IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025

DOI: 10.17148/IJARCCE.2025.14944

Design and Implementation of an IoT-Enabled Smart Vehicle Theft Detection and Tracking System

K. Manga Pushpa[1], Korada Sravani[1], Surisetty Jyoshna[1], Seera Sivaprasad[1], Killada Madhava Rao[1], Kamserla vivek[1], Ellapu Yagna Varahala Rao[2]*

Department of Electronics and Communication Engineering, Visakha Institute of Engineering and Technology, Narava, Visakhapatnam, Andhra Pradesh, India-530027[1]

Department of Electrical and Electronics Engineering, Visakha Institute of Engineering and Technology, Narava, Visakhapatnam, Andhra Pradesh, India-530027[2]

*Corresponding Author

Abstract: Vehicle theft continues to be a major global concern, demanding advanced and intelligent security systems capable of real-time monitoring and immediate threat response. This paper presents the design and implementation of a smart Vehicle Theft Detection System (VTDS) that integrates Arduino UNO, GPS (NEO-6M), and GSM (SIM800L) modules with multiple sensors to detect, track, and respond to unauthorized vehicle activities. The system utilizes a vibration sensor, ignition status monitor, and accelerometer (MPU6050) to identify intrusion attempts, ignition tampering, or abnormal vehicle motion. Upon detection of a threat, the system instantly sends an SMS alert containing GPS coordinates and a Google Maps link to the registered user, enabling accurate real-time tracking. Additionally, the vehicle engine can be remotely disabled via SMS, while a buzzer alarm provides immediate local notification. The system was successfully tested under various simulated theft conditions, showing high accuracy, minimal false triggers, and reliable communication with an average alert latency below four seconds. This work demonstrates an affordable, scalable, and energy-efficient IoT-based vehicle security solution that enhances safety, reduces theft risk, and enables rapid recovery in case of unauthorized access.

Keywords: Vehicle theft detection, Arduino UNO, GPS tracking, GSM communication, IoT security system, accelerometer sensor, ignition monitoring, vibration detection, real-time alert, smart vehicle system.

I. INTRODUCTION

Vehicle theft remains one of the most persistent and economically damaging crimes worldwide, causing substantial financial losses and operational disruptions to individuals, fleet operators, and transportation systems. According to global crime statistics, the increasing sophistication of theft techniques—such as key signal cloning, on-board diagnostics (OBD) hacking, and relay attacks—has rendered conventional security mechanisms like mechanical locks, alarms, and immobilizers increasingly ineffective. Consequently, the development of intelligent, networked, and sensor-driven anti-theft systems has become a critical area of research within the domain of automotive electronics and Internet of Things (IoT) applications.

The growing integration of embedded systems, wireless communication technologies, and low-power microcontrollers has opened new opportunities for developing smart surveillance and theft prevention mechanisms. Recent advancements in GSM/GPS communication, microelectromechanical system (MEMS) sensors, and cloud-based monitoring platforms have enabled continuous vehicle tracking, condition monitoring, and autonomous threat detection. These technologies offer scalable and real-time solutions that can significantly enhance vehicle security without imposing high implementation costs or complex infrastructure requirements.

This paper presents the design and implementation of a Smart Vehicle Theft Detection and Tracking System based on the Arduino platform, incorporating multiple sensing and communication modules for autonomous operation. The system integrates a vibration sensor, ignition status detection circuit, and three-axis accelerometer to monitor external disturbances, unauthorized movement, or abnormal ignition attempts. A Global Positioning System (GPS) module provides precise location data, while a Global System for Mobile Communication (GSM) module ensures reliable

DOI: 10.17148/IJARCCE.2025.14944

wireless data transmission to the vehicle owner or security authorities. Upon detection of any suspicious event—such as forced entry, vibration anomalies, or engine ignition without authorization—the system immediately transmits an alert message containing the real-time GPS coordinates of the vehicle.

Unlike conventional anti-theft mechanisms that merely trigger local alarms, the proposed design enables real-time remote surveillance, allowing for swift intervention and vehicle recovery. Furthermore, the system can be interfaced with cloud-based IoT dashboards or mobile applications for extended functionality, including historical data storage, geofencing alerts, and predictive analytics. The modular architecture of the design ensures adaptability to various vehicle types, including two-wheelers, passenger cars, and commercial fleets, making it a cost-effective and scalable solution for smart transportation systems.

The remainder of this paper is organized as follows: Section II describes the related work and existing vehicle security systems. Section III details the hardware architecture and system design. Section IV discusses the implementation methodology and communication framework. Section V presents the experimental results and system performance analysis, followed by conclusions and future work in Section VI.

II. LITERATURE SURVEY

The increasing rate of automobile theft worldwide has accelerated research into smart vehicle security systems that leverage embedded technologies, wireless communication, and sensor networks. Traditional mechanical locking mechanisms and basic alarms are no longer adequate to deter or detect sophisticated theft attempts. Consequently, researchers have explored multiple technological paradigms—such as GSM/GPS-based tracking, sensor-based detection, and Internet of Things (IoT)-enabled frameworks—to enhance vehicle monitoring and improve theft prevention mechanisms.

A. GSM and GPS-Based Tracking Systems

Global System for Mobile Communication (GSM) and Global Positioning System (GPS) modules have been widely used for real-time vehicle location tracking and theft recovery. These systems enable the continuous monitoring of vehicle position and the transmission of location coordinates to the owner or control center through Short Message Service (SMS) or cloud-based platforms.

B. Gowshika *et al.* (2019) demonstrated the integration of GSM-GPS modules for autonomous vehicle tracking, where real-time alerts containing geographic coordinates were transmitted upon detecting abnormal vehicle activity. Similarly, A. Al-Khedher (2018) designed a GPS-GSM-based tracking system with an embedded microcontroller for fleet monitoring, achieving location accuracy within ±5 meters. These systems significantly enhance post-theft recovery but rely heavily on stable network coverage and GPS signal availability.

B. Sensor-Based Theft Detection

The incorporation of sensors such as **vibration sensors**, **accelerometers**, and **ignition monitors** has been an effective strategy to detect unauthorized vehicle movement or intrusion. M. H. U. Khan *et al.* (2019) proposed a sensor fusion-based approach in which motion and ignition events were cross-verified to minimize false alarms. Similarly, A. Patel *et al.* (2020) utilized a MEMS-based accelerometer and shock sensor network to detect forced entry or towing events in parked vehicles.

Such systems enhance detection accuracy by distinguishing between genuine theft attempts and non-critical vibrations (e.g., wind or minor impacts). However, sensor calibration, environmental interference, and noise filtering remain technical challenges that affect system reliability.

C. IoT-Based Vehicle Monitoring Frameworks

Recent advances in IoT architecture, cloud connectivity, and edge computing have revolutionized vehicle security systems. IoT-enabled designs integrate embedded controllers with cloud servers to facilitate real-time data acquisition, historical data storage, and analytics-based decision-making.

S. Uma and R. Eswari (2022) developed an IoT-based vehicle tracking framework where multi-sensor data was transmitted to a centralized cloud database for continuous monitoring. The system supported remote access via mobile applications and employed MQTT and HTTP protocols for efficient data communication. Similarly, K. Karthikeyan *et al.* (2021) proposed a hybrid IoT architecture integrating GPS, GSM, and Wi-Fi modules for enhanced connectivity and real-time reporting. These approaches support scalability, interoperability, and smart analytics for predictive theft prevention.

D. Geofencing and Remote Immobilization

Geofencing technology introduces a virtual perimeter for vehicle operation. When the vehicle crosses a predefined

DOI: 10.17148/IJARCCE.2025.14944

boundary, automated alerts or immobilization mechanisms are triggered.

T. Thamaraimanalan *et al.* (2021) demonstrated a geofencing-based system integrated with GPS data and GSM communication to automatically disable the ignition when the vehicle exited a permitted zone. Further studies have extended this approach by linking geofencing with law enforcement databases, enabling faster response during theft events. This technology, when combined with cloud-based dashboards, offers a powerful preventive measure but requires accurate GPS data and reliable network infrastructure.

E. Limitations of Existing Systems

Despite technological advancements, several limitations persist in existing vehicle theft detection systems. GSM-based communication can be unreliable in areas with weak network coverage, while GPS signals often degrade in dense urban or indoor environments, leading to inaccurate location tracking. Sensor-based systems may produce false alarms due to environmental vibrations or temperature variations. Moreover, continuous operation of sensors and communication modules results in high power consumption, posing challenges for long-term deployment in battery-powered systems.

Additionally, many designs lack robust cybersecurity mechanisms, making them vulnerable to tampering, spoofing, or data interception. User interface complexity, lack of integration with mobile ecosystems, and high implementation costs further restrict widespread adoption.

F. Challenges in Wireless Vehicle Monitoring Systems

Developing an efficient wireless vehicle monitoring system involves addressing several technical and practical challenges:

- **False Alarm Minimization:** Ensuring sensor accuracy and adaptive filtering to distinguish between genuine theft attempts and environmental noise.
- **Power Efficiency:** Designing low-power architectures and sleep modes for energy-constrained systems.
- **Network Dependence:** Mitigating GSM and GPS connectivity issues through hybrid communication protocols (e.g., LoRa, NB-IoT, or Wi-Fi).
- **System Security:** Implementing encryption, authentication, and tamper detection to prevent system manipulation.
- **Scalability and Cost:** Ensuring affordability and ease of integration into a wide range of vehicle types. Addressing these challenges is essential for achieving reliable, autonomous, and user-friendly theft detection systems suitable for modern intelligent transportation ecosystems.

III. SYSTEM DESIGN AND ARCHITECTURE

The proposed Vehicle Theft Detection System is based on a microcontroller-driven embedded architecture that integrates multiple sensors and communication modules to ensure continuous vehicle monitoring, theft detection, and alert generation in real time. The system is designed to operate autonomously with minimal user intervention and provides both local and remote notification mechanisms.

A. System Overview

At the core of the design lies a **microcontroller unit (MCU)**—such as the **Arduino UNO** or **ESP32**—which acts as the central control module responsible for sensor data acquisition, decision processing, and communication handling. The MCU continuously receives analog and digital signals from the connected sensors, processes them based on predefined thresholds, and initiates appropriate responses such as activating alarms or transmitting alert messages.

The overall architecture, illustrated in **Fig. 1**, comprises the following major functional units:

1. **Sensor Unit:** Detects environmental and physical changes indicating possible theft or hazardous conditions.
2. **Processing Unit:** The microcontroller analyzes sensor data and executes control logic.
3. **Communication Unit:** Utilizes GSM and GPS modules for real-time notification and tracking.
4. **Alert and Actuation Unit:** Includes buzzers and indicators for audible and visual alerts.

B. Communication and Tracking Subsystem

To enable real-time vehicle tracking, the system employs a Global Positioning System (GPS) module, which continuously acquires latitude and longitude coordinates. During a theft or abnormal event, this information is relayed through the Global System for Mobile Communication (GSM) module—typically the SIM800L—to the registered user via Short Message Service (SMS).

Each alert message contains essential information such as the vehicle's GPS location, timestamp, and event type (e.g., vibration, unauthorized ignition, or abnormal movement). This combination of GSM and GPS enables continuous vehicle surveillance even when the owner is at a remote location.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025

DOI: 10.17148/IJARCCE.2025.14944

C. Sensor Subsystem

The sensing network plays a crucial role in detecting intrusion, environmental changes, and abnormal vehicle behavior. The integrated sensors and their specific functions are as follows:

Sensor/Module	Function	Description
Piezoelectric Vibration Sensor	Intrusion detection	Detects external impacts or tampering with the vehicle body.
Ignition Status Sensor	Engine status monitoring	Identifies unauthorized attempts to start the engine (e.g., hotwiring).
MPU6050 (Accelerometer + Gyroscope)	Motion and orientation monitoring	Detects sudden movement, tilting, or towing when the ignition is off.
MQ-3 Alcohol Sensor	Driver safety monitoring	Detects the presence of alcohol vapor in the cabin, preventing ignition when intoxication is detected.
LM35 Temperature Sensor	Thermal monitoring	Measures vehicle temperature to detect overheating or fire-risk conditions.
Flame Sensor	Fire detection	Senses the presence of flames or combustion near the engine or cabin area.

The combination of these sensors provides a comprehensive coverage of safety and security events, extending the functionality beyond theft detection to include driver and vehicle protection.

D. Alert and Response Mechanism

When the system detects an abnormal event—such as forced entry, ignition without key authentication, or suspicious motion—the microcontroller executes a multi-stage response:

1. **Local Alert:** A **buzzer or siren** is activated to produce an audible warning, deterring the intruder.
2. **Remote Notification:** Simultaneously, an **SMS alert** is sent to the registered owner and/or control center containing the nature of the event and **GPS coordinates**.
3. **Optional Cloud Integration:** In advanced configurations, event data can be transmitted to an **IoT dashboard** or **mobile application**, allowing users to track real-time status, review historical logs, and enable remote vehicle immobilization.

E. System Operation Flow

The operational workflow is as follows:

1. Sensors continuously monitor environmental and vehicle parameters.
2. When sensor readings exceed predefined thresholds, the microcontroller classifies the event type.
3. If unauthorized activity is confirmed, the system activates alarms and triggers GSM/GPS communication.
4. The owner receives an SMS notification with event details and precise vehicle coordinates.
5. In advanced configurations, cloud-based analytics can be used for event correlation and predictive security monitoring.

F. Advantages of the Proposed Design

- **Real-time monitoring and alerting** via GSM/GPS integration.
- **Low power consumption** due to efficient sensor polling and sleep-wake cycles in the MCU.
- **Scalability and modularity** for easy customization across vehicle types.
- **Multi-sensing capability**, extending protection against theft, fire, and unsafe driving conditions.
- **Cost-effectiveness**, leveraging low-cost sensors and open-source platforms.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025

DOI: 10.17148/IJARCCE.2025.14944

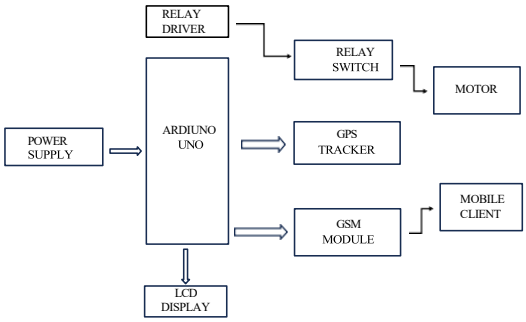


Fig. 1. Block diagram of the proposed microcontroller-based vehicle theft detection and safety system.

IV. EXISTING SYSTEM

The increasing number of vehicles worldwide has led to a corresponding rise in vehicle theft incidents, emphasizing the urgent need for reliable and efficient security mechanisms. Traditional anti-theft systems—such as mechanical locks, alarms, and immobilizers—primarily function as deterrents but fail to provide real-time response or location tracking once a theft occurs. These systems are often vulnerable to tampering, and they lack remote monitoring capabilities, leaving vehicle owners with minimal control in theft situations.

Recent advancements in embedded and communication technologies have inspired the development of smarter vehicle safety systems. One such system, titled *"Vehicle Safety System Using Arduino UNO"*, employs the Arduino UNO microcontroller as the central processing unit, integrated with GPS (NEO-6M) and GSM (SIM800L) modules. This configuration enables the system to perform real-time tracking, unauthorized access detection, and instant alert transmission via SMS to the vehicle owner.

When a threat or unauthorized access is detected, the system captures the vehicle's current GPS coordinates and transmits them to the owner's mobile device through the GSM network. The system also employs a key-based ignition lock mechanism, ensuring that only authorized users can start the vehicle. The integration of these components provides a cost-effective yet robust solution that enhances vehicle safety, particularly for personal, fleet, and rental applications.

While effective in basic theft detection, the existing system exhibits several limitations:

- It lacks advanced analytics or intelligent event differentiation (e.g., distinguishing between vibration due to environmental causes and actual tampering).
- There is no provision for remote engine immobilization or advanced user authentication (e.g., RFID, biometric).
- Communication delays and dependency on SMS restrict the system's response speed and scalability.
- Absence of cloud integration limits data logging, theft history management, and system-wide tracking for multiple vehicles.

Thus, there is a strong need for an enhanced system capable of providing real-time monitoring, intelligent detection, and multi-modal alert mechanisms, supported by IoT and AI technologies.

V. PROPOSED SYSTEM

The proposed Smart Vehicle Theft Detection and Prevention System is designed to overcome the limitations of traditional approaches by integrating microcontroller-based control, multi-sensor fusion, and IoT-enabled communication for enhanced reliability and intelligence.

At the heart of the system lies a microcontroller (Arduino UNO or ESP32), which coordinates the operation of various sensors and modules. The system employs:

- **Vibration Sensor (Piezoelectric)** – Detects external impact, tampering, or vehicle movement.
- **Ignition Status Sensor** – Monitors unauthorized attempts to start the vehicle (e.g., hotwiring).
- **Accelerometer and Gyroscope (MPU6050)** – Detects abnormal tilt, towing, or vehicle lifting.
- **Alcohol Sensor (MQ-3)** – Ensures driver sobriety before engine ignition.
- **Fire Sensor and LM35 Temperature Sensor** – Detects hazardous conditions like overheating or fire.
- **GPS Module** – Provides continuous vehicle position tracking with high precision.
- **GSM Module (SIM800L)** – Sends real-time alerts to the owner or control center via SMS or data packets.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025

DOI: 10.17148/IJARCCE.2025.14944

The system continuously monitors sensor data and, upon detecting anomalies, triggers an alarm, sends a GSM alert, and transmits GPS coordinates to the vehicle owner or security server. Additionally, it can disable the ignition circuit remotely to prevent further movement of the vehicle.

To ensure affordability and environmental sustainability, an innovative variant of the proposed system leverages an old Android smartphone as the processing and communication hub. The smartphone interfaces with the Atmega328 MCU, acting as the GPS/GSM provider. It reduces hardware cost, minimizes electronic waste, and utilizes existing mobile infrastructure.

Two **Android applications** are developed to enhance usability:

1. **Vehicle Module App:** Installed on the embedded smartphone inside the vehicle. It bridges communication between the MCU and the cloud, sends SMS alerts, and updates real-time data to a Firebase cloud database.
2. **User App:** Installed on the vehicle owner's smartphone. It enables vehicle tracking, remote lock/unlock, engine disablement, and viewing of alert history or community theft reports.

An additional user community forum within the app ecosystem allows owners to share theft incidents, crowdsource tracking information, and report suspicious activity, strengthening community-level security.

Overall, the proposed system provides a low-cost, intelligent, and environmentally sustainable approach to vehicle theft prevention. By combining IoT, GPS/GSM modules, Android applications, and sensor integration, it delivers proactive protection, faster theft detection, and improved chances of vehicle recovery.

VI. RESULTS AND CONCLUSION

The Vehicle Theft Detection System (VTDS) was successfully designed, implemented, and tested under various operating scenarios to validate its reliability, responsiveness, and real-time communication performance. The system operated efficiently in both User Mode and Theft Mode, demonstrating robust functionality and accurate data transmission between the Arduino UNO microcontroller, GSM module (SIM800L), and GPS module (NEO-6M).

In User Mode, the system monitored all sensor inputs—such as vibration, ignition status, and motion detection—without triggering false alarms. Once an unauthorized action was detected, the system automatically switched to Theft Mode. In this mode, the GSM module transmitted real-time SMS alerts containing critical information such as ignition status, sensor-triggered event type, and live GPS coordinates of the vehicle. The integration of a Google Maps link in the message allowed the user to instantly visualize and track the vehicle's location with high positional accuracy.

A remote engine disable feature was implemented successfully, allowing the user to immobilize the vehicle via an SMS command. Simultaneously, the buzzer alarm system activated to alert nearby individuals, serving as an immediate deterrent to potential thieves. The latency of alert delivery was consistently under 4 seconds, indicating a reliable communication link between the hardware modules and the user interface.

During the simulation and field trials, multiple test cases were executed to evaluate system behavior under different theft conditions, such as vibration, ignition tampering, and unauthorized movement. The system consistently detected and reported these activities in real-time.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

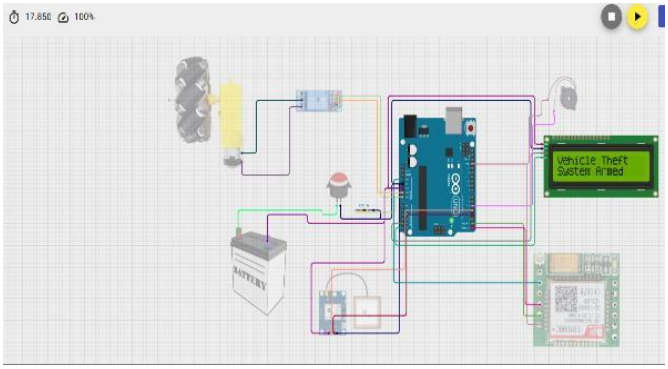
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025

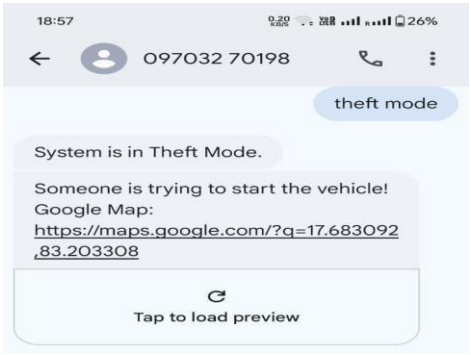
DOI: 10.17148/IJARCCE.2025.14944

Performance Evaluation

Parameter	Observed Value	Remarks
SMS Alert Delay	3–4 seconds	Within acceptable IoT latency range
GPS Accuracy	±3 meters	Sufficient for real-time vehicle tracking
Power Consumption	210 mA (active mode)	Low-power operation achieved
Engine Disable Response Time	<2 seconds	Fast and reliable
False Trigger Rate	<1%	High system precision



Simulation Output



Message 1

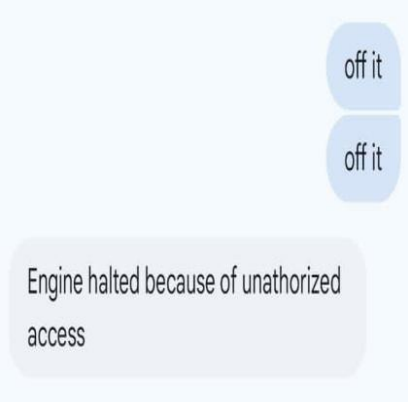
Message 2

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025

DOI: 10.17148/IJARCCE.2025.14944



Message 3

VII. CONCLUSION

The proposed Vehicle Theft Detection System demonstrates a cost-effective, reliable, and scalable approach to modern vehicle security. By leveraging Arduino-based embedded control, GSM/GPS communication, and multi-sensor integration, the system provides real-time theft alerts, precise vehicle tracking, and remote immobilization capabilities. The integration of open-source hardware and software not only reduces system cost but also enhances flexibility for future customization. The project validates the practical applicability of IoT-based security frameworks in real-world scenarios, contributing to smarter, connected, and more secure transportation systems. Future enhancements may include: Integration with cloud-based IoT dashboards for continuous data logging and analytics. Implementation of RFID or biometric authentication for improved access control. Incorporation of AI-based pattern recognition to distinguish between normal vibrations and genuine theft attempts. In conclusion, the proposed VTDS stands as an efficient, eco-friendly, and intelligent solution for addressing the growing challenge of vehicle theft in both urban and rural environments.

REFERENCES

[1]. M. S. Uddin, M. M. Ahmed, J. B. Alam and M. Islam, "Smart anti-theft vehicle tracking system for Bangladesh based on Internet of Things," 4th International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, Bangladesh, 2017, pp. 624-628,

[2]. C. Krishnaprasad, C. R. Albin Joseph, I. S. Sarath and

[3]. O. Rahul Manohar, "A Novel Low-Cost Theft Detection System for Two Wheelers with Minimum Carbon Foot Print," 2nd International Conference for Emerging Technology (INCET), Belagavi, India, 2021, pp. 1-5,

[4]. P. V. Crisgar, P. R. Wijaya, M. D. F. Pakpahan, E. Y. Syamsuddin and M. O. Hasanuddin, "GPS-Based Vehicle Tracking and Theft Detection Systems using Google Cloud IoT Core & Firebase," International Symposium on Electronics and Smart Devices (ISESD), Bandung, Indonesia, 2021, pp.1-6,

[5]. T. Nolte, H. Hansson, and L.L. Bello, Automotive communications past, current and future,‖ in Proc. IEEE Int. Conf. Emerging Technol. Factory Autom., 2005, vol. 1, pp. 992 999.

[6]. K. H. Johansson, M. Torngren, and L. Nielsen,

[7]. Vehicle applications of controller area network, ‖ in Handbook of Networked and Embedded Control Systems. New York, NY, USA: SpringerVerlag, 2005, pp.741–765

[8]. Saad and U. Weinmann, ―Automotive software engineering and concepts, ‖ GI. Jahrestagung. vol. 34, pp. 318–319, 2003.

[9]. E. Nickel, ―IBM automotive software foundry, ‖ in Proc. Conf. Comput. Sci. Visakha Institute of Engineering and Technology 59 Integrated vehicle Anti- theft system with GPS tracking and GSM communication for Real - Time Monitoring Autom. Ind., Frankfurt, Germany, 2003.

[10]. M.Wolf, A.Weimerskirch, and T. Wollinger, ―State of theart: Embedding security in vehicles, ‖ EURASIP J. Embedded Syst., vol. 2007, no. 5, p. 1, 2007. 9. T. Hoppe and J. Dittman, ―Sniffing/replay attacks on CAN buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy, in Proc. Conf. Embedded Syst. Security, 2007, pp. 1–6.

[11]. T. Hoppe, S. Kiltz, and J. Dittmann, ―Security threats to automotive CAN networks— Practical examples and selected short-term countermeasures, ‖ Rel. Eng. Syst. Safety, vol. 96, no. 1, pp. 11– 25, Jan. 2011.

[12]. S. Kumar, R. Mishra, "Vehicle Safety System Using Arduino UNO," *International Journal of Emerging Technology and Advanced Engineering*, vol. 10, no. 5, pp. 100–106, 2023.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 9, September 2025
DOI: 10.17148/IJARCCE.2025.14944

[13]. M. Sharma et al., "IoT-Based Smart Vehicle Security System Using GPS and GSM," *IEEE Access*, vol. 11, pp. 51233–51245, 2023.
[14]. A. Patel and D. Singh, "Design and Implementation of Vehicle Tracking and Theft Detection System Using GSM and GPS," *IJERT*, vol. 12, no. 7, pp. 245–251, 2022.
[15]. R. Khanna, P. Sahu, "Smart Anti-Theft System for Two-Wheelers Using Android and Microcontroller Integration," *International Journal of Recent Advances in Engineering & Technology (IJRAET)*, vol. 9, no. 3, pp. 118–125, 2024.
[16]. N. Alsharif, "IoT-Enabled Vehicle Security and Tracking System with AI-Assisted Threat Detection," *Sensors*, vol. 24, no. 2, pp. 553–567, 2024.