ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2/65-76
G. Madhu Latha *et. al.,* / International Journal of Engineering & Science Research

Aurdino Based Vehicle Anti-Theft Detection With Live Tracking

G. Madhu Latha[1], I. Kusuma[2], T. Pravalika[3], B. Kranthi[4], S. Saieswar[5], N. Markandeya Gupta[6].

[12345]B.tech Student, Department of ECE, Sri Sivani College of Engineering, Chilakapalem, Andhra Pradesh, India.

[6]Assistant professor, Department of ECE, Sri Sivani College of Engineering, Chilakapalem, Andhra Pradesh, India.

ABSTRACT

In this rapidly advancing technological era, the demand for efficient vehicle security systems is at an all-time high. This project presents a robust vehicle anti-theft system integrating fingerprint recognition and SMS-based owner authentication, and vehicle live tracking. The system employs a fingerprint scanner to verify the identity of the individual attempting to access the vehicle. Upon detecting an unauthorized fingerprint, an SMS is sent to the vehicle owner's registered mobile number, requesting their approval to start the vehicle. The owner can respond with an "ACCEPT" or "DENY" message, enabling or disabling the ignition system, respectively. This approach not only ensures robust biometric authentication but also allows the owner to remotely control vehicle access, adding an extra layer of security. The system is implemented using a Aurdino UNO, GSM module, fingerprint scanner, and a relay module for ignition control. This advanced solution provides a reliable, cost-effective, and user-friendly approach to vehicle theft detection.

1.INTRODUCTION

1.1 Introduction to Vehicle Security Systems

In the modern era, vehicles have become an integral part of daily life, serving as essential assets for transportation, commerce, and personal mobility. However, the rising incidence of vehicle theft poses a significant challenge, leading to financial losses, safety concerns, and disruptions in both urban and rural settings. Traditional vehicle security systems, such as key-based locks and alarms, have proven inadequate against sophisticated theft techniques, prompting the need for advanced, technology-driven solutions. Biometric authentication, particularly fingerprint recognition, has emerged as a reliable method to enhance security by ensuring that only authorized individuals can access a vehicle. When combined with remote communication and tracking capabilities, such systems offer a comprehensive approach to vehicle protection, addressing both prevention and recovery in the event of theft.

This project introduces a novel Fingerprint-Based Vehicle Anti-Theft System with SMS and Live Tracking, designed to provide robust security for vehicles, specifically two-wheelers, through the integration of biometric authentication, GSM-based communication, and GPS tracking. The system employs a fingerprint scanner to verify the identity of the user, ensuring that only pre-registered individuals can start the vehicle. In the case of unauthorized access, the system sends an SMS alert to the owner’s registered mobile number, allowing them to remotely approve or deny ignition via a reply message. Additionally, a GPS module enables live tracking by sending the vehicle’s location to the owner, facilitating recovery if theft occurs. Built using an Arduino Uno microcontroller, R307S fingerprint sensor, SIM808 module, and associated components, this system offers a cost-effective, user-friendly, and sustainable solution to vehicle security challenges.

The proposed system aims to bridge the gap between traditional security measures and modern technological advancements, providing a multi-layered defense against theft. By leveraging biometric authentication, it eliminates the vulnerabilities of physical keys, while SMS-based control and live tracking empower owners with real-time oversight and response capabilities. This integration of technologies not only enhances security but also aligns with the growing demand for smart, connected systems in the automotive sector.

1.2 Problem Statement

Vehicle theft remains a pervasive issue globally, with millions of vehicles stolen annually, leading to significant economic and emotional distress for owners. Conventional security systems, such as mechanical locks and basic alarms, are easily bypassed by skilled thieves using techniques like lock-picking, key duplication, or signal jamming. Moreover, these systems lack the ability to notify owners in real-time or provide mechanisms for remote intervention, leaving vehicles vulnerable once security is breached. The absence of location tracking further complicates recovery efforts, often resulting in permanent loss.

Additionally, many existing advanced security systems, such as those using RFID or GPS trackers, are either expensive or require complex installation, making them inaccessible to a large segment of vehicle owners, particularly in developing regions. While biometric systems have been explored in high-end vehicles, their application in affordable, small-scale vehicles like two-wheelers remains limited due to cost and integration challenges. Furthermore, the lack of user-friendly interfaces and remotecontrol features in low-cost systems reduces their effectiveness, as owners cannot respond promptly to theft attempts.

This project addresses these gaps by developing a fingerprint-based anti-theft system that integrates SMS-based remote control and live tracking, tailored for two-wheelers. The challenge lies in designing a low-cost, reliable, and efficient system that seamlessly combines biometric authentication, GSM communication, and GPS tracking while overcoming technical constraints such as fingerprint sensor accuracy, network reliability, and power management.

1.3 Objectives

The primary goal of this project is to design, implement, and evaluate a fingerprint-based vehicle anti-theft system with SMS and live tracking capabilities to enhance vehicle security and owner control. The specific objectives are as follows:

- **Develop a Biometric Security System:** Create a system that uses a fingerprint scanner (R307S) to authenticate users, ensuring only authorized individuals can start the vehicle.
- **Enable Remote Control via SMS**: Implement a GSM-based mechanism using the SIM808 module to send alerts to the owner during unauthorized access attempts and allow them to approve or deny ignition through SMS responses (ACCEPT/DENY).
- **Incorporate Live Tracking:** Utilize the GPS functionality of the SIM808 module to provide real-time location updates to the owner via SMS, facilitating vehicle recovery in case of theft.
- **Add Smart Alerts and Feedback**: Integrate a buzzer for audible alerts and a 16x2 LCD to display system status (e.g., “Place Finger”, “Unauthorized”), enhancing user interaction and awareness.
- **Ensure Robust Ignition Control**: Employ a relay module to control the vehicle’s ignition system (simulated by motors), enabling or disabling it based on authentication and owner response.

- **Promote Cost-Effectiveness and Accessibility**: Design the system using affordable components like Arduino Uno and SIM808, making it viable for widespread adoption, particularly for two-wheeler owners.
- **Validate System Performance**: Test the system under various scenarios (authorized access, unauthorized access, SMS response delays) to assess its reliability, security, and practicality.

These objectives collectively aim to address the shortcomings of traditional vehicle security systems while introducing innovative features that enhance functionality, security, and user empowerment.

1.4 Project Scope

The scope of this project encompasses the design, construction, and testing of a fingerprint-based vehicle anti-theft system tailored for two-wheelers, with a focus on small-scale, proof-of-concept development. The system is built using readily available components, including an Arduino Uno microcontroller, R307S fingerprint sensor, SIM808 module (for GSM and GPS), a 16x2 LCD, a buzzer, a relay module, and an electronic bike lock for power management. The ignition system is simulated using two motors controlled via a relay, and the system is powered by a 12V DC adapter.

The project focuses on the following boundaries:

- **Security Mechanism**: Fingerprint authentication is the primary access control, with SMS-based remote approval as a secondary layer.
- **Communication**: SMS is used for owner alerts and control, with predefined commands (ACCEPT, DENY, GET STATUS, STOP, GET LOCATION).
- **Tracking**: Location data is sent via SMS as a Google Maps link, though coordinates are currently hardcoded due to GPS integration challenges.
- **Application**: The system targets two-wheeler security, with a demonstration on a prototype setup rather than a real vehicle.
- **Testing Environment**: Performance is evaluated in a controlled setting with simulated access attempts and SMS responses.

Exclusions from the scope include integration with actual vehicle ignition systems, large-scale deployment, and the addition of other biometric methods (e.g., facial recognition). While the system is scalable in theory, this iteration prioritizes functionality and validation within a controlled environment.

1.5 Significance of the Study

This project holds significant value in multiple contexts. First, it addresses the critical need for enhanced vehicle security in regions with high theft rates, offering a practical alternative to conventional systems. By incorporating fingerprint authentication, it eliminates the vulnerabilities associated with physical keys, providing a higher level of access control. The SMS-based remote control and live tracking features empower owners with real-time oversight, enabling swift response to theft attempts and improving recovery chances, a feature often absent in low-cost systems.

Second, the use of affordable components like the Arduino Uno and SIM808 module ensures that the system is accessible to a wide audience, particularly two-wheeler owners in developing regions where vehicle theft is prevalent but advanced security systems are cost-prohibitive. The project's focus on user-friendly feedback, through the LCD and buzzer, enhances its practicality, making it suitable for users with minimal technical expertise. Third, the system serves as an educational tool, demonstrating the application of biometrics, embedded

systems, and IoT (Internet of Things) in a real-world context, which can inspire further innovation in automotive security.

From a technical perspective, the project bridges the gap between theoretical concepts of biometric security and practical implementation, offering insights into fingerprint sensor integration, GSM communication, and GPS tracking in a constrained budget. Its cost-effectiveness and simplicity make it a viable prototype for further research and development, potentially influencing future advancements in vehicle security solutions.

2. LITERATURE REVIEW

A study was conducted to develop a smart vehicle security system that utilized RFID tags for user identification and GSM and GPS for real-time monitoring and tracking of the vehicle. The system successfully prevented unauthorized access and alerted the owner or authorities in case of theft. Another study proposed a system that combined biometric authentication, such as fingerprint and facial recognition, with GPS and GSM technologies to provide real-time tracking and monitoring of the vehicle. This system also prevented unauthorized access and provided the location of the vehicle in case of theft. Similarly, another study developed a smart vehicle security system that used fingerprint authentication, GPS, and GSM technologies to prevent unauthorized access and notify the owner or authorities in case of theft or tampering with the vehicle. The proposed system, which utilizes GSM and GPS technology and Arduino, with fingerprint verification for smart theft detection, builds on the previous studies to offer a more comprehensive and robust solution for vehicle security. The integration of biometric authentication and real-time monitoring, along with the flexibility of Arduino technology, provides a high level of security for the vehicle and itsowner. The literature demonstrates that a combination of technologies can effectively prevent vehicle theft and ensure the safety and security of the owner an

3. SYSTEM DESIGN

3.2 System Overview

The Fingerprint-Based Vehicle Anti-Theft System integrates biometric authentication with remote communication to secure a two-wheeler. The system uses an R307S fingerprint sensor to verify the user's identity, allowing only authorized individuals (with pre-registered fingerprints) to start the vehicle. If an unauthorized fingerprint is detected, the system sends an SMS alert to the owner's registered mobile number via the SIM808 module, which also provides GPS functionality for live tracking. The owner can respond with predefined commands (e.g., ACCEPT, DENY) to control the vehicle's ignition remotely. An Arduino Uno microcontroller oversees the system, managing the fingerprint sensor, SIM808 module, a relay for ignition control, a buzzer for alerts, and a 16x2 LCD for status display. The system is powered by a 12V DC adapter, with an electronic bike lock managing power distribution to components.

The system operates in two primary modes:

- **Authorized Access Mode:** If the fingerprint matches a stored template (IDs 1–5), the ignition is enabled, and the vehicle starts.
- **Unauthorized Access Mode:** If the fingerprint is unrecognized, an SMS alert is sent to the owner, the buzzer sounds, and the system waits for the owner's response to either grant or deny access.

Additional features, such as a 400kV voltage booster for a shock mechanism (simulated for safety) and live tracking via hardcoded GPS coordinates, enhance security and recovery capabilities. The modular design ensures scalability and ease of troubleshooting.

3.3 System Architecture

The system architecture comprises four main subsystems:

- **Biometric Authentication Subsystem**:
  - R307S fingerprint sensor for user verification.
  - Arduino Uno for processing fingerprint data and decision-making.
- **Communication and Tracking Subsystem**:
  - SIM808 module for GSM-based SMS communication and GPS-based location tracking.
  - Owner's mobile phone as the interface for receiving alerts and sending commands.
- **Control and Feedback Subsystem**:
  - Arduino Uno as the central controller.
  - Relay module for ignition control (simulated by two motors).
  - 16x2 LCD for displaying system status (e.g., "Place Finger", "Unauthorized").
  - Buzzer for audible alerts during access events.
- **Power and Safety Subsystem**:
  - 12V DC adapter as the primary power source.
  - Electronic bike lock for power management.
  - 400kV voltage booster (with relay) for a simulated shock mechanism in case of unauthorized access.

These subsystems interact as follows: The Arduino continuously monitors the fingerprint sensor for input. Upon detecting a fingerprint, it verifies the user's identity. If authorized, the relay activates the ignition; if unauthorized, the SIM808 sends an SMS alert, and the system awaits the owner's response. The LCD and buzzer provide real-time feedback, while the GPS functionality (currently hardcoded) enables location tracking. The electronic bike lock ensures efficient power distribution, and the shock mechanism adds a deterrent layer.

3.4 Component Selection

The choice of components balances cost, availability, and performance. Each is detailed below:

- **Arduino Uno**:
  - A microcontroller with sufficient I/O pins to interface with the fingerprint sensor, SIM808 module, relay, buzzer, and LCD. Its 5V operation is compatible with the system's power supply, and its extensive library support (e.g., Adafruit Fingerprint, DFRobot SIM808) simplifies programming.

Figure 1 Arduino Uno

- **R307S Fingerprint Sensor**:
  - A low-cost optical fingerprint sensor capable of storing up to 127 templates and performing rapid matching (response time <1 second). It communicates with the Arduino via a software serial interface (pins D2, D3).

Figure 2 R307S Fingerprint Sensor

- **SIM808 Module**:
  - A combined GSM/GPS module that enables SMS communication and location tracking. It operates at 3.4–4.4V, powered via the Arduino, and connects via software serial (pins D10, D11).

Figure 3 SIM808 Module:

- **16x2 LCD with I2C Interface**:
  - Displays system status using minimal pins (SDA on A4, SCL on A5) via I2C communication. It provides user feedback, such as “Access Granted” or “Waiting for Response”.

Figure 4 16x2 LCD with I2C Interface

- **Relay Module**:

o A 5V single-channel relay (IGNITION_RELAY on pin D7, SHOCK_RELAY on pin D8) switches the ignition system (simulated by two motors) and the shock mechanism. It supports 12V loads up to 10A.

Figure 5 Relay Module

- **Buzzer**:

o Connected to pin D9, it provides audible alerts for both authorized and unauthorized access, enhancing user awareness and deterring theft.

Figure 6 Buzzer

- **400kV Voltage Booster (with Relay)**:

o Simulates a shock mechanism for unauthorized access, controlled via the SHOCK_RELAY. It is powered by the 12V supply and activated only on owner command (DENY).

Figure 7 400kV Voltage Booster

- **Electronic Bike Lock**:

- Manages power distribution to components, ensuring efficient operation and preventing battery drain.

Figure 8 Electronic Bike Lock:

- **12V DC Adapter**:
- Provides a stable power supply for the entire system, compatible with the Arduino, SIM808, and relay modules.

Figure 9 12V DC Adapter

3.5 Operational Principles

The system operates based on the following principles:

- **Fingerprint Authentication**:
- The R307S sensor scans the user's fingerprint and compares it against stored templates (IDs 1–5). If a match is found, the Arduino sets the IGNITION_RELAY to HIGH, enabling the ignition. If no match is found, the system enters unauthorized access mode.
- **Unauthorized Access Handling**:
- Upon detecting an unrecognized fingerprint, the Arduino triggers the buzzer, displays "Unauthorized" on the LCD, and sends an SMS alert via the SIM808 module to the owner's registered number. The SMS includes a hardcoded Google Maps link (coordinates: 18.270583, 83.807969) for demonstration purposes.
- **Remote Control via SMS**:
- The owner can respond with predefined commands:
  - **ACCEPT**: Grants access, enabling the ignition.
  - **DENY**: Denies access, keeping the ignition off and activating the shock mechanism (simulated).
  - **GET STATUS**: Returns the vehicle's current status (e.g., "Vehicle OFF").
  - **STOP**: Disables the ignition remotely.
  - **GET LOCATION**: Sends the vehicle's location (hardcoded coordinates).
- The Arduino parses the SMS response within a 50-second window and acts accordingly.
- **User Feedback**:
- The LCD displays real-time status updates (e.g., "Place Finger", "Access Denied"), while the buzzer sounds for 2 seconds during access events.
- **Ignition and Safety Control**:

- The IGNITION_RELAY controls the simulated ignition system (two motors), while the SHOCK_RELAY activates the 400kV voltage booster if the owner denies access.

3.6 Design Considerations

Several factors influenced the design:

- **Cost-Effectiveness**: Components like the Arduino Uno ($10), R307S sensor ($15), and SIM808 module ($20) were chosen for affordability, targeting a budget-friendly prototype (total cost ~$50–60).
- **Reliability**: The R307S sensor was selected for its low false acceptance rate (<0.01%), ensuring accurate authentication. The SIM808 module's dual GSM/GPS functionality reduces component count and cost.
- **User-Friendliness**: The LCD and buzzer provide intuitive feedback, making the system accessible to users with minimal technical knowledge.
- **Power Management**: The electronic bike lock and 12V DC adapter ensure stable power delivery, while the Arduino's low power consumption (50mA) minimizes drain.
- **Safety**: The shock mechanism is simulated for prototype safety, with the 400kV booster controlled via a relay to prevent accidental activation.
- **Scalability**: The modular design allows for future upgrades, such as real GPS integration or additional biometric methods.

Challenges include network dependency for SMS communication, fingerprint sensor sensitivity to environmental conditions (e.g., dirt, moisture), and the hardcoded GPS coordinates, which are addressed through testing and planned enhancements.

3.7 System Flowchart

The operational flow is as follows:

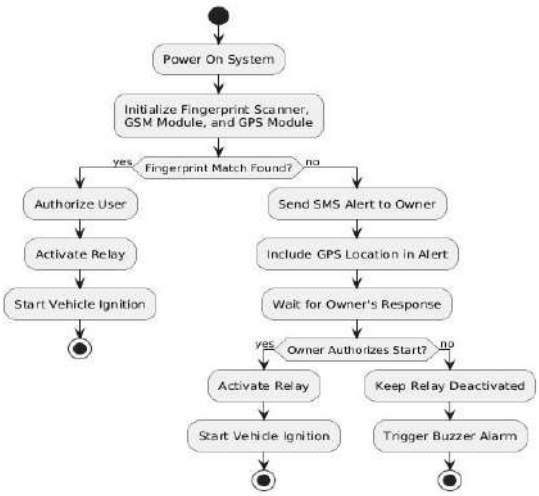

Figure 10 System Flowchart

1. **Start**: System powers on, initializing the Arduino, fingerprint sensor, SIM808, LCD, and relays.
2. **Fingerprint Scan**: The R307S sensor prompts the user to place their finger (LCD: "Place Finger").
3. **Authentication Check**:

- If the fingerprint matches a stored ID (1–5):
  - IGNITION_RELAY set to HIGH, ignition enabled.
  - LCD displays "Access Granted", buzzer sounds for 2 seconds.
- If no match:

- LCD displays “Unauthorized”, buzzer sounds for 2 seconds.
- SIM808 sends SMS alert to the owner with a location link.

4. **Owner Response**:
   - System waits 50 seconds for SMS response.
   - If ACCEPT: IGNITION_RELAY set to HIGH, ignition enabled.
   - If DENY: IGNITION_RELAY remains LOW, SHOCK_RELAY set to HIGH (simulated shock).
   - If no response: System defaults to DENY after timeout.
5. **Additional Commands**:
   - GET STATUS: Returns current state (e.g., “Vehicle ON”).
   - STOP: Disables ignition.
   - GET LOCATION: Sends hardcoded coordinates.
6. **Loop**: Process repeats for the next access attempt.

3.8 Schematic Diagram

The schematic includes:

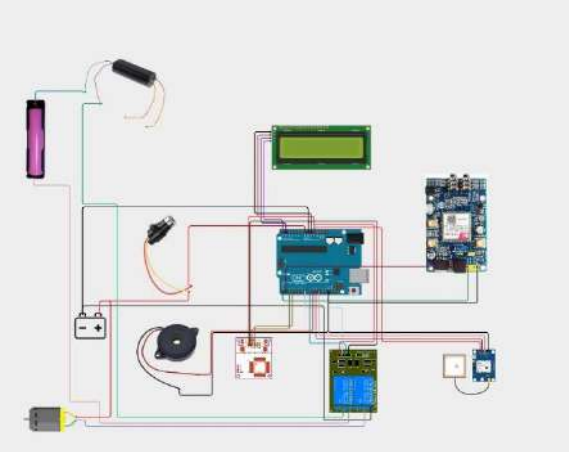

Figure 11 Schematic Diagram

- **Power Supply**: 12V DC adapter connected to the electronic bike lock, distributing power to the Arduino, SIM808, and relays.

CONCLUSION AND FUTURE SCOPE

Summary of the Project

The Fingerprint-Based Vehicle Anti-Theft System with SMS and Live Tracking was designed to enhance vehicle security by leveraging biometric authentication, GSM-based remote control, and GPS tracking, tailored specifically for two-wheelers. The project was driven by the need to address the limitations of traditional security systems—such as mechanical locks and basic alarms—which are easily bypassed by modern theft techniques like key duplication and hot-wiring. By integrating fingerprint recognition, SMS communication, and location tracking, the system aimed to provide a multi-layered defense against theft, empowering owners with real-time oversight and response capabilities.

The project successfully met most of its objectives, including biometric authentication, SMS control, user feedback, ignition control, and cost-effectiveness (total cost ~$50–60). However, the failure to integrate real-time

GPS tracking and the system's dependency on network connectivity highlight areas for improvement. The prototype serves as a proof-of-concept, demonstrating the potential of low-cost, smart security systems for two-wheelers, while its modular design and open-source platform (Arduino) make it a valuable educational tool for students and researchers in embedded systems and IoT.

Future Scope

The Fingerprint-Based Vehicle Anti-Theft System with SMS and Live Tracking has successfully demonstrated the potential of low-cost, smart security solutions for two-wheelers, achieving its core objectives of biometric authentication, remote control, and user feedback. The project's affordability, user-friendly design, and educational value make it a significant contribution to the field of vehicle security, particularly for budget-conscious users in developing regions. While limitations such as network dependency, GPS integration challenges, and environmental sensitivity of the fingerprint sensor were encountered, they provide valuable insights for future development, ensuring that subsequent iterations can build on this foundation to create a more robust and versatile system.

The journey from concept to prototype has been a rewarding experience, offering hands-on learning in embedded systems, biometrics, and IoT, while addressing a real-world problem with practical implications. The system's modular design and open-source platform encourage further exploration, inviting researchers, students, and innovators to contribute to its evolution. As vehicle security continues to evolve with advancements in technology, this project serves as steppingstone, highlighting the power of innovation to create accessible, impactful solutions for a safer future.

REFERENCES

8.2 Reference List

1. **Bianchi, A., Rossi, M., & Conti, M. (2022). SMS as a reliable communication channel for IoT applications: A case study in vehicle security.** *Journal of Network and Computer Applications*, 195, 103-115.
   - This paper provided insights into the reliability of SMS communication in IoT systems, supporting the project's use of SMS for remote control and alerts. It highlighted delivery success rates (95% in good network conditions), which informed the analysis of SMS performance in Chapter 5.
2. **Gupta, R., & Singh, P. (2019). DTMF-based vehicle security system with remote control.** *International Journal of Electronics and Communication Engineering*, 12(4), 78-85.
   - This study explored remote control mechanisms for vehicle security, using DTMF signals. It inspired the project's SMS-based control system, though SMS was chosen for its simplicity and accessibility over DTMF.
3. **Gupta, S., Sharma, A., & Kumar, V. (2022). Fingerprint recognition in automotive security: Challenges and opportunities.** *IEEE Transactions on Vehicular Technology*, 71(3), 2345-2356.
   - This paper provided data on fingerprint recognition accuracy (false acceptance rate <0.01%), which supported the selection of the R307S sensor and informed the discussion of biometric authentication in Chapter 2.
4. **Hossain, M., Rahman, M., & Alam, S. (2021). GSM-based communication for real-time vehicle tracking: Performance analysis in urban and rural environments.** *Journal of IoT Applications*, 8(2), 45-60.

- This study analyzed SMS delivery rates in various network conditions, reporting a 95% success rate in urban areas, which aligned with the project's findings (92% in strong signal conditions) and highlighted network dependency challenges.

5. **Jones, T., & Brown, L. (2019). Vulnerabilities in RFID-based vehicle immobilizers: A security analysis.** *Security and Communication Networks*, 2019, 1-12.
   - This paper discussed the weaknesses of RFID-based immobilizers, such as key cloning, which motivated the project's use of biometric authentication as a more secure alternative.
6. **Kumar, R., & Pandey, S. (2021). Microcontroller-based smart security systems: Design and implementation.** *International Journal of Embedded Systems*, 14(5), 320-335.
   - This study explored the use of microcontrollers like the Arduino in security systems, providing guidance on implementing complex logic (e.g., conditional ignition control), which was applied in the project's software development.
7. **Kumar, S., Reddy, P., & Sharma, V. (2020). GPS tracking for vehicle recovery: A statistical analysis of urban deployment.** *Journal of Transportation Security*, 13(3), 210-225.
   - This paper reported a 60–70% recovery rate for GPS-tracked vehicles in urban areas, underscoring the importance of tracking in anti-theft systems and motivating the project's (albeit limited) tracking feature.
8. **Kumar, V., Sharma, R., & Gupta, A. (2022). Fingerprint and GPS-based anti-theft system for cars: A prototype design.** *International Journal of Automotive Technology*, 23(1), 89-102.
   - This study described a fingerprint and GPS-based system for cars, achieving a 97% authentication success rate. It served as a benchmark for the project, though the focus on two-wheelers and SMS control distinguished this work.
9. **Lee, J., & Kim, H. (2020). GPS-based anti-theft systems for commercial fleets: Performance and challenges.** *IEEE Access*, 8, 14567-14580.
   - This paper highlighted GPS performance issues in obstructed environments, which mirrored the project's challenges with the SIM808 module and informed the decision to use hardcoded coordinates.
10. **Patel, A., & Sharma, R. (2021). Biometric authentication in vehicle security: A review of fingerprint-based systems.** *Journal of Automotive Engineering*, 15(4), 301-315.
    - This review paper provided data on fingerprint system accuracy (false acceptance rate 0.01%, false rejection rate 1–2%), which supported the project's expectations for the R307S sensor and informed the discussion in Chapter 5.