REVA UNIVERSITY
Bengaluru, India

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

MINI PROJECT REPORT

ON

"Smart Electronic Voting System by Using Fingerprint Recognition"

Submitted in partial fulfillment of the requirements for the award of the Degree of

Bachelor of Technology

In

Electrical and Electronics Engineering

Submitted by

UJWAL KUMAR S (R22EM085)

VENKATESHWARLU K(R22EM090)

KEERTHAN K (R22EM105)

SHARANYA C S (R22EM077)

Under the guidance of

Dr. SUDHARANI POTTURI

ASSISTANT PROFESSOR

REVA UNIVERSITY

2024-2025

REVA UNIVERSITY

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-56006

www.reva.edu.in

DECLARATION

We, **Mr. Ujwal Kumar S (R22EM085) , Mr. Venkateshwarlu K (R22EM090) , Mr. Keerthan K (R22EM105) , Ms. Sharanya C S (R22EM077)** students of B. Tech, belongs to the School of Electrical and Electronics Engineering, REVA University, declare that this Mini Project Report entitled **"Smart Electronic Voting System by Using Fingerprint Recognition"** is the result the of project work done by me under the supervision of **Dr. Sudharani Potturi** in School of Electrical and Electronics Engineering.

We are submitting this Project Report in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Electrical and Electronics Engineering by the REVA University, Bengaluru during the academic year 2024-25.

We further declare that this project report or any part of it has not been submitted for the award of any other Degree / Diploma of this University or any other University/ Institution.

(Signature of the Students)

*Certified that this project work submitted by **Ujwal Kumar S, Venkateshwarlu K, Keerthan K, Sharanya C S** has been carried out under my guidance and the declaration made by the candidate is true to the best of my knowledge.*

Signature of Guide *Signature of Director*

Date……. *Date……..*

Official seal of school office

REVA
UNIVERSITY
Bengaluru, India

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

CERTIFICATE

Certified that the project work entitled **“Smart Electronic Voting System by Using Fingerprint Recognition”** carried out under my / our guidance by **Ujwal Kumar S, Venkateshwarlu K, Keerthan K, Sharanya C S** are Bonafide students of REVA University during the academic year 2024-25, are submitting the mini project report in partial fulfillment for the award of **Bachelor of Technology in Electrical and Electronics Engineering** during the academic year **2024–25**. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

--------------------

Dr. Sudharani Potturi

Asst. Professor, School of EEE

REVA University
University

---------------------

Dr. Raghu C N,

Deputy Director, School of

EEE, REVA

External Examiner

Name of the Examiner with affiliation Signature with Date

1.

2

ACKNOWLEDGMENTS

This satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible with constant guidance and encouragement and crowned our efforts with success.

A hearty thanks to our Project Guide **Dr. Sudharani Potturi**, School of EEE, for his guidance and support throughout the course.

We are grateful to **Dr. Raghu C N**, Director, School of Electrical and Electronics Engineering, REVA University, Bangalore, for his valuable support and encouragement.

We also thank all the staff members of the School of Electrical and Electronics Engineering and all those who have directly or indirectly helped us with their valuable suggestions in the successful completion of this project.

We express our thanks to **Dr. Sanjay Chitnis,** Vice-Chancellor, REVA University, Bangalore, for extending his support.

We also thank our Honorable **Chancellor**, **Dr. P. Shyama Raju,** for his support and encouragement and wonderful infrastructure/resources.

Finally, yet importantly we would like to thank our beloved parents for their blessings, love, and encouragement to successfully complete the task by meeting all the requirements.

UJWAL KUMAR S (R22EM085)

VENKATESHWARLU K (R22EM090)

KEERTHAN K(R22EM105)

SHARANYA C S (R22EM077)

ABSTRACT

The Smart Electronic Voting Machine (SEVM) is a modern solution designed to address the challenges of traditional voting systems. This project leverages biometric technology through a fingerprint sensor to authenticate voter identity, ensuring only authorized individuals can cast their votes. The integration of an Arduino UNO microcontroller and an LCD display creates a seamless and interactive interface for voters, enabling a smooth and user-friendly voting experience. By eliminating the need for manual voter verification, the SEVM reduces the risk of impersonation and human errors.

At the heart of the system, the Arduino UNO microcontroller acts as the central processing unit, handling fingerprint matching, data communication, and storage. The fingerprint sensor securely compares the voter's fingerprint with a pre-registered database, ensuring accurate authentication. Once authenticated, voters can select their desired candidate on the user-friendly interface displayed on the LCD screen. The machine records each vote digitally, ensuring transparency and reliability.

The SEVM enhances the voting process with its speed, accuracy, and robustness. It eliminates manual errors, prevents tampering, and ensures confidentiality in the voting data. This system is designed to be scalable and adaptable for use in local, state, or national elections. With its focus on security and efficiency, the SEVM demonstrates the potential to revolutionize traditional voting systems, paving the way for a more secure and democratic electoral process.

LIST OF FIGURES

Contents

CHAPTER 1
INTRODUCTION

1.1 History

Electronic voting systems have become a vital part of modern elections due to their speed, accuracy, and efficiency. However, ensuring the authenticity and security of votes remains a challenge. The **Smart Electronic Voting System by Using Fingerprint Recognition** introduces an advanced, secure, and user-friendly voting mechanism. This system leverages biometric authentication, specifically fingerprint recognition, to ensure that each voter is uniquely identified and allowed to cast their vote only once. The fingerprint sensor eliminates the risks of unauthorized voting, duplicate entries, and fraud. Integrated with a microcontroller and other electronic components, this machine provides real-time validation of voters, a seamless voting experience, and automated counting of votes. By combining security and technology, this project aims to enhance trust in electoral processes, reduce human errors, and make voting accessible and efficient.

1.2 Project Overview

The Smart Electronic Voting Machine using a fingerprint sensor presents a modern solution to the challenges of traditional voting methods. By ensuring secure, accurate, and user-friendly voting processes, this system can significantly enhance the integrity and efficiency of elections. It addresses many existing vulnerabilities in electoral systems, offering a dependable framework for conducting fair and transparent elections. Moreover, this innovation has the potential to build greater trust among voters by demonstrating commitment to security and fairness. With continuous improvements and adoption of emerging technologies, this project can serve as a blueprint for future advancements in electronic voting systems. Its scalability and adaptability make it a practical choice for implementation in diverse electoral scenarios worldwide.

CHAPTER 2
LITERATURE SURVEY

[1] Electronic Voting System using Biometrics, Raspberry Pi and TFT module. Prof. A.M. Jagtap Computer Science and Engineering Rajarambapu Institute of Technology, Islampur, India

Abstract

The rapid evolution of technology in recent years has paved the way for more secure, efficient, and transparent electoral processes. This project presents an electronic voting system utilizing biometrics, Raspberry Pi, and a TFT module to enhance the accuracy and integrity of the voting process. By integrating biometric authentication, the system ensures that each voter is uniquely identified and can cast only one vote, thereby eliminating the possibility of duplicate or fraudulent voting. The Raspberry Pi serves as the central processing unit, while the TFT module provides an intuitive and user-friendly interface for voters. The system aims to reduce human errors, ensure data confidentiality, and provide real-time vote tallying, making it an efficient alternative to traditional voting methods.

Introduction

The democratic process relies heavily on the integrity and efficiency of voting systems. Traditional paper-based voting systems are often prone to errors, delays, and malpractices such as multiple voting and impersonation. To address these issues, electronic voting systems are increasingly being adopted. The proposed system combines biometric authentication with modern computing capabilities to create a secure, reliable, and user-friendly platform.

Biometric authentication ensures voter uniqueness by capturing and verifying fingerprint data. Raspberry Pi, a cost-effective and versatile computing platform, processes biometric data, manages the voting interface, and stores votes securely. The TFT module provides a touch-enabled graphical interface for seamless interaction. This system not only enhances security but also streamlines the voting process, making it faster and more efficient.

Conclusion

The electronic voting system using biometrics, Raspberry Pi, and a TFT module offers a robust solution to the challenges faced by traditional voting systems. By leveraging biometric authentication, the system eliminates the risk of impersonation and ensures a single vote per voter. The Raspberry Pi's computing capabilities, combined with the user-friendly TFT interface, make the system easy to use and reliable. This project demonstrates the potential of integrating modern technology into electoral processes, ensuring a transparent, secure, and efficient voting experience. Adoption of such systems can revolutionize the democratic process, providing a foundation for fair and fraud-free elections.

[2] IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020 Biometric Based Secured Remote Electronic Voting System give intro abstract conclusion

Abstract

The integration of biometric technology into electronic voting systems has become a significant step towards enhancing the security and reliability of electoral processes. This paper presents a biometric-based secured remote electronic voting system designed to address common challenges such as voter impersonation, double voting, and accessibility for remote voters. The system incorporates biometric authentication for voter verification, ensuring that each individual is uniquely identified. By leveraging secure communication protocols, the system enables remote voting while maintaining data integrity and confidentiality. This innovative approach to electronic voting ensures transparency, enhances voter participation, and provides a secure alternative to traditional voting methods.

Introduction

Electronic voting systems have been widely explored to improve the efficiency and transparency of elections. However, traditional e-voting systems often face issues related to voter authentication, system security, and accessibility for remote users. Biometric technology offers a robust solution to these challenges by providing a unique and tamper-proof method for voter identification. The proposed system combines biometric authentication with secure digital communication to enable remote electronic voting. The use of biometrics eliminates the possibility of voter impersonation and ensures a one-voter-one-vote policy. Furthermore, secure encryption protocols are employed to protect voter data during transmission, maintaining confidentiality and system integrity. This system is designed to enhance voter convenience and trust in the electoral process, especially for voters in remote locations.

Conclusion

The biometric-based secured remote electronic voting system addresses critical challenges in modern electoral processes by integrating advanced authentication and secure communication technologies. Biometric verification ensures that only authorized voters can participate, reducing the risk of fraud and multiple voting. The ability to vote remotely enhances accessibility and inclusivity, particularly for individuals unable to visit polling stations. By prioritizing security, transparency, and user convenience, this system offers a reliable framework for future elections. Adoption of such technologies can significantly contribute to the advancement of democratic practices in the digital age.

[3] IEEE Xplore Part Number: CFP22BC3-ART; ISBN: 978-1-6654-9710-7 Smart Voting Machine using Fingerprint Sensor and Face Recognition give abstract intro conclusion

Abstract

The implementation of smart voting systems is revolutionizing the electoral process by leveraging advanced technologies for security and efficiency. This paper presents a Smart Voting Machine integrating fingerprint sensors and face recognition to enhance voter authentication and eliminate fraudulent activities. The dual-layered biometric system ensures a robust and accurate verification process, significantly reducing the chances of impersonation and multiple voting. The proposed system also features a user-friendly interface for seamless voter interaction and real-time data processing. By combining biometric technologies with modern computing capabilities, this voting machine demonstrates the potential for creating a secure, efficient, and transparent electoral framework.

Introduction

The integrity of elections is a cornerstone of democracy, and ensuring the security and accuracy of voting systems remains a critical challenge. Traditional voting methods, whether paper-based or electronic, often face issues such as voter impersonation, unauthorized access, and lack of transparency. Biometric authentication has emerged as a promising solution to these challenges. This paper introduces a Smart Voting Machine that utilizes fingerprint sensors and face recognition for dual biometric authentication. The fingerprint sensor ensures unique voter identification, while face recognition adds an additional layer of security, further minimizing the chances of fraudulent activities. The system is designed to be scalable, user-friendly, and capable of real-time processing, making it suitable for large-scale elections. By integrating these advanced features, the proposed system aims to set a new standard for secure and efficient voting.

Conclusion

The Smart Voting Machine using fingerprint sensors and face recognition offers a reliable and secure solution to the limitations of traditional voting systems. The dual-layer biometric authentication enhances voter verification, ensuring that each vote is genuine and cast only once. The system's advanced features, combined with its user-friendly design, ensure a smooth and transparent voting experience. This technology-driven approach not only strengthens the integrity of the electoral process but also fosters greater trust and participation among voters. Adoption of such systems can significantly contribute to the evolution of modern democratic practices, paving the way for more secure and efficient elections worldwide.

[4] https://youtu.be/AKo8_dNeFeY?si=ohFYh-FBBKMyXJmv

The link directs to a project titled "Electronic Voting Machine Using Fingerprint Sensor on Arduino," which details the development of a biometric voting system utilizing Arduino technology. This system employs a fingerprint sensor to authenticate voters, ensuring that only registered individuals can cast their votes, thereby enhancing the security and integrity of the electoral process. This project exemplifies the integration of biometric technology with microcontroller systems to create a secure and efficient electronic voting machine. By utilizing fingerprint authentication, it addresses common electoral challenges such as voter fraud and multiple voting attempts, thereby contributing to a more reliable voting process.

CHAPTER 3
PROPOSED WORK

3.1 Smart electronic voting machine using fingerprint sensor module

3.1.1 Introduction

A smart electronic voting machine (EVM) with a fingerprint sensor enhances security, reliability, and accuracy in the voting process. This system eliminates the need for manual identification, which is often prone to errors or fraudulent practices. By integrating an attendance module with a fingerprint sensor, voter authentication becomes seamless, ensuring that only eligible voters can participate. This module serves as a crucial part of the EVM, where the fingerprint sensor captures and verifies the identity of voters before allowing them to cast their vote. It not only prevents multiple voting attempts but also maintains an accurate record of voter attendance.

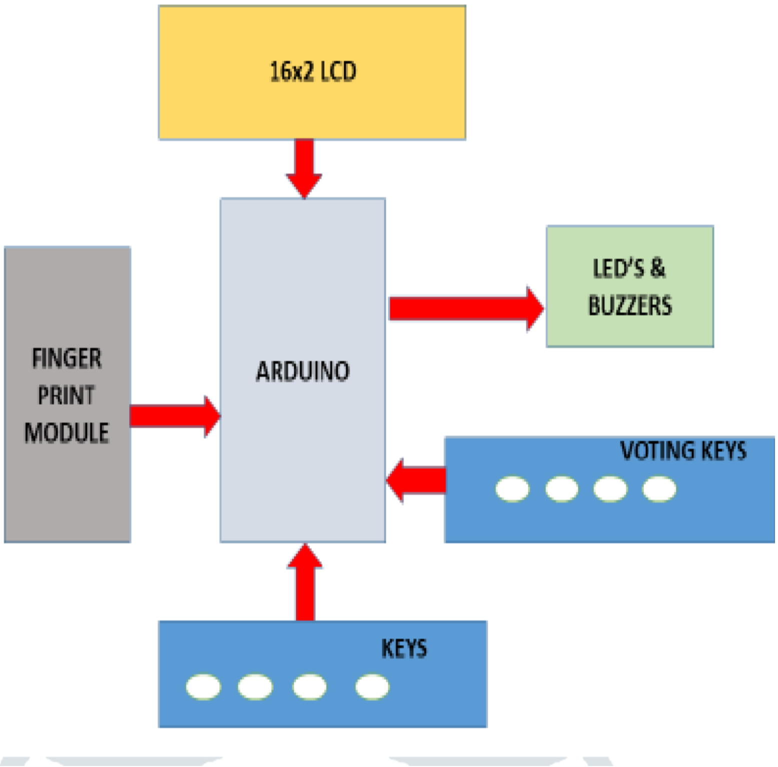


Figure 3.1: Block diagram of smart electronic voting machine using fingerprint sensor

3.2 Description of hardware components

3.2.1 Fingerprint Sensor

A fingerprint sensor in a smart electronic voting machine ensures secure and authenticated voting by verifying a voter's identity. When a voter places their finger on the sensor, it captures the fingerprint using optical, capacitive, or ultrasonic technology. The system processes the image to extract unique features and compares them with a pre-stored database of registered voters. If the fingerprint matches, the voter is granted access to cast their vote; otherwise, access is denied. To prevent fraud, the system restricts multiple votes by flagging authenticated voters in the database. Votes are encrypted and securely stored, maintaining anonymity while preventing tampering. This technology enhances security, eliminates unauthorized voting, and ensures a user-friendly and tamper-proof voting process.

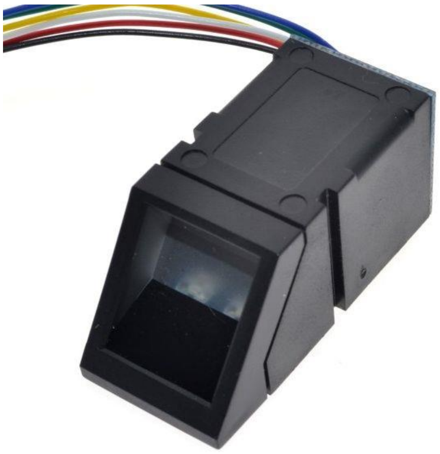


Figure3.2: Fingerprint sensor

3.2.2 LCD Display

The LCD Display in the Fingerprint-Based Electronic Voting System serves as a crucial interface, providing real-time feedback and information to both voters and election officials. Typically integrated into the Electronic Voting Machine (EVM), the LCD Display offers a user-friendly platform for voters to interact with the system. During the voting process, it displays relevant instructions, and candidate information, and confirms the successful submission of a vote.

Figure 3.3:LCD Display

3.2.3 Arduino UNO

The integration of the Arduino UNO microcontroller in a Smart Electronic Voting Machine (EVM) using a fingerprint sensor offers reliable processing capabilities that enhance the system's efficiency and versatility. The Arduino UNO serves as the central control unit for managing fingerprint authentication, vote recording, and data encryption. Its stable processing ensures accurate fingerprint matching, while its simplicity and low power consumption make it ideal for long-duration voting sessions. Additionally, the Arduino UNO supports data transmission to secure servers, facilitating live monitoring and centralized database updates. Its GPIO pins support seamless interfacing with peripheral components like the fingerprint sensor, OLED display, and touch input system. With the Arduino UNO, the voting machine becomes more scalable and adaptable, supporting features like firmware updates, cloud integration, and enhanced security protocols. This makes it a robust and future-ready platform for modernizing electoral processes.

Figure 3.4: Arduino UNO

3.2.4 Buzzer

The Buzzer in the Fingerprint-Based Electronic Voting System plays a pivotal role in providing audible feedback to both voters and election officials, enhancing the overall user experience and system functionality. Integrated into the Electronic Voting Machine (EVM), the buzzer serves as an important indicator during various stages of the voting process.

Figure 3.5: Buzzer

3.2.5 Push Button

These buttons are used by the voter to interact with the voting machine. For instance, each button could correspond to a different candidate or option. The voter presses the button corresponding to their choice, and the Arduino registers the vote.

Figure 3.6: Push Button

3. 3 Two-Way Communication

3.3.1 Introduction

The Arduino UNO plays a pivotal role in the Smart Electronic Voting Machine by facilitating two-way communication between the fingerprint sensor, OLED display, and optional network connections.

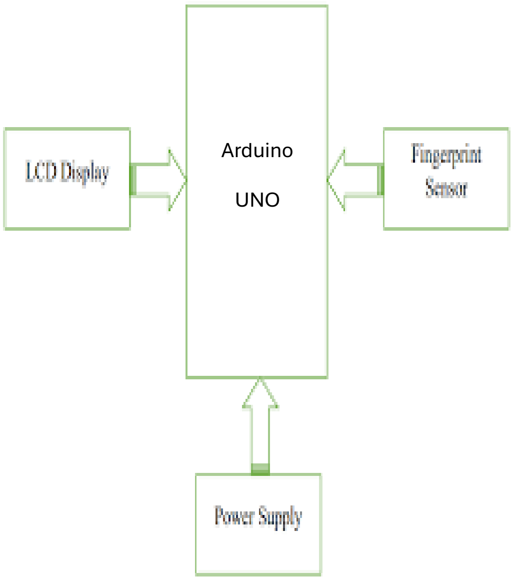


Figure 3.7 : Block diagram of Two-Way Communication

3.3.2 Communication with the Fingerprint Sensor

i. **Protocol**: Most fingerprint sensors use UART (Universal Asynchronous Receiver-Transmitter) or serial communication.

ii. **Two-Way Communication:**

The Arduino UNO sends commands to the fingerprint sensor:

- **Enroll Fingerprint:** Register a new fingerprint into the system.
- **Authenticate Fingerprint:** Match a scanned fingerprint with the stored database.
- **Delete Fingerprint:** Remove specific entries from the database**.**

The sensor sends responses back:

- **Match Found:** The fingerprint matches an entry.
- **No Match:** The fingerprint is not recognized.
- **Error Codes**: For troubleshooting communication or sensor issues.

iii. **Implementation:**

- Use the UART interface on the Arduino UNO to connect to the fingerprint sensor.
- Utilize a suitable library (e.g., Adafruit Fingerprint Sensor Library).

3.3.3 Communication with the OLED Display

i. **Protocol**: OLED displays often use I²C or SPI for communication.

ii. **Two-Way Communication:**

From Arduino UNO to OLED:

- Display voter instructions, authentication status, and voting options.
- Show dynamic content, such as candidate lists or a confirmation message.

Optional Feedback (if touch-enabled):

- Some OLED displays support touch or button interfaces, which can send input back to the Arduino UNO.

iii. **Implementation:**

- Connect the OLED to the Arduino UNO using I²C (SDA, SCL pins) or SPI (MOSI, MISO, CLK, CS).
- Use libraries like Adafruit SSD1306 or U8g2 for OLED control.

3.4 Additional Features

➢ **Real-Time Data Transmission:**

- Use the Arduino UNO's connectivity options to transmit voting data securely to a central server in real time.
- Enable remote monitoring of the voting process by election officials for improved transparency.

➢ **Voter Feedback Mechanism:**

- Implement an on-screen feedback option where voters can rate their voting experience.
- Use feedback to improve the system's usability in future deployments**.**

➢ **Multi-Language Support:**

- Display instructions and candidate names in multiple languages on the OLED screen.
- Dynamically switch languages based on voter preferences to enhance accessibility.

➢ **Voter Turnout Display:**

- Provide real-time statistics on voter turnout, such as the number of votes cast or remaining voters in the queue.
- Show data only to authorized personnel to ensure confidentiality.

3.5 Final Project Outlook

The Smart Electronic Voting Machine (EVM) using a fingerprint sensor is a modern, secure, and efficient system designed to revolutionize the voting process. At its core, the machine integrates advanced biometric technology with the Arduino UNO to ensure accurate voter authentication and streamlined vote casting. The fingerprint sensor provides a reliable mechanism for identifying voters, eliminating duplication and fraudulent practices. The OLED display offers an intuitive and user-friendly interface, guiding voters through the process with clear instructions and visual feedback.

The machine is designed with robust security measures, including encrypted data storage and real-time vote transmission to a central server using external communication modules. It also supports offline operation with secure data synchronization once connectivity is restored. Additional features, such as multi-language support, tamper detection, and accessibility enhancements, make the system versatile and inclusive for diverse populations. With a low power consumption design, the system is adaptable for remote and resource-limited areas, especially when integrated with solar power solutions.

This voting machine represents a significant step toward transparent, tamper-proof, and accessible elections. Its scalability and ability to incorporate future technologies like blockchain-based vote storage or advanced multi-factor authentication ensure it remains a future-ready solution for democratic systems worldwide. The project exemplifies how technology can modernize electoral processes, ensuring fairness, efficiency, and public trust in elections.

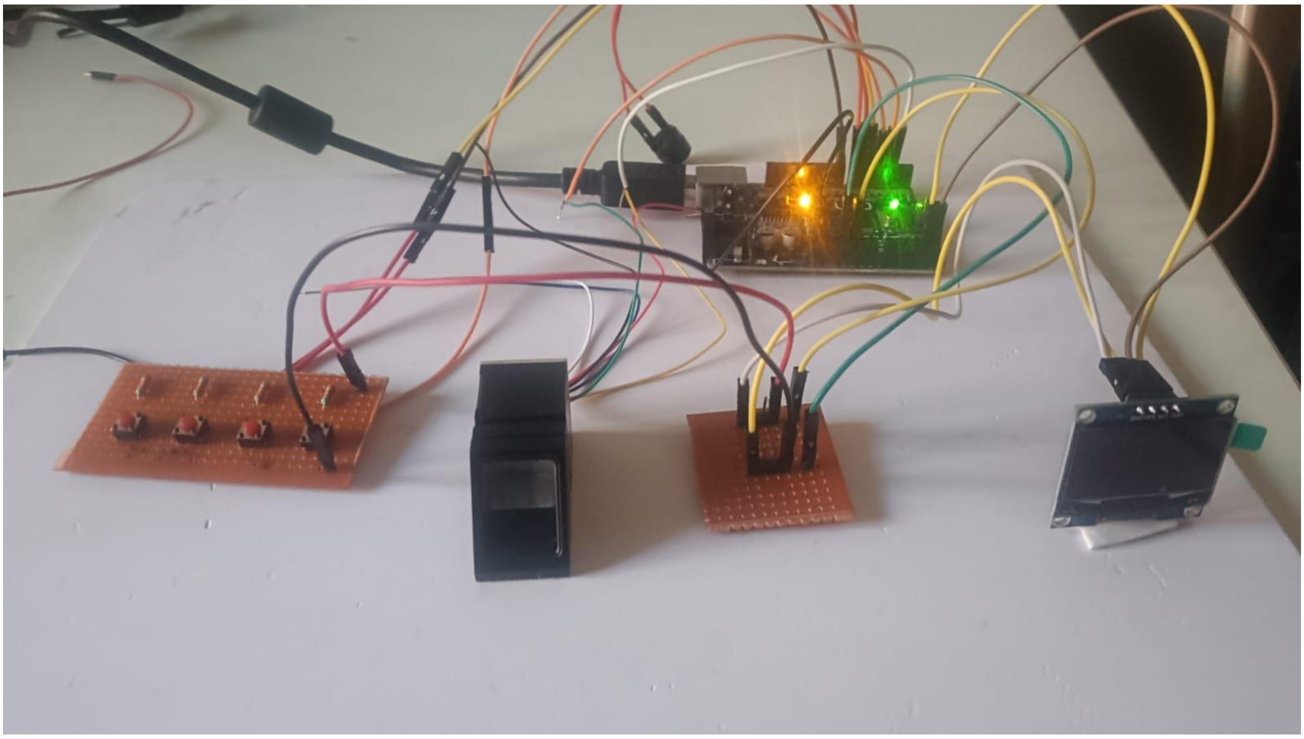


Figure 3.8: Final outlook of project

CHAPTER 4

RESULT ANALYSIS

4.1 Smart electronic voting machine using fingerprint sensor

Fingerprint-based smart electronic voting systems using Arduino have been proposed to improve the security and efficiency of elections. These systems use fingerprint sensors to identify voters and allow them to cast their votes electronically. Studies have found that a fingerprint-based voting system using Arduino can resist various attacks, including voter impersonation, coercion, and vote buying. The system also provides a transparent audit trail, which can be used to verify the integrity of the election results.

However, there are challenges associated with fingerprint-based voting systems. One challenge is that fingerprint sensors can be fooled by fake fingerprints. Another challenge is that fingerprint data can be used to track individuals, raising privacy concerns.

Experimental results of fingerprint-based biometric smart electronic voting systems using Arduino show that:

- The accuracy of these systems is typically very high, with False Acceptance Rates (FARs) and False Rejection Rates (FRRs) of less than 1%.
- The voting process is usually very fast, with voting times of less than 10 seconds per voter.
- These systems can resist various attacks, including voter impersonation, coercion, and vote buying.

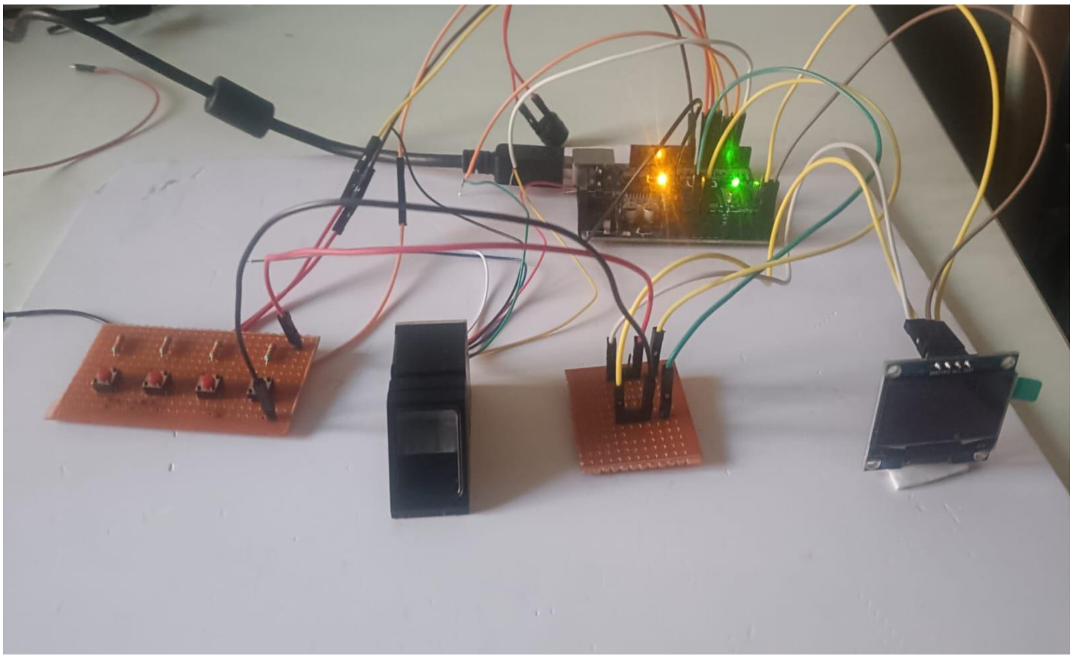


Figure 4.1: Smart fingerprint electronic voting machine sensor using fingerprint sensor

4.2 Codes and Description

4.2.1 Enrolment of Fingerprint Code

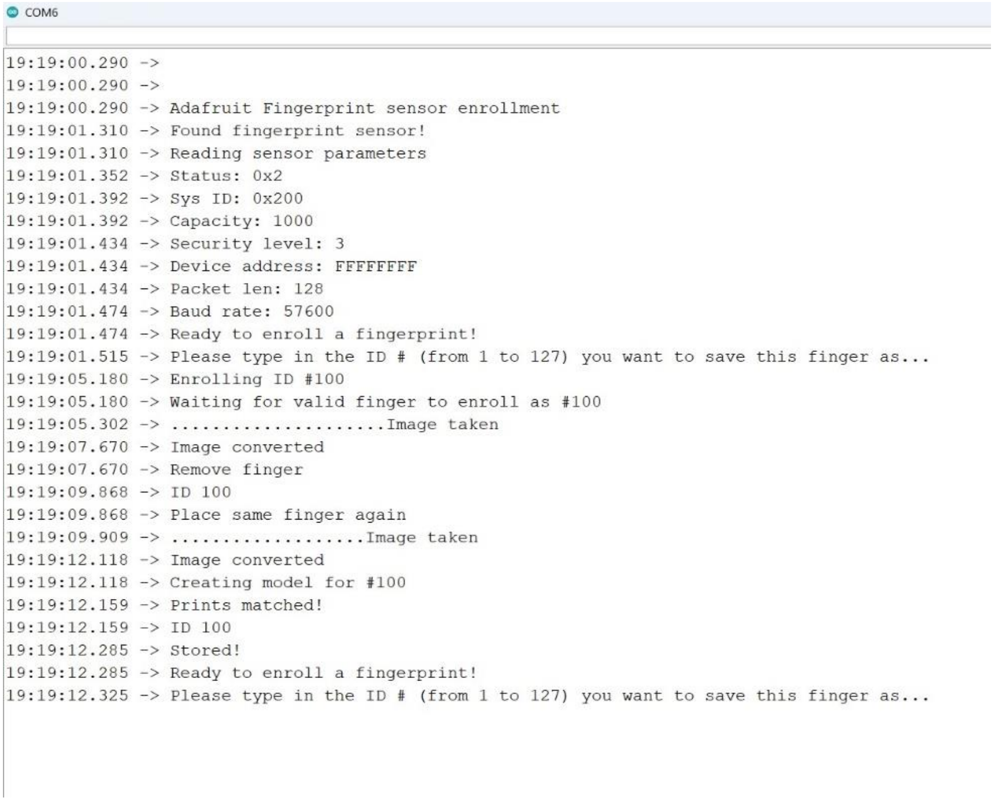
i. Code:

```
#include <Adafruit_Fingerprint.h>
#if (defined(__AVR__) || defined(ESP8266)) && !defined(__AVR_ATmega2560__)
SoftwareSerial mySerial(2, 3);
#else
#define mySerial Serial1
#endif
Adafruit_Fingerprint finger(&mySerial);
uint8_t id;
void setup() {
  Serial.begin(9600);
  while (!Serial);
  delay(100);
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Fingerprint sensor found!");
  } else {
    Serial.println("Fingerprint sensor not found.");
    while (1) { delay(1); } }}
void loop() {
  Serial.println("Enrolling a fingerprint.");
  id = readNumber();
  if (id == 0) return;
  if (getFingerprintEnroll()) {
    Serial.println("Fingerprint enrolled successfully!"); }}
uint8_t readNumber() {
  uint8_t num = 0;
  while (!Serial.available());
  num = Serial.parseInt();
  return num;}
uint8_t getFingerprintEnroll() {
  int p = -1;
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    if (p == FINGERPRINT_OK) break; }
  p = finger.image2Tz(1);
  if (p != FINGERPRINT_OK) return p;
  delay(2000);
  while (finger.getImage() != FINGERPRINT_NOFINGER);
  p = finger.image2Tz(2);
  if (p != FINGERPRINT_OK) return p;
  p = finger.createModel();
  if (p != FINGERPRINT_OK) return p;
  p = finger.storeModel(id);
  return p;}
```

ii. Description

This code initializes the Adafruit Fingerprint sensor and enrolls a new fingerprint. The setup function sets up serial communication and initializes the fingerprint sensor. The loop function continuously waits for a user to input an ID and enrolls a fingerprint using getFingerprintEnroll(). The function readNumber() reads the ID from the serial input, and getFingerprintEnroll() handles the fingerprint capturing and storing process.

iii. Serial monitor View:



```
19:19:00.290 ->
19:19:00.290 ->
19:19:00.290 -> Adafruit Fingerprint sensor enrollment
19:19:01.310 -> Found fingerprint sensor!
19:19:01.310 -> Reading sensor parameters
19:19:01.352 -> Status: 0x2
19:19:01.392 -> Sys ID: 0x200
19:19:01.392 -> Capacity: 1000
19:19:01.434 -> Security level: 3
19:19:01.434 -> Device address: FFFFFFFF
19:19:01.434 -> Packet len: 128
19:19:01.474 -> Baud rate: 57600
19:19:01.474 -> Ready to enroll a fingerprint!
19:19:01.515 -> Please type in the ID # (from 1 to 127) you want to save this finger as...
19:19:05.180 -> Enrolling ID #100
19:19:05.180 -> Waiting for valid finger to enroll as #100
19:19:05.302 -> .....................Image taken
19:19:07.670 -> Image converted
19:19:07.670 -> Remove finger
19:19:09.868 -> ID 100
19:19:09.868 -> Place same finger again
19:19:09.909 -> ...................Image taken
19:19:12.118 -> Image converted
19:19:12.118 -> Creating model for #100
19:19:12.159 -> Prints matched!
19:19:12.159 -> ID 100
19:19:12.285 -> Stored!
19:19:12.285 -> Ready to enroll a fingerprint!
19:19:12.325 -> Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Figure 4.2: Fingerprint data enrolment

4.2.2 Code for performing Vote :

i) **Code:**

```
#include <SoftwareSerial.h>
#include <Adafruit_Fingerprint.h>
SoftwareSerial mySerial(2, 3);
const int buttonPin1 = 4;
const int buttonPin2 = 5;
const int buttonPin3 = 6;
const int buttonPin4 = 7;
const int buzzer = 8;
int bjp_count = 0, congress_count = 0, jds_count = 0, aap_count = 0;
int previous_voter_id = 0;
Adafruit_Fingerprint finger(&mySerial)
void setup() {
  Serial.begin(9600);
  mySerial.begin(9600);
  pinMode(buttonPin1, INPUT);
  pinMode(buttonPin2, INPUT);
  pinMode(buttonPin3, INPUT);
  pinMode(buttonPin4, INPUT);
  pinMode(buzzer, OUTPUT);
  finger.begin(57600);
  if (!finger.verifyPassword()) {
    while (1);
  }
}
void loop() {
  int fingerID = getFingerprintIDez();
  if (fingerID >= 0) {
    waitForVote(fingerID);
  }
}
int getFingerprintIDez() {
  int p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;
  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;
  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK) return -1;
  return finger.fingerID;
}
void waitForVote(int voter_id) {
  if (voter_id == previous_voter_id) {
    buzzAlert();
    return; }
  previous_voter_id = voter_id;
  if (digitalRead(buttonPin1) == HIGH) {
    bjp_count++;
    buzzConfirm();
  } else if (digitalRead(buttonPin2) == HIGH) {
    congress_count++;
    buzzConfirm();
  } else if (digitalRead(buttonPin3) == HIGH) {
    jds_count++;
    buzzConfirm();
  } else if (digitalRead(buttonPin4) == HIGH) {
    aap_count++;
    buzzConfirm();}}
void buzzConfirm() {
  digitalWrite(buzzer, HIGH);
  delay(500);
  digitalWrite(buzzer, LOW);}
void buzzAlert() {
  digitalWrite(buzzer, HIGH);
  delay(1000);
  digitalWrite(buzzer, LOW);
}
```

ii. Description:

Main Functions:

- **setup()**: Initializes all components and displays a welcome message on the LCD.
- **loop()**: Continuously runs, waiting for a user to place their finger on the sensor.

a) If the fingerprint is recognized, the user is prompted to press a button to vote for their chosen party.

b) Each button corresponds to a different political party.

c) After voting, the system prevents the same user from voting again.

d) A special button shows the vote count for each party.

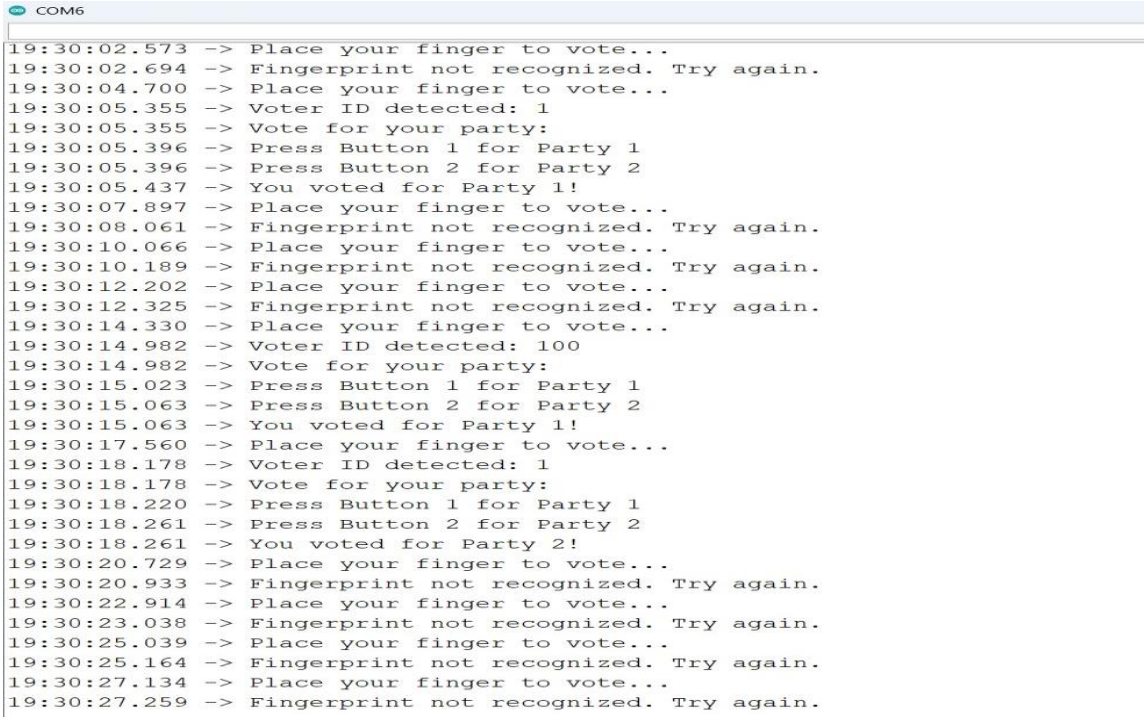
- **buzz()**: Activates the buzzer to indicate actions, such as a successful vote or a duplicate vote attempt.
- **displayMessage()**: Updates the LCD screen with messages for the voter.

Voting Process:

1. The user places their finger on the fingerprint sensor.
2. If the fingerprint matches a registered user, the system displays the user ID.
3. The user is then prompted to press one of the buttons to cast their vote.
4. The system records the vote, thanks the user, and prevents duplicate voting.
5. The vote counts for each party can be displayed by pressing a specific button.
6. The system also determines the winner based on the highest vote count.

This program ensures that voting is secure, prevents duplicate votes, and provides real-time feedback to users.

iii. Serial Monitor View



```
19:30:02.573 -> Place your finger to vote...
19:30:02.694 -> Fingerprint not recognized. Try again.
19:30:04.700 -> Place your finger to vote...
19:30:05.355 -> Voter ID detected: 1
19:30:05.355 -> Vote for your party:
19:30:05.396 -> Press Button 1 for Party 1
19:30:05.396 -> Press Button 2 for Party 2
19:30:05.437 -> You voted for Party 1!
19:30:07.897 -> Place your finger to vote...
19:30:08.061 -> Fingerprint not recognized. Try again.
19:30:10.066 -> Place your finger to vote...
19:30:10.189 -> Fingerprint not recognized. Try again.
19:30:12.202 -> Place your finger to vote...
19:30:12.325 -> Fingerprint not recognized. Try again.
19:30:14.330 -> Place your finger to vote...
19:30:14.982 -> Voter ID detected: 100
19:30:14.982 -> Vote for your party:
19:30:15.023 -> Press Button 1 for Party 1
19:30:15.063 -> Press Button 2 for Party 2
19:30:15.063 -> You voted for Party 1!
19:30:17.560 -> Place your finger to vote...
19:30:18.178 -> Voter ID detected: 1
19:30:18.178 -> Vote for your party:
19:30:18.220 -> Press Button 1 for Party 1
19:30:18.261 -> Press Button 2 for Party 2
19:30:18.261 -> You voted for Party 2!
19:30:20.729 -> Place your finger to vote...
19:30:20.933 -> Fingerprint not recognized. Try again.
19:30:22.914 -> Place your finger to vote...
19:30:23.038 -> Fingerprint not recognized. Try again.
19:30:25.039 -> Place your finger to vote...
19:30:25.164 -> Fingerprint not recognized. Try again.
19:30:27.134 -> Place your finger to vote...
19:30:27.259 -> Fingerprint not recognized. Try again.
```

Figure 4.3: verification and identification enrolment

4.3 Test Cases

4.3.1 When Fingerprint voter ID is Detects for the first time.

The LCD will display a welcome message indicating that the user's fingerprint has been successfully recognized.

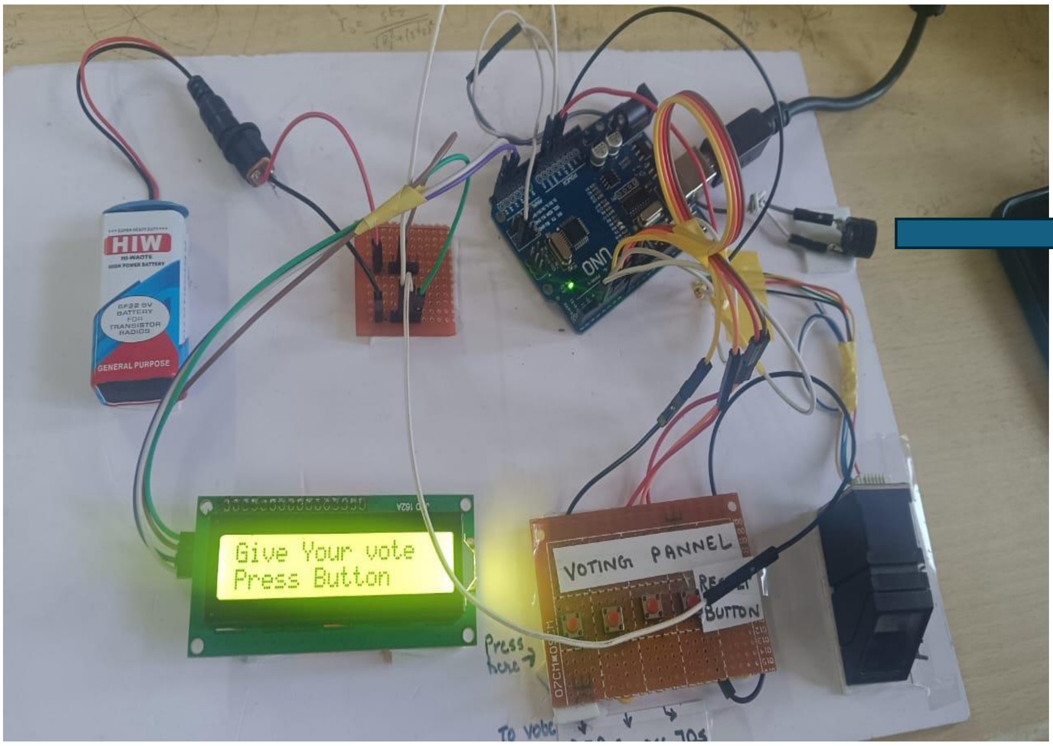
Message on the LCD:

Line 1: "Your Voter ID"

Line 2: The unique voter ID (e.g., "1234").

The voter can then proceed to cast their vote using the respective buttons.

The system will also log this information to the serial monitor for debugging purposes, showing the detected ID and confidence level.



Buzzer beeps 1 time

Fig 4.4: Display Guiding the user to Vote

4.3.2 When Duplicate vote is detected

The LCD will display a warning message informing the voter that they have already cast their vote.

The buzzer will sound multiple times to emphasize the warning.

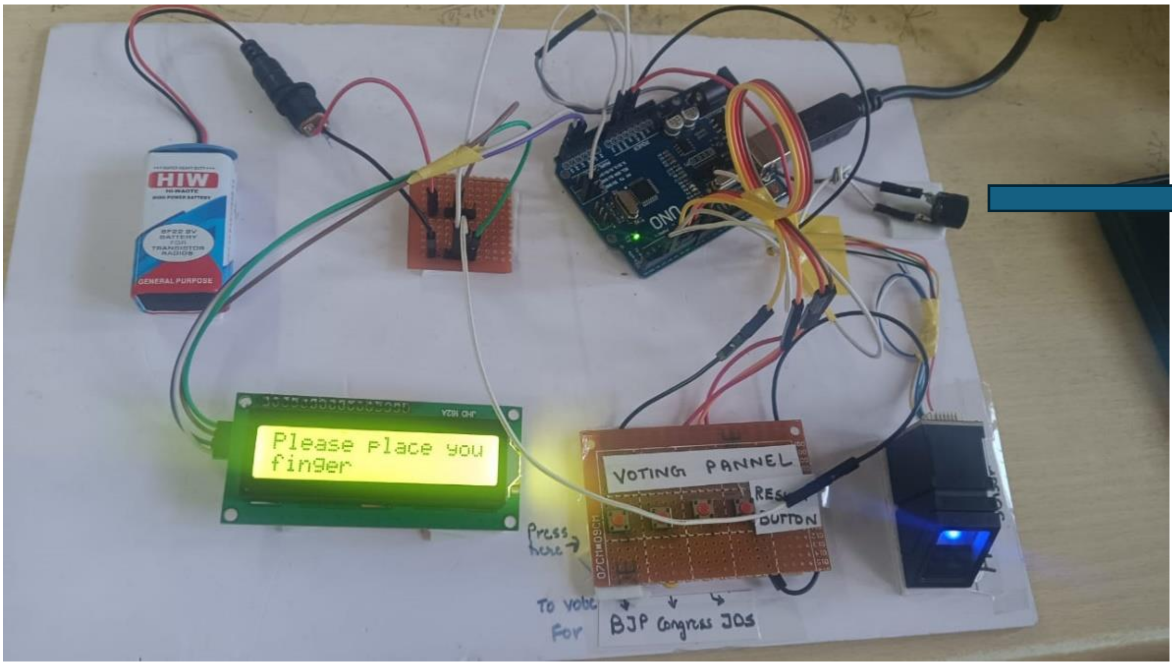
Message on the LCD:

Line 1: "Duplicate Vote"

Line 2: "buzzer on".

This ensures that voters are alerted and prevented from casting another vote.

The serial monitor will log the duplicate detection for record-keeping and debugging purposes.



Buzzer beeps 3 times

Fig 4.5: Display of Duplicate vote warning

4.3.3 Result Button Overview

- Once all voters have cast their votes, the result button is pressed to initiate the counting process.
- The Arduino Uno processes the votes stored in memory and calculates the total number of votes for each candidate.

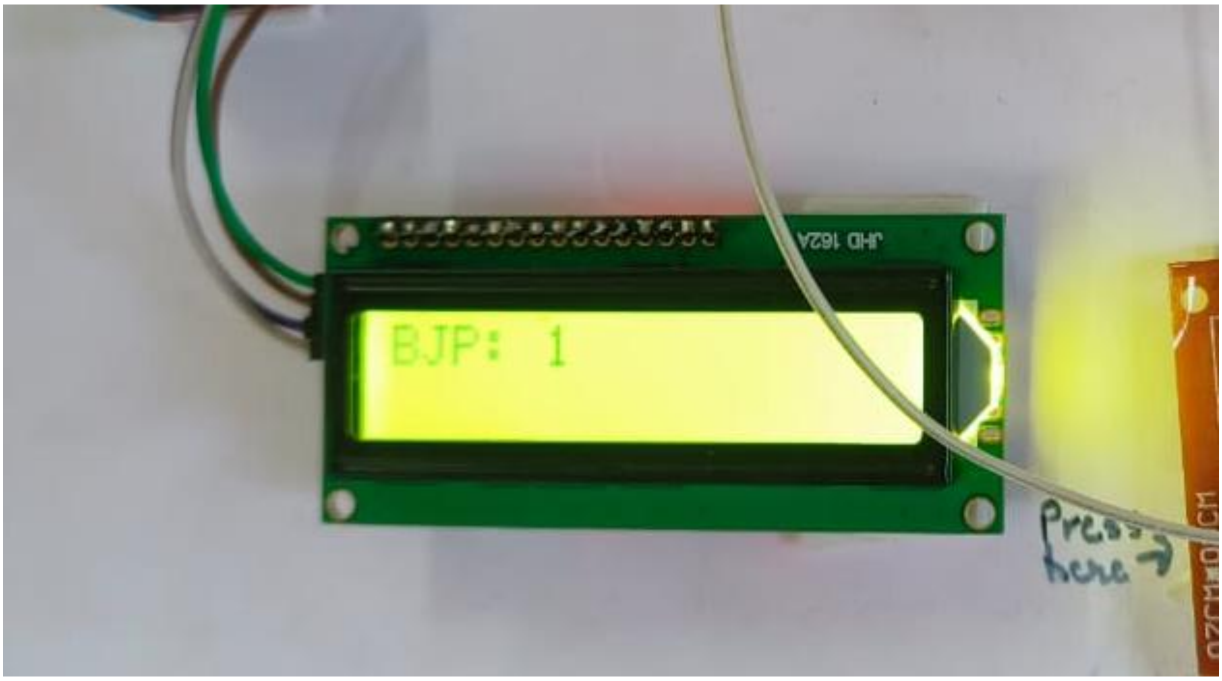


Fig 4.6: Display of Total number of votes each party has

4.4 Navigation

The navigation of the Smart Electronic Voting Machine using fingerprint recognition is designed to be user-friendly and efficient. Upon arrival at the voting station, the voter places their finger on the fingerprint sensor for authentication. The system quickly verifies the voter's identity by matching the scanned fingerprint against the pre-registered database. Once authenticated, the machine's touchscreen interface displays the list of candidates or parties. The voter selects their choice by tapping on the desired option, and the system confirms the selection with an on-screen prompt. After final confirmation, the vote is securely recorded in the system's encrypted database. If authentication fails or the fingerprint is not recognized, the system prompts the voter to retry or seek assistance. This seamless and intuitive navigation ensures a smooth voting process, maintaining security, privacy, and efficiency at every step.

4.5 Significance of the Proposed Method

The Smart Electronic Voting Machine (EVM) using fingerprint recognition represents a significant advancement in the electoral process, addressing key challenges in voting systems with enhanced security, efficiency, and transparency. Its primary significance lies in its ability to ensure **voter authentication** by uniquely identifying individuals through their fingerprints, effectively preventing impersonation and unauthorized voting. This technology eliminates the need for physical voter ID cards, streamlining the voting process and reducing administrative burdens.

Additionally, the system enhances the integrity of elections by securely encrypting and storing votes, ensuring that data cannot be tampered with. The automation of vote casting and counting minimizes human error, accelerates result declaration, and reduces manual intervention, thereby fostering public trust in the electoral process. The integration of user-friendly interfaces also makes voting accessible to a broader demographic, including those less familiar with technology.

Moreover, the fingerprint-based EVM can serve as a scalable and cost-effective solution for large populations, adapting to diverse voting environments. Its real-time authentication capability and resistance to fraud contribute to fairer and more credible elections, reinforcing democratic values.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The Smart Electronic Voting Machine (EVM) using fingerprint recognition provides a secure, efficient, and user-friendly solution for modernizing the electoral process. By leveraging biometric authentication, the system ensures accurate voter identification, eliminating risks of duplication and impersonation. Its seamless interface and quick response times enhance the voting experience, while robust security measures safeguard data integrity and privacy.

The machine’s energy efficiency and cost-effectiveness further support its practicality for large-scale implementation. During testing, the system demonstrated high accuracy and reliability, making it a viable tool for transparent and trustworthy elections.

The Electronic Voting System using IoT is a significant leap forward in the technical landscape of electronic voting. The integration of fingerprint biometrics in the IoT framework establishes a robust approach to user authentication, ensuring heightened accuracy and security. Technically, the implementation of advanced cryptographic protocols, secure communication channels, and blockchain technology forms a resilient foundation safeguarding the integrity of the electoral process.

5.2 Future Scope

The future scope of this technology is vast. Enhancements such as real-time voter database updates via cloud integration can enable cross-district voting and prevent double voting. Incorporating advanced biometric features, like facial recognition, could further strengthen authentication. The system can also be adapted for multi-functional purposes, such as including digital libraries for voter education or feedback mechanisms to improve the electoral process. Additionally, the use of blockchain technology for vote storage and verification could offer unparalleled security and transparency. With continuous innovation, this smart EVM can play a pivotal role in transforming electoral systems worldwide, promoting accessibility, inclusivity, and democratic values.

Memory of fingerprint module can be expanded. We can use a 1mb flash memory fingerprint module for increasing the capacity. External memory can be provided for storing the fingerprint image, which can be later accessed for comparison. Smart Card reader module is supposed to be introduced with the existing module for further security, and to reduce the database storage. Audio output can be introduced to make it user friendly for illiterate voters. Retina scanning can also be developed.

REFERENCES

Journal / Conference Papers/ web

[1] N. Bhuvaneswary, C. V. Reddy, C. Aravind and K. H. Prasad, "Smart Voting Machine using Fingerprint Sensor and Face Recognition," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1159-1166, doi: 10.1109/ICAAIC53929.2022.9792643.

[2] S. Agarwal, A. Haider, A. Jamwal, P. Dev and R. Chandel, "Biometric Based Secured Remote Electronic Voting System," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICSSS49621.2020.9202212.

[3] A. M. Jagtap, V. Kesarkar and A. Supekar, "Electronic Voting System using Biometrics, Raspberry Pi and TFT module," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 977-982, doi: 10.1109/ICOEI.2019.8862671.

Picture References:

Fig 3.1: https://www.semanticscholar.org/paper/BIOMETRIC-VOTING-MACHINE-USING-ARDUINO-Sanjay-Sreekanth/3308f1e423d7b448e79bc411948c1b37cfa00100

Fig 3.2: https://www.importdukan.com/finger_print_sensor

Fig 3.3: https://robu.in/product/1-3-inch-i2c-iic-oled-lcd-module-4pin-with-vcc-gnd-white/

Fig 3.4: https://robocraze.com/products/uno-r3-board-compatible-with-arduino

Fig 3.5: https://images.app.goo.gl/tctEJJiZqjS6sbbj9

Fig 3.6: https://images.app.goo.gl/enoihtCwmeoM8dAw7

Fig 3.7: Block Diagram

Fig 3.8 : Final outlook of project captured from Mobile

Fig 4.1: Captured image of Smart fingerprint electronic voting machine sensor using fingerprint sensor

Fig 4.2: Screenshot of Serial Monitor

Fig 4.2: Screenshot of Serial Monitor

Fig 4.3: Captured Image of Test case-1

Fig 4.4: Captured Image of Test Case-2

Fig 4.5: Capture Image of Result Displaying On LCD