International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-Jun-2026, ISSN (Online): 2395-566X

Vehicle Theft Protection

Mrs. Vidyashree B.P Assistant Professor
Manjunath A J, Pradeep Nagavath, Shreyank S D, Poorna Chandra Thejaswi M D
Dept of ECE, PESCE, Mandya

Abstract- Vehicle theft remains a significant concern worldwide, especially in urban areas where vehicle density is high and traditional security systems are often insufficient. This project presents a cost-effective and intelligent Vehicle Theft Protection System that enhances vehicle security through biometric authentication and real-time user intervention using GSM communication. The core of the system is built around the Arduino UNO microcontroller, interfaced with a fingerprint sensor module (R305S), a GSM module (SIM800L), and a relay module to control the ignition system. Authorized users register their fingerprints in the system memory. Upon an unauthorized access attempt, the system sends an SMS alert to the vehicle owner, who can remotely allow or deny engine start. The proposed system provides a high-speed, reliable, and cost-effective solution for automotive embedded security applications.

Keywords- Vehicle Theft Protection, Arduino UNO, Fingerprint Authentication, GSM Module, SIM800L, R305S Sensor, Relay Module, Biometric Security, Embedded Systems, SMS Alert, Ignition Control, Buzzer, Low-Cost Security, Real-Time Monitoring.

I. INTRODUCTION

Vehicle theft is a growing concern globally, posing a significant threat to both individual vehicle owners and commercial transportation systems. Despite advancements in conventional vehicle security systems such as mechanical locks, immobilizers, and car alarms, experienced thieves often find ways to bypass them. As a result, there is a pressing need for more advanced, intelligent, and user-controlled security solutions that can prevent unauthorized vehicle access and provide real-time monitoring and response capabilities.

This project introduces a microcontroller-based Vehicle Theft Protection System that leverages biometric authentication using a fingerprint sensor, combined with GSM-based communication for remote owner intervention. The system is designed to permit only authorized users to start the vehicle, thereby ensuring enhanced security.

The system provides a high-speed, reliable, and cost-effective solution for modern embedded and automotive security applications.

II. LITERATURE SURVEY

Patel & Rajan (2025):

The authors integrated AI with IoT sensors and GSM modules to detect unusual behavior and block vehicle operation. Their system also sends owner alerts via SMS and a mobile app. This work reinforced the practicality of GSM-based alerts and owner decision-making for our design.

Lakshmi & Sravani (2020):

This project used multiple sensors including vibration, GPS, and GSM to detect theft and notify the user through SMS. Although feature-rich, it lacked biometric authentication and real-time user control. This encouraged our use of GSM alerting while focusing on biometric access and owner permission via SMS rather than complex multi-sensor integration.

Sonawane & More (2019):

Combined fingerprint authentication with GSM-based alerts to detect unauthorized users. However, the system lacked a confirmation mechanism from the owner before enabling ignition..This helped structure our fingerprint-based security logic and led us to implement owner confirmation via SMS to allow or deny engine start after an unauthorized attempt.

Bhosale & Nerkar (2017):

Focused on GPS tracking and SMS alerts to inform the owner about vehicle movement during theft. It did not include

biometric security or physical access restriction. This influenced the integration of GSM-based messaging in our system, combined with fingerprint access control for higher security.

III. PROBLEM STATEMENT AND OBJECTIVES

Conventional vehicle security systems are vulnerable to theft due to lack of biometric verification and remote user control. There is a pressing need for a smart, low-cost solution that restricts unauthorized access and alerts the owner in real time. Current vehicle security solutions are not fully effective in preventing theft and often fail to provide real-time updates to the owner. This creates a need for a smarter system that can both detect and restrict unauthorized access ensuring that only verified users are able to start the vehicle.

1. To implement fingerprint authentication for secure vehicle access.
2. To send SMS alerts to the owner using a GSM module upon unauthorized access.
3. To enable the owner to remotely allow or deny vehicle ignition via SMS.
4. To control ignition through a relay based on fingerprint match and owner's approval.

IV. DESIGN METHODOLOGY

The Vehicle Theft Protection System is developed using the Arduino UNO as the central microcontroller. The design integrates a fingerprint sensor module (R305S), a GSM module (SIM800L), a relay module for ignition control, and a buzzer for audible alerts along with status LEDs.

The R305S optical fingerprint sensor stores registered fingerprint templates in onboard non-volatile Flash memory. When a user attempts to start the vehicle, the fingerprint is scanned and compared against stored templates. A multiplexer-like decision structure selects the action based on the match result. Low-power and efficient design techniques are incorporated by activating only the required modules during each operation phase.

This methodology ensures reliable biometric verification while maintaining real-time communication and efficient hardware utilization.

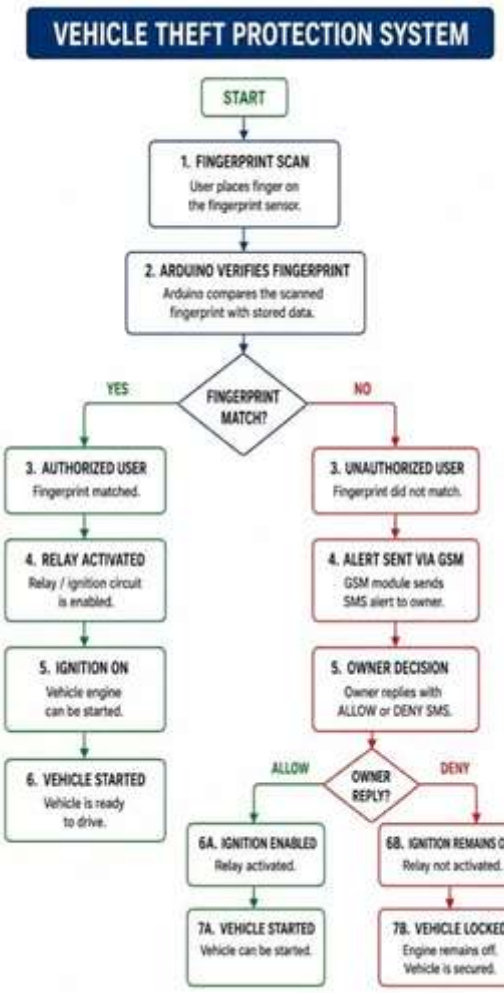

Figure 1: Flowchart of Vehicle Theft Protection System

Block Diagram

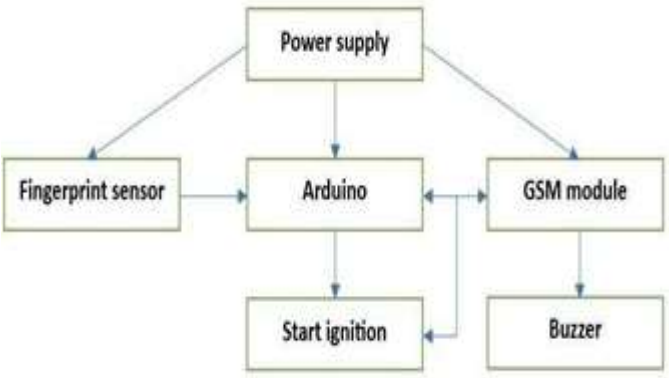

Figure 2: Block Diagram of Vehicle Theft Protection

V. RESULTS AND ANALYSIS

The proposed Vehicle Theft Protection System was successfully designed, implemented, and verified using Arduino IDE and Tinkercad simulation. The architecture integrates fingerprint authentication, GSM-based communication, and relay-controlled ignition into a single cohesive framework. Functional verification was carried out using the Arduino serial monitor, and the results confirmed the correct execution of all operations for various input combinations.

The fingerprint sensor successfully enrolled and verified authorized user fingerprints. When a registered fingerprint (ID: 101) was placed on the sensor, the system confirmed a match, activated the relay, and enabled the ignition. The serial monitor output confirmed: Fingerprint Matched – Authorized User Detected – Relay ON, Vehicle Ignition Started – SMS Sent: Vehicle Started Successfully.

For an unauthorized fingerprint (ID: 333), the relay remained OFF and the ignition was locked. The GSM module immediately dispatched an SMS alert to the registered owner. The owner was given 30 seconds to respond with either YES or NO to allow or deny engine start.

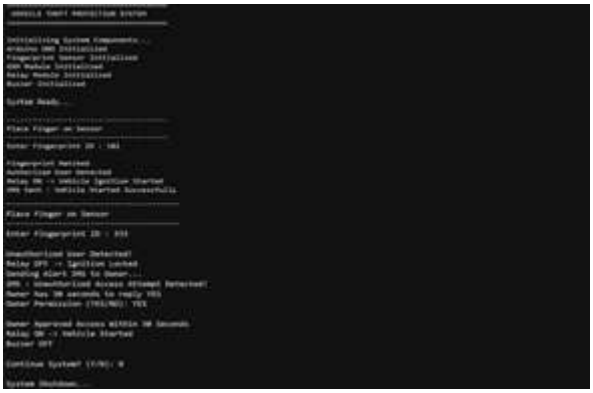

Figure 3: Result of Vehicle Theft Protection System

To improve security, the Telegram bot dashboard was integrated to provide real-time notification delivery and remote control functionality. When the owner replies YES, the system grants temporary access, activates the relay, and allows the vehicle to start. If the owner replies NO, access is denied, the relay remains OFF, the ignition stays locked, and the buzzer turns ON to indicate a security threat.

Simulation results demonstrated the successful operation of all system functions under different test conditions. The results confirmed that the proposed design achieved a balance between reliable biometric authentication and real-time remote control. The integration of biometric authentication with GSM-based owner intervention enhanced overall system performance while maintaining design reliability.

The developed Vehicle Theft Protection System provides an efficient solution for modern vehicles, embedded systems, and automotive security applications.

Acknowledgment

We thank the Department of Electronics and Communication Engineering, PES College of Engineering, Mandya, for providing the resources and support required for the successful completion of this project. We express our sincere gratitude to our guide, faculty members, and laboratory staff for their valuable guidance and encouragement throughout the project.

REFERENCES

1. N. Patel and A. R. Rajan, "AI-Enabled Smart Vehicle Theft Detection and Control Using IoT and GSM," International Journal of Embedded Systems and Applications, vol. 13, no. 1, pp. 12–18, Jan. 2025.
2. B. Lakshmi and S. Sravani, "Advanced Vehicle Security System with Theft Control and Accident Notification," IJITEE, vol. 9, no. 6, pp. 1043–1047, Apr. 2020.
3. T. D. Sonawane and P. V. More, "Smart Vehicle Security System Using Biometric and GSM Technology," IRJET, vol. 6, no. 3, pp. 982–985, Mar. 2019.
4. M. J. Bhosale and A. A. Nerkar, "Vehicle Theft Detection and Prevention Using GSM and GPS," IJERA, vol. 7, no. 1, pp. 51–54, Jan. 2017.
5. K. Ramesh and A. Kumar, "Design and Implementation of GSM Based Vehicle Theft Control System," IJET, vol. 8, no. 2, pp. 132–136, Feb. 2016.
6. S. K. Mandal and R. S. Pawar, "Vehicle Protection System Using Microcontroller," International Journal of Engineering Research, vol. 4, no. 3, pp. 78–82, 2015.
7. A. Kumar and R. Mishra, "IoT-Enabled Smart Vehicle Anti-Theft System with Real-Time Tracking and Remote Engine Immobilization Using ESP32," IJESAT, vol. 26, no. 3, pp. 148–154, Mar. 2026.

8. S. Sharma, M. Verma, and R. Gupta, "IoT-Based Smart Vehicle Security System Using GPS and GSM," IEEE Access, vol. 11, pp. 51233–51245, 2023.