DAYANANDA SAGAR COLLEGE OF ENGINEERING
(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade,
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078.

MINI-PROJECT

On

"Fingerprint based fraud detection Voting system"

BACHELOR OF ENGINEERING
IN
INFORMATION SCIENCE AND ENGINEERING

Submitted by

NISARGA K (1DS20IS065)

NITHYA M (1DS20IS067)

SAIJYOTI G M (1DS20IS085)

SANJANA GOUD (1DS20IS092)

Under the guidance of

Dr Chandrakala B M
(Associate professor)

Department Of Information Science and Engineering
DAYANANDA SAGAR COLLEGE OF ENGINEERING
S M Hills, Kumara Swamy Layout, Bengaluru-560078

2022-23

DAYANANDA SAGAR COLLEGE OF ENGINEERING

Shavige Malleshwara Hills, Kumaraswamy Layout

Bangalore-560078

Department of Information Science and Engineering

ACCREDITED BY NBA & NAAC

2022-2023

Certificate

This is to certify that the Project Work entitled **Fingerprint based fraud detection Voting system** is a bonafide work carried out by **NISARGA K (1DS20IS065), NITHYA M (1DS20IS067), SAIJYOTI G M (1DS20IS085), SANJANA GOUD (1DS20IS092) in** partial fulfillment for the 6th semester of Bachelor of Engineering in Information Science & Engineering of the Visvesvaraya Technological University, Belgaum during the year 2022-2023. The Mini-Project Report has been approved as it satisfies the academics prescribed for the Bachelor of Engineering degree.

Signature of Guide	Signature of Domain Expert	Signature of HOD

Name of the Examiners	Signature with Date
1.)	
2.)	

CONTENTS

Abstract

Chapter1 :Introduction.....Page No.1-2

1.1 Introduction

1.2 Problem statement

1.3 Objectives and Scope of Project

1.4 Motivation of Project

Chapter 2: Literature Survey.....Page No.3

Chapter 3 Requirements .....Page No.4

3.1 Software Requirements

3.2 Hardware Requirements

Chapter 4 :System Design .....Page No.5-7

4.1 Existing system

4.2 Proposed system

4.3 System Architecture

4.4 Flow chart

Chapter 5:Methodology.....page No.8-9

5.1 Proposed Technique.....page No.8-9

Chapter 6: Implementation.....Page No10-17

Results & Conclusions.....Page No.18-26

References ..Page No.27

Abstract

Security has been playing a key role in many of our places like offices, institutions, libraries, laboratories etc. in order to keep our data confidentially so that no other unauthorized person could have an access on them. Nowadays, at every point of time, we need security systems for protection of valuable data and even money. This paper presents a fingerprint based door opening system which provides security which can be used for many banks, institutes and various organizations etc..,. There are other methods of verifying authentication through password, RFID but this method is most efficient and reliable. To provide perfect security to the bank lockers and to make the work easier, this project is taking help of two different technologies viz. EMBEDDED SYSTEMS and BIOMETRICS. Unauthorized access is prohibited by designing a lock that stores the fingerprints of one or more authorized users. Fingerprint is sensed by sensor and is validated for authentication. If the fingerprint matches, the door will be opened automatically otherwise the buzzer connected to an audio amplifier will be activated so that the people near the surroundings will get an alert. A proposed solution to address the inefficiency and vulnerabilities in India's current voting system is the development of an online, biometric fingerprint-based voting machine. This system eliminates the need for voters to carry identification cards, as their fingerprints serve as identification at the polling booth. The fingerprint reader acquires the voter's fingerprint and verifies it with pre-stored data during registration. If the data matches, the person is allowed to cast their vote manually using push buttons. The system ensures anonymity by assigning each user a unique and random ID, ensuring no connection to their personal details. The interface is designed to be user-friendly and simple, prioritizing visual representation of data and basic functionalities.

Chapter 1

Introduction

1.1 Introduction

Security is of primary concern and in this busy, competitive world, human cannot find ways to provide security to his confidential belongings manually. Instead, he finds an alternative which can provide a full-fledged security as well as atomized. In the ubiquitous network society, where individuals can easily access their information anytime and anywhere, people are also faced with the risk that others can easily access the same information anytime and anywhere. Because of this risk, personal identification technology, which can distinguish between registered legitimate users and imposters, is now generating interest. Generally passwords, identification cards and PIN verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost. The most secured system is fingerprint recognition because a fingerprint of one person never matches the other. Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among these available biometric traits fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable

1.2 Problem statement

The existing voting system in India is plagued by inefficiency and vulnerabilities in voter authentication. Relying solely on voter ID cards, which can be easily faked, poses significant security risks. Additionally, manual identity verification processes require a substantial workforce. The system lacks real-time monitoring of Electronic Voting Machines (EVMs), leading to delays, and the manual vote counting process is time-consuming. These issues highlight the need for a more secure and efficient voting system that automates authentication, reduces the risk of fraud, and ensures faster and accurate vote counting.

1.3 Objectives and Scope of Project

- The possible solution is, if a person is identified using his/her fingerprint rules out the possibility of fake votes and it provides the result immediately after the voting process is completed. The whole process is done automatically by the voting machine.

- The environment of this voting system is designed in such a way that it won't allow voters inside the voting room if another voter is casting his vote.
- The project scope includes designing and implementing a system that captures and stores voters' fingerprints securely, develops algorithms for real-time fingerprint matching and authentication, integrates with existing voter registration databases, and provides a user-friendly interface for smooth and efficient voting while ensuring the prevention of fraudulent activities such as duplicate voting or identity theft.

1.4 Motivation of Project

- Enhancing Voter Confidence: Fingerprint-based fraud detection increases voter trust in the electoral process.
- Preventing Voter Impersonation: Fingerprint authentication ensures only eligible voters participates, preventing impersonation.
- Strengthening Election Integrity: Fingerprint-based detection minimizes manipulation and ensures a fair voting process.
- Combating Electoral Fraud: Fingerprint authentication acts as a deterrent, reducing various types of fraud in elections.
- Streamlining Voter Registration: Fingerprint systems simplify registration, eliminating duplicates and improving accuracy.
- Leveraging Biometric Technology: Fingerprint authentication offers robust and reliable identification, enhancing security.

Chapter 2

Literature Survey

- One paper [1] explains the working principle of the fingerprint sensor and its potential for detecting fraud in Electronic Voting Machines (EVMs).
- Another paper [2] explores the use of Internet of Things (IoT) in building such a system, highlighting the interconnectivity of devices and the associated risks. Additionally, a paper [3] proposes storing fingerprints in a database, providing immediate notifications of casted votes for transparency, and delivering prompt election results.
- Furthermore, another paper [4] suggests using fingerprint sensors to input data without duplication and enabling online voting from the comfort of one's location. These studies contribute valuable insights to the development of an efficient and secure fingerprint-based voting system.
- [5] The research paper titled "Wireless Fingerprint Based Security System using Zigbee" published in the International Journal of Inventive Engineering and Sciences (IJIES) in April 2013 presents a wireless security system that utilizes fingerprints for authentication. The system employs Zigbee technology to establish communication between the fingerprint sensor and the central security unit.
- [6] The research paper titled "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar provides an overview of fingerprint matching techniques. It is likely to cover various algorithms and methodologies employed in fingerprint matching for identification and verification purposes, with a focus on the work done by the authors from the Department of Computer Science and Engineering at Michigan State University.

Chapter 3

Requirements

3.1 Software Requirements

1. Arduino –UNO IDE Suite
2. C Programming

3.2 Hardware Requirements

1. Micro controller : Arduino
2. Finger print reader
3. Power Supply : 12V DC
4. DC Motor
5. 16x2 LCD Display

Chapter 4

System Design

4.1 Existing system

The existing system for fingerprint-based fraud detection in a voting system might involve traditional paper-based voting methods where individuals cast their votes by marking their preferences on paper ballots. This system typically relies on manual verification processes, such as signature verification or ID checks, to detect fraudulent activities. However, these methods are susceptible to human errors and can be easily manipulated, leading to potential voting fraud.

4.2 Proposed system

The proposed system is a fingerprint-based fraud detection voting system that leverages biometric technology to enhance the security and integrity of the voting process. In this system, each eligible voter's fingerprint is enrolled and stored in a database before the election. During the voting process, voters' fingerprints are captured and compared against the enrolled fingerprints to verify their identity and eligibility to vote.

The proposed system utilizes advanced fingerprint recognition algorithms to ensure accurate identification and prevent fraudulent activities, such as multiple voting or impersonation. It may also incorporate additional security measures, such as encryption techniques, to protect the integrity and privacy of the biometric data.

4.3 System Architecture

The system architecture of a fingerprint-based fraud detection voting system typically consists of several components working together to ensure a secure and reliable voting process. Here are the key components:

Fingerprint Capture Devices: These devices capture the fingerprints of voters during the registration and voting phases. They can be specialized fingerprint scanners or integrated into electronic voting machines.

Database: A central database stores the enrolled fingerprints of eligible voters, along with their corresponding voter information. It provides a repository for efficient retrieval and matching of fingerprints during the voting process.

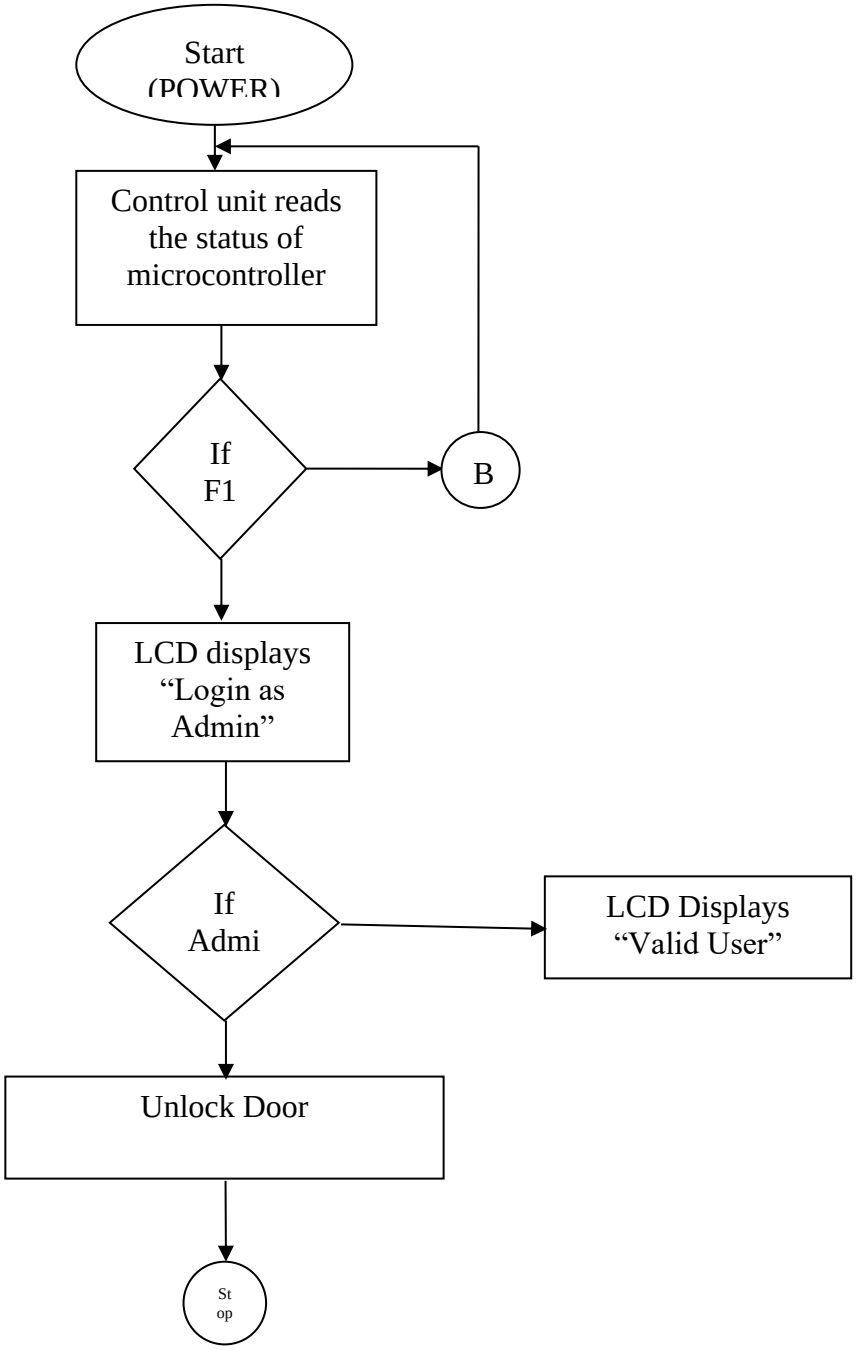
Voting Interface: This component includes the user interface through which voters interact with the system to cast their votes. It may be a touchscreen interface or a combination of physical buttons and displays.

Fraud Detection System: This system analyses the voting data and fingerprint patterns to detect any suspicious activities or anomalies that may indicate fraud, such as multiple votes from the same individual or mismatched fingerprints.

Security Measures: To ensure the integrity and confidentiality of the system, various security measures are implemented. These may include encryption of sensitive data, secure communication protocols, access control mechanisms, and audit trails for monitoring and tracking system activities.

Reporting and Result Generation: Once the voting process is complete, the system generates accurate and tamper-proof voting results based on the authenticated and verified votes. Reports and statistics can be generated for auditing and transparency purposes.

4.4 Flow chart



Chapter 5

Methodology

5.1 Proposed Technique

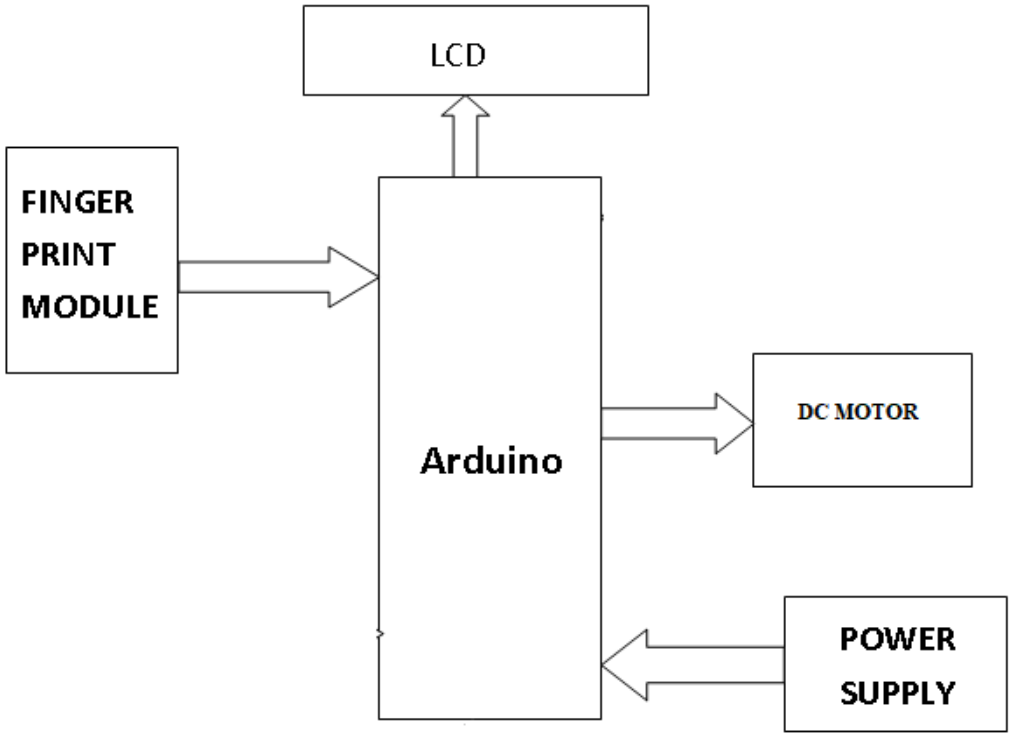
Our proposed system overcomes all the security problems in existing system and provides high security and efficiency. This is a perfect/optimal solution for saving/protecting one from the hassle of stolen/lost key or an unauthorized entry. Fingerprint is a boon solution for these problems which provides high level of recognition accuracy. The skin on our palms and soles exhibits a flow like pattern of ridges called friction ridges. The pattern of friction ridges on each finger is unique and immutable. This makes fingerprint a unique identification for everyone. Fingerprint door lock incorporates the proven technology. Fingerprint scanner scans the fingerprints of users and used for ensuring authentication. Fingerprint scanning is more accurate and cost effective method and duplication is virtually impossible. A Fingerprint recognition system can easily perform verification. In verification, the system compares an input fingerprint to the enrolled fingerprint of a specific user to determine if they are from the same finger. Now the security of our home/office is literally in our hands or rather on our fingertips. After the scanning has been completed, user has to enter the password to open his locker with the help of a keypad. Immediately the locker will be opened. After the work has been completed if key is pressed again with help of keypad the locker door will be closed again. If an unauthorized person tries to scan his fingerprint image then an indication will be given by a buzzer which is interfaced to the controller and also if wrong password is entered by the user again indication will be given by the buzzer. The current user instead of him/her can make a new person as the user of the same locker by new registration process and the old user's fingerprint image will be deleted. Option for changing the password is also available.

Project flow:

- Initially the voters should register their fingerprint with the voting system by placing their finger on the fingerprint reader.
- After registering the fingerprints of different voters, the voting process is conducted further.
- The voter enters the ballot room, places his fingerprint on the fingerprint module to identify his details and if it matches with the details given during registration, he is further allowed to cast his vote
- If the fingerprint matches with the already registered fingerprint, the LCD will display that the voter is authorized.
- Candidate options are given to the voter, and he is allowed to vote for the candidate whom he decides to cast his vote for.
- If a voter is voting for the first time, they can vote without any interruption. However, if the voter attempts to vote for the second time, the buzzer will signal an alert.
- At the end, the admin can view the results of the voting process.

Chapter 6

Implementation



Software code for Arduino Uno that enrolls the fingerprint

```
void Enroll()
{
  int count=0;
  lcd.clear();
  lcd.print("Enter Finger ID:");
  while(1)
 {   lcd.setCursor(0,1);
    lcd.print(count);
```

```
    if(digitalRead(up) == 0)     {
      count++;
      if(count>25)
      count=0;
delay(500);
    }
    else if(digitalRead(down) == 0)     {
      count--;
      if(count<0)
count=25;
      delay(500);
    }
    else if(digitalRead(del) == 0)     {
        id=count;
        getFingerprintEnroll();
        for(int i=0;i<records;i++)          {
          if(EEPROM.read(i+10) == 0xff)            {
            EEPROM.write(i+10, id);
            break;
          }  }  }
        return;
 }
      else if(digitalRead(enroll) == 0)     {
        return;   }}}
#include<EEPROM.h>
#include<LiquidCrystal.h>
LiquidCrystal lcd(13,12,8,9,10,11);
#include <SoftwareSerial.h>
SoftwareSerial fingerPrint(2, 3);
```

```
#include <Adafruit_Fingerprint.h>

uint8_t id;

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&fingerPrint);

#define enroll 4#define del 5#define up 6#define down 7

#define indVote 19


#define sw1 14

#define sw2 15

#define sw3 16

#define resultsw 17

#define indFinger 7

#define buzzer 18

#define records 25

int vote1,vote2,vote3;

int flag;

void setup() {

   delay(1000);

   pinMode(enroll, INPUT_PULLUP);

   pinMode(up, INPUT_PULLUP);

   pinMode(down, INPUT_PULLUP);

   pinMode(del, INPUT_PULLUP);

   pinMode(sw1, INPUT_PULLUP);

   pinMode(sw2, INPUT_PULLUP);

   pinMode(sw3, INPUT_PULLUP);

   pinMode(resultsw, INPUT_PULLUP);

   pinMode(buzzer, OUTPUT);

   pinMode(indVote, OUTPUT);
```

```
    pinMode(indFinger, OUTPUT);
lcd.begin(16,2);
  if(digitalRead(resultsw) ==0)  {
       for(int i=0;i<records;i++)
          EEPROM.write(i+10,0xff);
       EEPROM.write(0,0);
       EEPROM.write(1,0);
       EEPROM.write(2,0);
       lcd.clear();
       lcd.print("System Reset");
       delay(1000);  }
    lcd.clear();
    lcd.print("Voting Machine");
    lcd.setCursor(0,1);
    lcd.print("by Finger Print");
    delay(2000);
  if(EEPROM.read(0) == 0xff)
   EEPROM.write(0,0);
     if(EEPROM.read(1) == 0xff)
   EEPROM.write(1,0);
     if(EEPROM.read(1) == 0xff)
   EEPROM.write(1,0);
fingerPrint.begin(9600);
    Serial.begin(9600);
    lcd.clear();
    lcd.print("Finding Module");
    lcd.setCursor(0,1);
```

```
  delay(1000);
  if (finger.verifyPassword())     {
    //Serial.println("Found fingerprint sensor!");
    lcd.clear();
    lcd.print("Found Module ");
    delay(1000);    }
  else     {
  //Serial.println("Did not find fingerprint sensor :(");    lcd.clear();
  lcd.print("module not Found");
  lcd.setCursor(0,1);
  lcd.print("Check Connections");
  while (1);    }
lcd.clear();
lcd.setCursor(0,0);
lcd.print("BJP");
lcd.setCursor(4,0);
lcd.print("CON");
lcd.setCursor(8,0);
lcd.print("JDS");
lcd.setCursor(12,0);
lcd.print("RESULT");
lcd.setCursor(0,1);
vote1=EEPROM.read(0);
lcd.print(vote1);
lcd.setCursor(6,1);
vote2=EEPROM.read(1);
lcd.print(vote2);
```

```
  lcd.setCursor(12,1);
  vote3=EEPROM.read(2);
  lcd.print(vote3);
  delay(2000);}
void loop() {
START();
void START()
{
   while(1)
   {
    lcd.clear();
     lcd.setCursor(0,0);
     lcd.print("Press UP/Down ");
     lcd.setCursor(0,1);
     lcd.print("to start System");
     if(digitalRead(up)==0 || digitalRead(down)==0)
     {
      while(1)
      {
        SerialEvent();
      }
     }
     checkKeys();
     delay(1000);
   } }
void delet() {
   int count=0;
```

```
  lcd.clear();
  lcd.print("Enter Finger ID");
  while(1)  {
   lcd.setCursor(0,1);
    lcd.print(count);
    if(digitalRead(up) == 0)     {
      count++;
      if(count>25)
      count=0;
      delay(500);     }
    else if(digitalRead(down) == 0)     {
      count--;
      if(count<0)
      count=25;
      delay(500);     }
    else if(digitalRead(del) == 0)     {
        id=count;
        deleteFingerprint(id);
        for(int i=0;i<records;i++)       {
          if(EEPROM.read(i+10) == id)          {
            EEPROM.write(i+10, 0xff);
            break;
       }  }   return;    }
      else if(digitalRead(enroll) == 0)     {
        return;    }
void Vote(){
 lcd.clear();
```

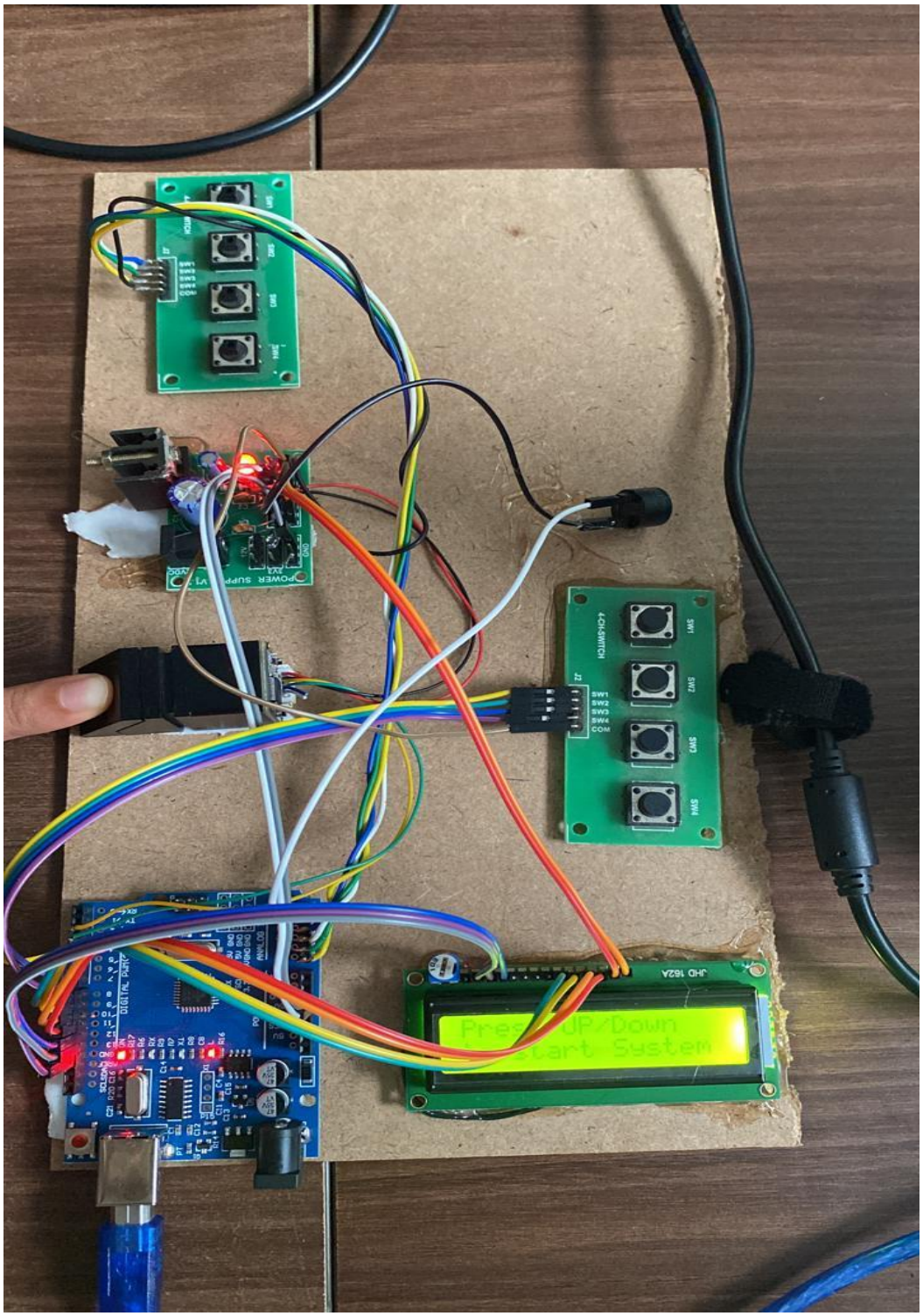
```
lcd.print("Please Place");
lcd.setCursor(0,1);
lcd.print("Your Vote");
digitalWrite(indVote, HIGH);
digitalWrite(indFinger, LOW);
digitalWrite(buzzer, HIGH);
delay(500);
digitalWrite(buzzer, LOW);
delay(1000);
lcd.clear();
lcd.setCursor(0,0);
lcd.print("1.BJP  2.CONG");
lcd.setCursor(0,1);
lcd.print("3.JDS  4.RESULT");
while(1)  {
     if(digitalRead(sw1)==0)       {
       vote1++;
       voteSubmit(1);
       EEPROM.write(0, vote1);
       while(digitalRead(sw1)==0);
       return;
     }
     if(digitalRead(sw2)==0)                          {
       vote2++;
         voteSubmit(2);
         EEPROM.write(1, vote2);
       while(digitalRead(sw2)==0);
```

```
  return;
    }
    if(digitalRead(sw3)==0)    {
      vote3++;
        voteSubmit(3);
        EEPROM.write(2, vote3);
      while(digitalRead(sw3)==0);
      return;      }
}
```

Results & Conclusions

Snapshots of result

1. Overall representation

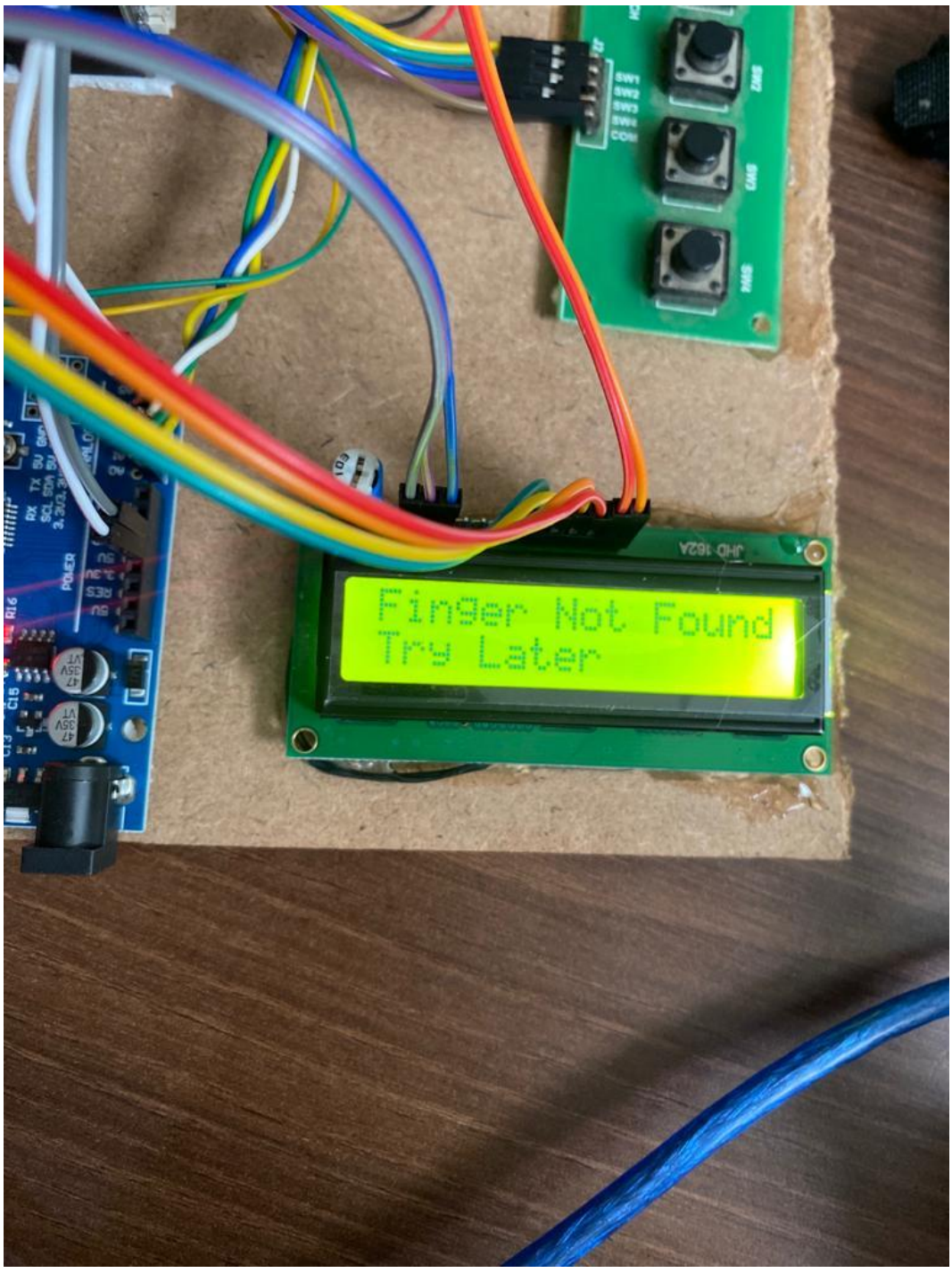


2. Fingerprint Enrolment: Eligible voters are registered by capturing their fingerprints using fingerprint scanners. The captured fingerprint data is processed and stored securely in a centralized database for future verification.

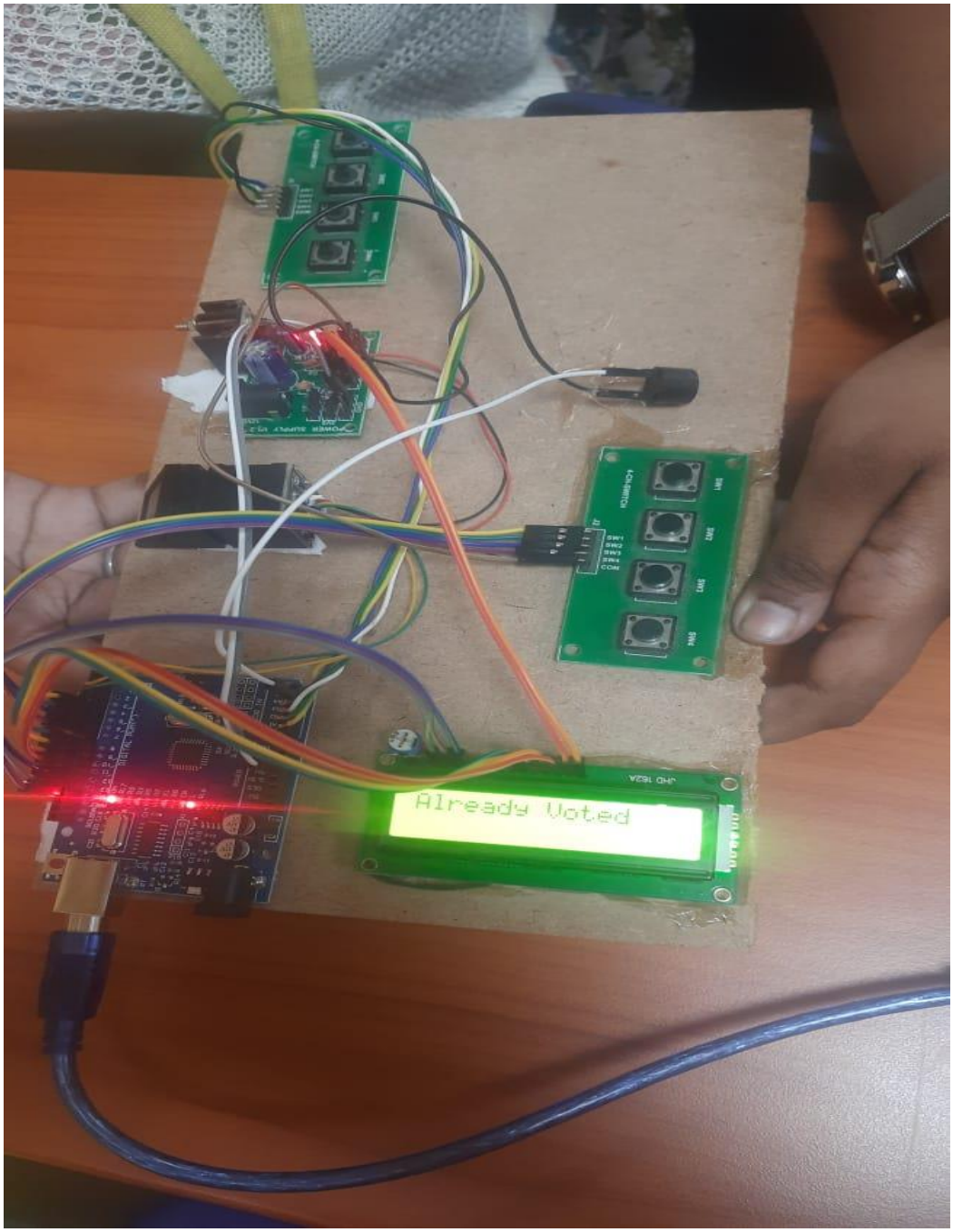
3. Real-time Fingerprint Matching: During the voting process, the system compares the captured fingerprint with the enrolled fingerprints in real-time. Advanced fingerprint matching algorithms, such as minutiae extraction and matching, are implemented to ensure accurate identification.

4. Voting Interface: Voter is given with candidate keys and they can choose one candidate

5. Fingerprint not registered: If the voter's fingerprint is not registered with voting system then LCD will display a message



6. Fraud detection: If the voter is trying to cast vote for second time then buzzer will give signal



7. Result analysis: Admin can view the result after casting vote.

Conclusion

In conclusion, the implementation of a fingerprint-based fraud detection voting system offers significant advancements in the security and integrity of the voting process. By leveraging the unique biometric characteristics of fingerprints, this system ensures accurate identification of voters and effectively detects fraudulent activities. Through the development and integration of fingerprint enrolment, real-time matching, fraud detection mechanisms, and a user-friendly interface, the voting system provides a robust solution. It enables authorized voters to cast their vote seamlessly while preventing unauthorized individuals from participating multiple times. The system's ability to integrate with existing voter registration databases further enhances its effectiveness and reliability. The administrator's access to comprehensive result analysis and reporting facilitates informed decision-making and ensures transparency in the electoral process. Through rigorous testing and evaluation, the system's functionality, accuracy, and security are validated, instilling confidence in its performance. Once deployed, ongoing maintenance and support are essential to ensure the system's continuous operation and adaptability to evolving needs.

Overall, the fingerprint-based fraud detection voting system addresses the critical challenges of voter authentication and fraud prevention. Its successful implementation significantly contributes to fair and trustworthy elections, safeguarding the democratic principles of transparency, accuracy, and inclusivity.

References

[1] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication 7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.

[2] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[3] International Journals of Biometric and Bioinformatics, Volume (3): Issue (1).

[4] Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar "Wireless Fingerprint Based Security System using Zigbee" , International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-5, April 2013.

[5] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[6] "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, Department of Computer Science and Enginnering, Michign State University. About Authors:A.Aditya Shankaris a final year undergraduate student, Dept. Of Electronics and Communication Engineering from Dadi Institute of Engineering and Technology, Visakhapatnam,Andhra Pradesh. His main areas of interest are Sensor Technology, Analog and Digital Circuits, Embedded Systems andWireless Communication &Networking.