Fingerprint Based Vechicle Anti-Theft Security System and Vechicle Ignition with Location Tracking

Mrs.D. Ramadevi[1], N. Shravya[2], S. Sandeep[3], S. Sushmitha[4,] P. Gopichand[5]
[1]*Professor, Dept. Of ECE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad*
[2,3,4,5] *UG Student, Dept. Of ECE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad*

***Abstract*—In modern times, the use of vehicles has become increasingly significant for individuals. Similarly, vehicle theft has been a growing concern for vehicle owners, primarily due to traditional key entry methods. Therefore, it is crucial to secure vehicles, which can be achieved through a vehicle tracking system coupled with a fingerprint sensor. To address the issue of theft, we propose a fingerprint-based anti-theft vehicle security system with location tracking, offering a convenient and secure approach for starting and stopping vehicles. Fingerprint technology has gained widespread use in various fields, such as educational institutions and companies. GPS and GSM technologies are cost-effective solutions for vehicle monitoring and communication. By integrating a fingerprint sensor, GPS, GSM modules, and the ESP32 micro controller, this research presents an effective and secure solution for vehicle protection.**

***Index Terms*—ESP32, fingerprint sensor, GPS, GSM, anti -theft system.**

1. INTRODUCTION

In the current landscape, one of the major challenges facing individuals and law enforcement alike is the lack of robust vehicle security systems. With the growing number of automobile theft incidents, the ability to efficiently trace and retrieve stolen vehicles has emerged as a pressing necessity. For instance, over 7.6 million vehicle theft cases were recorded in 2016, highlighting the scale of this problem. Although security technologies have evolved, many vehicle owners still experience substantial vulnerabilities, as recovery mechanisms are often insufficient once theft occurs. To counter this trend, the implementation of cutting-edge technologies has become essential. Embedded systems have gained prominence for their ability to deliver effective surveillance and tracking capabilities [1][4]. Conventional security measures, such as locks and alarms, are increasingly inadequate in preventing unauthorized vehicle access. This highlights the need for a more dynamic and responsive system. Establishing a real-time communication link between vehicle and owner significantly improves the odds of recovering stolen property. Advanced systems utilizing smart tracking and instant alert mechanisms can notify owners immediately upon detecting suspicious activity, allowing them to intervene quickly. Such innovations not only serve as theft deterrents but also contribute to strengthening transportation security as a whole [2][6].

The system presented in this study enhances vehicle protection by incorporating fingerprint-based biometric authentication as its central control mechanism. By validating the authorized user's fingerprint before allowing ignition, the system blocks unauthorized individuals from operating the vehicle, thereby significantly reducing the risk of theft [5]. Unlike conventional methods relying on keys or passcodes, fingerprint scanning provides a more secure and individualized form of access control. To further reinforce the security framework, the system integrates an ESP32 microcontroller with GPS and GSM modules. This combination allows for continuous real-time location tracking and seamless communication between the vehicle and its owner [3][7]. The GPS component ensures precise positional data, while the GSM module facilitates the transmission of alerts via SMS. In case of any unauthorized entry or suspected theft attempt, the system immediately alerts the owner, enabling rapid response and reducing potential losses. By merging biometric verification with intelligent tracking technology, this solution offers a well-rounded defense mechanism, addressing both preemptive and reactive aspects of vehicle safety. Ultimately, it delivers enhanced reliability and assurance for vehicle users.

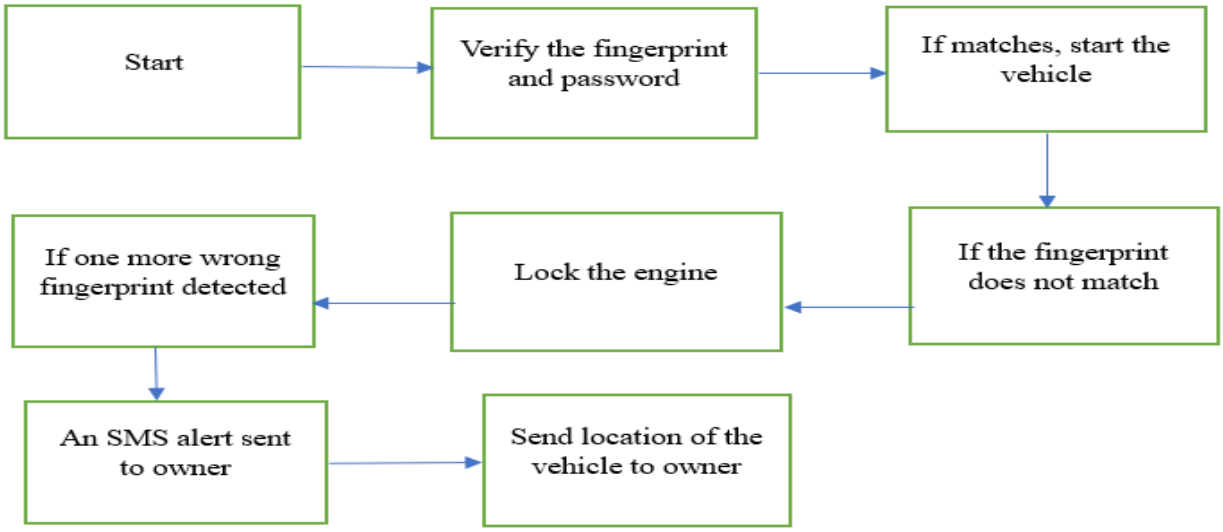

Fig 1.1: Overview of anti-theft system

2. LITERATURE REVIEW

As outlined in [1], an automobile security framework was implemented combining RFID and GPS technologies to facilitate both theft prevention and real-time vehicle tracking. The design incorporated mobile network communication within the embedded system, enabling continuous monitoring. A buzzer system was employed to issue an audible alert whenever an incorrect password was input. Simultaneously, the owner received an immediate notification via GSM, along with real-time GPS coordinates (latitude and longitude) pinpointing the vehicle's location. This approach enhanced the system's ability to identify unauthorized access attempts swiftly.

In [2], a GPS and GSM-based multi-vehicle tracking system was introduced, focusing on continuous navigation data collection. The GPS unit regularly captured the vehicle's coordinates and related metrics, while GSM was utilized to transmit this data to a remote tracking server. The server stored the incoming data into a dedicated database, allowing both live tracking and retrospective analysis. The system also allowed users to remotely control the vehicle's ignition using SMS-based commands, supporting efficient vehicle management and theft intervention.

A different approach was adopted in [3], which introduced a vehicle identification and access control system using Zigbee for intra-campus surveillance. The system utilized a radio frequency module with unique IDs assigned to each vehicle, while driver verification was achieved through a keypad. When a vehicle approached the entry point, the Zigbee-enabled RF module communicated with a centralized database to verify credentials. Depending on the authentication result, the gate system permitted or denied access, enhancing controlled entry within secured areas.

In [4], a real-time vehicle tracking setup was built using GPS, GSM, and Google Earth. This system determined a vehicle's location through GPS, which was then sent via SMS to a central station using GSM. A Kalman filter was applied to refine location accuracy, and the processed coordinates were displayed on Google Earth for visualization. The primary objective was fleet management, resource deployment (such as dispatching police units), and issuing alerts for potential vehicle theft. However, the system lacked features like remote vehicle disabling, limiting its utility in certain theft scenarios.

A cost-efficient security solution was presented in [5], employing a microcontroller and RF communication to create an anti-theft system. It supported wireless data exchange between the vehicle and the owner through a 434 MHz RF module, offering up to 400 feet of coverage in clear areas. Nonetheless, the presence of obstacles significantly reduced the range, making the system unsuitable for long-distance monitoring or urban use. This limited the practicality of the solution for wide-area vehicle protection.

In [6], a GSM-controlled vehicle security system was introduced, allowing remote operation through SMS commands. This setup enabled the vehicle owner to send instructions to the system for monitoring and activating safety mechanisms, including relay control to disable the vehicle. However, a notable drawback was the absence of a user verification mechanism, which made the vehicle vulnerable to hot-wiring or unauthorized physical intervention. Furthermore, areas with weak GSM signals posed a significant challenge, reducing the reliability of the system in those environments.

To address increasing car theft rates, a GPS-GSM-based vehicle tracking system was developed in [7]. This system retrieved live GPS coordinates using a single embedded program that handled both GPS and GSM modules through an interrupt-driven approach. It could send standard location data via SMS and activate actuators for vehicle control. However, a major limitation was the absence of Cell Tower Triangulation capabilities. In scenarios where satellite connectivity was lost, the system failed to provide alternative location tracking, thereby reducing its effectiveness in some environments.

3. METHODOLOGY

The newly proposed system introduces fingerprint-based ignition control, where the fingerprint serves as the primary means of authentication. Unlike other biometric approaches previously implemented for vehicle access, which have often proven unreliable or insufficiently secure, this method emphasizes a more dependable solution. The system ensures that only pre-authorized users are permitted to start the vehicle, moving beyond simple ignition protection. By making biometric verification an essential condition for ignition, it significantly enhances vehicle security and minimizes the risk of unauthorized operation.

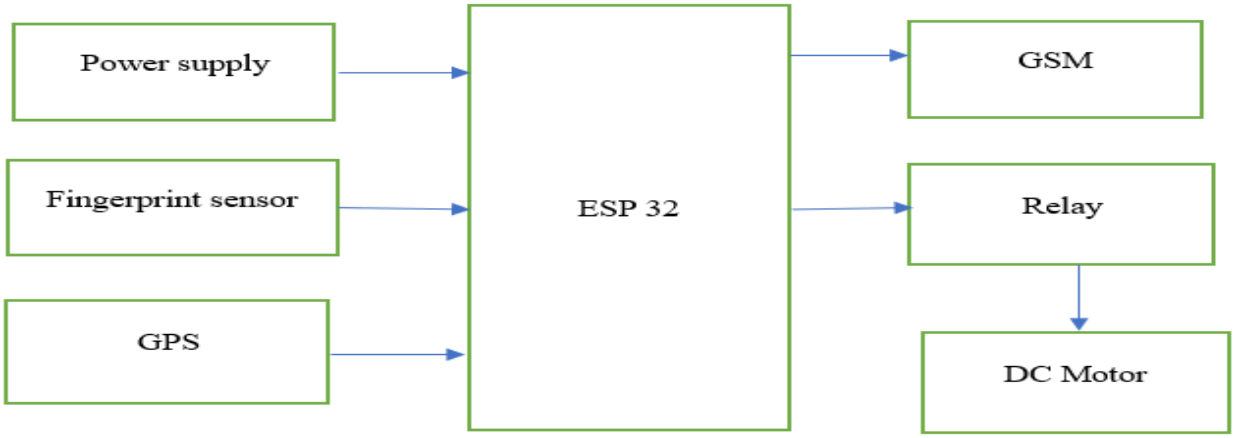

Fig 3.1: Block diagram of the system

ESP32: The ESP32, developed by Espressif Systems, is a highly efficient and affordable microcontroller that features a system-on-chip (SoC) design, making it particularly well-suited for embedded and IoT-based applications. It integrates dual-mode wireless communication capabilities, supporting both Wi-Fi and Bluetooth (Classic and BLE), which facilitates smooth and reliable connectivity for smart technologies. The ESP32 is compatible with major operating systems such as macOS, Linux, and Windows, allowing developers to program and deploy code across diverse platforms. At its core, the device operates on a 2.4 GHz radio frequency that simultaneously supports Wi-Fi and Bluetooth functionalities. Manufactured using TSMC's 40-nanometer ultra-low-power fabrication technology, the ESP32 achieves excellent performance while maintaining low energy consumption, making it a preferred choice for power-sensitive applications.

Fig 3.2: ESP 32 micro controller

Fingerprint Sensor: The R307 is a compact optical fingerprint module designed for dependable biometric identification in embedded systems. It captures fingerprint data at a resolution of 512×288 pixels, offering clear and precise image quality for accurate recognition. With the ability to store up to 1000 distinct fingerprint templates, it is well-suited for applications such as secure access control, identity verification, and attendance systems. The module supports internal processing, including image capture, template generation, matching, and deletion, eliminating the need for external computation. Its UART-based serial interface allows for seamless integration with a variety of microcontrollers, including Arduino and Raspberry Pi platforms. Equipped with an onboard DSP engine, the R307 delivers fast and efficient fingerprint processing while consuming minimal power, making it a practical and reliable choice for security-focused embedded designs.

Fig 3.3: Fingerprint sensor

GPS (Global Positioning System): The NEO-6 series GPS module is a compact and power-efficient solution known for delivering high-precision location tracking, operating at an update rate of up to 10Hz with support for 56 tracking channels. Built around the advanced U-blox 7 GNSS chipset, it can interface with multiple satellite navigation systems such as GPS, GLONASS, SBAS, and QZSS, enhancing positioning accuracy and reliability. The module is designed with robust RF architecture and interference-reduction features, enabling stable performance in environments where signal quality may fluctuate. Its small footprint, versatile interface options, and streamlined RF integration make it ideal for embedded systems and GPS-based applications requiring consistent and fast location updates.

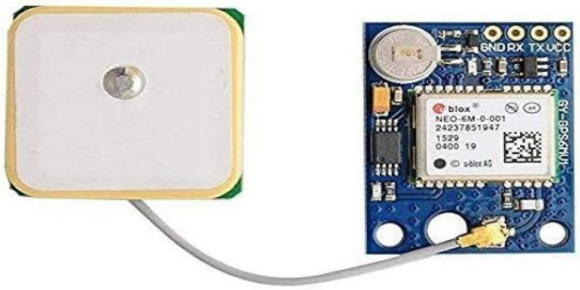

Fig 3.4: NEO-6M GPS Module

GSM (Global System for Mobile Communications): The SIM800L is a small-sized GSM/GPRS modem produced by Simcom, designed to provide cellular communication capabilities in embedded systems. It can be interfaced with various microcontrollers to enable mobile connectivity features such as voice calling, SMS messaging, and internet access over GPRS using TCP/IP protocols. This module offers seamless integration for wireless communication by supporting quad-band GSM/GPRS frequencies, making it compatible with global mobile networks. Its compact design and versatile functionality make it a reliable option for incorporating mobile network features into embedded applications.

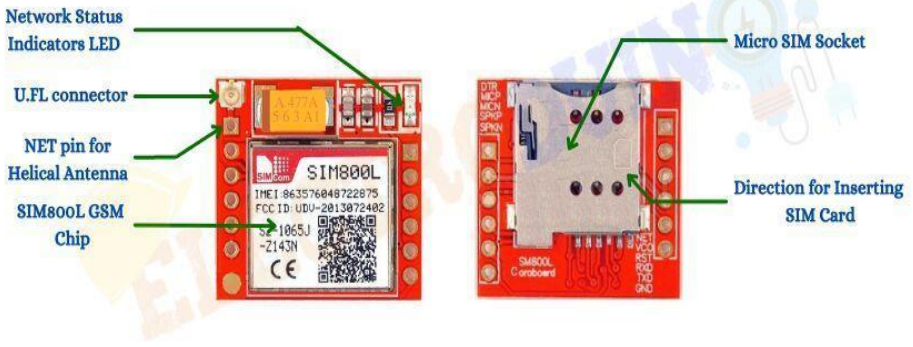

Fig 3.5: SIM800I GSM Module

Relay: A function used in microcontrollers to introduce a pause or time gap in the execution of instructions. It is useful for synchronizing processes, controlling response times, and ensuring smooth operation.

Fig 3.6: Relay Module

DC Motor: A motor that runs on direct current and is used to control vehicle movement. In security systems, it can be used for locking/unlocking mechanisms or controlling specific mechanical operations.

Fig 3.7: DC Motor

Power supply: The power supply delivers the required electrical energy to operate the system. It converts AC power from the mains into DC power which is suitable for the components, ensuring stable voltage and current for dependable operation.

Fig 3.8: Power supply

4. FLOWCHART

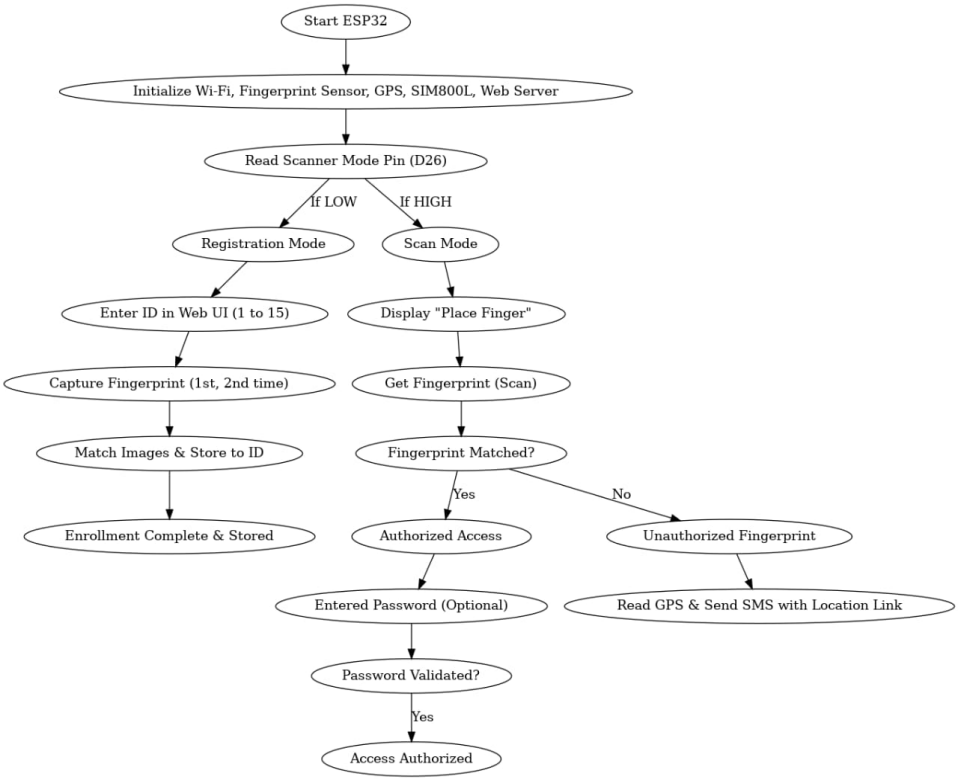

Fig 4.1: Flow chart of the system

Start & Initialization
The system begins by powering on the ESP32. It initializes the Wi-Fi module, fingerprint sensor, GPS, GSM module (SIM800L), and a web server.

Mode Selection (Scanner Mode Pin - D26)
The system reads the Scanner Mode Pin (D26) to determine its operating mode:
Registration Mode (if the pin is LOW)
Scan Mode (if the pin is HIGH)
Registration Mode (LOW State)
In this mode, the user enters an ID (1-15) through a Web UI. The system captures the fingerprint twice, matches the fingerprint images, and stores them under the provided ID. The enrollment is completed and saved for future authentication.
Scan Mode (HIGH State)
In Scan Mode, the system prompts the user to place their finger on the sensor for scanning. It compares the scanned fingerprint with the stored database.
If the fingerprint matches:The system grants authorized access. An optional password can be entered for additional security. If the password is validated, access is granted.
If the fingerprint does not match:The system identifies it as an unauthorized fingerprint. It triggers a GPS location reading and sends an SMS alert with the location link to the owner.

5. RESULTS

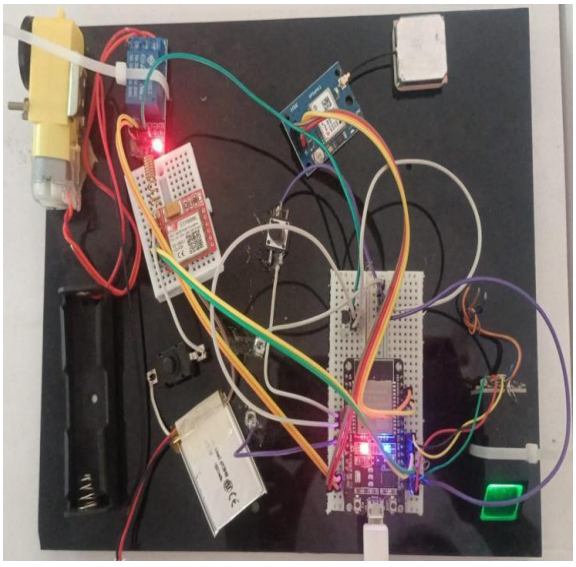

Fig 5.1: Set up of the system

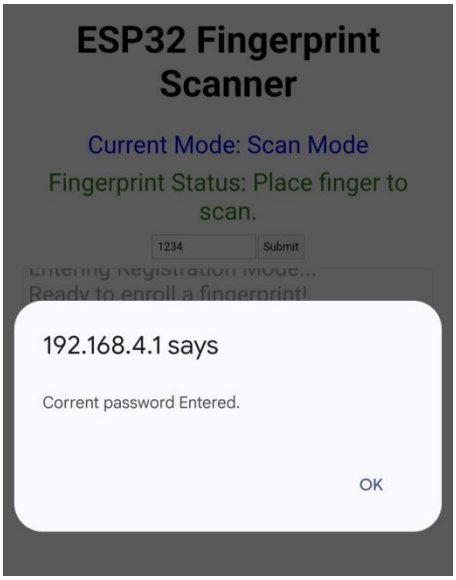

Fig 5.2: If the password is correct

Fig 5.3: Unauthorized fingerprint detected

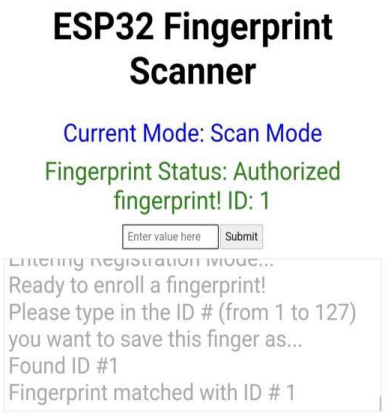

Fig 5.3: Fingerprint Capture

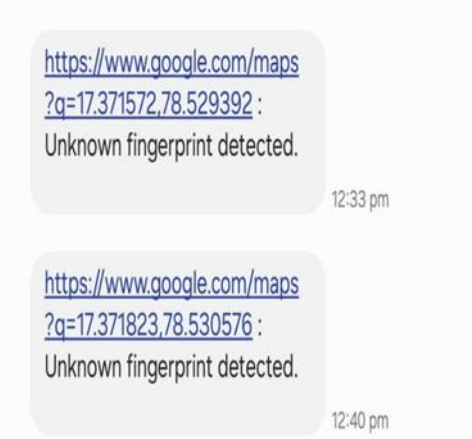

Fig 5.4:SMS Alert

Enrollment Test Result

Figure 5.3: illustrates the system's match certainty, which represents the level of evaluation of the user's fingerprint stored in the on-site database and the fingerprint that is being examining. This confidence indicates how closely the scanned print matches the saved print, reflecting the accuracy and reliability of the system's identification process.

6. CONCLUSION

The designed vehicle protection system offers an efficient response to the increasing threat of vehicle theft by combining biometric verification with live tracking capabilities. Through fingerprint-based authentication, the system ensures that only authorized users are able to start the vehicle, thereby minimizing the chances of unauthorized entry. Alongside this, the use of GPS and GSM modules allows for round-the-clock location monitoring and real-time SMS alerts to the vehicle owner, enabling swift action if any unusual activity is detected.

Future enhancements could involve the integration of artificial intelligence for advanced recognition, IoT-based connectivity for remote access and control, and 5G communication to improve responsiveness and data transmission speed. This approach provides a practical, scalable, and secure framework to tackle current vehicle security challenges, offering both deterrent features and real-time intervention capabilities to reduce theft-related incidents.

REFERENCES

[1] C. Ram Kumar, B.Vijayalakshmi, C. Ramesh, S. Chenthur Pandian, Vehicle Theft Alert and Tracking the Location using RFID and GPS, vol.3, no 12, pp 2- 28, 2013.

[2] K. Yuvraj, G. Suraj, G. Shravan and K. Ajinkya, Multi-Tracking System for vehicle using GPS and GSM, International Journal of Research in Engineering and Technology (IJRET), vol.3, no 3, pp 127-130, 2014.

[3] 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.

[4] A. A. Mohammad, Hybrid GPS-GSM Localization of Automobile Tracking System, International Journal of Computer Science & Information Technology, vol. 3, no.6, pp 75–85, 2011.

[5] 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(3), 2013.

[6] 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(5), pp 405-418, 2015.

[7] M. F. Saaid, M. A. Kamaludin, and A. S. Megat, Vehicle Location Finder Using Global Position System and Global System for Mobile. IEEE 5th Control and System Graduate Research Colloquium, 2014.