SMART VOTING SYSTEM

A DESIGN PROJECT REPORT

Submitted by

DEREL JASPER. M

KAMALNATH. S

RAGUL. S

SITHARTH. R

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

K.RAMAKRISHNAN COLLEGE OF TECHNOLOGY

(An Autonomous Institution, affiliated to Anna University Chennai
and Approved by AICTE, New Delhi)

SAMAYAPURAM -621112

DECEMBER 2024

K.RAMAKRISHNAN COLLEGE OF TECHNOLOGY
(AUTONOMOUS)
SAMAYAPURAM - 621112

BONAFIDE CERTIFICATE

Certified that this design project report titled **“SMART VOTING SYSTEM”** is the bonafide work of **DEREL JASPER.M (REG NO: 811722001008), KAMALNATH.S (REG NO:811722001020), RAGUL.S (REG NO: 811722001041), SITHARTH.R (REG NO:811722001047)** who carried out the project work under my supervision.

SIGNATURE	**SIGNATURE**
Dr. T. Avudaiappan, M.E, Ph.D.	Mr. T. Praveen Kumar, M.E.
HEAD OF THE DEPARTMENT	**SUPERVISOR**
Associate Professor	Assistant Professor
Department of Artificial Intelligence	Department of Artificial Intelligence
K. Ramakrishnan College of Technology (Autonomous)	K. Ramakrishnan College of Technology (Autonomous)
Samayapuram - 621 112	Samayapuram - 621 112

Submitted for the viva-voce examination held on ………………

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION

We jointly declare that the project report on “**SMART VOTING SYSTEM”** is the result of original work done by us and best of our knowledge, similar work has not been submitted to **“ANNA UNIVERSITY CHENNAI”** for the requirement of Degree of **BACHELOR OF TECHNOLOGY**. This design project report is submitted on the partial fulfilment of the requirement of the award of Degree of **BACHELOR OF TECHNOLOGY**.

SIGNATURE

____

DEREL JASPER. M

____

KAMALNATH. S

____

RAGUL. S

____

SITHARTH. R

PLACE: SAMAYAPURAM

DATE:

ACKNOWLEDGEMENT

It is with great pride that we express our gratitude and in-debt to our institution **"K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY (AUTONOMOUS)"** for providing us with the opportunity to do this project.

We are glad to credit honorable Chairman **Dr. K. RAMAKRISHNAN, B.E.,** for having provided for the facilities during the course of our study in college.

We would like to express our sincere thanks to our beloved Executive Director **Dr.S. KUPPUSAMY, MBA, Ph.D.,** for forwarding to our project and offering adequate duration in completing our project.

We would like to thank **Dr. N. VASUDEVAN, M.E., Ph.D**., Principal, who gave opportunity to frame the project the full satisfaction.

We whole heartily thanks to **Dr. T. AVUDAIAPPAN, M.E., Ph.D.,** Head of the Department, **ARTIFICIAL INTELLIGENCE** for providing his encourage pursuing this project.

We express our deep and sincere gratitude to our project Guide **Mr.T.PRAVEEN KUMAR, M.E.,** Assistant Professor, **ARTIFICIAL INTELLIGENCE** for his incalculable suggestions, creativity, assistance and patience which motivated us to carry out the project successfully.

We render our sincere thanks to our Project Coordinator **Mrs. G. NALINA KEERTHANA M.E.,** and other staff members for providing valuable information during the course. We wish to express our special thanks to the officials and Lab Technicians of our departments who rendered their help during the period of the work progress.

ABSTRACT

A secure, multi-layered electronic voting system designed to enhance the integrity, security, and transparency of voting processes. The system combines modern digital verification technologies, such as QR code authentication and biometric fingerprint verification, to ensure that only authorized voters can access the voting platform. Each voter is assigned a unique QR code embedded with personal details. Upon successful QR and fingerprint verification, the voter is granted access to a voting page, where they can select their preferred candidate from a displayed list. After casting a vote, a real-time confirmation SMS is sent to the voter's registered mobile number, containing essential details such as the date, time, and location. The database automatically updates each voter's status to "voted," preventing multiple votes and reinforcing the system's reliability. The project aims to create a user-friendly and secure voting experience that can be scaled for government use, addressing critical challenges in identity verification and vote confirmation to build voter trust and support electoral integrity.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
API	Application Programming Interface
DB	DataBase
HTTP	HyperText Transfer Protocol
OTP	One Time Password
QR	Quick Response
SMS	Short Message Service
UI	User Interface

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

An innovative and secure electronic voting system designed to enhance transparency, accuracy, and trust in the voting process. As traditional voting methods face challenges such as unauthorized access, voter impersonation, and lack of real-time verification, there is a growing need for a technology-driven solution that addresses these issues. This system employs a multi-layered security protocol involving QR code authentication and biometric fingerprint verification to ensure that only registered and verified individuals can participate in the election.

Each voter is issued a unique, single-use QR code containing their personal details, which is protected by an admin-only password. Upon scanning the QR code, the system initiates a fingerprint verification process, which serves as an additional layer of identity confirmation by matching the scanned fingerprint with records in a pre-existing database. After successful verification, the voter gains access to a secure online platform displaying a list of election candidates and their associated parties. The voter selects their candidate of choice and casts their vote with confidence, knowing that the system is secure and private. Upon completion of voting, the system automatically sends a confirmation SMS to the voter's registered mobile number, including details such as the voting booth name, date, time, and location of the vote, thereby offering instant assurance that their vote has been recorded. The system also updates the database by marking each verified voter as "voted," preventing any duplicate votes and ensuring the integrity of the results.

1.2 OBJECTIVE

The main objective of this project is to develop a secure and reliable electronic voting system that addresses existing vulnerabilities in traditional voting methods. By incorporating QR code-based authentication and fingerprint verification, the system aims to safeguard the voting process from unauthorized access and impersonation, ensuring that only legitimate, verified voters can participate. This project seeks to establish an end-to-end secure voting experience that enhances the transparency and accuracy of each vote, fostering trust and integrity in the election results. A critical aspect of this objective is to empower voters with real-time feedback on their voting status through an SMS confirmation message. This instant confirmation not only reassures voters of their participation but also reinforces the transparency of the electoral process.

In addition to promoting voter confidence, the objective is to prevent multiple voting attempts by automatically updating the voter's status to "voted" after each cast ballot, thus eliminating duplicate votes and preserving the integrity of the system. With a user-friendly interface and layered security features, this project aspires to create a scalable solution that can be deployed across various voting scenarios, including government elections and organizational polls. Ultimately, this project envisions a future where voting is both technologically secure and easily accessible, setting a new standard for security, accountability, and ease of use in electronic voting systems.

CHAPTER 2

LITERATURE SURVEY

2.1 SECURED E-VOTING SYSTEM USING TWO-FACTOR BIOMETRIC AUTHENTICATION

Authors: H. Kim, J. Lee, S. Park

Year: 2020

Abstract

This paper proposes an e-voting system with two-factor biometric authentication to ensure secure voter identity verification. Combining fingerprint and facial recognition, the system enhances security by confirming both unique physical attributes and digital credentials. This multi-layer approach aims to prevent unauthorized voting, reduce fraud, and ensure election integrity in a scalable digital platform.

Merits

- Enhanced voter verification with dual-factor biometrics.
- Increased election security by reducing fraud.
- Scalable for large-scale use with strong data protection.

Demerits

- High implementation cost with biometric devices.
- Potential privacy concerns for biometric data.
- Increased system complexity may affect usability.

2.2 BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM WITH BIOMETRIC VERIFICATION DETECTION

Authors: Zhang et al.

Year: 2021

Abstract

This research explores blockchain as the foundation for a secure e-voting system, leveraging the decentralized nature of blockchain to secure vote integrity. With biometric verification, this framework ensures only eligible voters can cast ballots while maintaining transparency and immutability in vote recording. The paper examines blockchain's role in preventing vote tampering, while biometrics addresses authentication concerns

Merits

- Immutable records via blockchain for vote integrity.
- Transparency enhances voter trust in results.
- Biometric verification ensures only authorized voters.

Demerits

- High computational resource demand for blockchain.
- Potential scalability issues for large elections.
- Blockchain transaction fees may increase costs.

2.3 PRIVACY-PRESERVING BIOMETRIC VOTING SYSTEMS IN IOT ENVIRONMENETS

Authors: Kumar, S., and Chen, X

Year: 2021

Abstract

This paper examines a biometric voting system built for IoT environments with a focus on privacy preservation. The system safeguards voter data with encrypted biometric features and is optimized for IoT devices, allowing a more connected voting setup. It leverages privacy-preserving mechanisms that limit data sharing and potential breaches, while ensuring ease of access across IoT-enabled voting stations

Merits

- High data security with privacy-preserving encryption.
- Efficient in IoT networks for remote voting.
- Privacy-focused design limits data exposure risks.

Demerits

- Complex IoT setup may require high technical expertise.
- Privacy concerns if IoT devices are hacked.
- High dependency on device security, limiting flexibility.

2.4 QR CODE AND FACIAL RECOGNITION FOR SECURE VOTING

Authors: Patel, R. et al

Year: 2022

Abstract

This study introduces a secure voting method using QR codes and facial recognition to authenticate voters. QR codes store voter information securely, while facial recognition verifies identity at the time of voting. This dual verification method reduces the chance of vote duplication and unauthorized access, aiming for a straightforward user experience with high security.

Merits

- QR codes make user interaction simple and cost-effective.
- Facial recognition reduces unauthorized access risk.
- Easy to deploy with minimal infrastructure requirements.

Demerits

- Facial recognition affected by environmental conditions.
- QR codes may risk data security if not properly managed.
- Scalability may vary with facial recognition accuracy.

2.5 QR AND OTP BASED ONLINE VOTING WITH BIOMETRICS

Authors: Singh, P., and Arora, T

Year: 2023

Abstract

This paper presents an online voting system that integrates QR code and OTP verification along with biometric authentication. Each voter receives a unique QR code and OTP for secure login, followed by biometric verification to confirm identity. This layered approach minimizes the risk of unauthorized voting and ensures voter authenticity in a remote setting.

Merits

- Multi-layered security with QR, SMS, and biometrics.
- Accessible for remote voting with easy QR and SMS entry.
- Adaptable across various election types and scales.

Demerits

- SMS requires internet, which may not be reliable.
- SMS interception could pose a security risk.
- Slower verification if network issues arise.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing voting systems, particularly in traditional elections, face several challenges related to security, efficiency, and transparency. Most elections use paper ballots or electronic voting machines (EVMs) to collect votes. Paper-based systems require voters to mark their choices on physical ballots, which are then counted manually or scanned into a system for tallying. While this method has been used for many years, it is prone to human error in both the voting and counting processes. Issues such as misprints, lost or damaged ballots, and invalid votes frequently arise, compromising the integrity of the election. Furthermore, the manual counting process is time-consuming and can take days, which may cause delays in announcing the results and can lead to public mistrust. The physical nature of the system also makes it difficult to store, safeguard, and transport ballots, introducing the potential for tampering or theft.

On the other hand, electronic voting systems such as EVMs were introduced to streamline the voting process and reduce human error. However, these systems come with their own set of vulnerabilities. For instance, they are susceptible to technical failures, such as system crashes or malfunctions, which can affect the outcome of the election. Additionally, EVMs are often criticized for their lack of transparency and the potential for hacking or unauthorized tampering. The lack of an accessible audit trail means that voters may not have confidence in the final results, as they cannot independently verify that their vote was correctly recorded. The challenge of ensuring proper voter authentication is also a major concern. Existing EVM systems typically rely on minimal or no voter identification methods, leading to possible impersonation and fraudulent votes. Moreover, these systems require extensive infrastructure, personnel training, and technical support, all of which incur significant costs, making them unaffordable or impractical for use in some regions.

3.1.1 Demerits

Identity Verification Issues

Traditional voting systems primarily rely on government-issued ID cards, which are susceptible to forgery, identity theft, and impersonation. With limited verification mechanisms, unauthorized individuals may vote on behalf of legitimate voters.

Duplicate Voting and Fraud

Without a real-time, unified database to monitor voting status, voters may attempt to vote more than once in different locations or under false identities. This practice can lead to skewed results and erode public trust in the voting process.

Lack of Immediate Feedback

In traditional systems, voters do not receive any immediate confirmation of their voting status. This lack of feedback leaves voters uncertain if their vote has been accurately recorded, raising concerns about transparency and accountability.

Long Queues and Inefficiencies

Manual voting methods, including electronic voting machines, often result in long waiting times due to limited verification mechanisms, leading to voter frustration and reduced participation. Physical polling station setups can be resource-intensive and challenging to manage in high-population areas.

Security Vulnerabilities

Older electronic voting machines may be vulnerable to hacking, tampering, or manipulation, as they often lack updated security protocols. This can lead to concerns about election result validity, especially when there are no advanced verification measures.

Logistical Challenges

Setting up and maintaining physical polling stations, training personnel, and distributing resources are significant logistical tasks, especially for large-scale elections. These requirements create high operational costs and may introduce potential points of failure in remote area.

3.2 PROPOSED SYSTEM

The proposed voting system addresses the shortcomings of the existing methods by incorporating modern technologies such as QR code scanning, biometric fingerprint verification, and automated SMS confirmation to enhance security, improve user experience, and increase transparency. Under this new system, each voter is issued a unique QR code that contains their personal information, ensuring that each vote cast is tied to an individual, and that the voter can only cast one vote. The QR code is password-protected and can only be accessed by authorized personnel, adding an additional layer of security against unauthorized access.

Once the QR code is scanned, the voter is required to verify their identity using biometric authentication, specifically fingerprint scanning. This ensures that only the registered voter can cast their vote, eliminating the possibility of voter impersonation. After successful biometric authentication, the voter is redirected to a secure website where they can view a list of candidates and make their selection. The website is designed to be intuitive and user-friendly, allowing voters to easily navigate through the process. The system then records the vote and sends an automated SMS to the voter's registered mobile number, confirming their vote and providing details such as the booth name, voting time, and location. This real-time confirmation offers transparency and accountability, as voters are immediately notified that their vote has been successfully cast.

Additionally, the voter's status in the database is updated to reflect that they have voted, ensuring that no one can vote more than once. This feature adds a layer of verification and prevents the occurrence of double voting, a problem that can arise in paper or EVM-based systems. The integration of biometric authentication and QR code scanning ensures that the proposed system is highly secure and resistant to fraud, significantly reducing the risk of voter impersonation or tampering. The use of SMS notifications also increases voter confidence in the electoral process, as they are kept informed of the status of their vote. Overall, the proposed system offers a more streamlined, secure, and transparent method of voting, addressing many of the challenges faced by traditional and electronic voting methods. By automating many of the processes and using advanced technologies to verify voter identity and securely record votes, this system has the potential to significantly improve the integrity and efficiency of the voting process.

3.2.1 Merits

Enhanced Identity Verification

The use of a unique QR code for each voter, embedded with personal details and secured by an admin-only password, provides the first layer of identity verification. This ensures that only authorized voters can access the voting platform. Additionally, biometric fingerprint verification offers a second layer of authentication, matching each voter's fingerprint with a pre-existing database, which significantly reduces the risk of identity theft and impersonation.

Prevention of Duplicate Voting

The system's database automatically updates the voting status of each verified voter to "voted," preventing individuals from voting multiple times. This real-time status update ensures the integrity of election results and eliminates the possibility of double voting across polling stations.

Real-Time Confirmation and Transparency

After casting a vote, each voter receives a confirmation SMS to their registered mobile number, including details such as the voting booth name, date, time, and location. This immediate feedback reassures voters that their vote has been successfully recorded, promoting transparency and accountability in the voting process.

Improved Efficiency and Reduced Queues

By employing a fully digital system that requires QR code scanning and biometric verification, this method streamlines the voting process, significantly reducing wait times and eliminating the need for manual identity checks. This efficient flow encourages higher voter turnout and enables quicker and more manageable election day operations.

Heightened Security

The proposed system integrates modern encryption and secure data management practices to protect voter data and prevent unauthorized access. QR code information is securely stored, and the entire voting process is monitored in real-time, mitigating the risk of hacking or tampering that is often associated with older electronic voting machines.

Cost and Resource Optimization

Unlike traditional systems that require significant personnel and physical resources, this digital system minimizes logistical demands. By reducing the need for physical ballots, extensive staff training, and multiple voting stations, the proposed system can save both time and money while still ensuring a secure voting environment.

Scalability and Adaptability

The proposed system's digital nature makes it scalable for use across local, regional, or national elections. It can be easily adapted for various voting scenarios, including organizational elections and public polls, making it versatile and suitable for a wide range of applications.

User-Friendly Interface

The secure voting website offers a simple and intuitive design that guides voters through the candidate selection process. This accessibility, coupled with high-security measures, ensures that voters of all experience levels can navigate the platform comfortably, increasing voter confidence and participation.

CHAPTER 4
SYSTEM SPECIFICATION

4.1 HARDWARE SPECIFICATION

Processor: Intel Core i5 or higher

RAM: 8 GB or higher

OS: Windows 10

Storage: 500 GB SSD

Network Interface: Gigabit Ethernet or Wi-Fi

Fingerprint Scanner

Camera QR Code Scanner

Mobile Devices for QR code

4.2 SOFTWARE SPECIFICATION

Web Framework: DotNet

Database: SQL

Fingerprint Recognition: Digital Persona SDK

Backend: C#

CHAPTER 5
SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE

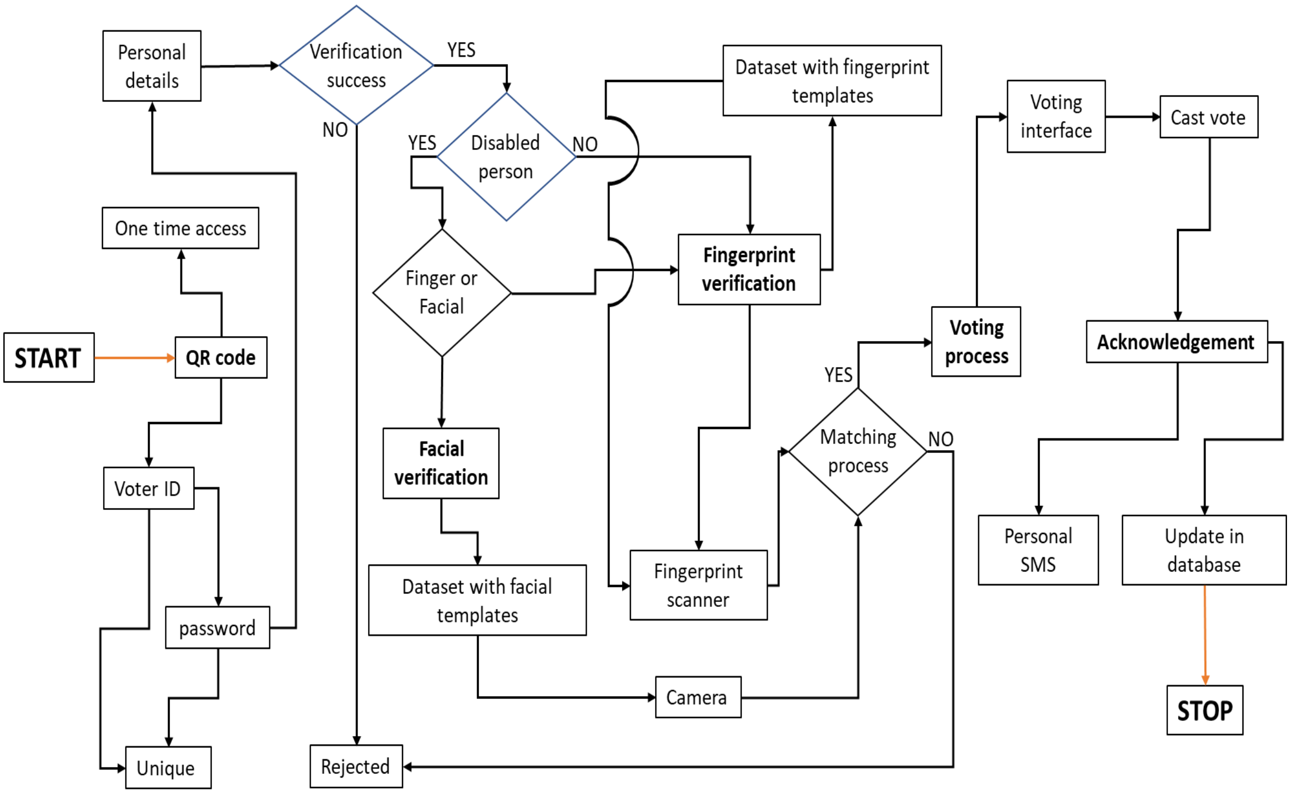


Figure No.5.1 System Architecture

The system architecture of the proposed voting system is carefully designed to ensure the smooth flow of the election process, from voter registration to the final casting of votes and confirmation. It integrates several components working in harmony, each contributing to the overall functionality of the system.

At the core of the architecture is the voter authentication layer, which includes both QR code and biometric verification. Each registered voter is assigned a unique QR code, which contains personal details. This QR code can only be used once, ensuring that the voter cannot vote multiple times. Upon scanning the QR code, the voter is prompted to enter a password, known only to the admin. After the password is validated, the voter undergoes fingerprint authentication. This biometric verification step guarantees that only the correct individual can proceed to cast their vote.

The voting module is an essential part of the architecture, providing voters with an intuitive interface to select their preferred candidates. Once authenticated, voters are directed to a webpage displaying a list of candidates along with their respective political parties. The page also includes a confirmation button for voters to cast their votes. The system ensures that the voter's selection is recorded in the database and that their voting status is updated in real-time.

The backend server is responsible for managing all the data related to the election process, including voter details, candidate lists, voting records, and voting statuses. The backend interacts with a database that stores and retrieves information securely. The server also communicates with external services, such as an SMS gateway, to send real-time notifications to the voter upon successful vote submission. These notifications include essential details such as the booth name, the date and time of voting, and a confirmation message that assures the voter their vote has been successfully cast.

The security architecture ensures the confidentiality, integrity, and authenticity of the voting process. The communication between the frontend and backend is encrypted using SSL/TLS protocols to prevent unauthorized access and data breaches. Biometric data, including fingerprint scans, is securely encrypted and stored in the system, with access limited to authorized personnel only. This multi-layered security architecture is designed to prevent identity theft, vote manipulation, and other forms of electoral fraud.

Additionally, the architecture is designed to be scalable, enabling the system to handle a wide range of elections, from small community polls to large national elections. The system can easily accommodate the growing number of voters, candidates, and vote submissions without compromising performance or security. The modular nature of the system allows for easy updates and maintenance, ensuring the long-term viability of the voting system.

CHAPTER 6

MODULE DESCRIPTION

6.1 QR CODE VERIFICATION MODULE

The QR Code Verification Module in this voting system is essential for initiating the verification process, ensuring that each voter can only cast a vote once and that their identity is securely validated from the start. This module generates and scans unique QR codes for every registered voter, containing personal details essential for identification. Below is a detailed overview of this module:

Purpose and Importance

The QR Code Verification Module serves as the initial layer of security in the voting system. By assigning each voter a unique QR code, this module ensures that only eligible, registered voters can proceed to the next steps in the voting process. The QR code also helps streamline voter verification and prevents unauthorized or multiple voting attempts.

QR Code Generation

Data Encoding

The module generates a QR code for each voter that encodes essential information, including the voter's name, ID number, and unique voter credentials. This data is securely stored within the QR code.

Password Protection

Each QR code is protected with a password that is only known by the admin or system administrator, adding an extra layer of security. This feature prevents unauthorized access in case the QR code is intercepted or misplaced.

One-Time Use Constraint

The QR code is programmed to work only once per voter. After the voter successfully scans and verifies their identity, the QR code becomes invalid for further use, ensuring a single vote per voter.

QR Code Scanning and Verification

Secure Scanning Interface

When a voter enters the polling station, they scan their QR code through a secure scanning interface, which could be either a desktop application or a dedicated hardware scanner.

Password Prompt

Upon scanning, the system prompts for the password associated with the QR code. The voter provides the password, which the system verifies against the stored admin-provided password.

Verification Process

After the password is verified, the system extracts the embedded data within the QR code and cross-references it with the existing voter database to confirm the voter’s identity.

Integration with Fingerprint Verification

Once the QR code and password are successfully verified, the voter proceeds to the next module for fingerprint verification.

The system generates a signal or notification to trigger the Fingerprint Verification Module, thereby maintaining a smooth, step-by-step flow in the voting process.

Security Considerations

Data Encryption

All data encoded within the QR code is encrypted to prevent unauthorized access or data breaches. Even if a QR code is intercepted, its content cannot be easily read without the encryption key.

Admin-Only Password Access

The password associated with each QR code is only accessible by the admin, adding another layer of access control.

Time Constraints

The QR codes could be configured with a time-sensitive component, expiring after a specified period if not used, which adds another layer of control over the voting process.

Technical Specifications

QR Code Libraries

For generating and scanning QR codes, libraries such as qrcode for Python (or equivalent libraries in other languages) are used.

Database Integration

The module is integrated with the backend database, where each QR code's information is matched with registered voter data.

Frontend Interface

The module includes a user-friendly scanning interface for both administrators and voters, ensuring that the verification process is simple and intuitive.

Advantages of the QR Code Verification Module

Efficiency

This module provides a quick and reliable way to authenticate voters, reducing waiting times and streamlining the overall voting process.

Security and Integrity

QR codes with password protection add a strong layer of security, ensuring that each vote is securely linked to an individual voter’s identity.

Reduced Manual Errors

Automated QR code scanning reduces the chance of human error, improving accuracy and reliability in voter identification.

This QR Code Verification Module forms a critical part of the voting system’s security infrastructure, working seamlessly with subsequent modules to ensure a safe and accurate voting experience. By combining unique identifiers with encrypted data, it upholds both efficiency and security throughout the voting process.

6.2 FINGERPRINT VERIFICATION MODULE

The Fingerprint Verification Module is a critical security layer in the voting system, following the QR code verification stage. This module uses biometric fingerprint scanning to confirm each voter's identity, ensuring that only authorized individuals can access the voting platform. Fingerprints are unique to each individual, making them an effective security measure to prevent impersonation and unauthorized voting.

Process and Functionality

Once the voter completes the QR code verification, they move to fingerprint verification. The process involves the voter placing their finger on a scanner, which captures the fingerprint data and converts it into a digital format. The module then compares this data against a secure database containing pre-stored fingerprints. If there is a match, access to the voting interface is granted; otherwise, the system denies access, recording the attempt for security purposes. This approach ensures that only registered voters with verified identities can cast their votes.

Fingerprint Database Integration

During the voter registration phase, each voter's fingerprint is captured, encrypted, and stored in a secure database along with their unique voter ID and personal details. This database is essential for efficient and accurate verification during the voting process. When voters scan their fingerprints, the module retrieves and matches the data with the stored records, allowing for a quick and seamless experience, even during peak times.

Security Measures

The Fingerprint Verification Module incorporates several layers of security. Once fingerprint data is captured, it is encrypted and stored securely, protecting voter privacy and maintaining the system's integrity. In cases of multiple failed attempts, additional security protocols are activated, such as notifying an administrator or restricting access temporarily. This ensures that the voting system remains safe from potential misuse and maintains high accuracy and trustworthiness.

Handling Errors and User Experience

The module is designed to handle common errors, such as scanning issues or user-related challenges, efficiently. If a fingerprint scan fails, the system prompts the voter to try again with clear instructions. After a set number of failed attempts, access may be temporarily restricted, and the event is logged. These logs allow administrators to monitor system usage and improve the process for a smooth voting experience.

Compatibility and Flexibility

The module is compatible with various fingerprint scanning devices, ensuring flexibility in different polling environments. It uses specialized libraries for efficient fingerprint capture and processing, allowing it to adapt to various hardware setups. This compatibility ensures that the Fingerprint Verification Module can be used in diverse voting locations and across multiple types of scanning devices.

Accessibility and Ease of Use

Fingerprint verification simplifies the process for voters by removing the need for additional passwords or PINs. It is an accessible and user-friendly option, especially for voters who may not be technologically inclined. This intuitive approach provides a seamless experience, enabling voters to participate in the voting process without additional barriers.

The Fingerprint Verification Module is an essential component of the voting system's security framework. It provides an effective second layer of verification, safeguarding against unauthorized voting and identity fraud. By using fingerprint biometrics, the module ensures that only verified voters can proceed to cast their votes, preserving the integrity of the electoral process. This module, working in tandem with the QR Code Verification Module, strengthens the voting system, delivering both security and convenience for all participants.

6.3 VOTING INTERFACE CREATION MODULE

The Voting Interface Creation Module is a core component of the voting system. It is responsible for presenting the voter with a user-friendly, visually appealing interface to cast their vote. This module serves as the bridge between voter authentication and the final voting action, ensuring that the voting process is seamless, clear, and efficient. The interface is designed to guide the voter through a simple process of selecting their candidate, confirming their vote, and proceeding to the next steps with ease.

Design and Layout

The voting interface is designed with a user-centric approach, ensuring it is simple and intuitive to navigate. The interface includes several key features:

Candidate List

A list of election candidates is displayed, along with their political party affiliations. This information is presented clearly and in an organized manner, making it easy for voters to review and select their choice.

Voting Button

Each candidate's name is accompanied by a "Vote" button. Voters can click on this button after reviewing the list to make their selection.

Confirmation Option

After a voter selects their candidate, the system prompts them with a confirmation pop-up asking if they are sure about their choice. This step helps avoid accidental votes and ensures that the voter has considered their decision carefully.

Functionality and Flow

The voting process starts after the voter has successfully passed the QR code and fingerprint verification steps. Upon entering the voting interface, the voter is presented with a list of available candidates and their parties. The user can scroll through the candidates' names and information, making an informed decision before selecting their preferred candidate.

Once the voter clicks the "Vote" button next to their chosen candidate, a confirmation pop-up appears. The pop-up message asks the voter to verify their selection, ensuring that the choice made is intentional and correct. If the voter confirms, the vote is recorded, and the system sends a confirmation message, completing the voting process.

User Experience Considerations

The Voting Interface Creation Module focuses on providing an optimal user experience by being responsive, accessible, and clear. The interface is designed to be compatible with various devices, including desktop computers, tablets, and mobile phones, allowing voters to participate in the election from any location.

Accessibility Features

The interface includes options for font resizing, color contrast adjustments, and keyboard navigation, making it accessible for users with disabilities or those who need additional assistance.

Responsive Design

The design adjusts seamlessly across different screen sizes and devices, ensuring voters have a consistent and smooth experience, regardless of the platform used to access the voting system.

Security and Data Integrity

While the interface is designed for ease of use, security remains a top priority. The voting interface is protected by robust encryption protocols to ensure that each vote is securely transmitted and stored. This minimizes the risk of vote tampering and ensures that the voting process remains confidential and trustworthy.

The Voting Interface Creation Module works in conjunction with other system modules, such as the QR code and fingerprint verification modules, to ensure that only authenticated voters can access the interface and submit a valid vote. This tight integration helps protect the integrity of the entire voting process.

Error Handling and Support

To ensure smooth operation, the voting interface includes built-in error handling mechanisms:

Invalid Selection

If a voter tries to submit an empty or invalid vote, the system alerts them to make a valid choice and retry.

Timeouts

If the system detects inactivity for a certain period, it prompts the voter to continue or log out, preventing unauthorized actions and maintaining the security of the process.

In case of technical issues or user error, the system offers on-screen help messages and instructions, guiding the voter through the correction process. Support channels, such as helplines or online chat, can also be integrated into the interface for real-time assistance if necessary.

Compatibility with Backend System

The voting interface is fully integrated with the backend system, ensuring that votes are recorded and stored accurately in the database. Once a voter submits their selection, the backend system processes and records the vote, updating the voter’s status as "voted" in the database. This prevents multiple voting attempts by the same individual and ensures the data is consistent throughout the system.

The Voting Interface Creation Module plays a crucial role in the overall voting system. By offering an intuitive, secure, and responsive platform for voters to cast their ballots, this module enhances the accessibility and ease of voting. It ensures that the voting process is straightforward and free from confusion, while maintaining high standards of security and integrity. Through its seamless integration with the QR code and fingerprint verification modules, the voting interface helps streamline the entire voting process, creating a robust and trustworthy election system.

6.4 CONFIRMATION MESSAGE GENERATION MODULE

The Confirmation Message Generation Module is an essential component of the voting system, designed to provide confirmation to voters after they have cast their vote. This module sends an instant confirmation message to the voter's registered contact details, verifying that their vote has been successfully recorded. It ensures that the voter receives a clear and professional notification of their voting activity, reinforcing trust and transparency in the electoral process.

Purpose and Functionality

The primary purpose of the Confirmation Message Generation Module is to inform the voter that their vote has been cast successfully. After completing the voting process in the voting interface, the voter receives an immediate confirmation message, which serves multiple purposes:

Confirmation of Vote

It assures the voter that their vote has been successfully recorded in the system.

Vote Details

The confirmation message includes critical information, such as the voting booth name, location, and the exact date and time the vote was cast.

Voting Status Update

The system updates the voter's status in the database to reflect that the vote has been cast (marked as "voted"), preventing multiple votes from the same individual.

The Confirmation Message Generation Module is vital for ensuring that the entire voting process is clear and that each voter is aware that their participation has been securely documented.

Key Features of the Confirmation Message

Personalized Message

Each voter receives a personalized confirmation message, which includes:

Name of the Voter

To make the message specific to the voter.

Voting Booth Details

The name and address of the voting booth where the vote was cast.

Date and Time of Voting

The exact date and time when the vote was successfully submitted. This personalized approach helps the voter feel secure in the knowledge that their vote has been correctly processed.

SMS or Email Notification

Depending on the design of the system, the confirmation message can be sent via SMS to the voter's registered mobile number or via email. Sending both SMS and email ensures that the voter receives the message through the most reliable medium, depending on their communication preferences.

SMS Confirmation

In the case of SMS, the message is sent as a short text with essential voting details. SMS is quick, highly accessible, and universally supported, making it the preferred option for many voters.

Email Confirmation

For users who prefer email communication or those who have provided their email addresses, the system can send a more detailed email, which can include further instructions or additional resources related to the election.

Security and Privacy

The confirmation message ensures security by containing only essential details, such as the voting booth name, time, and date. No sensitive voter information (such as a full address or party choice) is included in the confirmation, maintaining voter privacy. The transmission of the message is secured using appropriate encryption methods to prevent unauthorized access to voter data.

Workflow of the Confirmation Message Generation

Vote Casting

After the voter successfully selects their candidate in the voting interface, a confirmation pop-up appears. If the voter confirms their choice, the vote is recorded in the system's database.

Database Update

Once the vote is cast, the system immediately updates the voter's status in the database to reflect that the vote has been completed. This prevents any duplicate votes from being cast by the same voter and ensures that the system remains accurate and up-to-date.

Message Generation

The Confirmation Message Generation Module triggers the creation of the confirmation message, which includes: The voter's personal information (name), The voting booth name and location, The date and time of voting.

Message Dispatch

The message is then sent to the voter’s registered mobile number (via SMS) or email address (via email), depending on the system configuration.

Acknowledgment

Once the confirmation message is successfully delivered, the voter is reassured that their vote has been recorded. If the voter does not receive the message, they can reach out to support or verify their status via the election portal.

Benefits of the Confirmation Message Generation Module

Transparency and Trust

Sending a confirmation message to the voter reinforces trust in the election system. It assures voters that their vote has been counted and provides a record they can refer to if needed. This transparency is crucial for fostering voter confidence in the electoral process.

Auditability

The confirmation message acts as an audit trail, providing proof of voting. This can be valuable in cases where voters need to verify their voting activity or when investigating discrepancies.

Voter Convenience

The system provides voters with immediate feedback after they cast their vote. The confirmation message ensures that voters are not left in doubt, offering peace of mind that their participation in the election was successfully completed.

CHAPTER 7

CONCLUSION AND FUTURE ENHANCEMENT

7.1 CONCLUSION

The implementation of a secure and user-friendly voting system using QR code and biometric verification significantly enhances the reliability, security, and transparency of the electoral process. By integrating multiple security features—such as unique QR codes with admin-only passwords, fingerprint verification, and real-time confirmation messages—this system addresses many of the limitations seen in traditional voting systems. The inclusion of confirmation messages not only reassures voters that their vote was recorded successfully but also strengthens their confidence in the integrity of the voting process.

A seamless, modernized approach to voting that prevents unauthorized access, minimizes fraud, and reduces the chance of errors by verifying each voter's identity at multiple levels. The system architecture is designed to provide an efficient, convenient experience for both voters and administrators, supporting higher voter turnout and smoother election management. With the added benefit of a professional and intuitive interface, this voting system stands as an innovative step towards a secure and accountable democratic process, adaptable to local and national elections alike.

7.2 FUTURE ENHANCEMENT

The secure voting system has a strong foundation, yet there are several enhancements that could further improve its efficiency and security. Future improvements might include incorporating facial recognition as an additional biometric verification layer, allowing for even more accurate voter identification and a contactless experience. Another potential upgrade would be integrating blockchain technology for secure and tamper-proof vote recording, ensuring transparency and traceability without compromising voter privacy.

Additionally, the system could be extended to support remote voting for eligible citizens, such as military personnel or citizens abroad, by developing a secure mobile application that utilizes the same multi-factor authentication. Enhanced data analytics could be integrated to provide election officials with real-time statistics, voting patterns, and turnout rates, assisting with resource allocation and providing insights into voter engagement. Finally, employing AI-driven monitoring for identifying unusual voting patterns or potential fraud in real-time would contribute to maintaining a safe and trustworthy voting environment. These future enhancements would make the system more resilient, accessible, and adaptable to various voting scenarios, further solidifying its role in modern democratic processes.

APPENDIX 1 SAMPLE CODE

Admin.cs

```
namespace Security_based_Voting_System
{
    partial class AdminHome
    {
        private System.ComponentModel.IContainer components = null;
otherwise, false.</param>
        protected override void Dispose(bool disposing)
        {
            if (disposing && (components != null))
            {
                components.Dispose();
            }
            base.Dispose(disposing);
        }
        private void InitializeComponent()
        {
            this.menuStrip1 = new System.Windows.Forms.MenuStrip();
            this.userInfoToolStripMenuItem = new
System.Windows.Forms.ToolStripMenuItem();
            this.candiateToolStripMenuItem = new
System.Windows.Forms.ToolStripMenuItem();
            this.resultToolStripMenuItem = new
System.Windows.Forms.ToolStripMenuItem();
            this.newUserToolStripMenuItem = new
System.Windows.Forms.ToolStripMenuItem();
```

```
    this.menuStrip1.SuspendLayout();
    this.SuspendLayout();
    this.menuStrip1.Items.AddRange(new
System.Windows.Forms.ToolStripItem[] {
    this.newUserToolStripMenuItem,
    this.userInfoToolStripMenuItem,
    this.candiateToolStripMenuItem,
    this.resultToolStripMenuItem});
    this.menuStrip1.Location = new System.Drawing.Point(0, 0);
    this.menuStrip1.Name = "menuStrip1";
    this.menuStrip1.Size = new System.Drawing.Size(760, 24);
    this.menuStrip1.TabIndex = 0;
    this.menuStrip1.Text = "menuStrip1";
    this.userInfoToolStripMenuItem.Name = "userInfoToolStripMenuItem";
    this.userInfoToolStripMenuItem.Size = new System.Drawing.Size(63, 20);
    this.userInfoToolStripMenuItem.Text = "UserInfo";
    this.userInfoToolStripMenuItem.Click += new
System.EventHandler(this.userInfoToolStripMenuItem_Click);
this.candiateToolStripMenuItem.Name = "candiateToolStripMenuItem";
    this.candiateToolStripMenuItem.Size = new System.Drawing.Size(73, 20);
    this.candiateToolStripMenuItem.Text = "Candidate";
    this.candiateToolStripMenuItem.Click += new
System.EventHandler(this.candiateToolStripMenuItem_Click);
    this.resultToolStripMenuItem.Name = "resultToolStripMenuItem";
    this.resultToolStripMenuItem.Size = new System.Drawing.Size(51, 20);
    this.resultToolStripMenuItem.Text = "Result";
    this.resultToolStripMenuItem.Click += new
System.EventHandler(this.resultToolStripMenuItem_Click);
```

```
            this.newUserToolStripMenuItem.Name = "newUserToolStripMenuItem";
            this.newUserToolStripMenuItem.Size = new System.Drawing.Size(66, 20);
            this.newUserToolStripMenuItem.Text = "NewUser";
            this.newUserToolStripMenuItem.Click += new
System.EventHandler(this.newUserToolStripMenuItem_Click);
            this.AutoScaleDimensions = new System.Drawing.SizeF(6F, 13F);
            this.AutoScaleMode = System.Windows.Forms.AutoScaleMode.Font;
            this.BackgroundImage =
global::Security_based_Voting_System.Properties.Resources.Brazil___Elections_2
010___4;
            this.BackgroundImageLayout =
System.Windows.Forms.ImageLayout.Stretch;
            this.ClientSize = new System.Drawing.Size(760, 435);
            this.Controls.Add(this.menuStrip1);
            this.MainMenuStrip = this.menuStrip1;
            this.Name = "AdminHome";
            this.Text = "AdminHome";
            this.menuStrip1.ResumeLayout(false);
            this.menuStrip1.PerformLayout();
            this.ResumeLayout(false);
            this.PerformLayout();
        }
        private System.Windows.Forms.MenuStrip menuStrip1;
        private System.Windows.Forms.ToolStripMenuItem
userInfoToolStripMenuItem;
        private System.Windows.Forms.ToolStripMenuItem
candiateToolStripMenuItem;
        private System.Windows.Forms.ToolStripMenuItem
```

```
resultToolStripMenuItem;
        private System.Windows.Forms.ToolStripMenuItem
newUserToolStripMenuItem;
    }
}
```

Result.cs

```
namespace Security_based_Voting_System
{
    partial class Result
    {
        private System.ComponentModel.IContainer components = null;

        protected override void Dispose(bool disposing)
        {
            if (disposing && (components != null))
            {
                components.Dispose();
            }
            base.Dispose(disposing);
        }
        private void InitializeComponent()
        {
            this.dataGridView1 = new System.Windows.Forms.DataGridView();
            this.label1 = new System.Windows.Forms.Label();
```

```
((System.ComponentModel.ISupportInitialize)(this.dataGridView1)).BeginInit();
        this.SuspendLayout();
        this.dataGridView1.BackgroundColor = System.Drawing.Color.White;
                                        this.dataGridView1.ColumnHeadersHeightSizeMode    =
System.Windows.Forms.DataGridViewColumnHeadersHeightSizeMode.AutoSize;
        this.dataGridView1.Location = new System.Drawing.Point(53, 73);
        this.dataGridView1.Name = "dataGridView1";
        this.dataGridView1.Size = new System.Drawing.Size(468, 204);
        this.dataGridView1.TabIndex = 0;
        this.label1.AutoSize = true;
        this.label1.BackColor = System.Drawing.Color.Transparent;
              this.label1.Font = new System.Drawing.Font("Palatino Linotype", 12F,
System.Drawing.FontStyle.Bold, System.Drawing.GraphicsUnit.Point, ((byte)(0)));
        this.label1.Location = new System.Drawing.Point(233, 22);
        this.label1.Name = "label1";
        this.label1.Size = new System.Drawing.Size(57, 22);
        this.label1.TabIndex = 1;
        this.label1.Text = "Result";
        this.AutoScaleDimensions = new System.Drawing.SizeF(6F, 13F);
        this.AutoScaleMode = System.Windows.Forms.AutoScaleMode.Font;
                                                                  this.BackgroundImage        =
global::Security_based_Voting_System.Properties.Resources.images;
                                                            this.BackgroundImageLayout        =
System.Windows.Forms.ImageLayout.Stretch;
        this.ClientSize = new System.Drawing.Size(558, 320);
        this.Controls.Add(this.label1);
        this.Controls.Add(this.dataGridView1);
```

```
            this.Name = "Result";
            this.Text = "Result";
            this.Load += new System.EventHandler(this.Result_Load);

((System.ComponentModel.ISupportInitialize)(this.dataGridView1)).EndInit();
            this.ResumeLayout(false);
            this.PerformLayout();
        }
        #endregion
        private System.Windows.Forms.DataGridView dataGridView1;
        private System.Windows.Forms.Label label1;
    }
}
```

APPENDIX 2 SCREENSHOTS

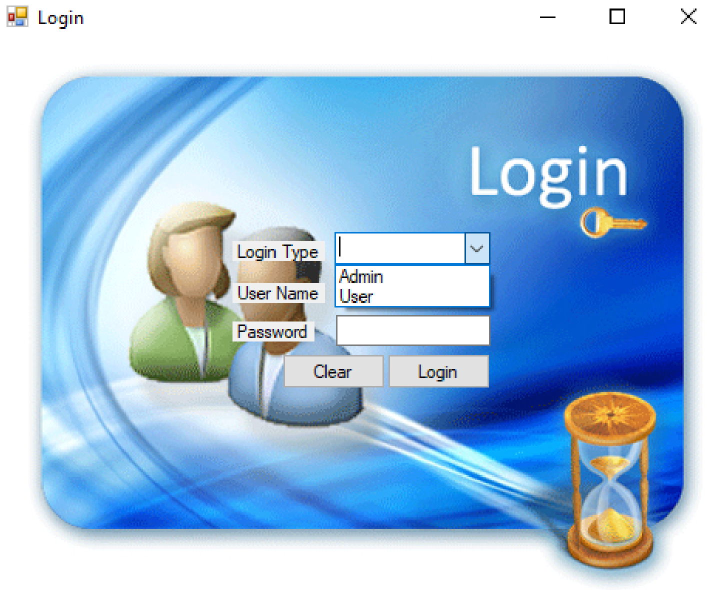
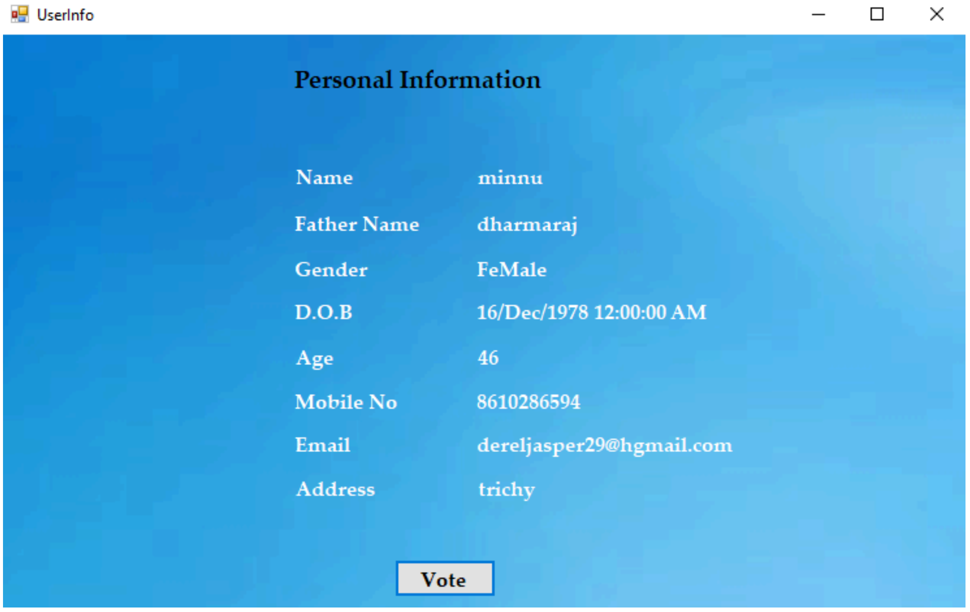


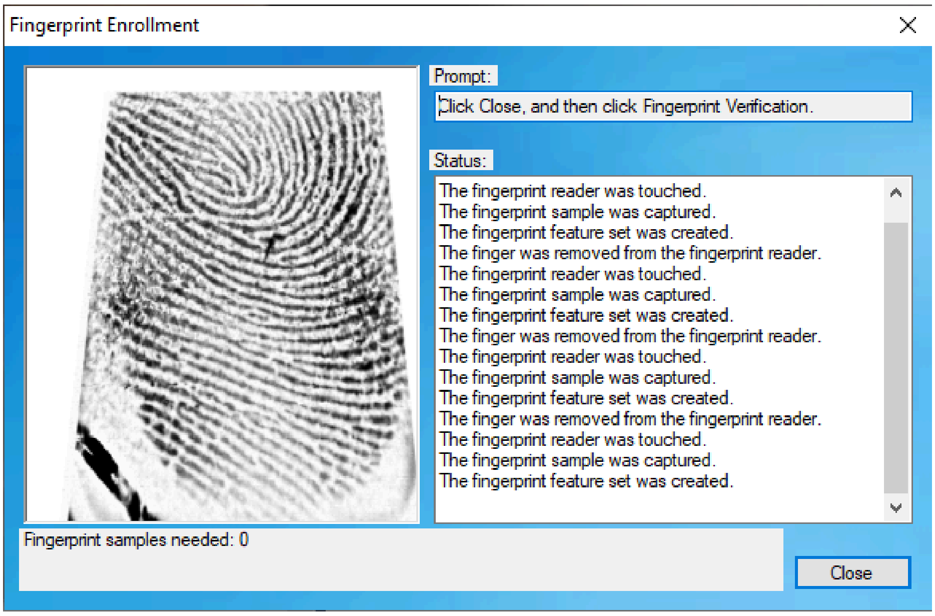
Figure No. A.2.1 Login Page



Personal Information

Name	minnu
Father Name	dharmaraj
Gender	FeMale
D.O.B	16/Dec/1978 12:00:00 AM
Age	46
Mobile No	8610286594
Email	dereljasper29@hgmail.com
Address	trichy

Figure No. A.2.2 Personal Information Verification



Fingerprint Enrollment

Prompt:

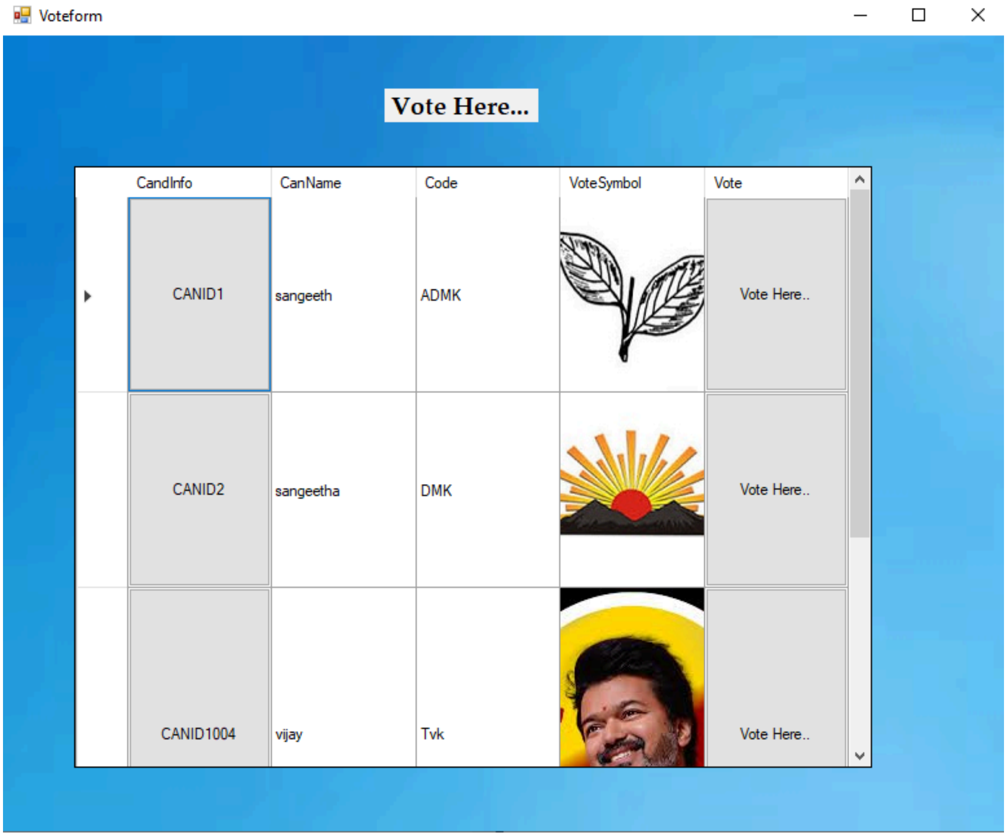
Click Close, and then click Fingerprint Verification.

Status:

```
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.
```

Fingerprint samples needed: 0

Figure No. A.2.3 FingerPrint Verification

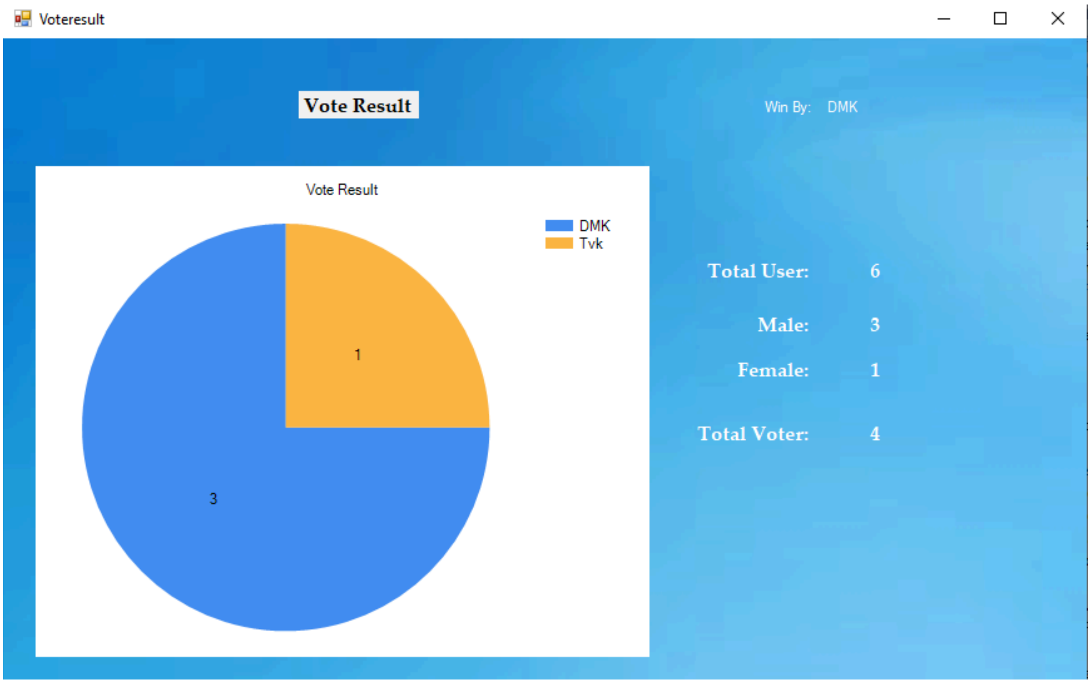


Voteform

Vote Here...

CandInfo	CanName	Code	VoteSymbol	Vote
CANID1	sangeeth	ADMK		Vote Here..
CANID2	sangeetha	DMK		Vote Here..
CANID1004	vijay	Tvk		Vote Here..

Figure No. A.2.4 Voting Interface



Voteresult

Vote Result

Win By: DMK

Total User: 6

Male: 3

Female: 1

Total Voter: 4

Figure No. A.2.5 Results Analysis

REFERENCES

1. Alshahrani, S. S., & Aljamaan, H. (2021). "Design and Implementation of Secure QR Code Authentication System for Mobile Payment Applications." International Journal of Network Security 23(1): 27-35.

2. Chakraborty, A., & Mukhopadhyay, S. (2020). "Blockchain Technology in Secure Electronic Voting: A Review." IEEE Access 8: 183850-183866.

3. Chen, L., Jiang, T., & Wang, H. (2021). "Enhancing Election Security: Biometric and QR Code-Based Approaches." Journal of Systems and Software 181: 110983.

4. Kaur, G., & Singh, D. (2021). "Biometric Authentication using Fingerprint Recognition: An Overview." Journal of Information Security Research 12(4): 159-167.

5. Kumar, S., & Rani, R. (2020). "Recent Developments in E-Voting Security: A Comprehensive Review." Journal of Information Security and Applications 52: 102467.

6. Park, J., & Kim, H. (2022). "A Two-Step User Verification Method for QR Code Scanning in Secure Voting Systems." IEEE Transactions on Dependable and Secure Computing.