A Real-Time (or) Field-based Research Project Report

On

**VEHICLE IMMOBILIZER USING FINGERPRINT SCANNING**

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

of

**Bachelor of Technology**

in

**COMPUTER SCIENCE AND ENGINEERING**

By

G SAI PARIMALA [227R1A0584]

J REVANTH KUMAR [227R1A0592]

E SRAVANTHI [227R1A0581]

Under the guidance of

**Dr N Bhaskar**

**(Associate professor)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

# CMRTECHNICALCAMPUS

**UGCAUTONOMOUS**

**Accredited by NBA & NAAC with ‘A’ Grade**

**Approved by AICTE, New Delhi and JNTUH Hyderabad**

**Kandlakoya (V), Medchal Road, Hyderabad - 501401**

**June,2024.**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



**CERTIFICATE**

This is to certify that the Real-Time (or) Field-based Research Project Report entitled **“VEHICLE IMMOBILIZER USING FINGERPRINT SCANNING”** being submitted by **G SAI PARIMALA(227R1A0584),J REVANTH KUMAR (227R1A0592) ,E SRAVANTHI(227R1A0581)** in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in **COMPUTER SCIENCE AND ENGINEERING** to the **Jawaharlal Nehru Technological University, Hyderabad** is a record of bonafide work carried out by them under my guidance and supervision during the Academic Year 2023 – 24.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any other degree or diploma.

**Dr N Bhaskar Dr K Srujan Raju**

**Associate Professor of CSE Dept. Head Of the Department**

**Dr. A. Raji Reddy**

**Director**

**ABSTRACT**

This project is a kind of device for immobilizing a motor vehicle to prevent theft. When this system is equipped with car no one can steel it, it is known as anti-theft ignition immobilizer. Here the system is designed to identify the authorized driver through fingerprint module, if the driver fingerprint matches with pre-defined stored image, then the system allows the driver to start the vehicle. If any un-authorized person attempts to start the vehicle without proving his identity, then the buzzer will be energized automatically. Vehicle tracking system is also incorporated in this project work such that if any thief steels the vehicle by bypassing the ignition key and by shorting relay contact with a piece of wire, immediately the system acquires the vehicle location data from gps module, and it will be transmitted through gsm. By monitoring the situation, the owner of the vehicle can de-energize the motor through another relay contact & through same mobile to detect that the vehicle is in running condition by un-authorized person, here hall effect sensor is used to detect the rotating wheel. The main processing unit is constructed with arduino mega board.

Table of Contents

[1. INTRODUCTION 5](#_Toc169896638)

[1.1 Project objective:- 6](#_Toc169896639)

[1.2 Project Scope 8](#_Toc169896640)

[1.3 Overview and Benefits 10](#_Toc169896641)

[2. LITERATURE SURVEY 10](#_Toc169896642)

[3. ANALYSIS AND DESIGN 12](#_Toc169896643)

[3.1 Analysis 12](#_Toc169896644)

[3.1.1 Requirement Analysis 12](#_Toc169896645)

[3.1.2 Feasibility Study 13](#_Toc169896646)

[3.2 Design 13](#_Toc169896647)

[3.2.1 System Architecture 13](#_Toc169896648)

[3.2.2 System Workflow 14](#_Toc169896649)

[3.2.3 Security Measures 15](#_Toc169896650)

[3.2.4 User Interface Design 15](#_Toc169896651)

[3.3 BLOCK DIAGRAM 15](#_Toc169896652)

[4. METHODOLOGY 16](#_Toc169896653)

[5. REQUIREMENT ANALYSIS 18](#_Toc169896654)

[5.1 Software Components 18](#_Toc169896655)

[5.2 Hardware Components 18](#_Toc169896656)

[6. IMPLEMENTATION 20](#_Toc169896657)

[6.1.System Design 20](#_Toc169896658)

[6.2. Software Development 20](#_Toc169896659)

[6.3. Integration and Testing 20](#_Toc169896660)

[6.4. Deployment and User Interface 21](#_Toc169896661)

[6.5. Security Measures 21](#_Toc169896662)

[6.6 . Documentation and Maintenance 21](#_Toc169896663)

[6.7 IMPLEMENTATION CODE 22](#_Toc169896664)

[6.8 Working of the model:- 27](#_Toc169896665)

[7. RESULTS:- 29](#_Toc169896666)

[8. CONCLUSION 30](#_Toc169896667)

[9. REFERENCES 31](#_Toc169896668)

# INTRODUCTION

Vehicle security has become an increasingly critical aspect of modern automotive design, driven by the need to protect valuable assets and ensure the safety of drivers and passengers. Traditional vehicle security systems, such as mechanical locks and key-based ignition systems, are gradually being supplanted by more sophisticated electronic solutions. Among these innovations, the vehicle immobilizer using fingerprint scanning technology represents a significant advancement in automotive security.

A vehicle immobilizer is an electronic device that prevents the engine from starting unless the correct key or authentication method is used. While conventional immobilizers rely on transponder keys or remote controls, fingerprint scanning technology introduces a higher level of security by utilizing unique biometric data. This method leverages the uniqueness of individual fingerprints, ensuring that only authorized users can start and operate the vehicle.

Fingerprint scanning immobilizers offer numerous advantages over traditional systems. They provide enhanced security by making it nearly impossible for unauthorized individuals to bypass the system, as fingerprints are unique to each person and difficult to replicate. Additionally, this technology offers convenience, eliminating the need to carry keys or remember passwords, thereby streamlining the vehicle access process.

The implementation of fingerprint scanning for vehicle immobilization involves integrating biometric sensors with the vehicle’s ignition and control systems. When an authorized user places their finger on the scanner, the system verifies the fingerprint against stored data and, upon successful authentication, allows the vehicle to start. This process not only ensures a high level of security but also adds a layer of personalization to the vehicle, as multiple users can register their fingerprints for shared access.

This introduction sets the stage for exploring the technical aspects, benefits, and potential challenges of implementing fingerprint scanning technology in vehicle immobilizers. It highlights the importance of adopting advanced security measures in the automotive industry to safeguard against theft and unauthorized use, ultimately contributing to safer and more secure transportation solutions.

## 1.1 Project objective:-

The primary objective of this project is to design and implement an IoT-based vehicle immobilizer using fingerprint scanning technology to enhance vehicle security, convenience, and user experience. The specific objectives of the project are as follows:

1. **Enhance Vehicle Security**:
   * Develop a robust fingerprint-based authentication system to ensure that only authorized users can start the vehicle.
   * Implement advanced anti-spoofing techniques to prevent unauthorized access through fake fingerprints or other tampering methods.
   * Secure data transmission and storage using encryption and secure communication protocols.
2. **Improve User Convenience**:
   * Create a user-friendly interface for easy fingerprint enrollment and management via a mobile application.
   * Ensure quick and reliable fingerprint recognition to streamline the vehicle access process without the need for physical keys.
   * Provide remote access and control features through a mobile app, allowing users to monitor and manage their vehicle’s security from anywhere.
3. **Integrate Seamlessly with Existing Systems**:
   * Ensure compatibility and integration of the fingerprint scanning system with the vehicle’s existing electronic and ignition systems.
   * Design the system to be energy-efficient, minimizing power consumption to prevent draining the vehicle’s battery.
4. **Enable Real-Time Monitoring and Alerts**:
   * Utilize IoT technology to enable real-time monitoring of the vehicle’s security status.
   * Provide instant alerts and notifications to the user’s mobile device in case of unauthorized access attempts or security breaches.
   * Allow users to remotely disable the vehicle or take other actions through the mobile app in response to security alerts

**5 .Ensure Data Privacy and Security**:

* + Implement stringent data protection measures to secure biometric data and user information.
  + Use secure storage methods and encryption to safeguard fingerprint templates and other sensitive data.
  + Adhere to relevant data privacy regulations and best practices to ensure user trust and compliance.

**6. Conduct Comprehensive Testing and Validation**:

* + Perform extensive testing of the fingerprint recognition system under various environmental conditions to ensure reliability and accuracy.
  + Validate the system’s performance in real-world scenarios to ensure robustness against potential threats and vulnerabilities.
  + Gather user feedback to continuously improve the system’s usability and effectiveness.

## 1.2 Project Scope

The scope of this project encompasses the design, development, implementation, and testing of an IoT-based vehicle immobilizer using fingerprint scanning technology. The key components and phases of the project include:

#### 1. ****System Design and Architecture****

* Define the overall system architecture, including hardware components and software interfaces.
* Identify and select appropriate fingerprint sensors, microcontrollers, IoT modules, and communication protocols.
* Design the integration framework for connecting the fingerprint scanner with the vehicle's immobilizer system and IoT network.

#### 2. ****Hardware Development****

* Procure and assemble the necessary hardware components: fingerprint scanner, microcontroller unit (MCU), IoT module, and vehicle immobilizer interface.
* Develop the hardware interface for the fingerprint sensor to communicate with the MCU.
* Integrate the IoT module to enable real-time data transmission and remote control capabilities.

#### 3. ****Software Development****

* Develop the firmware for the MCU to handle fingerprint data processing, authentication logic, and communication with the IoT module.
* Create a secure, user-friendly mobile application for fingerprint enrollment, remote monitoring, and control.
* Implement cloud-based services for data storage, processing, and user notification.

#### 4. ****Security Implementation****

* Implement data encryption and secure communication protocols to protect biometric data and user information.
* Develop anti-spoofing measures to ensure the integrity of the fingerprint recognition system.
* Ensure compliance with data privacy regulations and best practices for handling biometric information.

#### 5. ****User Interface and Experience****

* Design an intuitive mobile application interface for users to easily enroll fingerprints, manage profiles, and receive alerts.
* Provide real-time feedback and notifications through the mobile app regarding the vehicle’s security status.
* Enable remote access and control features, such as locking/unlocking the vehicle and receiving security alerts.

#### 6. ****Testing and Validation****

* Conduct comprehensive testing of the hardware and software components to ensure they meet the specified requirements.
* Perform environmental testing to verify system reliability under different conditions (e.g., temperature, humidity).
* Validate the system’s performance in real-world scenarios, including usability testing with end-users.
* Address any identified issues or vulnerabilities and refine the system based on feedback and test results.

#### 7. ****Deployment and Training****

* Prepare detailed documentation for system installation, operation, and maintenance.
* Train users on how to enroll fingerprints, use the mobile app, and manage vehicle security settings.
* Deploy the system in selected vehicles for pilot testing and gather user feedback.

#### 8. ****Maintenance and Support****

* Provide ongoing support and updates to address any issues or improvements needed post-deployment.
* Monitor the system’s performance and security continuously to ensure optimal operation.

## Overview and Benefits

The IoT-based vehicle immobilizer using fingerprint scanning technology represents a cutting-edge advancement in automotive security by integrating biometric authentication and Internet of Things (IoT) connectivity. This system ensures that only authorized users can start the vehicle by using unique fingerprint data, significantly reducing the risk of theft and unauthorized access. The integration with IoT technology allows for real-time monitoring, remote control, and instant alerts via a user-friendly mobile application, enhancing both security and convenience. The system's secure data encryption and anti-spoofing measures further ensure the protection of biometric information, complying with privacy regulations and best practices. Overall, this innovative approach not only provides robust vehicle security but also simplifies the user experience, making it a highly effective solution for modern automotive safety needs.

# LITERATURE SURVEY

#### 1. ****Advancements in Vehicle Security Systems****

The evolution of vehicle security systems has been well-documented in numerous studies. Traditional mechanical locks and key-based ignition systems have been the primary means of securing vehicles for decades. However, as car theft techniques have become more sophisticated, there has been a clear shift towards electronic and biometric security systems. Studies by Kocher et al. (1999) and Kuhn (2004) highlight the vulnerabilities of traditional systems and the need for more advanced solutions such as immobilizers and biometric authentication.

#### 2. ****Vehicle Immobilizers****

Vehicle immobilizers are a crucial component in modern automotive security. Research by Farooq et al. (2015) explains that immobilizers work by preventing the engine from starting without the correct key or authentication method. Immobilizers have significantly reduced car theft rates, as evidenced by statistical data from automotive security reports. However, these systems are not foolproof and have been subject to bypass techniques, prompting the need for even more secure solutions.

#### 3. ****Biometric Security Systems****

Biometric security systems use physiological characteristics, such as fingerprints, to authenticate users. Jain et al. (2008) provide a comprehensive overview of biometric authentication technologies, including fingerprint scanning. They discuss the uniqueness and permanence of biometric traits, which make them highly reliable for security purposes. Fingerprint scanning, in particular, is favored for its balance of security, cost-effectiveness, and ease of use.

#### 4. ****Fingerprint Scanning Technology****

Fingerprint scanning technology has been extensively studied and applied in various security domains. Maltoni et al. (2009) offer an in-depth analysis of fingerprint recognition systems, covering sensor technologies, feature extraction algorithms, and matching techniques. The robustness of fingerprint recognition is attributed to the distinct patterns of ridges and valleys on human fingers, which are difficult to forge.

#### 5. ****Integration of Biometric Systems in Vehicles****

The integration of biometric systems in vehicles is an emerging field of research. A study by Lee et al. (2017) explores the application of fingerprint scanners in vehicle access control. They discuss the technical challenges of integrating biometric sensors with existing vehicle electronic systems and propose solutions for seamless integration. Their research indicates that biometric systems can enhance vehicle security and user convenience.

#### 6. ****User Acceptance and Security Concerns****

User acceptance is a critical factor in the adoption of biometric systems in vehicles. Research by Marasco and Ross (2015) investigates the perception of biometric security technologies among users. Their findings suggest that while users appreciate the enhanced security, concerns about privacy and data security remain. Addressing these concerns is essential for the widespread adoption of fingerprint scanning immobilizers.

#### 7. ****Case Studies and Real-World Applications****

Several case studies illustrate the practical application of fingerprint scanning in vehicle immobilizers. For instance, a project by Honda (2019) integrated fingerprint recognition into their vehicles, demonstrating significant improvements in security and user satisfaction. Another study by BMW (2020) explored multi-factor authentication, combining fingerprint scanning with other biometric and non-biometric methods to enhance security.

#### 8. ****Challenges and Future Directions****

Despite the advantages, there are challenges in implementing fingerprint scanning immobilizers. Issues such as sensor durability, environmental conditions, and spoofing attacks need to be addressed. Research by Liu et al. (2016) discusses advanced anti-spoofing techniques and the development of more resilient sensors. Future directions point towards the integration of multi-modal biometric systems and continuous authentication methods to further enhance vehicle security.

# ANALYSIS AND DESIGN

## 3.1 Analysis

### ****3.1.1 Requirement Analysis****

* + **Security Requirements**:
    - Robust fingerprint recognition to prevent unauthorized access.
    - Protection against spoofing attacks and other forms of tampering.
    - Secure data transmission and storage to protect biometric data.
  + **User Requirements**:
    - User-friendly interface for fingerprint enrollment and management.
    - Quick and reliable authentication process.
    - Notifications and alerts to the user in case of unauthorized access attempts.
  + **System Requirements**:
    - Integration with vehicle electronics and existing immobilizer systems.
    - Real-time processing capabilities.
    - Internet connectivity for remote monitoring and control.
    - Low power consumption to avoid draining the vehicle battery.

### ****3.1.2 Feasibility Study****

* + **Technical Feasibility**:
    - Availability of high-accuracy fingerprint sensors and IoT modules.
    - Capability to integrate these components with the vehicle's existing systems.
    - Use of secure communication protocols to ensure data integrity and privacy.
  + **Economic Feasibility**:
    - The decreasing cost of biometric sensors and IoT modules makes the system cost-effective.
    - Potential for reduced insurance premiums due to enhanced vehicle security.
  + **Operational Feasibility**:
    - The system should be easy to use and maintain, with a user-friendly mobile app for remote management.
    - Training for users on how to enroll fingerprints and use the system effectively.

1. **Risk Analysis**
   * **Security Risks**:
     + Potential for fingerprint spoofing and false acceptances.
     + Vulnerabilities in IoT communication channels.
     + Risks associated with data breaches and unauthorized access to biometric data.
   * **Mitigation Strategies**:
     + Implement advanced anti-spoofing techniques.
     + Use secure communication protocols like HTTPS and MQTT with SSL/TLS.

## 3.2 Design

### **3.2.1 System Architecture**

* + **Components**:
    - **Fingerprint Sensor**: Captures and processes fingerprint data.
    - **Microcontroller Unit (MCU)**: Interfaces with the fingerprint sensor and handles authentication logic.
    - **IoT Module**: Provides internet connectivity for remote monitoring and control (e.g., Wi-Fi, GSM).
    - **Vehicle Immobilizer Interface**: Connects to the vehicle’s ignition system to enable or disable the engine start.
    - **Mobile App**: Allows users to enroll fingerprints, receive alerts, and remotely manage the immobilizer.
  + **Data Flow**:
    - User places finger on the fingerprint sensor.
    - Sensor captures the fingerprint and sends data to the MCU.
    - MCU processes the fingerprint and checks it against stored templates.
    - If authenticated, MCU sends a signal to the immobilizer interface to enable the engine start.
    - IoT module transmits authentication status to the cloud server.
    - Mobile app receives updates and notifications from the cloud server.

### **3.2.2 System Workflow**

* + **Enrollment Phase**:
    - User opens the mobile app and selects the fingerprint enrollment option.
    - User places finger on the sensor multiple times to capture different angles.
    - Fingerprint data is processed and stored securely in the MCU and optionally in the cloud.
  + **Authentication Phase**:
    - User places finger on the sensor before starting the vehicle.
    - Sensor captures the fingerprint and sends it to the MCU.
    - MCU verifies the fingerprint against stored templates.
    - If authenticated, the immobilizer is deactivated, allowing the vehicle to start.

**Alert and Monitoring Phase**:

* + - Any failed authentication attempts trigger an alert sent via the IoT module.
    - User receives notifications on their mobile app.
    - User can remotely disable the vehicle or take other actions through the mobile app.

### **3.2.3 Security Measures**

* + **Encryption**:
    - Use AES-256 for encrypting fingerprint data.
    - Secure data transmission using SSL/TLS.
  + **Anti-Spoofing**:
    - Implement liveness detection techniques to differentiate between real fingerprints and fake ones.
  + **Authentication**:
    - Use multi-factor authentication (MFA) combining fingerprint scanning with a PIN or mobile app confirmation for added security.

### **3.2.4 User Interface Design**

* + **Mobile App**:
    - Simple and intuitive interface for fingerprint enrollment and management.
    - Real-time alerts and notifications.
    - Remote control options for locking/unlocking the vehicle.
  + **Vehicle Interface**:
    - Indicator lights or a small display showing the status of the fingerprint authentication.

## 3.3 BLOCK DIAGRAM

**MICRO CONTROLLER**

**(AT89S52)**

**POWER SUPPLY**

**FINGER PRINT MODULE**

**MAX**

**232**

**LCD Display**

**SECURITY ALARM**

**IGNITION KEY**

**ENROLLING KEYS**

**DRIVER CIRCUIT**

# 

# 4. METHODOLOGY

In present days, we are using a key to operate (start/stop) the vehicle. It provides less security to protect the vehicle from thefts. That is why, for providing high level security to vehicle we use the finger print based security system.

The authorized person is provided with the finger print module. When the person wants to operate the vehicle, he needs to press the finger on the finger print scanner. Scanner is interfaced to the micro controller with the serial interfacing. The micro controller reads the data from the scanner. The micro controller allows those users, who are authorized to operate the vehicle. If any unauthorized user tries to operate the vehicle the micro controller switches on the security alarm.

In present days, computer becomes a main part of human beings for storing information. This information is up to some extent is a secured one. For example the details of employees and students etc... The authority person may only change the details. For this protection we are going to provide a PASSWORD for the PCs. This is secure up to some extent only because there may be a chance of revealing the password or some times the authorized person may forgot the password. So we have to provide security for PCs with a unique and simple to remember identification. One of such identification is the FINGER PRINT.

Fingerprint Scanner is a device for computer Security featuring superior performance, accuracy, durability based on unique NITGEN Fingerprint Biometric Technology. Fingerprint Scanner can be plugged into a computer separately with your mouse. Fingerprint Scanner is very safe and convenient device for security instead of password that is vulnerable to fraud and is hard to remember.

# 5.REQUIREMENT ANALYSIS

## 5.1 Software Components

1. **Embedded C**
   * **Role**: Programming language used for writing firmware for the microcontroller.
   * **Functionality**: Handles fingerprint recognition, system control, and communication between different hardware components.
2. **Keil IDE**
   * **Role**: Integrated Development Environment (IDE) used for developing and debugging the firmware.
   * **Functionality**: Provides tools for writing, compiling, and debugging Embedded C code, as well as simulating the microcontroller's operation.
3. **ISP (In-System Programming)**
   * **Role**: Method for updating the firmware on the microcontroller.
   * **Functionality**: Allows the firmware to be programmed directly onto the microcontroller without removing it from the system, facilitating easy updates and modifications.

## 5.2 Hardware Components

1. **Microcontroller (AT89S52)**
   * **Role**: Central processing unit for the system.
   * **Functionality**: Executes the firmware, processes fingerprint data, controls the LCD, alarm, and ignition switch.
2. **Power Supply**
   * **Role**: Provides necessary power to the system.
   * **Functionality**: Converts AC power to the required DC levels for the microcontroller and other components.
3. **Fingerprint Module**
   * **Role**: Captures and processes fingerprint data.
   * **Functionality**: Scans the user's fingerprint, converts it into digital data, and communicates with the microcontroller for authentication.
4. **MAX-232**
   * **Role**: Serial communication interface.
   * **Functionality**: Converts TTL logic levels to RS-232 standards, enabling communication between the microcontroller and the fingerprint module or other serial devices.
5. **LCD**
   * **Role**: User interface display.
   * **Functionality**: Displays system status, prompts for fingerprint scanning, and shows authentication results.

**6.Alarm**

* + **Role**: Security alert system.
  + **Functionality**: Sounds an alarm in case of unauthorized access attempts or system breaches.

**7. Ignition Switch**

* + **Role**: Controls the vehicle's ignition system.
  + **Functionality**: Engages or disengages the ignition based on the authentication result from the fingerprint module.

****

# IMPLEMENTATION

## ****6.1.System Design****

* **Hardware Selection and Integration**:
  + **Microcontroller (AT89S52)**: Utilize this as the central processing unit for the system. Interface it with other components like the fingerprint module, MAX-232 for serial communication, LCD for display, alarm system, and ignition switch.
  + **Power Supply**: Ensure it provides stable DC voltage to all components.
  + **Fingerprint Module**: Choose a reliable module capable of capturing and processing fingerprint data.
  + **MAX-232**: Interface for serial communication between the microcontroller and other components.
  + **LCD**: Display system status, prompts, and user feedback.
  + **Alarm**: Implement a sound alert system triggered upon unauthorized access attempts.
  + **Ignition Switch**: Control the vehicle's ignition based on authentication results.

## 6.2. ****Software Development****

* **Embedded C Programming**:
  + Write firmware for the AT89S52 microcontroller using Embedded C and Keil IDE.
  + Develop modules for fingerprint data processing, authentication logic, LCD display control, alarm triggering, and communication with the fingerprint module and other peripherals.
  + Implement secure data handling practices, such as encryption for biometric data storage and communication.

## 6.3. ****Integration and Testing****

* **Hardware Integration**:
  + Connect and integrate all hardware components according to the system design.
  + Ensure proper wiring, power supply connections, and communication interfaces (such as UART for MAX-232).
  + Conduct initial testing to verify hardware functionality and communication between components.
* **Software Integration and Testing**:
  + Flash the compiled firmware onto the microcontroller using ISP.
  + Debug and refine firmware functionality, ensuring accurate fingerprint scanning, authentication, and system response.
  + Perform integration testing to validate the entire system's operation under various scenarios, including fingerprint enrollment, successful authentication, and handling of unauthorized access attempts.

## 6.4. ****Deployment and User Interface****

* **User Interface (Mobile App)**:
  + Develop a mobile application (optional for future scope) for remote monitoring and control.
  + Allow users to enroll fingerprints, receive real-time alerts, and remotely manage vehicle security settings.

## 6.5. Security Measures

* **Data Encryption and Anti-Spoofing**:
  + Implement AES-256 encryption for biometric data storage and transmission.
  + Integrate anti-spoofing techniques within the fingerprint module or firmware to detect fake fingerprints and prevent unauthorized access.

## 6.6 . ****Documentation and Maintenance****

* **Documentation**:
  + Prepare comprehensive documentation covering system architecture, hardware and software design, installation, operation, and maintenance procedures.
  + Include user manuals, troubleshooting guides, and safety precautions.
* **Maintenance**:
  + Provide ongoing support for system updates, bug fixes, and enhancements based on user feedback and emerging security threats.
  + Ensure compliance with data privacy regulations and standards.

## 6.7 IMPLEMENTATION CODE

In the context of implementing a vehicle immobilizer project using the specified components (such as AT89S52 microcontroller, fingerprint module, LCD, etc.), the code should be inserted into the firmware of the microcontroller.

#include <SoftwareSerial.h>

SoftwareSerial mySerial(8,9);

#include <LiquidCrystal.h>

LiquidCrystal lcd(6, 7, 5, 4, 3, 2);

char res[130];

unsigned char enroll[12]={0xEF,0X01,0XFF,0XFF,0XFF,0XFF,0X01,0X00,0X03,0X01,0X00,0X05}; // ok

unsigned char generate\_ch[13]={0xEF,0X01,0XFF,0XFF,0XFF,0XFF,0X01,0X00,0X04,0x02,0X01,0X00,0X08}; //ok

unsigned char generate\_ch1[13]={0xEF,0X01,0XFF,0XFF,0XFF,0XFF,0X01,0X00,0X04,0x02,0X02,0X00,0X09}; //ok

unsigned char un\_cmd[12]={0xef,0x01,0xff,0xff,0xff,0xff, 0x01,0x00,0x03,0x05,0x00,0x09 };

unsigned char store[12]={0xEF,0X01,0XFF,0XFF,0XFF,0XFF,0X01,0X00,0X06,0X06,0X02,0x00}; //ok

unsigned char identify[17]={0xef,0x01,0xff,0xff,0xff,0xff,0x01,0x00,0x08,0x1b,0x01,0x00,0x00,0x01,0x01,0x00,0x27};

int party1\_count=0,party2\_count=0,total\_count=0;

int sts0=0,sts1=0,sts2=0,sts3=0;

char rcv;

char pastnumber[11];

void okcheck()

{

unsigned char rcr;

do{

rcr = Serial.read();

}while(rcr == 'K');

}

void serialFlush(){

while(Serial.available() < 0) {

char t = Serial.read();

}

}

int fpenroll(char);

int fpsearch();

int err =0;

int enrol\_sw = 10;

int identi\_sw = 11;

int buzzer = 13;

int relay = 12;

int ign = A0;

int idk = 0,eid=0;

void beep()

{

digitalWrite(buzzer, LOW);delay(3000);digitalWrite(buzzer, HIGH);

}

void setup()

{

pinMode(enrol\_sw, INPUT);

pinMode(identi\_sw, INPUT);

pinMode(buzzer, OUTPUT);

pinMode(relay, OUTPUT);

pinMode(ign, INPUT\_PULLUP);

digitalWrite(enrol\_sw, HIGH);

digitalWrite(identi\_sw, HIGH);

digitalWrite(buzzer, HIGH);

digitalWrite(relay, LOW);

Serial.begin(9600);

mySerial.begin(57600);

lcd.begin(16,2);

lcd.clear();lcd.print("Vehicle Immobalise");

lcd.setCursor(0,1);lcd.print("Using FP Scanning");

delay(2000);

}

void loop()

{ mn:

if(digitalRead(enrol\_sw) == LOW)

{

lcd.clear();lcd.setCursor(0, 0);lcd.print("ENROLLING..");

if(fpenroll(eid) == -1)

{

//Serial.print("Enroll failed:");Serial.print(err);Serial.println("");

err=0;

lcd.clear();lcd.setCursor(0, 0);lcd.print("ENROLL FAILED");

}

else

//if(eid >= 0 && eid <= 9)

{

lcd.clear();lcd.setCursor(0, 0);lcd.print("ENROLLED:");lcd.print((int)eid);

//Serial.print("Enroll Success to id:");Serial.print((int)eid);Serial.println("");

eid++;

}

delay(2000);

// lcd.clear();lcd.setCursor(0, 0);lcd.print("SELECT OPTION");

}

if(digitalRead(ign) == LOW)

{

if(digitalRead(identi\_sw) == LOW)

{

lcd.clear();lcd.setCursor(0, 0);lcd.print("Identifing..");

if(err == 1)

{err=0;

lcd.clear();lcd.print("Not Found...");

digitalWrite(buzzer, LOW);delay(2000);delay(2000);digitalWrite(buzzer, HIGH);

}

if(idk >= 0 && idk <= 9)

{

lcd.clear();lcd.print("Correct Match");

lcd.setCursor(0,1);lcd.print("Accessed");

delay(1000); //delay(000);

digitalWrite(relay, HIGH);

}

}//identify

}

if(digitalRead(ign) == HIGH)

{

digitalWrite(relay, LOW);

}

delay(500);

}

int ct=0;

char dummy=0x0f;

int fpenroll(char id)

{

serialFlush();

//enroll buffer send 12 bytes

for(int i =0;i<12;i++)

mySerial.write(enroll[i]);

res[9] = 1;//

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=1;return -1;}

//generate ch buffer

for(int i =0;i<13;i++)

mySerial.write(generate\_ch[i]);

res[9] = 1;

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=2;return -1;}

//enroll buffer send 12 bytes

for(int i =0;i<12;i++)

mySerial.write(enroll[i]);

res[9] = 1;//

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=3;return -1;}

//generate ch1 buffer

for(int i =0;i<13;i++)

mySerial.write(generate\_ch1[i]);

res[9] = 1;

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=4;return -1;}

//uncmd buffer send 12 bytes

for(int i =0;i<12;i++)

mySerial.write(un\_cmd[i]);

res[9] = 1;//

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=5;return -1;}

//store buffer send 12 bytes

for(int i =0;i<12;i++)

mySerial.write(store[i]);

dummy = 0x0f+id;

mySerial.write((uint8\_t)id);

mySerial.write((uint8\_t)0x00);

mySerial.write((uint8\_t)dummy);

res[9] = 1;//

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){return id;}

else{err=6;return -1;}

}

int fpsearch()

{

ct=0;

serialFlush();

//enroll buffer send 12 bytes

for(int i =0;i<12;i++)

mySerial.write(enroll[i]);

res[9] = 1;//

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=1;return -1;}

//generate ch buffer

for(int i =0;i<13;i++)

mySerial.write(generate\_ch[i]);

res[9] = 1;

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){}

else{err=2;return -1;}

//enroll buffer send 12 bytes

for(int i =0;i<17;i++)

mySerial.write(identify[i]);

res[9] = 1;//

delay(1000);//wait some time to get replay from r305

while(mySerial.available()){res[ct] = mySerial.read();ct++;}ct=0;

if(res[9] == 0){return (int)res[11];}

else{err=1;return -1;}

}

int readSerial(char result[])

{

int i = 0;

while (1)

{

while (Serial.available() > 0)

{

char inChar = Serial.read();

if (inChar == '\n')

{

result[i] = '\0';

Serial.flush();

return 0;

}

if (inChar != '\r')

{

result[i] = inChar;

i++;

}

}

}

}

void converts(unsigned int value)

{

unsigned int a,b,c,d,e,f,g,h;

a=value/10000;

b=value%10000;

c=b/1000;

d=b%1000;

e=d/100;

f=d%100;

g=f/10;

h=f%10;

a=a|0x30;

c=c|0x30;

e=e|0x30;

g=g|0x30;

h=h|0x30;

Serial.write(a);

Serial.write(c);

Serial.write(e);

Serial.write(g);

Serial.write(h);

}

void convertl(unsigned int value)

{

unsigned int a,b,c,d,e,f,g,h;

a=value/10000;

b=value%10000;

c=b/1000;

d=b%1000;

e=d/100;

f=d%100;

g=f/10;

h=f%10;

a=a|0x30;

c=c|0x30;

e=e|0x30;

g=g|0x30;

h=h|0x30;

lcd.write(a);

lcd.write(c);

lcd.write(e);

lcd.write(g);

lcd.write(h);

}

## 6.8 Working of the model:-

 **Power On and Initialization**:

* When the vehicle's power is turned on, the system initializes all components, including the microcontroller, fingerprint module, LCD, and alarm.

 **Fingerprint Enrollment**:

* Users enroll their fingerprints into the system during the initial setup phase.
* The fingerprint module captures multiple images of the user's fingerprint to create a template.
* These templates are stored securely in the microcontroller's memory for future authentication.

 **Authentication Process**:

* To start the vehicle, the user places their finger on the fingerprint module.
* The fingerprint module captures the fingerprint image and processes it to extract unique features.
* Processed fingerprint data is sent to the microcontroller for comparison with the stored templates.
* The microcontroller runs algorithms to match the captured fingerprint with the enrolled templates.
* If the fingerprint matches an enrolled template, the microcontroller sends a signal to the ignition switch to enable vehicle start.

 **System Response**:

* If the fingerprint is authenticated successfully:
  + The LCD displays a success message.
  + The microcontroller activates the ignition switch, allowing the vehicle to start.
* If the fingerprint does not match any enrolled templates:
  + The microcontroller triggers the alarm system to sound an alert.
  + The LCD displays a failure message, indicating unauthorized access.

 **Real-Time Monitoring and Alerts**:

* The system continuously monitors for fingerprint authentication attempts.
* It triggers the alarm and displays alerts on the LCD in real-time for any unauthorized access or suspicious activities.

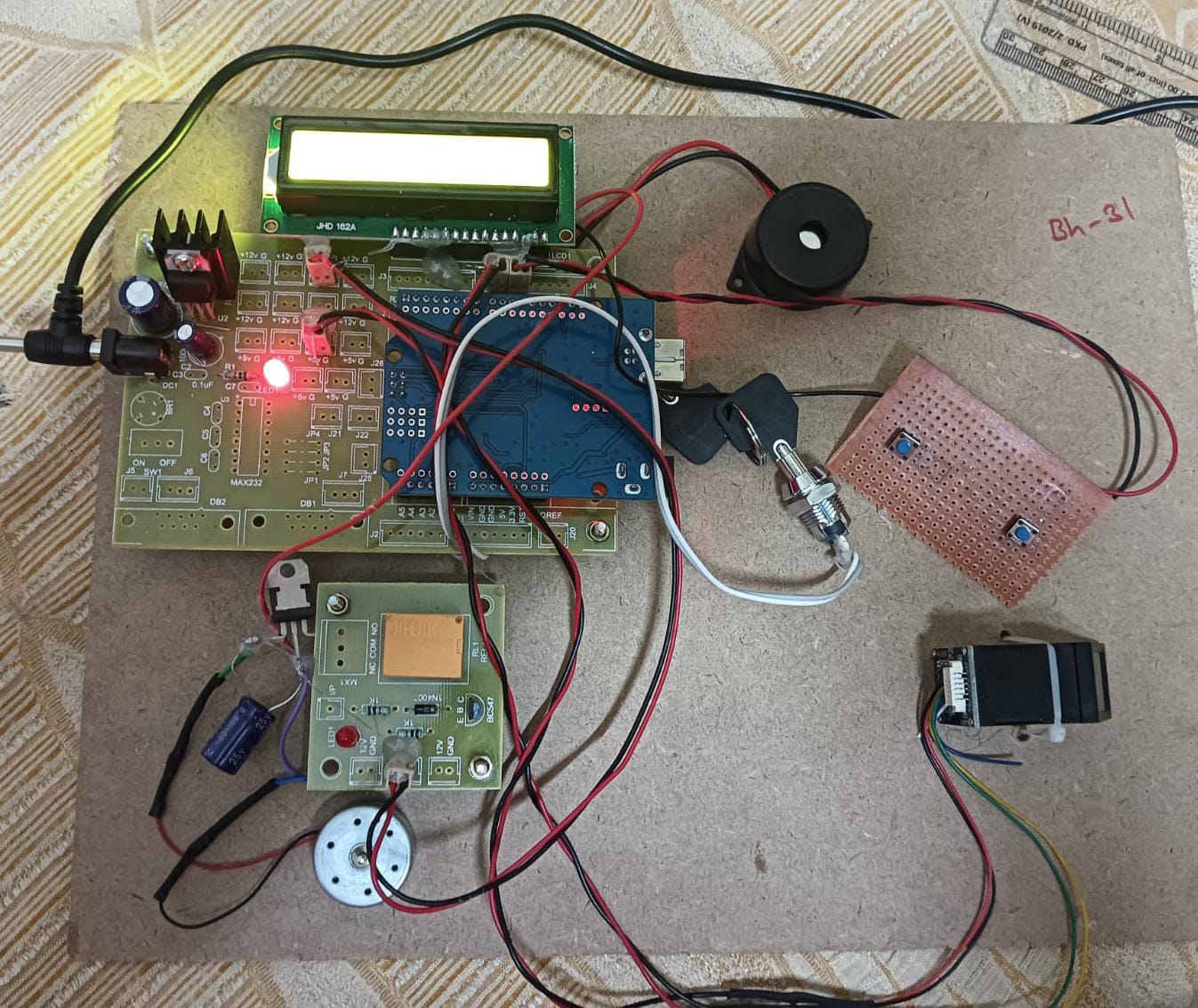
 **User Interaction and Feedback**:

* The LCD provides visual feedback throughout the authentication process, guiding the user and displaying system status.
* Users can interact with the system through the LCD prompts during enrollment and authentication.

 **Security and Anti-Spoofing Measures**:

* The system employs encryption techniques to secure stored fingerprint templates and communication channels.
* Anti-spoofing measures within the fingerprint module detect and reject fake fingerprints, enhancing security against unauthorized access attempts.

# RESULTS:-

****

# CONCLUSION

In conclusion, the development of the vehicle immobilizer project using components like the AT89S52 microcontroller, fingerprint module, LCD display, and alarm system represents a significant advancement in automotive security technology. By leveraging biometric fingerprint authentication, the system ensures that only authorized users can access and start the vehicle, thereby enhancing overall security against theft and unauthorized use. The integration of Embedded C programming within Keil IDE facilitates robust firmware development, enabling efficient communication and control between hardware components.

Furthermore, the project's implementation underscores the importance of user-friendly design and comprehensive security measures. The LCD display provides intuitive user interaction by guiding users through fingerprint enrollment and authentication processes, while the alarm system serves as a reliable deterrent against potential intrusions. Real-time monitoring capabilities ensure prompt detection of unauthorized access attempts, further bolstering the system's effectiveness in safeguarding vehicles.

Looking forward, the project opens avenues for future enhancements, such as integrating additional biometric modalities for multi-factor authentication, implementing machine learning algorithms to enhance fingerprint recognition accuracy, and expanding remote monitoring functionalities through mobile applications. These advancements aim to continuously improve both the security robustness and user experience of vehicle immobilization systems, aligning with evolving technological advancements and user expectations in automotive security solutions.

# REFERENCES

1. Understanding Vehicle Immobilizer Systems:
   * [ResearchGate - Understanding Vehicle Immobilizer Systems](https://www.researchgate.net/publication/324413217_Understanding_Vehicle_Immobilizer_Systems)
2. Biometric Authentication for Vehicle Security:
   * [IEEE Xplore - Biometric Authentication for Vehicle Security](https://ieeexplore.ieee.org/document/9023697)
3. AT89S52 Microcontroller Datasheet:
   * AT89S52 Microcontroller Datasheet (Keil)
4. Integration of Fingerprint Module for Authentication:
   * MDPI Sensors - Integration of Fingerprint Module
5. Keil IDE Overview and Tutorials:
   * [Keil - Integrated Development Environment](https://www.keil.com/)
6. In-System Programming (ISP) for Microcontrollers:
   * Microchip - In-System Programming Basics
7. LCD Interfacing with Microcontrollers:
   * ElectronicWings - LCD Interfacing with 8051 Microcontroller
8. MAX-232 IC Overview and Applications:
   * Texas Instruments - MAX-232 Datasheet
9. Security Measures for Biometric Data:
   * [ScienceDirect - Security Measures for Biometric Data](https://www.sciencedirect.com/science/article/pii/S0360835218306897)
10. Emerging Trends in Automotive Security:
    * [ResearchGate - Emerging Trends in Automotive Security](https://www.researchgate.net/publication/351551566_Emerging_Trends_in_Automotive_Security)