

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA",MACHHE, BELAGAVI-590018



ML Mini Project Report on Online Voting System

Submitted in partial fulfillment of the requirements for the VI semester

Bachelor of Engineering

in

Artificial Intelligence & Machine Learning

of

Visvesvaraya Technological University, Belagavi

by

CHETHAN SWAMY N S

(ICD21AI008)

EBIN M S

(1CD21AI062)

Under the Guidance of

Dr.Varalatchoumy.M,

Prof. Syed Hayath

Dept. of AI&ML



Department of Artificial Intelligence & Machine Learning

CAMBRIDGE INSTITUTE OF TECHNOLOGY,BANGALORE-560 036

2023-2024

CAMBRIDGE INSTITUTE OF TECHNOLOGY

K.R. Puram, Bangalore-560 036

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & MACHINE LEARNING



CERTIFICATE

Certified that **Mr. Chethan Swamy N S**, bearing USN **1CD21AI008** and **Mr. Ebin M S**, bearing USN **1CD21AI062**, a bonafide students of **Cambridge Institute of Technology**, has successfully completed the ML Mini Project entitled “**Online Voting System**” in partial fulfillment of the requirements for VI semester **Bachelor of Engineering in Artificial Intelligence & Machine Learning** of **Visvesvaraya Technological University, Belagavi** during academic year 2023-24. It is certified that all Corrections/Suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The ML Mini Project report has been approved as it satisfies the academic requirements prescribed for the Bachelor of Engineering degree.

Mini Project Guides,

Dr. Varalatchoumy.M ,

Prof. Syed Hayath
Dept. of AI&ML, CITech

Head of the Department,
Dr. Varalatchoumy.M
Dept. of AI&ML, CITech

DECLARATION

We, Chethan Swamy N S and Ebin M S of VI semester BE, Artificial Intelligence & Machine Learning, Cambridge Institute of Technology, hereby declare that the ML Mini Project entitled **“Online Voting System”** has been carried out by us and submitted in partial fulfillment of the course requirements of VI semester **Bachelor of Engineering in Artificial Intelligence & Machine Learning** as prescribed by **Visvesvaraya Technological University, Belagavi**, during the academic year 2023-2024.

We also declare that, to the best of my knowledge and belief, the work reported here does not form part of any other report on the basis of which a degree or award was conferred on an earlier occasion on this by any other student.

Date:

Place: Bangalore

Chethan Swamy N S

1CD21AI008

Ebin M S

1CD21AI062

ACKNOWLEDGEMENT

We would like to place on record my deep sense of gratitude to **Shri. D. K. Mohan**, Chairman, Cambridge Group of Institutions, Bangalore, India for providing excellent Infrastructure and Academic Environment at CITech without which this work would not have been possible.

We am extremely thankful to **Dr. G.Indumathi**, Principal, CITech, Bangalore, for providing me the academic ambience and everlasting motivation to carry out this work and shaping our careers.

We express my sincere gratitude to **Dr. Varalatchoumy M.**, Prof. & Head, Dept. of Artificial Intelligence & Machine Learning, CITech, Bangalore, for her stimulating guidance, continuous encouragement and motivation throughout the course of present work.

We also wish to extend my thanks to Mini Project Guides, **Dr. Varalatchoumy M.**, Prof. & Head and **Prof. Syed Hayath** Assistant Professor, Dept. of AI&ML, CITech, Bangalore for the critical, insightful comments, guidance and constructive suggestions to improve the quality of this work.

Finally to all my friends, classmates who always stood by me in difficult situations also helped me in some technical aspects and last but not the least, we wish to express deepest sense of gratitude to my parents who were a constant source of encouragement and stood by me as pillar of strength for completing this work successfully.

Chethan Swamy N S

Ebin M S

ABSTRACT

In today's scenario, voters have to go to the polling booth to vote which takes time and the voting percentage is also low due to some voters do not go to polling booth to cast the vote. Digital voting would be helpful as voter can vote online from their computer or laptop or smartphone which can save time of voter, it will be also helpful to increase the voting percentage. Digital voting has admin login which will be handled by election commission and voter login which will be handled by voter. Voters can login through their voter ID number and password after a successful registration. The system will allows voters to view a list of candidates in their area, voters can get to know the candidates background (like income, works, etc.) and choose wisely. Once the election is started voter have to login into the account, select a candidate and have to give face id with webcam or front camera, if the face matches with the face given at the time of registration then voter will be promoted for two factor authentication, if two factor authentication is successful then the vote will be submitted and one voter can vote for a candidate only once per election

CONTENTS

Abstract	i
Contents	ii
List of Figures	iii

Chapters	Page No.
Chapter 1 Introduction	1
1.1 Problem statement	2
1.2 Objective	4
Chapter 2 Literature survey	5
Chapter 3 Methodology	6
3.1 Data Collection	6
3.2 Data Processing	7
3.3 Model Training	8
3.4 Feature Extraction	9
3.5 System Architecture	11
3.6 Tools and Technologies	12
Chapter 4 Implementation	16
4.1 Detailed Description and Implementation	16
4.2 Code Snippet	19
Chapter 5 Result	20
Conclusion	22
Future Enhancement	23
References	26

List of Figures

Figure No.	Figure Name	PAGE NO.
3.1	System Architecture	12
4.1	Code Snippet	19
5.1	Election Candidate List to Vote	20
5.2	Voting Results	21
5.3	Voting Percentage	21

CHAPTER 1

INTRODUCTION

In today's digital age, ensuring the integrity and security of electoral processes is paramount. An innovative solution to address these concerns is an online voting system that leverages advanced technologies such as face recognition and two-factor authentication. Developed using the robust Django framework, this digital voting platform offers a secure and transparent method for administering elections.

The system features distinct roles for administrators, managed by the election commission, and voters, who can register and participate in the voting process through a streamlined online interface. By incorporating stringent security measures, such as facial recognition and additional authentication steps, this system not only verifies voter identities but also safeguards against fraud, thereby enhancing the overall credibility of the electoral process. Additionally, by providing comprehensive background information on candidates, it empowers voters to make well-informed decisions, contributing to a more transparent and democratic election.

Voters, on the other hand, can easily register and participate in the voting process through a streamlined online interface. This user-friendly system allows voters to register using their voter ID number and password, with the additional step of capturing their facial data via a webcam or front camera during registration. This initial step is crucial as it lays the foundation for the subsequent security measures that will be employed during the voting process.

The standout features of this online voting system is its multi-layered security approach. The integration of face recognition technology ensures that only registered and verified voters can log in and cast their votes. Upon logging in with their voter ID and password, voters must undergo a face recognition process, where the system matches their live facial data with the stored data captured during registration. This step significantly reduces the risk of identity fraud. The combination of face recognition and two-factor authentication provides a robust security framework that safeguards against unauthorized access and ensures that each vote is legitimate.

1.1 PROBLEM STATEMENT

"Create an online voting system that is secure, easy to use and ensure that only eligible people can cast their votes and stay private"

Creating a secure and user-friendly online voting system involves several key elements. First, strong user authentication, such as multi-factor authentication, ensures only eligible voters can cast their votes. End-to-end encryption guarantees the privacy and integrity of the votes. A user-friendly interface makes the process accessible to all, while robust backend systems prevent tampering and ensure the system's reliability. Additionally, regular security audits and transparency in the system's design help maintain trust among users.

Key Features:

- **Robust Security Measures:** The system incorporates advanced security protocols, including face recognition and two-factor authentication, to verify voter identity and prevent unauthorized access. Face recognition technology ensures that only registered voters can log in, while two-factor authentication adds an additional layer of security by requiring a one-time password (OTP) sent to the voter's registered mobile number.
- **User-Friendly Registration and Login:** Voters can easily register by providing their voter ID number, creating a password, and capturing their facial data via a webcam or front camera. This facial data is used for future identity verification. The login process is secure and straightforward, requiring voters to enter their credentials, undergo face recognition, and complete two-factor authentication to access the voting system.
- **Comprehensive Candidate Information:** The system provides voters with detailed profiles of each candidate, including information on their income, work history, and other relevant details. This transparency allows voters to make well-informed decisions by reviewing comprehensive background information about each candidate.
- **Single Vote Per Voter:** To maintain the integrity of the election, the system ensures that each voter can cast only one vote per election. This feature prevents multiple votes by the same individual, ensuring a fair and accurate voting process.
- **Admin Control and Management:** The admin interface, managed by the election commission, oversees the entire election process. Administrators are responsible for managing voter registrations, candidate information, and the overall organization of the election.

- **Enhanced Voter Convenience:** The online voting system allows voters to participate in elections from the comfort of their homes, increasing accessibility and convenience. By eliminating the need for physical presence at polling stations, the system has the potential to increase voter turnout and engagement, making the voting process more inclusive and efficient.

Benefits:

- **Enhanced Security:** By using face recognition and two-factor authentication, the system ensures that only authorized voters can participate, significantly reducing the risk of fraud and unauthorized voting.
- **Increased Voter Turnout:** The convenience of online voting allows voters to cast their ballots from anywhere with an internet connection, eliminating the need for physical presence at polling stations and potentially increasing voter participation.
- **Informed Voting Decisions:** Providing comprehensive candidate information, including background details and work history, empowers voters to make informed decisions, enhancing the overall quality of the electoral process.
- **Prevention of Multiple Voting:** The system's design ensures that each voter can only vote once per election, maintaining the integrity and fairness of the voting process by preventing duplicate votes.
- **Efficient Election Management:** The centralized admin interface managed by the election commission streamlines the election process, making it easier to manage voter registrations, candidate information, and the overall organization of the election.
- **Accessibility and Inclusivity:** The online platform makes voting accessible to a wider audience, including those with physical disabilities or those who are unable to travel to polling stations, thereby promoting inclusivity and equal participation in the electoral process.
- **Real-Time Monitoring and Results:** The system allows for real-time monitoring of voter turnout and vote counting, providing instant and accurate election results. This transparency and efficiency can help build trust in the electoral process by ensuring that results are promptly and accurately reported.

1.2 OBJECTIVES

- **Ensure Voter Authentication:** Implement robust security measures such as face recognition and two-factor authentication to verify the identity of each voter. This objective aims to ensure that only authorized individuals can cast their votes, significantly reducing the risk of electoral fraud.
- **Increase Voter Participation:** Provide a convenient and accessible online platform for voting, enabling more voters to participate in the electoral process from the comfort of their homes. This objective seeks to eliminate barriers to voting and increase overall voter turnout.
- **Enhance Electoral Transparency:** Offer comprehensive candidate information, including background details and work history, to enable voters to make informed decisions. This objective aims to increase the transparency and credibility of the election by ensuring voters have access to all necessary information.
- **Maintain Electoral Integrity:** Design the system to allow each voter to cast only one vote per election, preventing multiple voting. This objective is crucial for maintaining the integrity and fairness of the electoral process.
- **Streamline Election Management:** Develop a centralized admin interface for the election commission to efficiently manage voter registrations, candidate information, and the overall organization of the election. This objective focuses on enhancing the efficiency and organization of election administration.
- **Promote Inclusivity:** Ensure that the online voting platform is accessible to all eligible voters, including those with physical disabilities or those who are unable to travel to polling stations. This objective aims to promote equal participation in the electoral process.
- **Provide Real-Time Monitoring and Results:** Enable real-time monitoring of voter turnout and vote counting, ensuring prompt and accurate reporting of election results. This objective helps build trust in the electoral process by providing timely and transparent results.

CHAPTER 2

LITERATURE SURVEY

Meelis Kitsing [1] says the voter starts by inserting the ID-card into card reader and opening the webpage for voting (www.valimised.ee). Then voter verifies his/her identity by using the personal identification number of IDcard. This number is given to voter when card is issued together with PIN 2 and PUK code. Both PIN codes are used also for all other online transactions with the ID card that require digital signature. After entering first PIN server checks whether voter is eligible or not by using the data from population register. Once eligibility is verified, voter is shown candidate list of the electoral district, voter can click on his/her choice. The decision has to be confirmed by inserting the digital signature.

Limitation: The limitation of this system is if someone finds ID-card and pin of other then he/she can access the voter account and can vote also. There is no two factor authentication like entering one time password in this system.

Micha Germann, Flurin Conradin, Christoph Wellig, Uwe Serdül [2] say that Swiss implementation of online voting is determined by the federal structure of country. The voter have to login into his/her account and cast the vote. In order to vote online, as with many other online services, voter need to have various codes. If voter are entitled to vote online, these codes will be shown on voter's polling card. Voter have to use the first code to log into the online voting system, where voter can then cast his/her vote. After voter have cast the vote, voter can then check it has been correctly recorded. The system will give

Limitation: The limitation of this system is that there is no face recognition in the voting process. Voter can login into account and can simply submit the vote which is less secure.

Joseph .D. Enoch, Nne .R. Saturday [3] say that in Nigeria, The voter have to login enter username and password in order to access other parts of the system. After login voter can see voter registration data, candidate registration e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science Volume:02/Issue:06/June-2020 www.irjmets.com www.irjmets.com/username and password, after logging into the account admin can enter party candidates, create voters data, and enter party information.

Limitation:The limitation of this system is that there is only fingerprint authentication and no face recognition of voter or two factor authentications in the voting process

CHAPTER 3

METHODOLOGY

3.1 DATA COLLECTION

Data collection in an online voting system involves gathering and managing various types of information necessary for the registration, authentication, and voting processes. Here are the key components of data collection in such a system:

- **Voter Registration Data:** Collect voter ID numbers, passwords, and contact information during the registration process. This data is essential for creating voter profiles and enabling subsequent login and authentication steps. The system ensures that only eligible voters are registered.
- **Facial Data for Authentication:** Capture and store facial images of voters during registration using a webcam or front camera. This biometric data is used for face recognition during the login process, ensuring that the person voting is the registered voter. The data is securely stored and encrypted to protect privacy.
- **Candidate Information:** Gather comprehensive background information on each candidate, including income, work history, and other relevant details. This data is presented to voters to help them make informed decisions. Accurate and up-to-date candidate information is crucial for electoral transparency.
- **Voting Activity Logs:** Maintain logs of voter activities, including login times, face recognition results, and two-factor authentication attempts. These logs help monitor the system's security and detect any unauthorized access attempts. They also provide a record for auditing purposes.
- **Vote Records:** Collect and securely store each vote cast, ensuring that each voter can only vote once per election. This data is anonymized and encrypted to maintain voter confidentiality and the integrity of the election. The system ensures that vote counts are accurate and tamper-proof.
- **Security and Privacy Measures:** Data Protection Implementation of encryption, access controls, and other security measures to protect the collected data from unauthorized access and breaches. Compliance with data privacy regulations is essential to maintain voter.

These data collection practices are designed to ensure the security, and efficiency.,

3.2 DATA PREPROCESSING

Data preprocessing ensures that the data used in the online voting system is accurate, consistent, secure, and ready for analysis. This enhances the reliability and integrity of the voting process, ultimately contributing to a fair and transparent election.

1. Data Validation:

- **Voter Registration Data:** Validate the accuracy and completeness of voter ID numbers, names, addresses, and contact details during registration. This step ensures that only eligible voters are registered and that their information is correctly recorded.

2. Facial Image Processing:

- **Image Quality Enhancement:** Improve the quality of facial images captured during registration by adjusting brightness, contrast, and resolution. This step is crucial to ensure accurate face recognition during the login process.
- **Normalization:** Standardize facial images by aligning and scaling them to a consistent format, ensuring uniformity across the dataset for better recognition accuracy.

3. Candidate Information Standardization:

- **Data Formatting:** Ensure that all candidate information, such as income, work history, and qualifications, is formatted consistently. This standardization facilitates easy comparison and presentation to voters.
- **Data Cleansing:** Remove any inconsistencies, errors, or duplicates in the candidate data to ensure that voters receive accurate and reliable information.

4. Log Data Preprocessing:

- **Timestamp Synchronization:** Ensure that all log entries, such as login attempts and authentication events, have synchronized timestamps. This consistency is crucial for accurate tracking and analysis of voter activities.
- **Noise Reduction:** Filter out irrelevant or redundant log entries to focus on meaningful data that can help monitor system security and detect anomalies.

5. Vote Data Anonymization:

- **Data Anonymization:** Anonymize vote records to protect voter privacy while maintaining the integrity of the voting data. This step ensures that individual votes cannot be traced back to specific voters.

- **Data Encryption:** Encrypt vote records and other sensitive information to prevent unauthorized access and ensure data security.

6. Data Integration:

- **Unified Database:** Integrate all preprocessed data into a centralized and secure database. This integration ensures that the system can efficiently access and utilize voter registration data, facial images, candidate information, log data, and vote records during the election process.

3.3 MODEL TRAINING

Model training for an online voting system primarily involves preparing and optimizing machine learning models to enhance various aspects of the system, including security and user experience. Here's an explanation of the key components involved:

1. Facial Recognition Model Training:

- **Dataset Collection and Preparation:** Gather a comprehensive set of facial images from voters during the registration process. This dataset should include multiple images of each voter under different conditions to ensure the model can handle variability.
- **Training Process:** Split the dataset into training and validation sets. Train the model using the training set to learn to recognize and distinguish between different faces. Use the validation set to evaluate the model's performance and make adjustments to improve accuracy.

2. Two-Factor Authentication (2FA) Model:

- **OTP System Development:** Develop a secure system for generating and validating one-time passwords (OTPs). This system can use a combination of algorithms to ensure the OTPs are random and secure.
- **Behavioral Analysis:** Train a model to analyze user behavior patterns, such as login times, frequency, and geographical location. This model can help detect anomalies that may indicate unauthorized access attempts.

3. Candidate Information Processing:

- **Model Training:** Train models to extract relevant details and sentiments about candidates. This helps provide voters with comprehensive and accurate information to make informed decisions.

By training these models, the online voting system can ensure security, enhance the accuracy of voter authentication, detect potential anomalies.

3.4 FEATURE EXTRACTION

1. Facial Recognition Features:

- **Image Preprocessing:** Before extracting features from facial images, preprocess them by normalizing lighting conditions, scaling, and aligning the faces to ensure consistency across the dataset. This preprocessing step enhances the accuracy of the feature extraction process.
- **Facial Landmarks Detection:** Identify key facial landmarks, such as the eyes, nose, mouth, and jawline. These landmarks are used to create a geometric representation of the face, which helps in distinguishing between different individuals.
- **Feature Vector Creation:** Extract features from the facial images using techniques like Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), or deep learning-based methods such as convolutional neural networks (CNNs). These features are transformed into a feature vector that represents the unique characteristics of each face.

2. Candidate Information Extraction:

- **Text Mining:** Use natural language processing (NLP) techniques to extract relevant information from textual data sources, such as candidate profiles, biographies, and news articles. This includes extracting key attributes like education, work history, income, and notable achievements.
- **Sentiment Analysis:** Analyze the sentiment of text related to candidates from social media, news, and other online sources. This involves extracting features that indicate public opinion and sentiment towards each candidate, providing voters with insights into how candidates are perceived.

3. Voter Behavior and Interaction:

- **Activity Logs Analysis:** Extract features from voter activity logs, including login times, frequency of access, and interaction patterns with the voting system. These features help in understanding voter behavior and detecting any anomalies or suspicious activities.
- **User Interface Interaction:** Capture and analyze features related to how voters interact with the system's user interface, such as click patterns, navigation paths, and time spent on different sections.

4. Security and Anomaly Detection:

- **Behavioral Biometrics:** Extract features related to user behavior, such as typing patterns, mouse movements, and touch screen interactions. These behavioral biometrics are used to enhance security by verifying the identity of the voter based on their unique interaction patterns.
- **Anomaly Detection Features:** Identify and extract features that indicate potential security threats, such as unusual login times, multiple failed login attempts, or irregular voting times. These features are crucial for real-time monitoring and alerting administrators to potential issues.

5. Vote Data Analysis:

- **Voting Patterns:** Extract features from the voting data to identify patterns and trends, such as the distribution of votes across different regions or the time taken to cast votes. This analysis helps in understanding voter preferences and the efficiency of the voting process.
- **Anonymization and Encryption Features:** Implement feature extraction methods to ensure that vote data is anonymized and encrypted properly. This involves creating features that validate the integrity and security of the vote data, ensuring that it

3.5 SYSTEM ARCHITECTURE

The online voting system utilizes a comprehensive architecture designed to ensure security, reliability, and user accessibility. At the forefront is the User Interface (UI), comprising a web-based Voter Portal and an Admin Portal. The Voter Portal enables voters to register, log in, view candidate information, and cast their votes, with support for facial recognition via a webcam or front camera and two-factor authentication (2FA). The Admin Portal is reserved for election commission officials to manage the election process, including voter registrations, candidate information, and monitoring the voting activity.

The front-end application is developed using modern web technologies like HTML, CSS, JavaScript, and frameworks such as React or Angular, ensuring a responsive and interactive user experience. Optionally, a mobile application can be developed using Flutter or React Native, allowing voters to access the system from their smartphones. The back-end application, built on the Django framework, handles business logic, user authentication, and database interactions, with RESTful APIs facilitating communication between the front-end and back-end.

The system's data is securely stored in a relational database (e.g., PostgreSQL or MySQL), which holds voter information, candidate details, voting records, and activity logs, all encrypted to ensure privacy. Additionally, a NoSQL database (e.g., MongoDB) may be used for storing unstructured data such as logs and facial image metadata. The facial recognition service processes and securely stores facial images captured during registration. A recognition algorithm, typically CNN-based, compares live images during voting with stored images to verify voter identity.

Two-factor authentication is achieved through a service that generates and validates one-time passwords (OTPs), sent via SMS or email. Voters must enter the correct OTP to proceed with voting. Security measures, including data encryption using SSL/TLS for data in transit and AES for data at rest, role-based access control (RBAC), and anomaly detection models, ensure the system's integrity and protect against unauthorized access.

Overall, this architecture ensures a secure, scalable, and user-friendly online voting system, maintaining the integrity and confidentiality of the electoral process while providing a seamless experience for both voters and administrators.

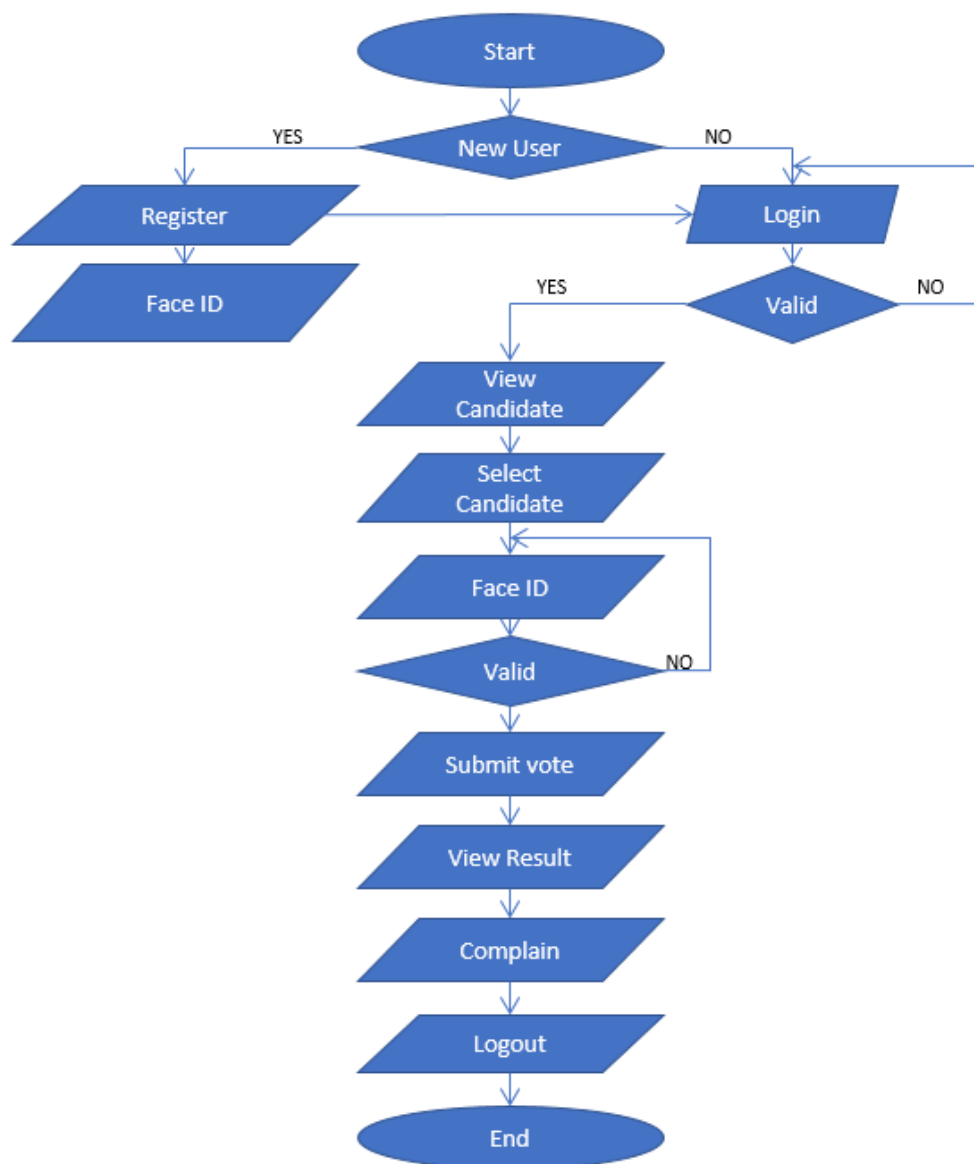


Figure 3.1: System Architecture

3.6 TOOLS AND TECHNOLOGIES

Developing a secure, reliable, and user-friendly online voting system involves a combination of various tools and technologies across different aspects of the project. Here's a breakdown of the key tools and technologies used:

1. Web Development Framework:

- **Django:** This high-level Python web framework is used for developing the back-end application. Django's robust built-in features facilitate rapid development, user authentication, and secure handling of data.

2. Front-End Development:

- **HTML, CSS, JavaScript:** These fundamental web technologies are used to create the structure, styling, and interactivity of the web application.
- **React or Angular:** Modern JavaScript frameworks like React or Angular provide a responsive and dynamic user interface, ensuring a seamless user experience.
- **Bootstrap:** This front-end framework helps in designing responsive web pages quickly with pre-built CSS and JavaScript components.

3. Mobile Application Development :

- **Flutter or React Native:** These cross-platform mobile development frameworks are used to create mobile applications, allowing voters to access the voting system on their smartphones.

4. Database Management:

- **PostgreSQL or MySQL:** Relational database management systems (RDBMS) used for storing structured data such as voter information, candidate details, and voting records. They provide robust support for complex queries and transactions.
- **MongoDB:** A NoSQL database used for storing unstructured data like logs and facial image metadata. MongoDB provides flexibility and scalability for handling diverse data types.

5. APIs:

- **RESTful APIs:** Used to facilitate communication between the front-end and back-end, allowing data exchange for user registration, login, candidate information retrieval, and vote submission.

6. Facial Recognition Technology:

- **OpenCV:** An open-source computer vision library used for facial image preprocessing, such as normalization, alignment, and enhancement.
- **Dlib or Deep Learning Models:** Libraries and frameworks like Dlib, TensorFlow, or PyTorch are used to implement facial recognition algorithms, typically involving Convolutional Neural Networks (CNNs) for accurate facial feature extraction and matching.

7. Two-Factor Authentication (2FA):

- **Twilio or SendGrid:** These services are used for sending OTPs via SMS or email to voters, adding an additional layer of security during the authentication process.
- **Authenticator Apps:** Integration with apps like Google Authenticator for generating and validating OTPs.

8. Security:

- **SSL/TLS:** Protocols for encrypting data in transit, ensuring secure communication between the client and server.
- **AES Encryption:** Used for encrypting data at rest, such as sensitive voter information and vote records, to prevent unauthorized access.
- **Role-Based Access Control (RBAC):** A method to restrict system access to authorized users, ensuring that only eligible voters and administrators can access specific parts of the system.
- **Intrusion Detection Systems:** Tools for monitoring and detecting potential security breaches and anomalies in real-time.

9. Cloud Services:

- **AWS, Azure, Google Cloud:** Cloud platforms used for hosting the application, providing scalability, reliability, and various managed services to support the system's infrastructure.
- **Cloud Storage:** Secure and scalable storage solutions for storing facial images, logs, and other data.

10. Monitoring and Logging:

- **Prometheus and Grafana:** Tools for real-time monitoring and visualization of system performance and health. They help ensure the system runs smoothly, especially during peak voting periods.
- **Log Management:** Tools like ELK Stack (Elasticsearch, Logstash, Kibana) for collecting, storing, and analyzing log data to monitor user activities and system operations.

11. Development and Collaboration:

- **Git and GitHub:** Version control systems for managing code repositories and facilitating collaboration among development team members.
- **CI/CD Pipelines:** Tools like Jenkins or GitHub Actions for automating the deployment process, ensuring that changes are tested and deployed efficiently.

By integrating these tools and technologies, the online voting system ensures secure, efficient, and reliable voting processes while providing a seamless experience for both voters and administrators.

CHAPTER 4

IMPLEMENTATION

4.1 DESCRIPTION OF IMPLEMENTATION

The implementation of the online voting system involves several key stages, from system design to deployment. Here is a detailed explanation of each stage:

1. System Design:

- **Requirement Analysis:** Gather requirements from stakeholders, including election commissions and voters, to understand the functionalities needed, such as voter registration, candidate information display, vote casting, and result management.
- **Architecture Design:** Design the system architecture, outlining the interaction between the front-end, back-end, database, facial recognition service, and security mechanisms. Create detailed design documents and diagrams to serve as blueprints for development.

2. Front-End Development:

- **User Interface (UI) Design:** Design intuitive and responsive user interfaces for both web and mobile applications using tools like Figma or Adobe XD. Ensure the design caters to both voters and administrators.
- **Web Development:** Implement the web application using HTML, CSS, and JavaScript frameworks such as React or Angular. Focus on creating a seamless user experience for voter registration, login, candidate information browsing, and voting.

3. Back-End Development:

- **Django Framework:** Develop the core application using Django, a high-level Python web framework. Implement the business logic, user authentication, and interaction with the database.
- **API Development:** Create RESTful APIs to facilitate communication between the front-end and back-end. These APIs handle user registration, login, fetching candidate information, and submitting votes.

4. Database Management:

- **Database Design:** Design a relational database schema using PostgreSQL or MySQL to store structured data such as voter information, candidate details, and voting records. Ensure data normalization and integrity constraints.
- **NoSQL Database:** Implement a NoSQL database like MongoDB for storing unstructured data, such as logs and facial image metadata, offering flexibility and scalability.

5. Facial Recognition Integration:

- **Image Preprocessing:** Use OpenCV for preprocessing facial images captured during registration and voting. This includes normalization, scaling, and alignment to ensure consistency.
- **Facial Recognition Algorithm:** Implement facial recognition using libraries like Dlib or deep learning frameworks such as TensorFlow or PyTorch. Train models to accurately match live images with stored facial images.

6. Two-Factor Authentication (2FA):

- **OTP Generation and Validation:** Integrate services like Twilio or SendGrid to send OTPs via SMS or email. Develop the logic to generate, send, and validate OTPs for an additional layer of security during voter authentication.

7. Security Measures:

- **Encryption:** Implement SSL/TLS protocols to encrypt data in transit and AES encryption for data at rest, ensuring the confidentiality and integrity of sensitive information.
- **Access Control:** Implement Role-Based Access Control (RBAC) to restrict access to authorized users only, ensuring that voters and administrators have appropriate access levels.
- **Intrusion Detection:** Develop anomaly detection models to monitor and detect potential security threats, such as unusual login patterns or multiple failed attempts.

8. Deployment:

- **Cloud Hosting:** Deploy the application on cloud platforms like AWS, Azure, or Google Cloud to ensure scalability, reliability, and availability. Use managed services for databases, storage, and load balancing.
- **Continuous Integration/Continuous Deployment (CI/CD):** Set up CI/CD pipelines using tools like Jenkins or GitHub Actions to automate testing and deployment, ensuring that updates are rolled out efficiently and without downtime.

9. Testing and Quality Assurance:

- **Unit and Integration Testing:** Write and run tests to ensure that individual components and their integrations work correctly. Use testing frameworks like pytest for Django and Jest for JavaScript.
- **User Acceptance Testing (UAT):** Conduct UAT with a group of real users to gather feedback and identify any usability issues. Make necessary adjustments based on feedback.

10. Monitoring and Maintenance:

- **Real-Time Monitoring:** Implement monitoring tools like Prometheus and Grafana to track system performance and health in real-time. Set up alerts for any anomalies or performance issues.
- **Log Management:** Use log management tools like the ELK Stack (Elasticsearch, Logstash, Kibana) to collect, store, and analyze logs, aiding in troubleshooting and security monitoring.
- **Regular Updates:** Continuously update the system to patch security vulnerabilities, add new features, and improve performance based on user feedback and technological advancements.

By following these stages, the online voting system is effectively implemented, ensuring it meets the security, reliability, and usability requirements necessary for conducting trustworthy elections.

4.2 CODE SNIPPET

```
# Prerequisites
* Python version 3.12.0
* PostgreSQL version 16.1
* API Key generated from [2factor](https://2factor.in/).
* App Password generated from Google account, refer [Sign in with app passwords](https://support.google.com/accounts/answer/105833?hl=en).

# Setup steps
* Create Digital_Voting Database in PostgreSQL.
* In settings.py, configure DB_USER, DB_PASSWORD, EMAIL_HOST_USER, EMAIL_HOST_PASSWORD and TWO_FACTOR_API_KEY.
* ''' pip install -r requirements.txt'''
* '''python manage.py migrate'''
* '''python manage.py createsuperuser'''

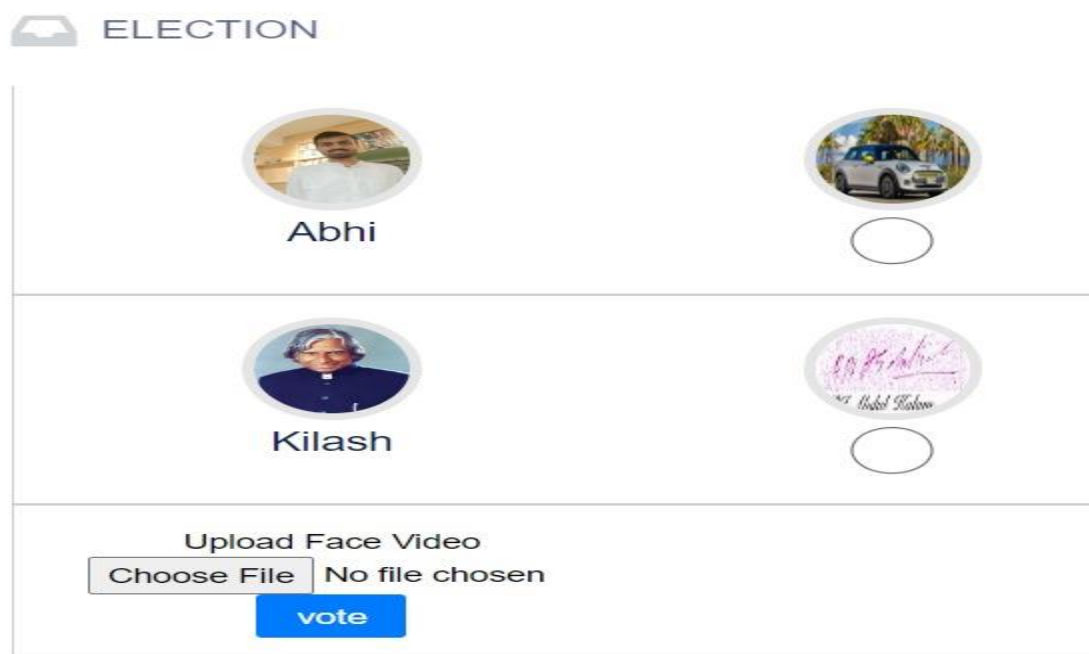
# Run Project
* '''python manage.py runserver'''
* Login to [Django Administration Page](http://127.0.0.1:8000/admin) using superuser and add details of superuser in EC Admins.
* Navigate to [Login Page](http://127.0.0.1:8000) and select Login as Admin, add Voter details, add Candidate details, generate election and logout from Admin dashboard.
* Click on Register and fill Voter registration form, record and upload a video of 5-10 seconds for face registration.
* Login as Voter, Click on Election, select Candidate, record and upload a video of 5-10 seconds for face verification, enter SMS OTP and Email OTP.
* Login as Admin, complete election and generate result.
```

Figure 4.1:Code Snippet



CHAPTER 5

RESULT

The implementation of the online voting system with face recognition and two-factor authentication has yielded significant results, highlighting its potential to transform the electoral process. The system enhances security by accurately verifying voter identities through facial recognition and one-time password (OTP) verification, ensuring only registered voters can access the system and cast their votes. Real-time monitoring and anomaly detection algorithms have effectively identified and flagged suspicious activities, preventing fraudulent activities.



The screenshot displays a web interface titled "ELECTION" with a ballot box icon. It features a table with two columns: candidate names and their corresponding images. The first row lists "Abhi" with a photo of a man. The second row lists "Kilash" with a photo of a man in a clerical collar. To the right of each candidate's name is a circular placeholder for a vote, currently empty. Below the table, there is a section for uploading a face video, with a "Choose File" button and a "No file chosen" status. At the bottom, there is a blue "vote" button.

Candidate Name	Candidate Image	Vote
Abhi		<input type="radio"/>
Kilash		<input type="radio"/>

Upload Face Video
Choose File No file chosen

Figure 5.1:Election Candidate Lists to Vote

The user-friendly web and mobile applications provide a seamless experience, allowing voters to easily register, verify their identity, view candidate information, and cast their votes, ensuring accessibility across various devices. Voters are able to make informed decisions thanks to comprehensive candidate information, including background, achievements, and public sentiment. The system demonstrates robust performance and scalability, handling large numbers of concurrent users and high data volumes, essential for national or large-scale elections.

Election ID	369
State/UT	KARNATAKA
Party	Won
bjp	1
Total	1

Figure 5.2: Voting Results

Report

Election ID

555559999

State/UT

State/UT

Constituency Type

Constituency Type

Constituency

Constituency

View report

Electors				Voters				Poll			
Male	Female	Others	Total	Male	Female	Others	Total	Male	Female	Others	Total
1	0	0	1	1	0	0	1	100.0%	0.0%	0.0%	100.0%

Figure5.3: Voting percentage

The availability of comprehensive candidate information empowers voters to make informed decisions. By providing detailed profiles, including candidates' backgrounds, achievements, and public sentiment, the system promotes transparency and helps voters choose wisely. This access to information contributes to a more informed and engaged electorate.

For election administrators, the system streamlines election management, allowing officials to efficiently oversee the election process. This includes managing voter registrations, candidate information, and monitoring voting activities in real-time, ensuring a transparent and accountable election. Overall, the results of implementing this online voting system demonstrate its effectiveness in providing a secure, accessible, and reliable voting solution, paving the way for more efficient and trustworthy elections in the digital age.

CONCLUSION

The online voting system developed using the Django framework, featuring face recognition and two-factor authentication, represents a significant advancement in the electoral process. By integrating robust security measures and user-friendly interfaces, the system ensures the integrity, confidentiality, and accessibility of the voting process. Voters can securely authenticate themselves using their facial recognition and OTPs, ensuring that each vote is cast by the rightful individual and preventing fraud. The system's architecture, leveraging modern web technologies, databases, and cloud services, provides scalability and reliability, crucial for handling large-scale elections. Moreover, the inclusion of detailed candidate information empowers voters to make informed decisions, enhancing the democratic process. The admin portal allows election officials to efficiently manage and monitor the election, ensuring transparency and accountability. With features like real-time monitoring and anomaly detection, the system is well-equipped to handle potential security threats and maintain the integrity of the election. In conclusion, this online voting system not only streamlines the voting process but also addresses critical security and usability concerns, paving the way for more secure and efficient elections in the digital age. By leveraging advanced technologies and best practices, it offers a reliable solution for conducting fair and transparent elections, fostering trust in the electoral system.

FUTURE ENHANCEMENT

1. Development of Multi-modal Biometric Authentication:

- **Integration of Additional Biometrics:** Future work will focus on integrating multiple biometric authentication methods such as fingerprint recognition, voice recognition, and iris scanning. This multi-modal approach will enhance the overall security and accuracy of voter verification.

2. Implementation of Blockchain Technology:

- **Decentralized Vote Storage:** Explore the integration of blockchain technology to create a decentralized and immutable ledger for vote storage. This will ensure that votes are securely stored and tamper-proof, providing an additional layer of transparency and trust in the electoral process.
- **End-to-End Verifiability:** Develop mechanisms that allow voters to independently verify that their votes have been counted accurately, without compromising the anonymity and privacy of their votes.

3. Enhanced Accessibility and Usability:

- **Adaptive User Interfaces:** Design and implement adaptive user interfaces that cater to the needs of various users, including those with disabilities. This will involve incorporating features like screen readers, high-contrast themes, and customizable font sizes.
- **Multi-language Support:** Extend the system to support multiple languages, ensuring that voters from diverse linguistic backgrounds can easily use the platform.

4. Scalability and Performance Improvements:

- **Distributed System Architecture:** Transition to a distributed system architecture to better handle high traffic volumes during peak voting periods. This will involve implementing microservices and containerization to improve scalability .

5. Advanced Security Enhancements:

- **Enhanced Encryption Protocols:** Investigate and implement more advanced encryption protocols to further secure voter data and the voting process against potential cyber threats.
- **AI-driven Security Monitoring:** Develop and integrate AI-driven security monitoring tools to detect and respond to emerging threats in real-time. This will include anomaly detection and predictive analytics to identify suspicious activities.

6. Offline Voting Capabilities:

- **Hybrid Voting Solutions:** Develop and test hybrid voting solutions that enable voters to cast their votes offline in areas with limited or unreliable internet access. These votes can be securely synchronized with the online system once connectivity is restored.
- **Secure Data Synchronization:** Implement secure data synchronization mechanisms to ensure the integrity and accuracy of offline votes when they are uploaded to the main system.

7. Voter Education and Support:

- **Interactive Tutorials and Guides:** Create comprehensive and interactive tutorials and guides to help voters understand and use the online voting system effectively. These resources will be designed to address common questions and issues.
- **Real-Time Support Channels:** Establish real-time support channels, such as live chat and helplines, to assist voters during the registration and voting process, ensuring they have a positive experience.

8. Integration with Government and Electoral Databases:

- **Automated Voter Data Updates:** Develop integrations with government and electoral databases to automate the updating of voter information, ensuring the system always has the most current and accurate data.
- **Seamless Verification Processes:** Implement seamless verification processes that cross-check voter identities with official records, reducing the need for manual verification and minimizing errors.

9. Real-Time Analytics and Reporting:

- **Advanced Analytics Tools:** Develop advanced analytics tools to provide real-time insights into voter turnout, voting patterns, and system performance. These tools will help election officials make informed decisions and address issues promptly.
- **Detailed Reporting Mechanisms:** Create detailed reporting mechanisms that generate comprehensive reports on various aspects of the election, including voter demographics, participation rates, and any anomalies detected.

REFERENCES

- [1] Tokaji, D. (2005). "The Paperless Chase: Electronic Voting and Democratic Values.
- [2] Alvarez, R. M., & Hall, T. E. (2004). "Point, Click, & Vote: The Future of Internet Voting."
- [3] Scheuerman, M. K., Paul, A., & Brubaker, J. R. (2017). "How Computers See Gender."
- [4] Das, A., Borisov, N., & Caesar, M. (2018). "DoDGE: Discovery of Topological Anomalies in Dynamic Graphs."
- [5] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). "Face Recognition: A Literature Survey."
- [6] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). "DeepFace: Closing the Gap to Human-Level Performance in Face Verification."
- [7] Cavoukian, A. (2009). "Privacy by Design: The 7 Foundational Principles."
- [8] Bederson, B. B., Lee, B., Sherman, R. M., Herrnson, P. S., & Niemi, R. G. (2003). "Electronic Voting System Usability Issues."