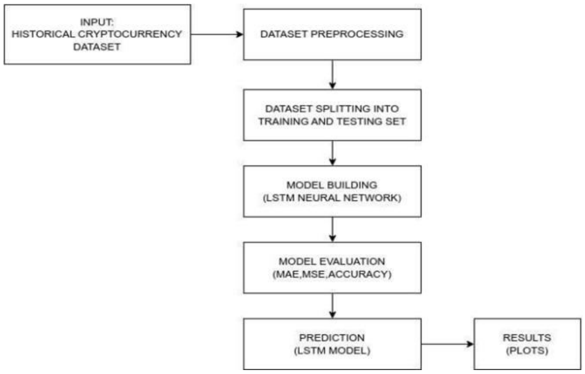

INPUT:
HISTORICAL CRYPTOCURRENCY DATASET
DATASET PREPROCESSING
DATASET SPLITTING INTO TRAINING AND TESTING SET
MODEL BUILDING (LSTM NEURAL NETWORK)
MODEL EVALUATION (MAE,MSE,ACCURACY)
PREDICTION (LSTM MODEL)
RESULTS (PLOTS)

FIG: SYSTEM ARCHITECTURE

IV. MODEL DESCRIPTION

The Smart Voting System is structured around several key modules, each responsible for a distinct aspect of the voting process. These modules work in concert to ensure a secure, efficient, and reliable voting experience.

Voter Registration and Data Collection

This module forms the foundation of the system by handling the crucial initial step of voter registration. Accurate and secure collection of voter information is paramount to the integrity of the entire system.

- **Detailed Process:**
- New users (voters) initiate the registration process through a user-friendly interface.
- The system prompts the user to provide their **Unique Identification Number (UID)**. This is a critical identifier, and the system may incorporate checks to ensure its validity (e.g., format
  - validation, checksum verification).
- The system also collects the **Election ID (EID)**. Similar to the UID, this ID is essential for voter authentication and may undergo validation.
- A high-resolution **facial image** of the voter is captured in real-time using a webcam (or potentially a mobile device camera). The system may guide the user to ensure proper image capture (e.g., adequate lighting, frontal view, focus).
- All the collected data (UID, EID, and the facial image) is then securely stored in a central database.
  - **Data Security:**
- Emphasis is placed on secure storage to protect sensitive voter information. This may involve:
- **Encryption:** Encrypting the data both during transmission and storage.
- **Access Control:** Implementing strict access controls to the database, limiting who can view or modify the data.
- **Data Integrity:** Employing mechanisms to ensure data integrity and prevent tampering.
- **Importance:**
  - This module is critical because it establishes the identity of each voter within the system.
  - The accuracy and security of this module directly impact the reliability of subsequent voting processes.

Data Preprocessing and Face Encoding

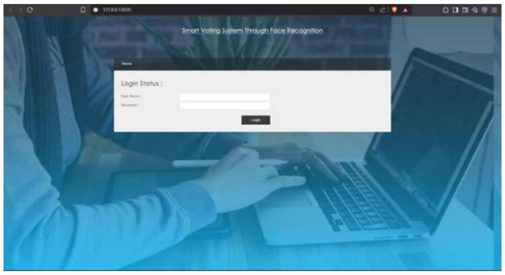
This module prepares the captured facial images for efficient and accurate facial recognition. Preprocessing enhances the quality of the images, while encoding extracts the essential facial features.

- **Data Preprocessing:**
  - The captured facial image undergoes several

preprocessing steps to standardize the image and reduce variability:

- **Resizing:** The image is resized to a consistent dimension to ensure uniformity.
- **Grayscale Conversion:** The image is converted to grayscale, reducing the amount of data and focusing on essential luminance information.
- **Noise Reduction:** Techniques like blurring or filtering may be applied to minimize noise and improve image clarity.
- **Image Enhancement:** Other enhancements, such as contrast adjustment or histogram equalization, might be used to improve feature visibility.

V. OUTPUT SCREENS



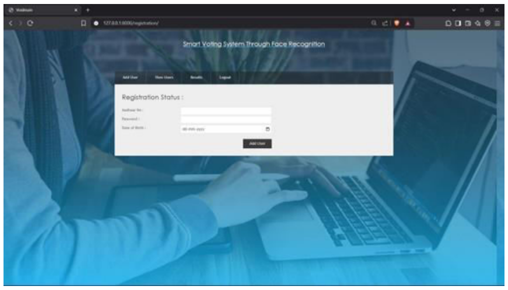
127.0.0.1:8000

Smart Voting System Through Face Recognition

Login Status :

User Name :

Password :



127.0.0.1:8000/registration/

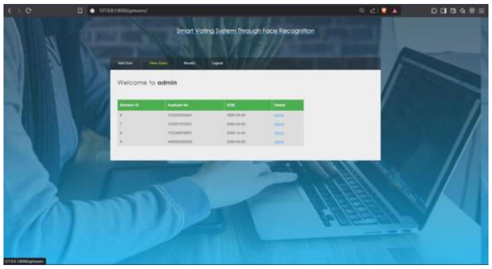
Smart Voting System Through Face Recognition

Registration Status :

Aadhaar No :

Password :

Date of Birth : dd-mm-yyyy

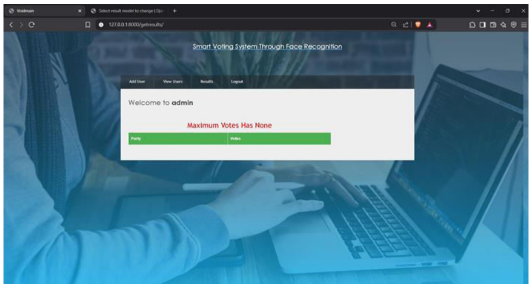


127.0.0.1:8000/getusers/

Smart Voting System Through Face Recognition

Welcome to **admin**

Election ID	Aadhaar No	DOB	Delete
6	[illegible]	[illegible]	Delete
7	[illegible]	[illegible]	Delete
8	[illegible]	[illegible]	Delete
9	[illegible]	[illegible]	Delete



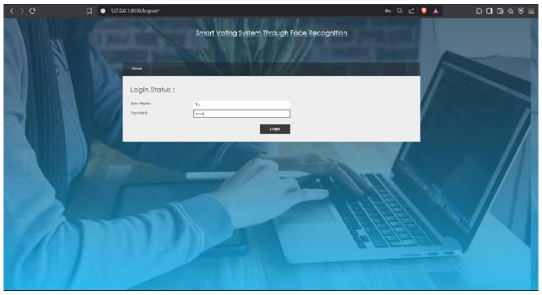
127.0.0.1:8000/getresults/

Smart Voting System Through Face Recognition

Welcome to **admin**

Maximum Votes Has None

Party	Votes



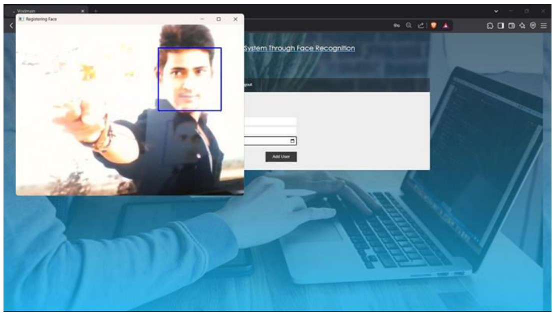
127.0.0.1:8000/logout/

Smart Voting System Through Face Recognition

Login Status :

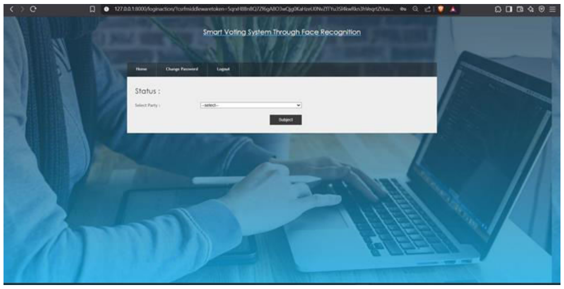
User Name : ts

Password : ••••



Registering Face

System Through Face Recognition

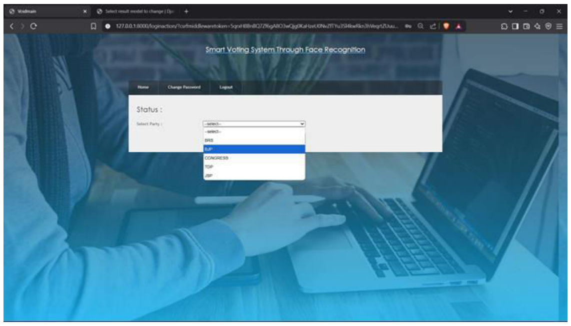


127.0.0.1:8000/loginaction/?csrfmiddlewaretoken=5qnH8BnBQ7Zf6gA8O3wQjg0KaHzeUXNvZfTYu3SI4kwRkn3hWeqrtZUuu...

Smart Voting System Through Face Recognition

Status :

Select Party : --select--

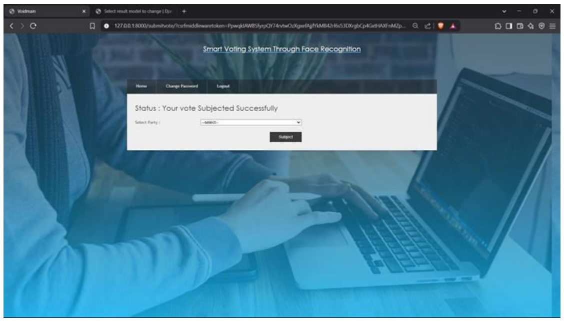


127.0.0.1:8000/loginaction/?csrfmiddlewaretoken=5qnH8BnBQ7Zf6gA8O3wQjg0KaHzeUXNvZfTYu3SI4kwRkn3hWeqrtZUuu...

Smart Voting System Through Face Recognition

Status :

Select Party : --select--

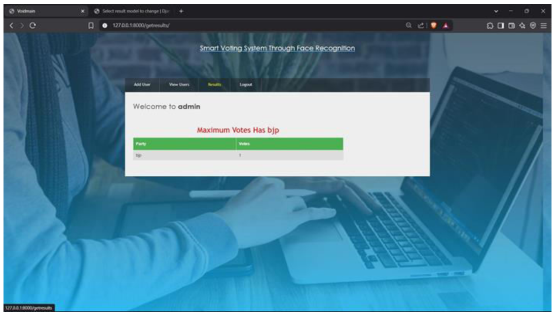


127.0.0.1:8000/submitvote/?csrfmiddlewaretoken=PpwqkIAWBSfyrpQY74rvtwOzXgxefAgfYkMB42rl6s53DXrgbCp4GxtHAXFnMZp...

Smart Voting System Through Face Recognition

Status : Your vote Subjected Successfully

Select Party : --select--


Voidmain
Select result model to change | Dj
127.0.0.1:8000/getresults/
Add User
View Users
Results
Logout
127.0.0.1:8000/getresults

Smart Voting System Through Face Recognition

Welcome to **admin**

Maximum Votes Has bjp

Party	Votes
bjp	1

VI. CONCLUSION

The “Smart Voting System Support through Face Recognition” project is a significant step forward in redefining the security, accessibility, and transparency of the electoral process. Traditional voting systems, while effective in the past, are increasingly vulnerable to issues such as fake voting, impersonation, and geographical limitations that hinder many voters from casting their votes. To overcome these challenges, this system introduces a novel approach by integrating facial recognition technology with a multi-level authentication mechanism that includes UID and Voter ID validation. This ensures that only genuine and authorized individuals are able to participate in the voting process.

The implementation of the Eigen Face algorithm for facial recognition ensures accuracy and reliability in voter verification. By capturing, encoding, and matching the facial features of the user against pre- registered data, the system minimizes the risk of identity fraud. Furthermore, by making the platform accessible online, it eliminates the need for physical presence at polling booths, thereby encouraging participation from remote voters and people with mobility issues.

In conclusion, the smart voting system not only addresses the critical shortcomings of conventional methods but also lays the foundation for future innovations in digital democracy. With further development and real-world integration, this model can significantly enhance the efficiency and trustworthiness of national and local elections, contributing to a more inclusive and fraud-free democratic ecosystem.

REFERENCES

1. Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *IEEE Conference on Computer Vision and Pattern Recognition*.
2. Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1), 71–86.
3. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
5. Russel, S., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (3rd ed.). Pearson Education.
6. Géron, A. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*. O’Reilly Media.
7. Bradski, G. (2000). The OpenCV Library. *Dr. Dobb’s Journal of Software Tools*.
8. Van Rossum, G., & Drake, F. L. (2009). *Python 3 Reference Manual*. Python Software Foundation.
9. Django Software Foundation. (2017). *The Django Book*. Version 2.0.
10. Pedregosa, F., Varoquaux, G., Gramfort, A., et al. (2011). Scikit-learn: Machine learning in Python.
11. *Journal of Machine Learning Research*, 12, 2825–2830.
12. Harris, C. R., Millman, K. J., van der Walt, S. J., et al. (2020). Array programming with NumPy. *Nature*, 585, 357–362.
13. McKinney, W. (2010). Data Structures for Statistical Computing in Python. *Proceedings of the 9th Python in Science Conference*, 51–56.
14. Abadi, M., et al. (2016). TensorFlow: A system for large-scale machine learning.

USENIX Symposium on Operating Systems Design and Implementation (OSDI).

15. Sharma, N., & Jain, R. (2015). Face recognition using Eigenfaces and Principal Component Analysis.
16. *International Journal of Computer Applications*, 109(10), 33–39.
17. Bhavani, R., & Suresh, S. (2018). Smart electronic voting system using facial recognition. *International Journal of Engineering Research & Technology (IJERT)*, 7(5), 22–26.
18. Pandit, Varad, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga, and Sachin Bojewar. "Intelligent security lock." In *Trends in Electronics and Informatics (ICEI), 2017 International Conference on*, pp. 713-716. IEEE, 2017.
19. Chauhan, C. U., Abhishek Kalnawat, Akshay Aswale, Ujwal Gautam, and Roshan Nemad. "Survey Paper on a Novel Approach: Web Based Online Voting System using Aadhaar Card & Face Recognition."
20. Patel, Fenil, Dhruvesh Patel, Shrey Patel, and Prof Maulik Trivedi. "Secure E-Voting System Using Aadhaar Card and Biometric Authentication."
21. Jaiswal, Ayush, Harsh Agrawal, and Prof. Nilima Pathak. "E-Voting System using Aadhar Card and Face Recognition."
22. Kumar, Rakesh, and Prachi Agarwal. "An Integrated Approach for Secure E-Voting System using Aadhar Card and Biometric Techniques." In *Proceedings of International Conference on Computing, Communication and Data Engineering*, pp. 1-5. Springer, Singapore, 2018.
23. Yadav, Pratiksha, and Jyoti Yadav. "Online Voting System Using Face Recognition Based on Aadhar Card."
24. Kishor, N., S. Indu, and M. Nithya. "Secure E-Voting System using Aadhar and Face Recognition." In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 963- 967. IEEE, 2020.
25. "Aadhaar Enabled Election System (AEES)." *Unique Identification Authority of India*.
26. Turk, Matthew, and Alex Pentland. "Eigenfaces for recognition." *Journal of cognitive neuroscience* 3, no. 1 (1991): 71-86.