AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2)(2025)

SMART VEHICLE SECURITY SYSTEM USING GPS, GSM ALERTS, AND FINGERPRINT-BASED ACCESS CONTROL

[1]M.Manoj Kumar,[2] B.Saipranay,[3] M.Venugopal,[4] G.Srikanth,[5] D.Dileep, [6] N.Ravindar
[1,2,3,4,5] *B. Tech Students, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*
[6] *Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301, Email:* nravindar89@ gmail.com

ABSTRACT
By integrating fingerprint verification and real-time tracking, the Anti-Theft Defence of Vehicle systems with GSM, GPS, as well as Fingerprint Verification aims to increase vehicle security. In order to supply a comprehensive anti-theft solution, this system incorporates a fingerprint sensor for driver identification, GPS for position monitoring, GSM for communication, and other components including an LCD display, relay, DC drive, and buzzer. This device greatly enhances the security of vehicles and helps prevent theft by limiting access to only authorized persons and providing real-time monitoring and notifications.

Keywords: Anti-theft, vehicle security, fingerprint verification, biometric authentication, real-time tracking, alert system.

I. INTRODUCTION

Vehicle theft has become a significant global concern, with millions of vehicles reported stolen each year, posing serious economic and personal security challenges. Traditional vehicle security mechanisms such as mechanical locks, steering locks, alarm systems, and conventional ignition keys have proven increasingly ineffective against modern theft techniques [4], [7]. These methods can often be bypassed easily, offering limited protection against unauthorized access. With advancements in embedded systems and communication technologies, more intelligent and secure vehicle protection solutions have emerged to address these limitations [1], [3].

One such advanced solution is the integration of GSM (Global System for Mobile Communications), GPS (Global Positioning System), and biometric fingerprint recognition technologies for vehicle security. Several studies have demonstrated that combining location tracking with biometric authentication significantly enhances vehicle theft prevention and recovery capabilities [1], [2], [5]. Biometric fingerprint verification provides a highly reliable and unique form of authentication, ensuring that only authorized users can access and operate the vehicle, thereby reducing the risk of unauthorized usage [6], [9].

This project aims to design and implement a comprehensive anti-theft protection system by integrating fingerprint-based biometric verification with GSM and GPS technologies. The primary objective is to deliver an advanced security framework that restricts vehicle ignition exclusively to authenticated users while enabling real-time vehicle location tracking in the event of theft [1], [3], [8]. The incorporation of GSM technology facilitates instant alert notifications and two-way communication between the vehicle and the owner, allowing timely responses to suspicious activities or intrusion attempts [2], [6]. Additionally, the GPS module provides continuous location updates, assisting vehicle owners and law enforcement agencies in tracking and recovering stolen vehicles efficiently [5], [7]. Furthermore, the system integrates auxiliary components such as a relay module for engine immobilization, a DC motor to simulate engine control, an LCD display for status information, and a buzzer for audible alerts. These components collectively enhance user interaction and system responsiveness by providing immediate visual and auditory feedback during authentication failures or theft attempts [4], [9]. Overall, the proposed system leverages modern biometric and communication technologies to offer a robust, reliable, and intelligent vehicle anti-theft solution

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com

capable of addressing the shortcomings of traditional security systems [1], [7].

II. LITERATURE SURVEY

1. A Vehicle Theft Detection and Controlling System Based on Internet of Things, P. V. Kiran, M. K. Ghosh, and A. S. Shinde, 2019

This paper presents an IoT-based vehicle theft detection and control system that integrates GPS, GSM, and microcontrollers for real-time vehicle monitoring. The proposed system enables vehicle owners to track the vehicle's location using GPS and receive instant alerts via GSM when suspicious activity is detected. Similar GPS–GSM-based tracking and alert mechanisms have been widely validated in previous studies for effective theft detection and response [1], [3], [7]. However, the system primarily focuses on location tracking and does not include biometric authentication, which has been shown to significantly enhance protection against unauthorized vehicle access [5], [6], [9]. Nevertheless, this work highlights the importance of integrating communication technologies for real-time vehicle monitoring and theft response.

2. Vehicle Tracking and Locking System Based on GSM and GPS, M. A. Mazidi and A. R. Ameen, 2017

This paper describes the design of a vehicle tracking and locking system using GSM and GPS modules. The system allows vehicle owners to remotely monitor vehicle location and send SMS-based commands to lock or immobilize the engine in the event of theft. Such remote immobilization and alert-based approaches are consistent with earlier vehicle security systems using GSM communication [1], [4]. However, the absence of user authentication or local biometric validation mechanisms, such as fingerprint sensors, limits the system's ability to prevent unauthorized ignition at the source. Prior research indicates that integrating biometric authentication with GSM and GPS technologies can substantially improve overall vehicle security [2], [6], [8].

3. A Review on Vehicle Anti-Theft System, S. Patil, P. L. Kadu, and M. D. Chaudhari, 2016

This review paper provides a comprehensive analysis of various vehicle anti-theft systems, ranging from traditional key-based locking mechanisms to advanced RFID- and biometric-based security solutions. The authors evaluate these approaches based on cost, effectiveness, and scalability, concluding that single-layer security systems are insufficient to address modern vehicle theft challenges. The study strongly supports the integration of multiple technologies—such as GPS, GSM, and biometric authentication—to achieve a more robust and reliable security framework. These conclusions align with recent implementations that demonstrate improved theft prevention through multi-layered vehicle security systems [1], [5], [7], [9].

4. Smart Anti-Theft System for Vehicle Security, M. K. Sharma, S. T. Solanki, and R. K. Patidar, 2020

This work proposes a smart vehicle anti-theft system utilizing GPS and GSM modules to monitor vehicle location and control engine operation through a relay-based immobilization mechanism. The system effectively provides real-time tracking and alert notifications during unauthorized access attempts. However, the authors acknowledge that the security level can be further enhanced by incorporating biometric authentication techniques. This observation is consistent with several recent studies that emphasize fingerprint-based access control as a highly reliable and difficult-to-bypass security layer when combined with GPS and GSM technologies [2], [5], [6], [9]. The paper reinforces the concept that integrating real-time tracking with user verification leads to a more comprehensive vehicle security solution.

III. EXISTING SYSTEM

Most traditional vehicle security systems rely primarily on basic protection mechanisms such as mechanical locks, remote key-based locking, and simple alarm units that generate audible alerts during unauthorized access attempts. Although these methods provide a basic level of security, they lack intelligent tracking, real-time alerting, and remote monitoring capabilities [4], [7]. Conventional systems typically do not incorporate GPS-based

location monitoring, making it difficult to locate vehicles promptly after theft occurs [1], [2]. Furthermore, many existing vehicle protection solutions depend heavily on physical keys or RFID cards, which are vulnerable to duplication, loss, or theft, thereby compromising system security [3], [6]. In addition, most traditional theft-prevention setups do not include biometric authentication mechanisms, allowing unauthorized individuals to operate the vehicle if they gain access to the key or remote control [5], [9]. Studies have shown that integrating biometric verification, such as fingerprint recognition, significantly enhances access control and reduces the likelihood of unauthorized vehicle usage [6], [8]. Overall, existing vehicle security systems offer limited protection, minimal owner control, and lack effective identity verification and real-time response mechanisms, highlighting the need for advanced, multi-layered security solutions that combine GPS, GSM, and biometric technologies [1], [7].

IV. PROPOSED SYSTEM

The proposed system introduces an intelligent, multi-layered vehicle security solution that integrates GPS tracking, GSM-based instant alerts, and fingerprint authentication to ensure only authorized users can access and start the vehicle. When a valid fingerprint is verified, the system unlocks the ignition; otherwise, it remains disabled and sends an immediate SMS alert to the vehicle owner. In case of unauthorized movement or suspected theft, the GPS module continuously updates the vehicle's location, allowing real-time tracking through GSM communication. This combination of biometric verification and live monitoring significantly enhances security by preventing unauthorized access, enabling quick recovery, and giving the owner full situational awareness. The system ultimately provides a smart, reliable, and tamper-resistant approach to modern vehicle protection.

V. SYSTEM ARCHITECTURE

1. Sensor & Authentication Modules (Edge Devices)

The system uses a fingerprint sensor module integrated with a microcontroller (such as NodeMCU or Arduino) to authenticate drivers before granting access to the vehicle. Additional sensors like vibration sensors, door status sensors, and ignition-status detectors monitor unauthorized entry attempts or unusual vehicle activity. These edge devices continuously collect biometric and physical security data. Each module runs embedded firmware responsible for validating fingerprints, detecting intrusion patterns, and initiating immediate lockout actions. Processed security events are transmitted via GSM/GPRS to the owner along with GPS-based location updates.

2. Edge Processing & Security Logic

At the microcontroller level, the system performs real-time fingerprint matching using stored templates and executes intrusion detection logic (e.g., vibration threshold checks, forced entry detection). When unauthorized attempts occur, the controller instantly blocks ignition and generates an alert. Sensitive data such as fingerprint templates are stored in encrypted form using AES-128 or similar encryption techniques. Only compressed event logs or verified authentication outcomes are sent to the cloud or owner's device, avoiding raw biometric data exposure.

3. Communication Network & Vehicle Gateway

The system communicates using GSM (SIM800/900 modules) for sending SMS alerts and GPS modules for real-time tracking of the vehicle. The microcontroller acts as a local gateway that aggregates authentication results, security sensor readings, and vehicle location coordinates. Data is securely transmitted over GSM with optional TLS support for enhanced security. In offline situations (poor network areas), the gateway stores alerts locally and triggers a buzzer or immobilizer action directly until communication is restored.

4. Cloud / Remote Monitoring Backend

The cloud backend (optional, depending on implementation) maintains logs of authentication attempts, vehicle locations, route history, and intrusion alerts. It hosts analytics tools that help identify suspicious activity patterns and provides a dashboard for vehicle owners to view security status

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com

in real time. GPS data is visualized on maps, while alert history is stored in an encrypted database. Role-based access ensures only verified users or administrators can access sensitive information like movement logs or biometric validation results. Notifications are pushed to owners through SMS, email, or app notifications.

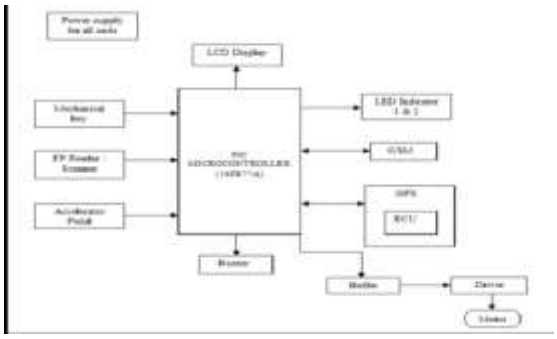

Fig. 5.1: Structure of the Proposed System

Microcontroller Module:

The microcontroller serves as the primary controller for biometric verification, GPS tracking, GSM alerting, and ignition control. It includes built-in communication interfaces and GPIO pins to integrate with various vehicle security sensors. The module handles fingerprint template matching, encryption of alert messages, and logic that decides whether to enable or block the ignition system.

Key components include:

Fingerprint Sensor Interface (TX/RX):

Used for capturing and validating biometric data.

GPS Module (UART):

Provides real-time coordinates (latitude, longitude) for vehicle tracking.

GSM Module (UART/SIM Slot):

Sends SMS alerts to the owner when unauthorized access or movement is detected.

Digital GPIO Pins:

Used for ignition relay control, door sensor inputs, vibration sensor signals, and status indicators.

Power Pins (5V/3.3V, GND):

Provide stable power to the microcontroller and connected modules.

Internal/External Antennas:

For stable GSM and GPS communication in various environments.

VI. IMPLEMENTATION

The assembled system includes all components such as the fingerprint sensor, GSM, GPS, LCD, relay, DC motor, and buzzer, integrated and functioning properly on the hardware board.

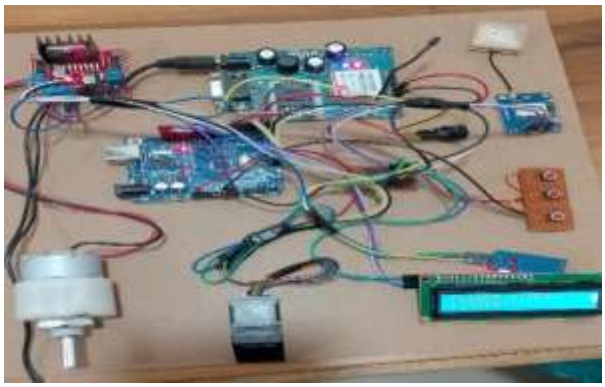

Fig. 6.1: Prototype Model of Smart Vehicle Security System with GSM, GPS, and Fingerprint Authentication

When the button is pressed, the system successfully enters fingerprint enrollment mode and stores the fingerprint data of the authorized user.

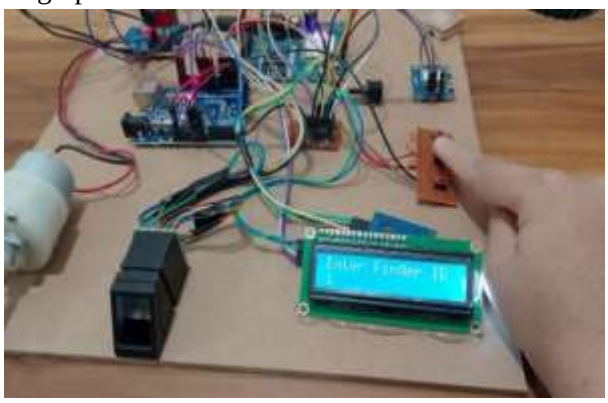

Fig. 6.2: Fingerprint Authentication Process in Smart Vehicle Security Prototype

Upon placing a finger on the sensor, the system accurately checks if the fingerprint is authorized. If matched, the vehicle (DC motor) is allowed to start.

VII. CONCLUSION

The "Anti-Theft Protection of Vehicle by GSM & GPS with Fingerprint Verification" project successfully addresses the growing need for advanced vehicle security systems in an increasingly technology-driven world. Traditional methods of vehicle protection, such as mechanical locks and alarm systems, have proven to be insufficient in preventing theft due to their vulnerability to

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com

physical tampering and bypassing. By integrating fingerprint biometric authentication with GSM and GPS technologies, the proposed system creates a comprehensive and multi-layered security framework that ensures only authorized users can access and operate the vehicle. The inclusion of a fingerprint sensor adds a significant level of security, making it nearly impossible for unauthorized individuals to start the vehicle. The GPS module provides real-time location tracking, allowing vehicle owners to monitor the vehicle's movements and respond swiftly in case of any unauthorized activity. Additionally, the GSM module ensures instant communication by sending SMS alerts during any suspicious attempt, enhancing the chances of timely theft prevention or recovery.The system also utilizes an LCD for visual feedback, a DC motor as part of the ignition mechanism, and a buzzer for audible alerts, providing a user-friendly interface and real-time notifications. This integration of various modules into a single embedded system not only improves security but also boosts user confidence and convenience.

VIII. FUTURE SCOPE

The proposed vehicle security system can be further enhanced with several advanced features to increase reliability, intelligence, and user convenience. Future versions can integrate IoT-based real-time monitoring apps, allowing users to track their vehicles through mobile dashboards with geofencing, live route replay, and remote ignition control. Upgrading fingerprint authentication to multi-biometric verification (face recognition, RFID, or smartphone-based digital keys) can improve accuracy and security. Artificial intelligence can be incorporated to detect abnormal driving patterns, predict theft attempts, and automatically trigger immobilization. The system can also adopt 4G/5G modules for faster data transmission and cloud-based predictive analytics for analyzing long-term vehicle security trends. Additional enhancements include tamper-proof hardware enclosures, solar-powered modules for reduced power dependency, OTA (Over-the-Air) firmware upgrades, and integration with smart city infrastructure for centralized monitoring of stolen vehicles. These improvements can transform the prototype into a fully scalable, commercial-grade intelligent vehicle security ecosystem.

IX. REFERENCES

[1]. M. Dey, M. A. Arif, and M. A. Mahmud, "Anti-theft protection of vehicle by GSM & GPS with fingerprint verification," in 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 2017, pp. 916–920, doi: 10.1109/ECACE.2017.7913034.

[2]. Aditya Bobade, Aditi Joshi, Tejas Patil, Sarvednya Gade, and U. M. Thorkar, "Vehicle security management system using GPS, GSM and fingerprint module," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 11, no. 6, pp. 2391–2394, Jun. 2023, doi: 10.22214/ijraset.2023.54023.

[3]. A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed, and M. A. M. Chowdhury, "Design and implementation of microcontroller-based anti-theft vehicle security system using GPS, GSM and RFID," in 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT), Dhaka, Bangladesh, 2018, pp. 97–101, doi: 10.1109/CEEICT.2018.8628051.

[4].S. R. Nelluri and K. M. Poluri, "Real-Time Marketing Optimization through Scalable Telemetry Data Engineering: A Framework for Enhanced Engagement and ROI," International Journal of Computer Trends and Technology, vol. 73, no. 1, pp. 26–31, Jan. 2025, doi: 10.14445/22312803/ijctt-v73i1p103.

[5].S. Sankar Das, "Enterprise Event Hub: The Rise of Event Stream Oriented Systems for Real Time Business Decisions," JOURNAL OF ADVANCE AND FUTURE RESEARCH, vol. 1, no. 10, Dec. 2023, doi: 10.56975/jaafr.v1i10.500878

[6].S. K. Immadi, "Optimizing ERP for Human Capital Management," Applied Research for Growth, Innovation and Sustainable Impact, pp. 377–384, Aug. 2025, doi: 10.1201/9781003684657-

63.
[7]. . Singh, T. Sethi, B. K. Balabantaray, and B. B. Biswal, “Advanced vehicle security system,” in 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 2015, pp. 1–6, doi: 10.1109/ICIIECS.2015.7193276.
[8].“Data Science–Enabled Anomaly Detection in Financial Transactions Using Autoencoders and Risk Evaluation Mechanisms,” Journal of Information Systems Engineering and Management, 2024, doi: 10.52783/jisem.v9i2.44.
[9]. K. Jeevitha, J. Venkatesh, V. Indhumathi, K. Krishna Veni, R. Prem Kumar, and M. Devadarshini, “A biometric vehicle theft identification and prevention scheme using GPS location tracking,” in 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2023, doi: 10.1109/ACCAI58221.2023.10199574.
[10]. N. Kiruthiga, L. Latha, and S. Thangasamy, “Real Time Biometrics Based Vehicle Security System with GPS and GSM Technology,” Procedia Computer Science, vol. 50, pp. 475–481, 2015, doi: 10.1016/j.procs.2015.03.231. DOI
[11]. Prof. Dr. Kaushika Patel, Manav Patel, and Vedant Patel, “Vehicle Tracking and Theft Detection,” Int. Journal of Scientific Research in Science & Technology, vol. 12, no. 2, pp. 730–735, 2025, doi: 10.32628/IJSRST251222615.
[12]. “Machine Learning–Enhanced Threat Intelligence for Understanding the Underground Cybercrime Market,” International Journal of Intelligent Systems and Applications in Engineering, 2022, doi: 10.17762/ijisae.v10i2s.7972.
[13]. K. Jeevitha, J. Venkatesh, V. Indhumathi, K. Krishna Veni, R. Prem Kumar, and M. Devadarshini, “A Biometric Vehicle Theft Identification and Prevention Scheme Using GPS Location Tracking,” in 2023 Int. Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2023, doi: 10.1109/ACCAI58221.2023.10199574. DOI
[14]. S. Mehta, S. Srivastava, T. P. Singh, and G. Raj, “Vehicle Anti-Theft System Using Fingerprint & Passcode with Speed Control and Obstacle Detection,” IJRASET, May 2024, doi: 10.22214/ijraset.2024.61914.

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com