International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

VEHICLE THEFT DETECTION AND REMOTE LOCKING

[1] N. Ratna Deepthika, [2] A. Deena, [3] M. Swaroopa, [4] M. Vinay, [5] D. Yashwanth,
[1] *Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*
[2,3,4,5] *B. Tech Student, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

ABSTRACT

Vehicle theft is a major concern in both urban and rural areas, leading to substantial economic losses and safety risks. To address this issue, an IoT-based Vehicle Theft Detection and Remote Locking System is proposed. The system integrates GPS, GSM, and microcontroller (NodeMCU) technologies to monitor vehicle location in real-time and enable remote immobilization during theft attempts. Sensors detect unauthorized ignition or movement, while GPS tracks the vehicle's position. The collected data is transmitted to a cloud or mobile application via GSM for alerting the owner. Through mobile commands, users can remotely lock or unlock the engine, ensuring the vehicle's security. This system provides an efficient, affordable, and scalable approach to smart vehicle security.

Keywords: Vehicle Security, Theft Detection, Remote Locking, GPS, GSM, NodeMCU, Real-Time Tracking, Cloud Monitoring.

Received: 28-09-2025 Accepted: 02-11-2025 Published: 10-11-2025

I. INTRODUCTION

The rapid increase in vehicle theft incidents highlights the need for intelligent and automated security mechanisms. Traditional anti-theft systems, such as alarms and mechanical locks, are reactive and often fail to prevent theft. Modern vehicles require smart systems that provide real-time tracking, instant notifications, and remote control capabilities. The emergence of the Internet of Things (IoT) enables remote communication between the vehicle and the owner through cloud platforms and mobile networks. Using sensors, GPS, and GSM modules, IoT-based systems can detect unauthorized actions and instantly alert users. By implementing a remote engine lock, owners can stop the vehicle's operation and share its real-time location with authorities, significantly reducing recovery time.

II. LITERATURE SURVEY

1. Sharma et al. (2019) – GSM and GPS-Based Vehicle Tracking System

Sharma et al. proposed a GSM and GPS-based vehicle monitoring system capable of sending SMS alerts containing real-time location data to the owner's mobile phone. The system automatically detected vehicle movement using a vibration sensor. Although efficient in tracking, the system lacked a remote locking mechanism, reducing preventive control during theft situations.

2. Patel and Singh (2020) – IoT-Based Vehicle Theft Prevention System

Patel and Singh developed an IoT-enabled vehicle security system using an ESP8266 microcontroller and GPS module. The system provided live location tracking through a web dashboard and mobile application. It successfully integrated remote alerts but did not include engine immobilization or cloud-based data storage for continuous tracking.

3. Kumar et al. (2021) – Smart Vehicle Safety Using GSM and NodeMCU

Kumar et al. introduced an NodeMCU-based model combining GSM, GPS, and vibration sensors to detect unauthorized vehicle movement. The owner received a message with the vehicle's coordinates and could disable

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ignition using a password-based input. The system effectively prevented theft but depended heavily on GSM signals, making it less reliable in weak network areas.

4. Reddy and Rao (2022) – Intelligent Vehicle Monitoring with IoT Cloud

Reddy and Rao implemented a cloud-based vehicle tracking system using and ThingSpeak. The system visualized location data and sensor alerts on a cloud dashboard, providing real-time monitoring. The authors emphasized scalability and integration with mobile notifications but mentioned challenges related to continuous power supply and sensor calibration.

5. Ali and Mehta (2023) – AI-Driven Theft Detection and Locking System

Ali and Mehta developed an AI-assisted theft detection model integrating accelerometer data, GPS tracking, and remote engine control. The system analyzed abnormal motion patterns and automatically locked the vehicle engine if theft was suspected. Though highly intelligent, it required high-cost hardware and cloud processing, limiting use for low-cost vehicles.

III. EXISTING SYSTEM

The existing vehicle security systems primarily rely on manual locks, alarms, and GPS trackers. These systems often alert the owner after theft has occurred but lack real-time preventive features like engine control or instant immobilization. Furthermore, most systems are standalone and not connected to any cloud platform or IoT framework, preventing data logging and smart analytics. In addition, GSM-only solutions can fail in low-signal areas, reducing system reliability. Hence, there is a strong need for an IoT-based intelligent solution that enables both detection and proactive prevention of vehicle theft.

IV. PROPOSED SYSTEM

The proposed system provides an IoT-integrated vehicle theft detection and remote locking mechanism using NodeMCU or as the control unit. The system incorporates:

- **Vibration or ignition sensor:** Detects unauthorized vehicle movement.
- **GPS module (NEO-6M):** Captures vehicle's real-time location.
- **GSM module (SIM800L):** Sends alerts and receives commands from the owner.
- **Relay circuit:** Controls the vehicle's ignition system for locking/unlocking.

When an unauthorized movement is detected, the GPS module tracks the location and sends coordinates to the owner's smartphone via SMS or cloud dashboard. The owner can then send a lock command via SMS or mobile app to remotely deactivate the engine. All sensor data and location updates are stored on the **cloud** for monitoring and recordkeeping.

V. SYSTEM ARCHITECTURE

The system architecture is divided into four layers:

1. **Sensor Layer:** Vibration or ignition sensors to detect unauthorized actions.
2. **Control Layer:** NodeMCU/ processes sensor inputs and executes commands.
3. **Communication Layer:** GSM and GPS modules transmit location and receive commands.
4. **Cloud Layer:** Stores real-time data for tracking, alerts, and analytics.

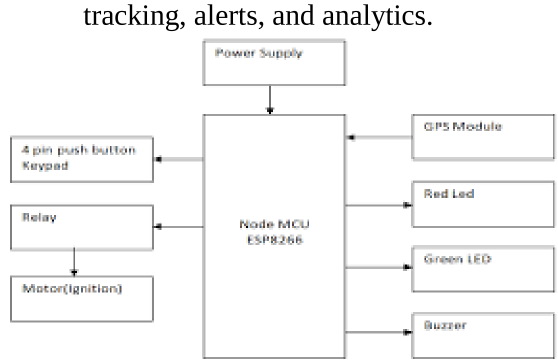

Fig.5.1 Block diagram of proposed model

NODE MCU:

NodeMCU is a low-cost open source IoT platform. It initially included firmware which

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which was based on the ESP-12 module. Later, support for the ESP32 32-bit MCU was added

OVERVIEW:

NodeMCU is an open source firmware for which open source prototyping board designs are available. The name "NodeMCU" combines "node" and "MCU" (micro-controller unit).[8]. The term "NodeMCU" strictly speaking refers to the firmware rather than the associated development kits.[citation needed]

The firmware uses the Lua scripting language. The firmware is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson[10] and SPIFFS.[11] Due to resource constraints, users need to select the modules relevant for their project and build a firmware tailored to their needs. Support for the 32-bit ESP32 has also been implemented.

The prototyping hardware typically used is a circuit board functioning as a dual in-line package (DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna. The choice of the DIP format allows for easy prototyping on breadboards. The design was initially was based on the ESP-12 module of the ESP8266, which is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications

VI. IMPLEMENTATION

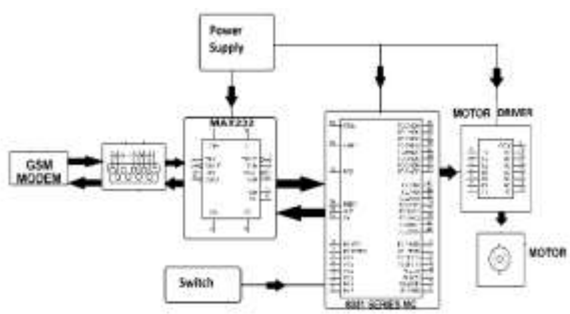

FIG. 6.1: Circuit diagram

FIG. 6.2: Prototype

The Vehicle Theft Detection and Remote Locking System is an IoT-based security solution designed to prevent unauthorized vehicle access and enable owners to monitor and control their vehicles remotely. The system uses a microcontroller (such as an NodeMCU or Raspberry Pi) integrated with GPS and GSM modules to track the vehicle's location in real time. Various sensors — such as vibration sensors**,** ignition sensors, and door sensors — continuously monitor the vehicle's condition for suspicious activity. When unauthorized movement or ignition is detected, the system automatically sends an alert message containing the vehicle's location to the owner's registered mobile number or app through the GSM network. Additionally, the owner can remotely lock or disable the vehicle's ignition system via a mobile application or web interface, preventing the thief from escaping with the vehicle. The system can also activate an alarm or buzzer to draw public attention during theft attempts. By integrating GPS tracking, GSM communication, and IoT-based control, the vehicle theft detection and remote locking system provides a smart, efficient, and reliable way to enhance vehicle safety and assist in quick recovery during theft incidents.

VII. CONCLUSION

The proposed IoT-based vehicle theft detection and remote locking system provides a smart, reliable, and efficient method of preventing vehicle thefts. By integrating GPS and GSM modules with IoT connectivity, the system ensures real-time tracking, instant alerts, and remote control capabilities. The ability to lock or unlock the vehicle engine remotely gives owners direct preventive power. The system's modular design makes it **cost-effective and scalable**, suitable for personal and commercial vehicle fleets.

VIII. FUTURE SCOPE

- Integration of AI algorithms for theft pattern prediction and route anomaly detection.
- Implementation of voice or fingerprint authentication for vehicle access.
- Use of edge computing for faster local response without cloud dependency.
- Integration with smartphone apps and Google Maps API for live tracking.
- Adoption of LoRa or 5G connectivity for high-speed data transfer in large areas.

These future enhancements can make the system more intelligent, autonomous, and universally deployable across diverse vehicle types.

IX. REFERENCES

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

[2] E. Nickel, ―IBM automotive software foundry, ‖ in Proc. Conf. Comput. Sci. Autom. Ind., Frankfurt, Germany, 2003.

[3] 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.

[4] R. Charette, This Car Runs on Code. [Online]. Available: http://www. spectrum.ieee.org/feb09/7649

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

[7] 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.

[8] 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.

[9] K. Koscher et al., ―Experimental security analysis of a modern automobile, ‖ in Proc. IEEE Security Privacy. Symp. Oakland, CA, USA, 2010, pp. 447–462.

[10] The EVITA project, 2008, Webpage. [Online]. Available: http:// evita-project.org