Letters in High Energy Physics
ISSN: 2632-2714

Volume 2021
December

Iot-Based Automobile Theft Detection, Tracking and Engine Immobilization System

K.S. Gowthaman[1], V. Gurukarthikeyan[2]

[1]Assistant Professor, Department of Electrical and Electronics Engineering, Government College of Engineering, Thanjavur, India. Email: ksgowthaman1989@gmail.com

[2]Assistant Professor, Department of Mechanical Engineering, Government College of Engineering, Thanjavur, India. Email: gurumech37@gmail.com

ABSTRACT

Vehicle theft has become a major concern worldwide due to the increasing number of automobiles and the growing sophistication of theft techniques. Conventional vehicle security systems often fail to provide adequate protection against unauthorized access and theft. To address these challenges, this paper presents an IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System that enhances vehicle security through real-time monitoring, location tracking and remote engine control.

The proposed system integrates the Internet of Things (IoT), Global Positioning System (GPS), Global System for Mobile Communication (GSM) and Biometric Fingerprint Authentication technologies to provide a comprehensive and intelligent anti-theft solution. The system authenticates the driver using a fingerprint sensor before allowing vehicle operation. The captured fingerprint is compared with the authorized records stored in the system database to verify the user's identity. In the event of unauthorized access, an immediate theft alert is transmitted to the vehicle owner through the GSM network.

To facilitate vehicle recovery, the GPS module continuously acquires the vehicle's real-time geographical location and shares it with the authorized user through a mobile application or web-based platform. Furthermore, the system incorporates an engine immobilization mechanism that enables the owner to remotely disable the vehicle's ignition system, thereby preventing further movement of the vehicle and reducing the possibility of theft.

The proposed system offers a cost-effective, reliable and user-friendly approach to automobile security. By combining biometric authentication, real-time location tracking, instant theft notifications and remote engine immobilization, the system significantly improves vehicle protection and provides enhanced control to vehicle owners. The integration of IoT technologies makes the system suitable for modern smart transportation and connected vehicle applications.

KEYWORDS- Internet of Things (IoT), Vehicle Theft Detection, Vehicle Tracking, GPS, GSM, Engine Immobilization, Remote Engine Control, Biometric Authentication, Fingerprint Recognition, Real-Time Location Tracking, Theft Alert System.

1. INTRODUCTION

The rapid growth of the automobile industry has significantly increased the number of vehicles on roads worldwide. Along with this growth, vehicle theft has emerged as a major concern for vehicle owners, law enforcement agencies and insurance companies. According to recent reports, thousands of vehicles are stolen every year, resulting in substantial financial losses and security concerns. Traditional vehicle security systems, such as mechanical locks, alarm systems and ignition keys, are often inadequate against modern theft techniques employed by criminals. As a result, there is a growing need for intelligent and reliable vehicle security solutions that can effectively detect, prevent and respond to theft attempts.

Recent advancements in the Internet of Things (IoT) have enabled the development of smart vehicle security systems capable of real-time monitoring, communication and control. IoT technology facilitates seamless interaction between vehicles, sensors, communication networks and users, thereby enhancing the overall security and management of automobiles. By integrating IoT with communication and positioning technologies,

vehicle owners can monitor vehicle status remotely and receive instant notifications during security breaches.

The Global Positioning System (GPS) has become one of the most widely used technologies for vehicle tracking applications. GPS enables accurate determination of a vehicle's geographical location and supports real-time tracking during theft incidents. Similarly, the Global System for Mobile Communication (GSM) provides an efficient communication platform for transmitting alerts, notifications and location information to vehicle owners. The combination of GPS and GSM technologies enables rapid theft detection and facilitates vehicle recovery. In addition to tracking and communication capabilities, modern vehicle security systems increasingly employ biometric authentication techniques to prevent unauthorized access. Fingerprint recognition is one of the most reliable biometric methods due to its uniqueness and ease of implementation. By allowing only authorized users to start and operate the vehicle, fingerprint-based authentication significantly enhances vehicle security and minimizes the risk of unauthorized usage.

Another important security feature is engine immobilization, which allows vehicle owners to remotely disable the vehicle's ignition system in the event of theft. This functionality prevents further movement of the vehicle and improves the likelihood of vehicle recovery. When integrated with IoT, GPS, GSM and biometric authentication technologies, engine immobilization provides a comprehensive security framework capable of detecting theft, notifying owners, tracking vehicle location and controlling vehicle operation remotely.

This paper presents an IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System that integrates fingerprint authentication, GPS-based location tracking, GSM-based alert communication and remote engine control into a unified platform. The proposed system is designed to provide enhanced vehicle security, real-time monitoring, theft prevention and rapid recovery support. By combining multiple security technologies, the system aims to overcome the limitations of conventional anti-theft solutions and offer a cost-effective, reliable and intelligent approach to automobile protection.

2.LITERATURE SURVEY

A real-time vehicle tracking system was developed using GSM and GPS technologies to provide continuous monitoring and location identification of vehicles. The system enabled vehicle owners to track vehicle movements and receive theft-related alerts. However, the proposed approach primarily focused on vehicle tracking and lacked advanced security features such as biometric authentication and remote engine immobilization [1].

A vehicle tracking and locking mechanism based on GSM and GPS technologies was introduced to improve vehicle security and recovery. The system provided real-time location information and supported remote locking operations. Despite its effectiveness in tracking stolen vehicles, the system did not incorporate user authentication techniques to prevent unauthorized vehicle access [2]. A vehicle theft detection system with remote engine locking capability was proposed to enhance vehicle protection against theft. The system allowed vehicle owners to immobilize the engine remotely after receiving theft notifications. However, the absence of IoT-based monitoring and intelligent decision-making reduced its overall effectiveness [3].

A GSM and GPS-based vehicle security and control system was developed to facilitate vehicle tracking and remote monitoring. The integration of communication and positioning technologies improved theft detection and recovery. Nevertheless, the system lacked biometric verification mechanisms for authorized vehicle operation [4]. An advanced vehicle tracking system utilizing Arduino electronic shields and web-based mapping services was designed to provide accurate location monitoring and visualization. Although the system offered reliable tracking performance, it focused primarily on vehicle location tracking and did not address theft prevention measures [5].

A vehicle theft detection and remote engine locking system was introduced to combine vehicle monitoring with immobilization functionality. The proposed system improved vehicle recovery prospects by allowing remote engine control. However, secure driver authentication was not included in the framework [6]. A fingerprint-based vehicle anti-theft system was developed to ensure that only authorized users could operate the vehicle.

The use of biometric authentication significantly reduced the risk of unauthorized access. However, the system did not provide vehicle tracking or theft notification capabilities [7].

A vehicle theft alert and location tracking system employing RFID and GPS technologies was proposed to assist in vehicle recovery. The system generated alerts and transmitted vehicle location information during theft incidents. Nevertheless, remote engine immobilization features were not incorporated [8]. A vehicular identification and authentication system based on ZigBee technology was designed to improve secure communication between vehicles and authorized users. The proposed system enhanced vehicle authentication but suffered from communication range limitations that restricted practical deployment [9].

A microcontroller-based automobile anti-theft system was developed to prevent unauthorized vehicle access through electronic security mechanisms. The system offered a low-cost solution but lacked real-time tracking and remote monitoring functionalities [10]. A remotely controlled vehicle anti-theft system using GSM communication was introduced to enable vehicle owners to monitor and control vehicle operations from distant locations. While the system improved theft response capabilities, it did not support location tracking services [11].

A fingerprint-based authentication system integrated with GSM and GPS technologies was proposed to strengthen vehicle security. The system combined user authentication and vehicle tracking features but lacked remote engine immobilization capabilities [12]. A vehicle ignition system controlled through fingerprint authentication was developed to restrict vehicle access to authorized users only. The approach improved access security but did not include vehicle tracking or theft alert generation mechanisms [13].

An IoT-based anti-theft detection and notification system was designed to provide real-time alerts and vehicle monitoring services. The use of IoT technologies improved connectivity and response time; however, the system lacked biometric authentication functionality [14]. An IoT-enabled anti-theft alarm system was proposed to improve vehicle monitoring through cloud-based communication. The system provided enhanced surveillance and notification features but did not include vehicle immobilization mechanisms [15]. A biometric anti-theft system using fingerprint recognition was implemented to prevent unauthorized vehicle operation. The proposed approach increased security levels but did not support real-time vehicle tracking functions [16].

A fingerprint-based vehicle security framework was introduced to strengthen authentication mechanisms in automobiles. Although the system enhanced access control, location tracking and remote monitoring functionalities were not integrated [17]. A vehicle theft detection and prevention system was developed to improve automobile security through electronic monitoring techniques. The system effectively identified theft attempts but lacked comprehensive tracking and recovery mechanisms [18]. A GSM and GPS-based vehicle theft control system was proposed to facilitate vehicle tracking and theft prevention. The solution improved recovery possibilities; however, biometric verification features were not included [19].

A CAN-based vehicle control system was designed to monitor and control stolen vehicles using in-vehicle communication networks. The system demonstrated improved control capabilities but lacked real-time location tracking services [20]. An IoT-based smart vehicle security and monitoring system was introduced to provide continuous vehicle surveillance through internet connectivity. The system enhanced monitoring efficiency but did not include biometric authentication methods [21].

A real-time vehicle tracking and theft detection system using IoT technologies was developed to improve vehicle monitoring and security. The proposed system provided instant updates but lacked remote engine locking functionality [22]. A smart vehicle security system integrating GPS and GSM technologies was proposed for theft prevention and vehicle recovery. The system improved location tracking accuracy but did not support driver authentication mechanisms [23]. An IoT-enabled vehicle anti-theft and tracking system was developed to provide real-time vehicle monitoring and theft notifications. However, the absence of biometric security features limited its effectiveness against unauthorized vehicle usage [24].

An automobile security enhancement framework using IoT and GPS technologies was introduced to improve vehicle safety. The system enabled effective vehicle tracking but lacked remote control and immobilization capabilities [25]. A remote vehicle immobilization and tracking system using GSM communication was developed to prevent further movement of stolen vehicles. Although the system enhanced recovery opportunities, user authentication features were not considered [26]. A biometric vehicle authentication system based on fingerprint recognition was proposed to improve vehicle access security. The system effectively prevented unauthorized access but did not incorporate location tracking functionalities [27].

An IoT-based vehicle monitoring and security system was designed to provide real-time vehicle status updates and security alerts. The solution improved monitoring performance but lacked remote engine control mechanisms [28]. A vehicle security system integrating GPS tracking and engine locking functionalities was developed to improve theft prevention. While the system combined tracking and immobilization features, biometric authentication was not included [29]. A cloud-based vehicle theft detection and recovery system was proposed to improve vehicle monitoring and recovery operations. The use of cloud services enhanced accessibility; however, secure user authentication mechanisms were absent [30].

A smart vehicle tracking and alert system utilizing IoT technologies was introduced to provide instant theft notifications and location updates. Despite improved connectivity, remote immobilization features were not available [31]. An intelligent vehicle security system using RFID and GPS technologies was developed to enhance vehicle identification and tracking. The system improved monitoring efficiency but lacked advanced theft prevention features such as engine locking [32]. An IoT-based vehicle tracking and monitoring system was designed to provide continuous vehicle surveillance and communication. However, the system focused primarily on tracking and did not address vehicle immobilization requirements [33].

A secure automobile access control system based on biometric authentication was introduced to improve vehicle security. The system effectively restricted unauthorized access but lacked tracking and theft alert functionalities [34]. An intelligent anti-theft vehicle security system integrating GSM, GPS and IoT technologies was proposed to improve vehicle protection and recovery. Although the system combined multiple security features, further improvements were required in user authentication and remote engine control mechanisms [35]. The advantages of the existing studies are summarized in Table 1.

Table 1 Advantages of Existing Studies

Ref. No.	Major Advantage
[1]	Provides real-time vehicle tracking using GSM and GPS technologies.
[2]	Supports both vehicle tracking and remote locking functionalities.
[3]	Enables remote engine immobilization during theft incidents.
[4]	Offers vehicle monitoring and remote-control capabilities.
[5]	Provides accurate location tracking through web-based visualization.
[6]	Combines vehicle tracking with engine locking mechanisms.
[7]	Prevents unauthorized vehicle access using fingerprint authentication.
[8]	Integrates RFID and GPS for improved vehicle identification and tracking.
[9]	Enhances secure vehicle authentication through ZigBee communication.
[10]	Provides a low-cost microcontroller-based anti-theft solution.
[11]	Enables remote vehicle control through GSM communication.
[12]	Combines fingerprint authentication with GSM and GPS technologies.
[13]	Improves vehicle access security using biometric ignition control.
[14]	Utilizes IoT technology for real-time theft notifications.

[15]	Provides cloud-based vehicle monitoring and security alerts.
[16]	Restricts vehicle operation to authorized users only.
[17]	Strengthens vehicle security through biometric verification.
[18]	Improves theft detection and prevention capabilities.
[19]	Facilitates vehicle tracking and theft control through GSM and GPS.
[20]	Uses CAN networks for efficient vehicle monitoring and control.
[21]	Provides smart vehicle monitoring through IoT connectivity.
[22]	Supports real-time vehicle tracking and theft detection.
[23]	Enhances vehicle security using GPS and GSM integration.
[24]	Enables IoT-based vehicle monitoring and theft alert generation.
[25]	Improves vehicle safety through IoT-enabled tracking.
[26]	Supports remote vehicle immobilization and location tracking.
[27]	Enhances security through biometric vehicle authentication.
[28]	Provides real-time vehicle monitoring and alert services.
[29]	Integrates GPS tracking with engine locking functionality.
[30]	Enables cloud-based theft detection and recovery operations.
[31]	Provides instant theft notifications using IoT technologies.
[32]	Combines RFID and GPS for intelligent vehicle security.
[33]	Facilitates continuous vehicle tracking and monitoring.
[34]	Enhances access control using biometric authentication.
[35]	Integrates GSM, GPS and IoT technologies for comprehensive vehicle security.

3.PROBLEM STATEMENT

The rapid increase in the number of automobiles has been accompanied by a corresponding rise in vehicle theft incidents worldwide. Despite the availability of conventional security measures such as mechanical locks, alarm systems and ignition keys, vehicle theft remains a significant challenge due to the advancement of theft techniques and the growing sophistication of criminals. In many cases, once a vehicle is stolen, the owner has very limited options for locating, tracking or recovering the vehicle. The absence of real-time monitoring and remote-control mechanisms significantly reduces the chances of successful vehicle recovery.

Most traditional vehicle security systems are designed only to prevent unauthorized access and do not provide adequate support after the theft has occurred. As a result, vehicle owners often face difficulties in identifying the exact location of the stolen vehicle, communicating with law enforcement agencies and preventing further movement of the vehicle. This lack of immediate response and control leads to financial losses, increased recovery costs and reduced confidence in existing security solutions.

Another major limitation of conventional systems is the absence of a centralized platform that allows vehicle owners to monitor their vehicles remotely. Without continuous location updates and instant notifications, owners are unable to take timely action during theft incidents. Furthermore, unauthorized individuals can continue operating the stolen vehicle without any restriction, making recovery even more difficult.

To overcome these challenges, there is a need for an intelligent and integrated vehicle security system capable of detecting theft, providing real-time vehicle tracking, notifying the owner instantly and remotely controlling vehicle operation. The proposed IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System addresses these issues by integrating GPS, GSM, IoT connectivity and remote engine

immobilization technologies. The GPS module enables accurate real-time location tracking of the vehicle, while GSM communication facilitates instant theft alerts and status updates to the owner. Through an Android-based mobile application, the vehicle owner can continuously monitor the vehicle's location and remotely immobilize the engine when unauthorized activity is detected.

By providing real-time tracking, immediate theft notifications and remote engine control, the proposed system significantly improves vehicle security and increases the probability of vehicle recovery. The system aims to minimize financial losses, enhance user confidence and provide a reliable and cost-effective solution for modern automobile theft prevention and management.

4.EXISTING MODEL

Existing vehicle security systems primarily focus on individual functionalities such as vehicle tracking, theft detection, alarm generation, biometric authentication, GPS-based monitoring, GSM-based notification and remote engine locking. Several studies have proposed systems that utilize GPS and GSM technologies for location tracking and theft alerts, while others employ fingerprint authentication to prevent unauthorized vehicle access. Recent IoT-based solutions have further improved vehicle monitoring by enabling real-time communication and remote access capabilities.

Although these systems contribute significantly to vehicle security, most of them address only specific aspects of theft prevention. Many existing approaches rely solely on alarm systems, location tracking or authentication mechanisms without providing a complete end-to-end security solution. In several cases, vehicle owners receive theft notifications but have limited control over the stolen vehicle. Similarly, some systems offer engine immobilization features but lack real-time tracking and continuous monitoring capabilities. Furthermore, the implementation cost of many commercial anti-theft products remains relatively high, making them less accessible to a wider range of vehicle owners.

Based on the analysis of the 35 research works reviewed in the literature survey, it is evident that most existing systems focus on either tracking, authentication, notification or immobilization individually rather than integrating all essential security features into a unified framework.

4.1 Drawbacks of Existing Models

1. Most existing systems provide only vehicle tracking or theft alerts without offering complete theft prevention mechanisms.
2. Several solutions rely solely on GPS and GSM technologies and do not incorporate biometric authentication for secure vehicle access.
3. Many systems can detect theft incidents but cannot remotely immobilize or control the vehicle after theft.
4. Existing biometric-based systems prevent unauthorized access but do not support real-time location tracking and theft notifications.
5. IoT-based monitoring systems often lack integrated engine immobilization functionality.
6. Some vehicle immobilization techniques may affect vehicle operation abruptly, creating safety concerns.
7. A majority of existing solutions operate as standalone systems and do not provide a comprehensive platform integrating tracking, authentication, notification and control.
8. Commercial anti-theft systems are often expensive and may not be affordable for all vehicle owners.
9. Several systems do not provide continuous real-time monitoring through mobile applications.
10. The absence of image-based evidence and advanced security features reduces the effectiveness of vehicle recovery efforts.

5. PROPOSED SYSTEM

The proposed IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System is designed to provide a comprehensive vehicle security solution by integrating Fingerprint Authentication, GPS Tracking, GSM Communication, IoT Monitoring and Remote Engine

Immobilization. The system enhances vehicle protection by ensuring that only authorized users can access the vehicle while enabling real-time monitoring and remote-control capabilities in the event of theft. The proposed system architecture is illustrated in Figure 1.

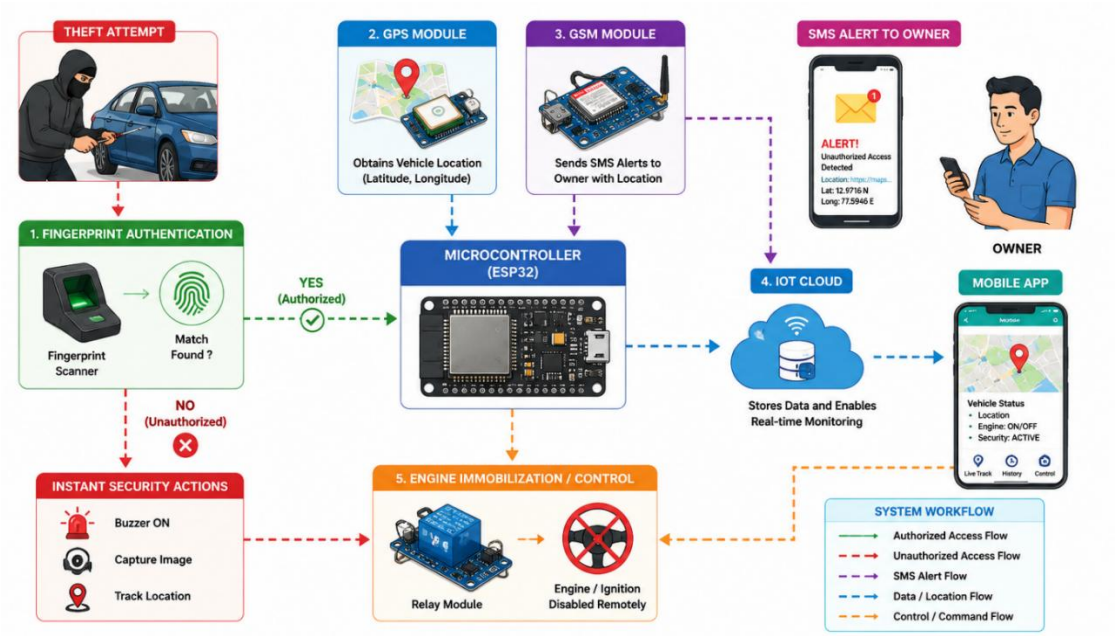

Fig 1. Proposed System Architecture

1. FINGERPRINT-BASED AUTHENTICATION

The proposed system employs a fingerprint sensor to verify the identity of the vehicle user before granting access to the ignition system. When a user attempts to start the vehicle, the fingerprint scanner captures the fingerprint image and compares it with the authorized fingerprints stored in the system database. If the fingerprint matches an authorized record, the ignition system is enabled, allowing the vehicle to start. Otherwise, access is denied and the system identifies the attempt as unauthorized. This biometric authentication mechanism significantly reduces the possibility of vehicle theft caused by duplicated keys or unauthorized access.

2. GPS-BASED VEHICLE TRACKING

The system incorporates a GPS module to continuously monitor the vehicle's geographical location. The GPS receiver collects precise information such as latitude, longitude, speed and route details. In the event of theft, the vehicle owner can access the real-time location through a mobile application or web interface. Continuous tracking enables efficient vehicle monitoring and significantly improves the probability of vehicle recovery.

3. GSM-BASED ALERT COMMUNICATION

A GSM communication module is integrated into the system to provide instant notifications and alerts. Whenever an unauthorized access attempt is detected, the system automatically sends alert messages to the registered vehicle owner's mobile phone. The transmitted information includes the vehicle status, location coordinates and security alerts. This ensures immediate awareness of suspicious activities and enables rapid response from the owner.

4. IOT-BASED REMOTE MONITORING

The proposed system utilizes IoT technology to establish communication between the vehicle and the user's mobile application. Through cloud-based connectivity, vehicle information such as location, security status, authentication logs and theft alerts can be monitored remotely. The IoT platform provides real-time access to vehicle data from any location, enhancing convenience and security.

5. REMOTE ENGINE IMMOBILIZATION

One of the key features of the proposed system is the remote engine immobilization mechanism. Upon detecting vehicle theft or

unauthorized operation, the owner can remotely disable the ignition system using the mobile application. This functionality prevents further movement of the vehicle and increases the likelihood of vehicle recovery. The immobilization process is designed to be safe and controlled, ensuring effective theft prevention.

6. INTEGRATED VEHICLE SECURITY FRAMEWORK

Unlike existing systems that focus on individual security features, the proposed system integrates fingerprint authentication, GPS tracking, GSM alerts, IoT monitoring and engine immobilization into a unified platform. This comprehensive approach enhances vehicle security, reduces theft risks, improves recovery rates and provides vehicle owners with greater control over their vehicles.

A comparative analysis of the existing works and the proposed system is presented in Table 2.

Table 2 Comparative Analysis of Existing Works and Proposed System

Ref. No.	GPS Tracking	GSM Alert	IoT Support	Fingerprint Authentication	Engine Immobilization	Real-Time Monitoring
[1]	✓	✓	✗	✗	✗	✓
[2]	✓	✓	✗	✗	✓	✓
[3]	✓	✓	✗	✗	✓	✗
[4]	✓	✓	✗	✗	✗	✓
[5]	✓	✗	✗	✗	✗	✓
[6]	✓	✓	✗	✗	✓	✗
[7]	✗	✗	✗	✓	✗	✗
[8]	✓	✗	✗	✗	✗	✗
[9]	✗	✗	✗	✓	✗	✗
[10]	✗	✗	✗	✗	✗	✗
[11]	✗	✓	✗	✗	✓	✗
[12]	✓	✓	✗	✓	✗	✗
[13]	✗	✗	✗	✓	✗	✗
[14]	✓	✓	✓	✗	✗	✓
[15]	✗	✓	✓	✗	✗	✓
[16]	✗	✗	✗	✓	✗	✗
[17]	✗	✗	✗	✓	✗	✗
[18]	✗	✗	✗	✗	✗	✗
[19]	✓	✓	✗	✗	✗	✓
[20]	✗	✗	✗	✗	✓	✓

[21]	✓	✓	✓	X	X	✓
[22]	✓	✓	✓	X	X	✓
[23]	✓	✓	X	X	X	✓
[24]	✓	✓	✓	X	X	✓
[25]	✓	X	✓	X	X	✓
[26]	✓	✓	X	X	✓	X
[27]	X	X	X	✓	X	X
[28]	X	✓	✓	X	X	✓
[29]	✓	X	X	X	✓	✓
[30]	✓	✓	✓	X	X	✓
[31]	✓	✓	✓	X	X	✓
[32]	✓	X	X	X	X	✓
[33]	✓	X	✓	X	X	✓
[34]	X	X	X	✓	X	X
[35]	✓	✓	✓	X	✓	✓
Proposed System	✓	✓	✓	✓	✓	✓

6. BLOCK DIAGRAM

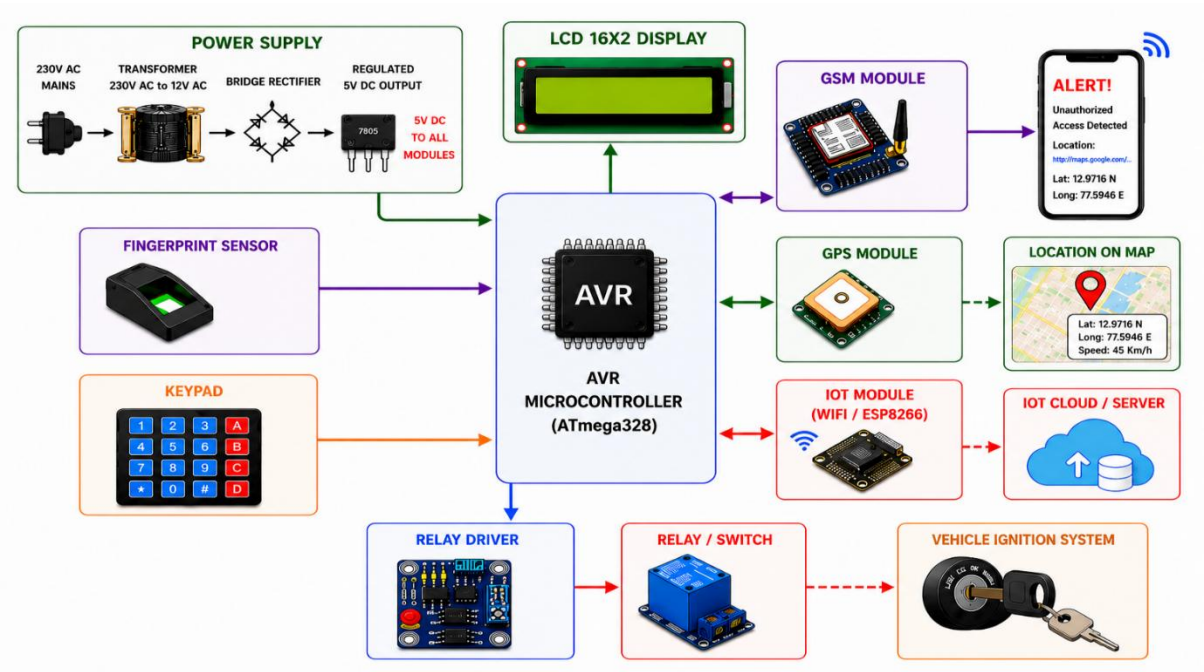

Fig 2. Block Diagram

The proposed IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System in Figure 2 consists of several hardware and communication modules that work together to provide enhanced vehicle security. The AVR ATmega328 microcontroller serves as the central processing unit of the system and coordinates the operation of all connected modules. The entire system is powered by a regulated power supply unit that provides a stable DC voltage to ensure reliable operation of the electronic components.

The fingerprint sensor acts as the primary authentication module of the system. Before starting the vehicle, the user is required to place a finger on the sensor for identity verification. The captured fingerprint is compared with the fingerprint templates stored in the system database. If a valid match is found, the microcontroller grants access and enables the vehicle ignition system. In contrast, if the fingerprint does not match any authorized record, the system identifies the attempt as unauthorized and activates the security mechanisms.

A keypad module is incorporated to provide additional user interaction and authentication capabilities. It allows users to enter passwords, administrative commands and security settings whenever required. The keypad serves as a secondary authentication mechanism and enhances overall system flexibility. The LCD 16×2 display provides real-time information regarding system status and operational activities. It displays messages such as fingerprint verification status, vehicle security status, GPS connectivity and engine lock conditions. This visual feedback helps users monitor the system effectively.

The GPS module continuously acquires the geographical coordinates of the vehicle, including latitude and longitude values. These coordinates are transmitted to the microcontroller and are used for real-time vehicle tracking. Whenever a theft attempt is detected, the GPS module enables the owner to monitor the exact location of the vehicle, thereby improving recovery possibilities.

The GSM module is responsible for communication between the vehicle and the owner. Upon detecting unauthorized access, the microcontroller activates the GSM module, which sends an alert message containing the vehicle's location details to the registered mobile number. This immediate notification allows the owner to take necessary action without delay. To facilitate remote monitoring and control, an IoT communication module is integrated into the system. The IoT module uploads vehicle information such as location data, authentication records and security alerts to a cloud server. Through a mobile application, the vehicle owner can access this information from any location and continuously monitor the vehicle's status.

The cloud server functions as a centralized storage platform for vehicle information. It maintains records related to vehicle location, user authentication activities, theft alerts and engine status. The cloud infrastructure enables real-time data accessibility and supports remote decision-making by the vehicle owner. The relay driver circuit serves as an interface between the microcontroller and the ignition control system. It receives control signals from the microcontroller and activates the relay accordingly. The relay switch is connected to the vehicle ignition circuit and plays a crucial role in engine immobilization.

During normal operation, when a valid fingerprint is detected, the relay remains activated and allows the ignition system to function normally. However, in the event of theft or unauthorized access, the vehicle owner can remotely send an immobilization command through the mobile application. Upon receiving this command, the microcontroller deactivates the relay, disconnects the ignition circuit and prevents further movement of the vehicle.

Thus, the integration of fingerprint authentication, GPS tracking, GSM communication, IoT monitoring, cloud connectivity and remote engine immobilization provides a comprehensive vehicle security framework capable of preventing theft, enabling real-time monitoring and improving vehicle recovery rates.

7.COMPONENTS USED

7.1 Power Supply Unit

The power supply unit provides the electrical energy required for the entire system to operate efficiently. It converts the available 230V AC mains supply into a regulated 5V DC output using a transformer, rectifier, filter and voltage regulator. This regulated voltage is supplied to the

ATmega328 microcontroller, fingerprint sensor, GSM module, GPS module, LCD display and other peripheral devices. A stable power supply is essential for ensuring uninterrupted communication and reliable system performance. Figure 3 presents the power supply unit used in the proposed system.

Fig 3 Power Supply Unit

7.2 AVR Microcontroller (ATmega328)

The ATmega328 microcontroller serves as the central processing unit of the proposed vehicle security system. It receives data from all input devices, processes the information according to the programmed logic and controls the operation of the entire system. The microcontroller is responsible for user authentication, theft detection, location tracking, alert generation and engine immobilization. Since all decisions are made by the microcontroller, it acts as the brain of the system. Figure 4 presents the AVR microcontroller (ATmega328), which serves as the central processing unit of the system.

Fig 4 AVR Microcontroller (ATmega328)

7.3 Fingerprint Sensor

The fingerprint sensor is used to authenticate the identity of vehicle users. It captures the fingerprint image of the person attempting to start the vehicle and compares it with the fingerprint templates stored in memory. If a valid match is found, the system grants access and enables vehicle ignition. If the fingerprint does not match any registered user, the system treats it as an unauthorized access attempt and activates the theft prevention mechanism. The fingerprint sensor employed for user authentication is shown in Figure 5.

Fig 5 Fingerprint Sensor

7.4 GSM Module

The GSM module enables wireless communication between the vehicle and the owner through the cellular network. It sends SMS notifications whenever important events occur, such as vehicle start-up, unauthorized access and engine locking. The module also transmits vehicle location information to the owner, allowing immediate action during theft situations. This communication feature significantly improves the responsiveness of the security system. The GSM module, which enables wireless communication, is depicted in Figure 6.

Fig 6 GSM Module

7.5 GPS Module

The GPS module continuously receives signals from satellites and calculates the exact geographical location of the vehicle. The obtained latitude and longitude coordinates are transmitted to the microcontroller and then forwarded to the vehicle owner through SMS alerts. This module enables real-time vehicle tracking and assists in locating and recovering stolen vehicles quickly and accurately. The GPS module employed for real-time location tracking is shown in Figure 7.

Fig 7 GPS Module

7.6 LCD 16×2 Display

The LCD display provides a visual interface between the user and the system. It displays important operational messages such as system initialization, fingerprint verification status, authorized user information, access granted notifications, theft alerts and module detection status. The display helps users understand the current state of the system and improves user interaction. The LCD 16×2 display, which provides visual feedback to the user, is depicted in Figure 8.

Fig 8 LCD 16×2 Display

7.7 Keypad

The keypad provides a manual interface for user interaction and system configuration. It can be used for entering passwords, registering users, changing system settings and performing administrative operations. The keypad serves as an additional layer of control and security within the system. Figure 9 illustrates the keypad used in the proposed system.

Fig 9 Keypad

7.8 Relay Driver Circuit

The relay driver circuit acts as an intermediary between the microcontroller and the relay module. Since the microcontroller cannot directly supply the current required to operate the relay, the relay driver amplifies the control signal and safely switches the relay ON or OFF. This ensures reliable operation while protecting the microcontroller from electrical damage. The relay driver circuit used to control the relay operation in the proposed system is illustrated in Figure 10.

Fig 10 Relay Driver Circuit

7.9 Relay/Switch Module

The relay module functions as an electronic switch that controls the vehicle ignition system. During normal operation, the relay allows the ignition circuit to remain active, enabling the engine to start. When unauthorized access is detected or a remote lock command is issued, the relay disconnects the ignition circuit and immobilizes the vehicle. This mechanism is the primary theft prevention feature of the proposed system. Figure 11 illustrates the relay/switch module used in the proposed system.

Fig 11 Relay/Switch Module

7.10 Vehicle Ignition System

The vehicle ignition system represents the engine starting mechanism that is controlled by the relay module. The ignition system remains disabled until a valid fingerprint authentication is completed. This ensures that only authorized users can operate the vehicle and prevents unauthorized vehicle usage. The vehicle ignition system, which enables the starting and stopping of the vehicle, is depicted in Figure 12.

Fig 12 Vehicle Ignition System

7.11 IoT Module (ESP8266)

The ESP8266 IoT module provides internet connectivity to the system and enables cloud-based monitoring. It collects information such as vehicle location, security status and system events from the microcontroller and uploads them to the cloud server. Through IoT integration, vehicle owners can monitor their vehicles remotely using mobile or web applications. The ESP8266 IoT module employed for wireless communication and cloud connectivity is shown in Figure 13.

Fig 13 IoT Module (ESP8266)

7.12 IoT Cloud Server

The cloud server stores and manages vehicle-related information received from the IoT module. It maintains records of vehicle locations, security alerts, authentication logs and system status updates. Cloud storage allows users to access real-time as well as historical information from any location, enhancing the effectiveness of the monitoring system. The IoT cloud server employed for data storage and remote monitoring is shown in Figure 14.

Fig 14 IoT Cloud Server

7.13 Mobile Phone

The mobile phone acts as the remote monitoring device for the vehicle owner. It receives SMS alerts, security notifications and Google Maps location links whenever significant events occur. Through these notifications, the owner can continuously monitor the vehicle and take immediate action in case of unauthorized access or theft attempts. The mobile phone employed for remote monitoring and user notifications is shown in Figure 15.

Fig 15 Mobile Phone

8. RESULT AND IMPLEMENTATION

The hardware kit representation of the proposed system is illustrated in Figure 16.

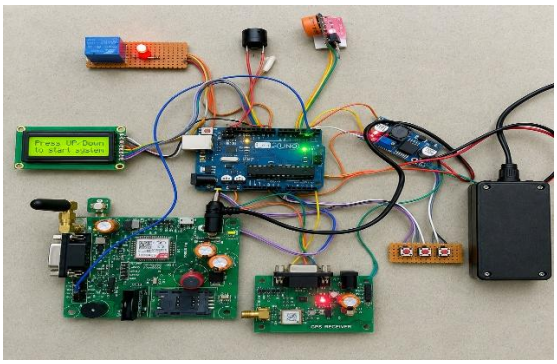

Fig 16 Kit Representation

The operational flowchart depicting the sequence of activities performed by the proposed system is illustrated in Figure 17.

During normal operation, the authorized user places a registered fingerprint on the fingerprint sensor. The microcontroller verifies the fingerprint with the stored database. If a valid match is found, access is granted and the relay activates the vehicle ignition system. The vehicle starts normally, while the GPS module continuously monitors the vehicle location. The LCD display shows the authentication status and system information. Thus, only

authorized users are allowed to operate the vehicle, ensuring secure access and normal vehicle functioning.

When an unauthorized user attempts to access the vehicle, the fingerprint verification process fails. The microcontroller immediately identifies the unauthorized access and prevents the vehicle from starting. Simultaneously, the GSM module sends an alert message containing the vehicle location to the registered owner's mobile phone. The GPS module continuously tracks the vehicle's position and updates the location information. Through the IoT platform, the owner can monitor the vehicle remotely and activate the engine immobilization feature. The relay then disconnects the ignition system, preventing further movement of the vehicle and improving the chances of vehicle recovery.

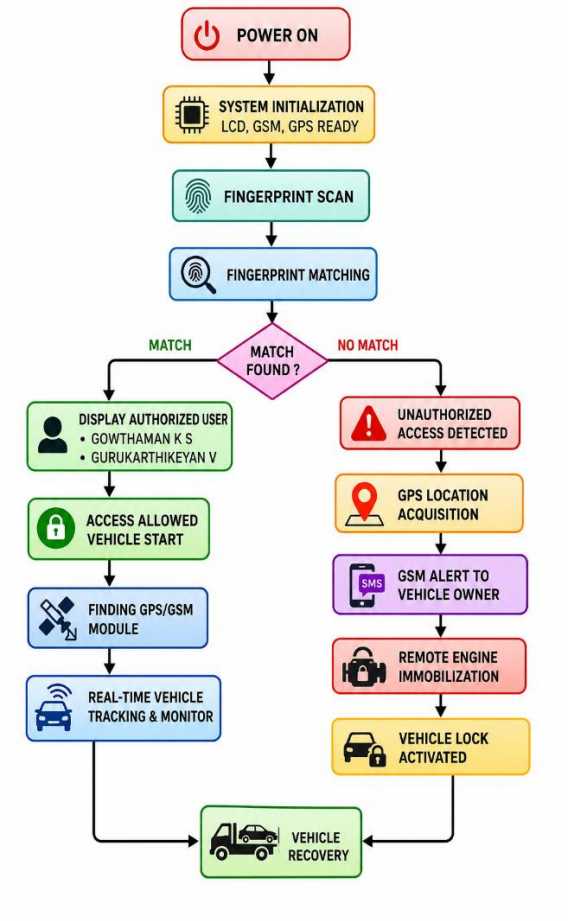

Fig 17 OPERATION FLOWCHART

8.1 OVERVIEW OF THE WORK – During Normal Operation

Fig 18 Experimental Results and Modes of Operation – During Normal Operation

The LCD displays shown in Figure 18 illustrate the different operating modes of the proposed IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System. Each display represents a specific stage in the vehicle authentication and security process.

1. System Initialization Mode

In this mode, the system is powered ON and all hardware modules such as the microcontroller, fingerprint sensor, GSM module, GPS module and LCD display are initialized. The LCD displays the work title “Biometric Authentication Vehicle”, indicating that the system is ready for operation and waiting for user authentication. During the System Initialization Mode, the system initializes all hardware modules, verifies the communication links among the connected devices, and prepares the fingerprint authentication mechanism for operation

2. Access Granted Mode

After successful fingerprint verification, the system grants access to the authorized user. The LCD displays the message “Access Allowed”, indicating that the authentication process has been completed successfully and the vehicle ignition system can be enabled. During the Access Granted Mode, the system verifies a successful fingerprint match, activates the relay circuit, and enables the vehicle engine to start.

3. Authorized User Identification Mode

Once the fingerprint is verified, the system identifies the corresponding registered user and

displays the user's name on the LCD. In the experimental setup, the LCD displays "GOWTHAMAN K S – Authorized User". Similarly, when another registered fingerprint is scanned, the system can display "GURUKARTHIKEYAN V – Authorized User". During the Authorized User Identification Mode, the system recognizes the authenticated vehicle owner, displays the corresponding registered user information, and enhances vehicle security by preventing unauthorized access.

4. Module Detection Mode

After authentication, the system verifies the availability of communication modules. The LCD displays "Finding Module", indicating that the GPS and GSM modules are being detected and initialized. Once the modules are successfully connected, vehicle tracking and alert functionalities become active. During the Module Detection Mode, the system identifies the GSM and GPS modules, verifies communication connectivity, and activates the vehicle tracking and notification functionalities.

8.2 OVERVIEW OF THE WORK – During Theft Condition

Fig 19 Experimental Results and Modes of Operation- During Theft Condition

The LCD displays shown in Figure 19 illustrate the different operating modes of the proposed IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System during an unauthorized access attempt. These modes are activated when the fingerprint authentication process fails and the system identifies a potential vehicle theft.

5. Unauthorized User Detection Mode

In this mode, an unregistered or invalid fingerprint is placed on the fingerprint sensor. The microcontroller compares the captured fingerprint with the stored database and determines that no matching record exists. As a result, access is denied and the LCD displays "Unauthorized User Detected.". During the Unauthorized User Detection Mode, the system identifies unauthorized access attempts, denies authentication for invalid fingerprints, disables engine ignition, and initiates theft prevention mechanisms.

6. Theft Alert Mode

Once unauthorized access is detected, the system immediately activates the GSM module and prepares to send an alert message to the registered vehicle owner. The LCD displays "Theft Alert Sending SMS..." indicating that the notification process is in progress. During the Theft Alert Mode, the system utilizes GSM communication to generate and transmit theft alert messages to the owner's mobile phone, thereby providing immediate notification of a potential security breach.

7. GPS Tracking Mode

After the alert message is sent, the GPS module starts acquiring the vehicle's current location. The LCD displays "Tracking Vehicle Getting Location" while searching for satellite signals and obtaining geographical coordinates. During the GPS Tracking Mode, the system obtains geographical coordinates from the GPS module, continuously monitors vehicle movement, provides real-time location updates, and facilitates vehicle recovery in case of theft or unauthorized use.

8. Vehicle Lock Mode

In this mode, the vehicle owner can remotely immobilize the engine through the GSM/IoT communication system. The relay disconnects the ignition circuit and the LCD displays "Vehicle Locked Engine Disabled.". During the Vehicle Lock Mode, the system immobilizes the vehicle by disabling the ignition mechanism, thereby preventing further movement and strengthening the overall security of the vehicle.

8.3 SMS RECEIVED BY OWNER

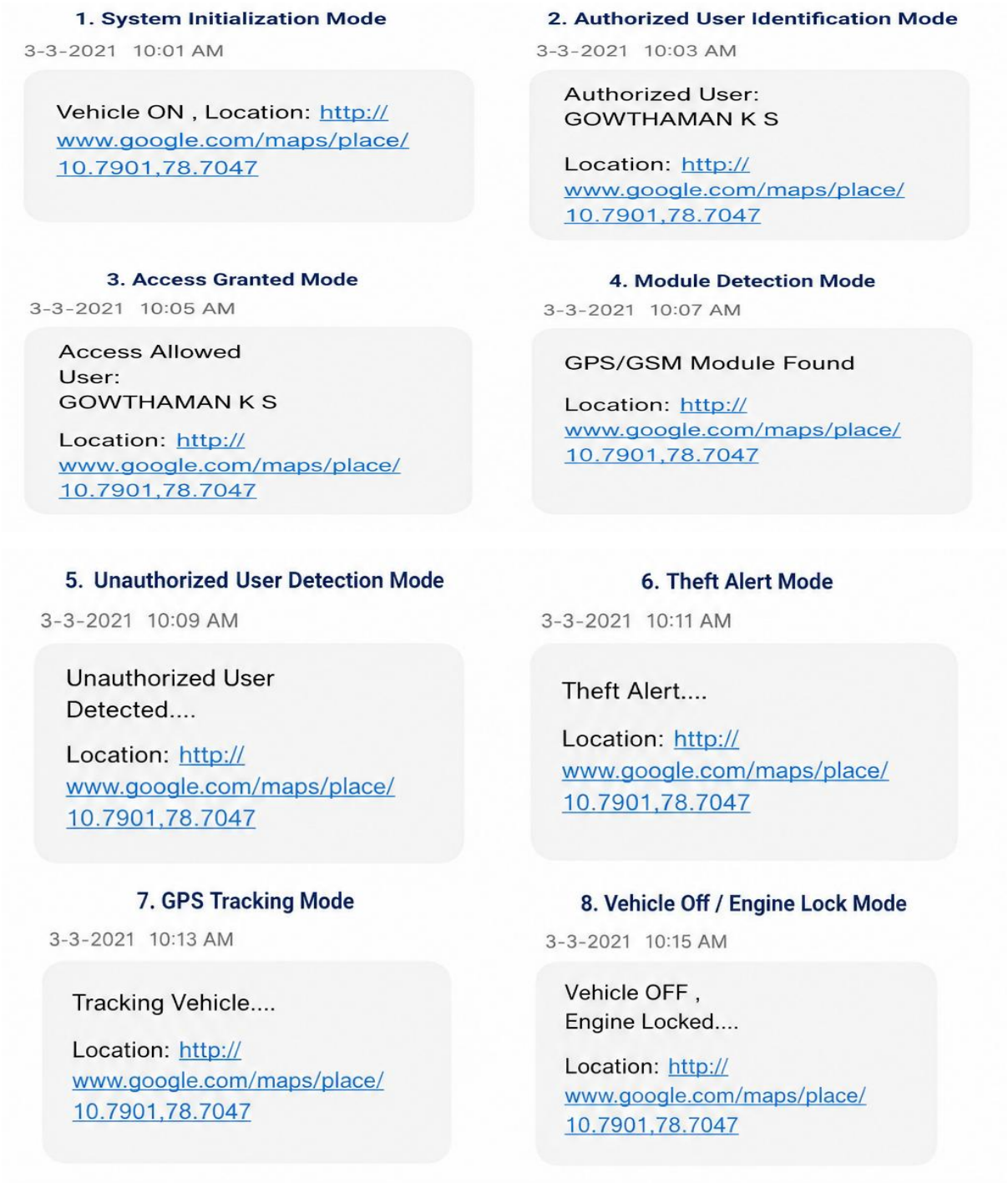

Fig 20 SMS RECEIVED

The SMS notification received on the user's mobile phone from the proposed system is illustrated in Figure 20.

9. CONCLUSION

This paper presented an IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System that enhances vehicle security through biometric authentication, real-time tracking and remote engine control. The proposed system utilizes fingerprint verification to ensure that only authorized users can access the vehicle. In the event of unauthorized access, the system immediately sends theft alerts to the vehicle owner

and provides the vehicle's real-time location through GPS and GSM technologies. Additionally, the remote engine immobilization feature helps prevent further movement of the stolen vehicle, thereby increasing the chances of vehicle recovery. The proposed system is cost-effective, reliable and suitable for modern vehicle security applications, offering an efficient solution for theft prevention and vehicle monitoring.

9.1 FUTURE ENHANCEMENT

The proposed IoT-Based Automobile Theft Detection, Tracking and Engine Immobilization System can be further enhanced by integrating advanced technologies to improve vehicle security and monitoring capabilities. Future versions of the system can incorporate a camera module (ESP32-CAM) to capture and transmit images of unauthorized users during theft attempts. The system can also be integrated with a mobile application that provides real-time vehicle status, location tracking and remote-control functionalities through the Internet. Cloud-based data storage can be employed to maintain vehicle logs, tracking history and security events for future analysis. Additionally, facial recognition, voice authentication and Artificial Intelligence (AI)-based threat detection can be implemented to strengthen user authentication and theft prevention. Integration with 4G/5G communication networks, geofencing and emergency response services can further enhance the reliability and effectiveness of the vehicle security system. These improvements would make the system more intelligent, secure and suitable for next-generation smart transportation applications.

REFERENCES

[1] K. Maurya and M. Singh, “Real Time Vehicle Tracking System Using GSM and GPS Technology—An Anti-Theft Tracking System,” *International Journal of Electronics and Computer Science Engineering*.

[2] R. Ramani, S. Valarmathy, S. Selvaraju, M. Thiruppathi and R. Thangam, “Vehicle Tracking and Locking System Based on GSM and GPS,” *International Journal of Intelligent Systems and Applications*.

[3] P. Ashwini, P. Madhuri and J. Vinoth Kumar, “Vehicle Theft Detection with Remote Engine Locking System,” 2021.

[4] V. Singh and S. P. Karmore, “GSM and GPS Based Vehicle Security and Controlling System,” *International Journal of Engineering Research and Applications*.

[5] M. S. Taha and M. H. Mahdi, “An Advanced Vehicle Tracking System Based on Arduino Electronic Shields and Web Map Browser,” 2021.

[6] M. M. Nayak, “Vehicle Theft Detection and Remote Engine Locking System,” 2020.

[7] B. Santosh Kumar, “Vehicle Anti-Theft System Using Fingerprint Recognition Technique,” 2017.

[8] C. Ram Kumar, B. Vijayalakshmi, C. Ramesh and S. Chenthur Pandian, “Vehicle Theft Alert and Tracking the Location Using RFID and GPS,” 2013.

[9] A. Somnath Karmude and G. R. Gidveer, “Vehicular Identification and Authentication System Using ZigBee,” *International Journal of Engineering Research and Technology*, vol. 3, no. 11, 2014.

[10] N. Abu, J. H. Rumel, H. Rokeb, P. Shuv, Y. Rashed and Adibullah, “Design and Implementation of Car Anti-Theft System Using Microcontroller,” *International Journal of Scientific & Engineering Research*, vol. 4, no. 3, 2013.

[11] K. S. Alli, C. Ijeh-Ogboi and S. L. Gbadamosi, “Design and Construction of a Remotely Controlled Vehicle Anti-Theft System via GSM Network,” *International Journal of Education and Research*, vol. 3, no. 5, pp. 405–418, 2015.

[12] S. Mali and J. A. Shaikh, “Fingerprint Based Authentication and Security System Using GSM and GPS Technology,” *International Journal of Engineering Trends and Technology (IJETT)*, vol. 45, no. 8, 2017.

[13] K. Rana Gill and J. Sachin, “Vehicle Ignition Using Fingerprint Sensor,” *IJIRST*, vol. 2, no. 12, 2016.

[14] S. Priyadarshini, "An IoT Based Anti-Theft Detection and Notification System for Vehicles," 2020.

[15] J. Arellano-Zubiate, "Design of an Anti-Theft Alarm System for Vehicles Using IoT," 2021.

[16] J. Sachin and K. Rana Gill, "Anti-Theft System for Vehicles Using Fingerprint Sensor," *International Journal of Scientific & Engineering Research*, vol. 7, no. 7, 2016.

[17] S. Mali, "Fingerprint Based Authentication and Security System," *International Journal of Engineering Trends and Technology*, 2017.

[18] C. B. R., B. R. Gowri, R. Kasturi and C. Pooja, "Vehicle Theft Detection and Prevention."

[19] S. S. Kanase et al., "GSM & GPS Based Vehicle Theft Control System," *International Research Journal of Engineering and Technology (IRJET)*, 2018.

[20] S. Patil and S. Tale, "CAN Based Control of Theft Vehicles," *International Journal of Science and Technology Research*, 2016.

[21] A. A. Ahmed and M. A. Mohammed, "IoT-Based Smart Vehicle Security and Monitoring System," *International Journal of Advanced Computer Science and Applications*, 2021.

[22] M. A. Hossain, M. R. Islam and S. Ahmed, "Real-Time Vehicle Tracking and Theft Detection Using IoT," *IEEE Conference Proceedings*, 2021.

[23] S. R. Prasad and P. V. Rao, "Smart Vehicle Security System Using GPS and GSM Technologies," *International Journal of Engineering Research*, 2020.

[24] K. Karthikeyan and R. Balaji, "IoT Enabled Vehicle Anti-Theft and Tracking System," *International Journal of Innovative Technology and Exploring Engineering*, 2020.

[25] P. Sharma and R. Verma, "Automobile Security Enhancement Using IoT and GPS," *International Journal of Computer Applications*, 2020.

[26] M. K. Singh and A. Kumar, "Remote Vehicle Immobilization and Tracking Using GSM Technology," *International Journal of Scientific Research in Engineering and Management*, 2019.

[27] A. Jain and S. Gupta, "Biometric Vehicle Authentication System Using Fingerprint Recognition," *International Journal of Engineering Science and Computing*, 2019.

[28] N. K. Patel and D. Shah, "IoT-Based Smart Vehicle Monitoring and Security System," *International Journal of Advanced Research in Computer Engineering and Technology*, 2019.

[29] V. Reddy and S. Kumar, "Vehicle Security System with Real-Time GPS Tracking and Engine Locking," *International Journal of Recent Technology and Engineering*, 2019.

[30] R. Srinivasan and P. Kumar, "Cloud-Based Vehicle Theft Detection and Recovery System," *International Journal of Computer Science and Information Security*, 2018.

[31] A. K. Mishra and S. Tiwari, "Smart Vehicle Tracking and Alert System Using IoT," *International Journal of Computer Applications*, 2018.

[32] S. Venkatesh and K. Ramesh, "RFID and GPS Based Intelligent Vehicle Security System," *International Journal of Engineering Research and Technology*, 2018.

[33] M. Prakash and S. Arulselvan, "IoT-Based Vehicle Tracking and Monitoring System," *International Journal of Pure and Applied Mathematics*, 2018.

[34] P. Gupta and A. Sharma, "Secure Automobile Access Control Using Biometric Authentication," *International Journal of Advanced Research in Electronics and Communication Engineering*, 2017.

[35] R. Kumar and V. Sharma, "Intelligent Anti-Theft Vehicle Security System Using GSM, GPS and IoT," *International Journal of Emerging Technologies and Innovative Research*, 2021.