Development of an Anti-Theft Vehicle Security System using GPS and GSM Technology with Biometric Authentication

Akinwole Bukola
Department of Electrical/Electronic Engineering
University of Port-Harcourt, Nigeria

Abstract:- Vehicle theft is on the increase in Nigeria due to an unprecedented level of insecurity. Fortifying vehicles against theft and unauthorized users is very important. Therefore, a system which is capable of identifying and tracking vehicle from any geographical location is needed. This research paper presents a vehicle anti-theft system using Global Positioning System (GPS) and Global System for Mobile Communication (GSM) with fingerprint recognition technique for enhancing security of vehicles in an automobile industry. The improvements done to the existing work are the integration of fingerprint recognition module and the use of the real-time cloud database for data storage. The fingerprint module identifies and regulates the access of an intruder in starting the engine. If the person is confirmed, access to the vehicle is allowed and if not, alert message will be sent to the owner either via SMS or mobile app to immobilize the engine, thus preventing vehicle theft and time wastage in tracking stolen vehicles. The system consists of GPS module, GSM modem, fingerprint scanner sensor, Espressif ESP32 development board, 4WD Double Layer Smart Car Chassis and Immobilizer anti-theft relay. The GPS and GSM modules are utilized to determine the exact location of vehicles and to establish a two-way communication between authorized user and the device installed in the vehicle. The microcontroller is programmed using embedded C/C++.

Keywords: *Vehicle security system, GSM, GPS, fingerprint, mobile app, SMS, microcontroller.*

I. INTRODUCTION

Vehicle theft is a problem that has plague our societies due to security issues in Nigeria. Currently, there is a rapid increase in vehicle theft as criminals are discovering new ways to foil antitheft measures provided by the vehicle manufacturers. The automobile antitheft features such as alarm, steering wheel, kill switch, hood-lock and baby monitor security have a lot of drawbacks and are regarded as being ineffective and unable to prevent vehicle theft. However, due to the alarming rate of vehicle theft, people already have started using more effective anti-theft control systems like immobilizers in their vehicles [1]. But, immobilizer systems are expensive, time consuming to replace if lost and can be hacked easily, letting a thief steal the car.

To resolve these problems, there is a need to have intelligent systems that are capable of providing constant surveillance with the vehicles after they have been stolen and rapid response to attacks by maintaining constant communication with the vehicle owners. This paper attempts to proffer a lasting solution by exploring GPS and GSM technologies incorporated with fingerprint pattern recognition. Data transfer between the user and the proposed system are achieved through the mobile app or SMS protocol available in the cellular phone. The proposed system is interfaced with an immobilizer which uses Fingerprint identification to turn on the engine and intimate the vehicle owner of any unauthorized entry. To start the ignition of the four-wheeler one should enter the authorized fingerprint. This prevents the car from being hot-wired after entry has been achieved and thus minimising vehicle theft. Another great feature is the integration of the Global Positioning System (GPS)/Global System for Mobile communication (GSM) technologies. The GPS technology made it easy to identify the vehicles location and provides information through the GSM to the vehicle owner. The GSM is used for communicating to the authorized user about the status of the system. The importance of this proposed project cannot be over emphasized since it will help to reduce the rate of vehicle theft in our society.

II. LITERATURE REVIEW

- ❖ *Biometric Technology*

Biometric technology has an elongated history of use as a means of dependably recognising individuals. In recent years, traditional means of personal identification are challenged by biometric technology and it has been enjoying increasing adoption rate across the globe. Fingerprints and some other forms of recognition have been successfully used in law enforcement and forensics to identify suspects and victims for over a century. Fingerprint recognition systems have become one of the most frequently used biometric systems in the world with numerous applications [2] based on the persistence and uniqueness of fingerprints.

- *Global System for Mobile communication*

The GSM system establishes a communication path between two devices in order to relay a constant stream of digital data and voice signal [3]. The GSM is divided into switching system, base station system and mobile station. The theft alarm message is transmitted to the mobile phone using SMS and mobile based android app developed using Android Studio Integrated Development environment.

- *Global Positioning System (GPS)*

Global Positioning System is one of the predominant inventions in the 20th century. It is a satellite based radio navigation system that provides consistent positioning, navigation and timing services to users [4][5]. The GPS system uses trilateration which is a basic geometric principle that allows users to find his location if its distance from other locations is known. The GPS system is an indispensable device to detect automobiles theft.

- *Related Works*

The use of anti-theft control systems has been very popular lately among automobile. Although, most of the recent systems use GSM and GPS modules to provide vehicle location information to the owner. A number of developments have taken place in anti-theft systems for vehicles theft alarm and tracking. Some of the related ones are: Authors in [6] presented the implementation of vehicle theft alarm and location tracking system using GPS and RFID technologies. The main concept in this paper was the introduction of mobile communications into the embedded system to track vehicles. The system composed of a buzzer which gave the alarm sound when the password entered did not match with the original password. An alert notification through GSM module was sent to the vehicle owner. The location in term of the latitude and longitude of the unauthorized user was tracked and sent to the owner. A reliable multi- tracking system for multiple vehicles using GPS and GSM was proposed by [7]. The system used GPS navigation device to calculate the coordinates with other related information at each position as the vehicle moved continuously. The data was then transmitted to the tracking server through GSM and stored in the database for further use. The system was used for live vehicle tracking by sending short messages to turn the vehicle ignition on. A vehicular identification and authentication system based on Zigbee communication technology for security monitoring in a campus setting was proposed by [8]. The system provided restricted access to vehicles with the identification and authentication of vehicle entering the campus. The automated system was equipped with a vehicle RF module which composed of vehicle information with unique serial number for each vehicle and a keypad for entering password for driver authentication; the gate side RF module used RF reader for accessing vehicle information and the information was transferred to central database server through Zig bee interface for verification of vehicle access and authentication of the driver. The results were sent to the gate side module for further action. Authors in [9] proposed a system to track vehicles using Google Earth Application which he incorporated a GPS-GSM framework. The use of GPS was to enable the system to identify the vehicle's current position and the GSM to transfer the data via SMS to a recipient station. After the received GPS coordinates filtered utilizing a Kalman filter to upgrade the precision of measured position, Google Earth application was used to view the current location and status of each vehicle. The objective of this system was to manage fleet, police automobiles distribution and car theft alerts. However, this system was only explored to track down the exact location of a vehicle but not to demobilize the vehicle from a distant place. In order to ensure maximum security for any kind of automobiles, [10] designed and implemented a low-cost anti-theft security system using microcontroller. This system used a wireless communication protocol between the car owner and the device to control the security system. Remote data transmission occurred through a Radio Frequency (RF) module Transmitter with the instruction of a microcontroller. In the project the developer used the available transceiver set of frequency 434 MHz which could cover only 400 feet in free space. So, it could not cover a long distance. This length coverage problem was one of the major restrictions of this work. As a result of this the system could not be accessed over distant locations. [11] designed and constructed a vehicle anti-theft system which could be remotely controlled through GSM network. Communication between the user and the vehicle sub-system was via SMS. The system was designed to be accessed from a remote/distant location where there was GSM coverage to monitor, control and initiate the vehicle immobilizer relay when the vehicle has been stolen. This system did not integrate an authentication system to identify the user of the vehicle, thus it could be hot wired and due to the drawback of inconsistency in the availability of GSM network in some areas, the vehicle could not be protected from theft. The design and development of a cost effective and reliable Internet of things (IoT) framework which composed of an array of RFID sensors for the real time monitoring and tracking of a vehicle on its transit from one location to other location on the high speed expressway was presented in [12]. In this system, the velocity of the vehicle was approximated in the real-time environment using Euler's algorithms. A timestamp generated from the RFID enabled node was transmitted to the internet cloud and thus by using these timestamps a real-time distance versus time plots of the particular vehicle could be generated. If the vehicle crossed the limit then the driver along with the highway traffic authority could be notified using the web applications to get the same data of the vehicle in real-time. This work did not implement a vehicle protection system to prevent the vehicle from theft.

III. MATERIAL AND METHODS

The antitheft system is divided into two main sections:

Hardware System Components

❖ Espressif ESP32S Microcontroller

Espressif ESP32 microcontroller is a low cost and low-power system on a chip (SoC) microcontroller with Wi-Fi and dual-mode Bluetooth capabilities. It is used and programmed using computer running on Windows, Linux and macOS. It incorporates a single 2.4 GHz Wi-Fi-and-Bluetooth combo chip designed with the TSMC ultra-low-power 40 nm technology. The integration of Bluetooth, Bluetooth LE and Wi-Fi ensure that a wide range of applications can be targeted, and that the module is future proof: using Wi-Fi allows a large physical range and direct connection to the internet through a Wi-Fi router, while using Bluetooth allows the user to conveniently connect to the phone or broadcast low energy beacons for its detection.

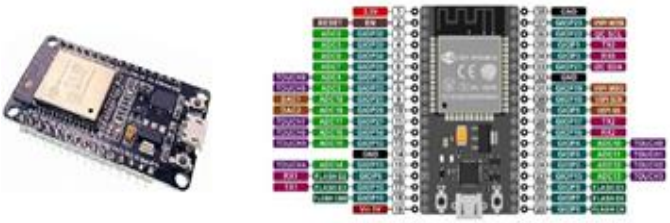


Fig 1:- Espressif ESP32 microcontroller and its pin configuration

❖ *Dual Antenna Interface GPS Mini NE0-7N EEPROM Satellite Positioning Module*

The NEO-7 series is a high sensitivity, low power GPS module that has 56 channels and outputs precise position updates at 10Hz. It is built on an exceptional performance of the u- blox 7 GNSS (GPS, GLONASS, QZSS and SBAS) engine. The NEO-7N provides best performance and easy RF integration. Sophisticated RF architecture and interference suppression ensure maximum performance even in GNSS hostile environments. It incorporates a high level of integration capability with flexible connectivity options in a small package. This makes it perfectly suited for industrial applications with strict size and cost requirements. The I2C compatible DDC interface provides connectivity and enables synergies with u-blox SARA, LEON and LISA cellular modules. For the purpose of the research work, the UART (Universal Asynchronous Receiver/Transmit--tter) interface will be used. The figure below shows the u-blox NEO-7 GPS module.

Fig 2:- U-blox NEO-7 GPS Module

❖ *A7 GSM, GPS and GPRS Module*

This is serial GSM / GPS core development board based on A7 and it supports GSM/GPRS Quad-Band (850/900/1800/1900）network, voice calls, SMS, GPRS data service and incorporates an embedded GPS function. The board features compact size and low current consumption. With power saving technique, the current consumption is as low as 3mA in sleep mode. T9his communicates with microcontroller via UART port, supports command including GSM 07.07, GSM 07.05 and Ai-Thinker enhanced AT Commands and supports 3.3V and 4.2V logical level. Figure 3 below illustrates the A7 GSM, GPS and GPRS Module.

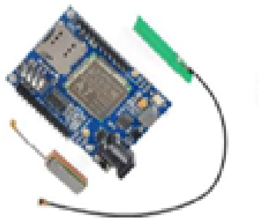


Fig 3:- A7 GSM, GPS and GPRS Module

❖ *Optical Fingerprint Reader Module (CAMA-SM25)*

The optical fingerprint scanner module is a fingerprint processing module for integrating the light path and fingerprint processing part. CAMA-SM25 is an ideal OEM embedded optical fingerprint module designed for biometric security solution. It is a small size, low power consumption, simple ports, high reliability, small fingerprint template (496bytes), large fingerprint capacity module which incorporates a fingerprint sensor and processor chip. The CAMA-SM25 embedded optical fingerprint module has outstanding features like self-learning function. During fingerprint authentication processing, the fingerprint module will update the latest fingerprint features to the fingerprint database automatically, so that the users will feel it and obtain better fingerprint verification performance. Figure 4 depicts the Optical Fingerprint scanner.

Fig 4:- Optical Fingerprint Sensor

- *4WD Double Layer Smart Car Chassis*

This 4WD double layer smart car chassis consists of two pairs of Geared Motors and Wheels. The chassis used in this kit is transparent acrylic board so as to create dynamic handling of the components mounted on the robotic vehicle. The Smart Car Chassis 4WD is made of imported acrylic material with high-precision laser cutting. It is featured with a double rotary encoder disk which can be used for speed.

Fig 5:- 4WD Double Layer Vehicle Chassis

- *2-Channel High Power H-Bridge L293D NodeMcu Motor Shield Board*

The GPIO pins of the microcontroller do not give the amount of current required by the geared motor, thus a motor driver is required. The NodeMcu Motor Shield is a driver module for motors that is used to control the working speed and direction of the motor.

Fig 6:- NodeMcu Motor Shield Board

- *Immobilizer Anti-Theft Relay*

Relays are switching devices that open and close circuits electromechanically or electronically. Relays control one electrical circuit by opening and closing contacts in another circuit. Figure 7 illustrates the immobilizer relay.

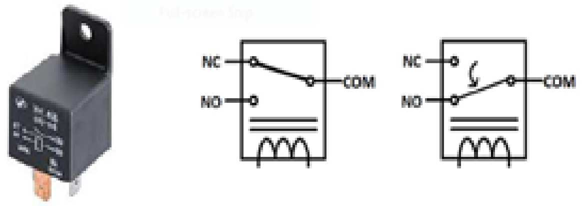


Figure 7:- Immobilizer Relay and Symbol

- *Power supply: NCR18650B 3.7 V12000mah 18650 Lithium Rechargeable Battery, 18650 Battery Charger for Li-ion Ni-MH Ni-Cd Ni-md, Capacitors, Resistors, AMS1117 3.3V and LM7805 Voltage Regulators.*
- Buzzer

Buzzer converts the received electrical signal into a vibration which gives the buzzing sound.

Software System Components

The ESP32S microcontroller is programmed using embedded C/C++, HTML and CSS for future improvements on the device.

- Android Mobile Application development

A Mobile Based Android Application was developed using Android Studio Integrated Development Environment (IDE) for Google's Android operating system. The Android Studio Integrated Development Environment (IDE) is an official environment used for Google's Android operating system (OS). The Android applications were written in Java. However, they run on Dalvik Virtual Machine (DVM), an android own Java Virtual Machine which is optimized to support only lightweight mobile operating system. The Android Studio and SDK tool were downloaded and installed from the Android platform. On running Android Studio on the OS, it automatically detected Java and downloaded some of the in-build tools. The Graphical User Interface (GUI) that enables the user to interact with the application, control the vehicle chassis for test purposes and register new users to the system.

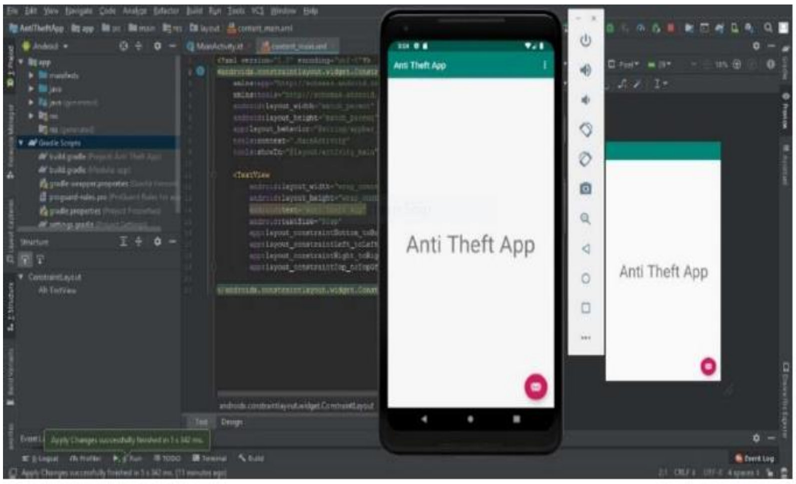


Figure 8: Android Studio Integrated Development Environment

❖ *Algorithm and Flow Chart of the System*

The algorithm of the anti-theft system consists of the overall system design algorithm which segments into GSM Control Subroutine. The algorithm is generated using C++programming language and graphically represented using flowcharts. The main purpose of the flowchart is to analyze the different processes of the program. The anti-theft system algorithm includes the following steps:

Step 1: Start
Step 2: Initialize ESP32-WROOM-32, GSM/GPRS module, GPS module, fingerprint scanner, immobilizer relay, buzzer and variables.
Step 3: Set ESP32-WROOM-32, GSM/GPRS module, GPS module, fingerprint scanner baud rates.
Step 4: Check fingerprint scanner status.
Step 5: Image capture on fingerprint scanner.
Step 6: Compare finger print with data stored in database. If fingerprint is recognized close the immobilizer relay and return to step 5, else open the immobilizer relay and notify the owner after three consecutive trials and then go to Step 15. Each trial triggers the buzzer to inform the user of invalid fingerprint entry.
Step 7: Check for GSM network Status.
Step 8: If network is available, query the GSM module for a new message and proceed to Step 9 otherwise go to Step 8.
Step 9: Compare the SMS received with commands stored in the database: If 'GET' character is received, get the GPS location of the vehicle and send to the user, else If 'ON' character is received, close the immobilizer relay, else If 'OFF' character is received, open the immobilizer relay. If commands match, execute command as stated above and proceed to Step 10 otherwise go to Step 8.
Step 10: Delete the SMS and proceed to Step 11.
Step 11: Check GPS receiver status.
Step 12: If GPS is connected get GPS data else turn on the GPS service and check for availability. If available, proceed to Step 13.
Step 13: Process and Extract useful GPS information
Step 14: Store GPS data in formatted string

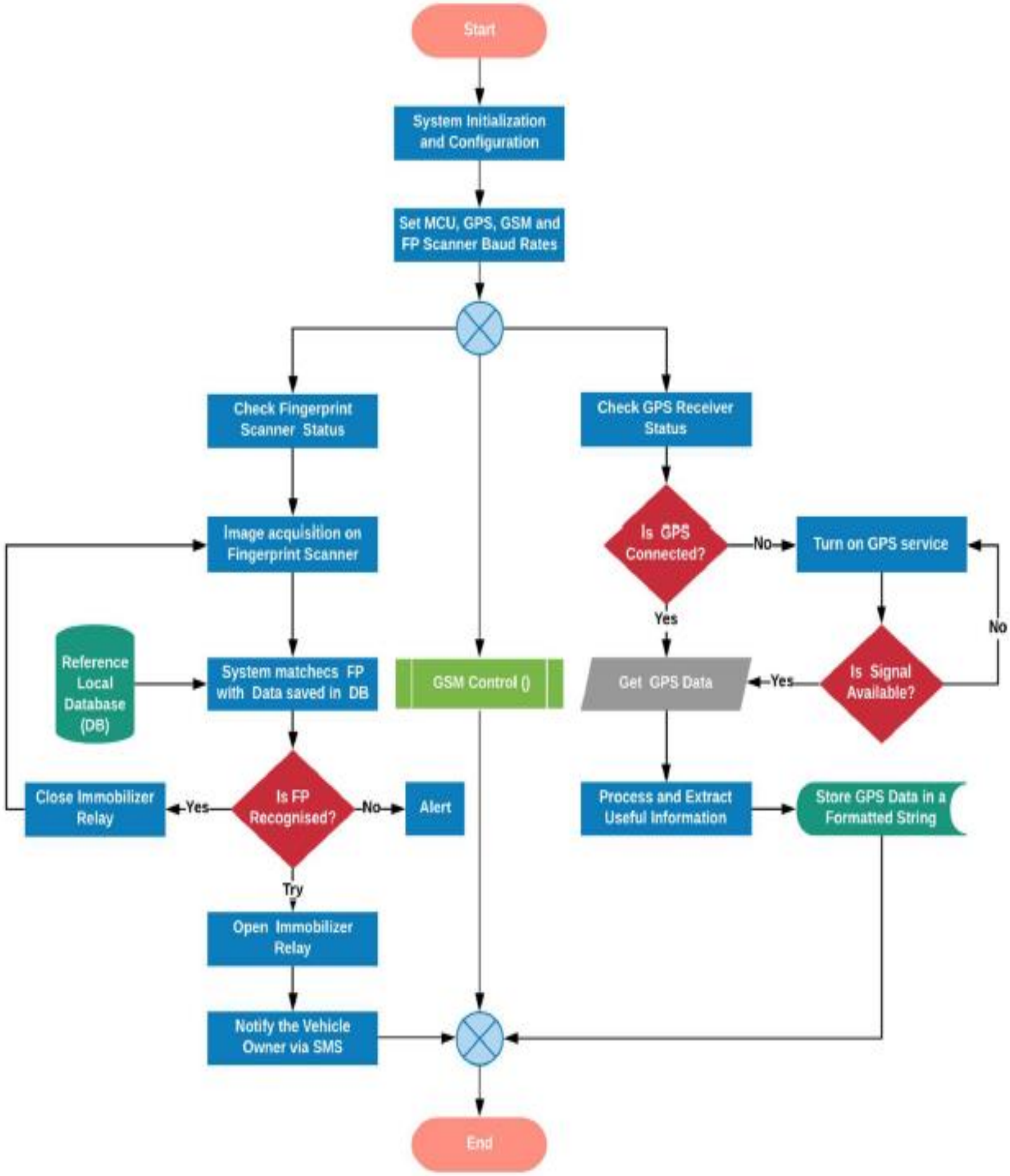

Start
System Initialization and Configuration
Set MCU, GPS, GSM and FP Scanner Baud Rates
Check Fingerprint Scanner Status
Check GPS Receiver Status
Image acquisition on Fingerprint Scanner
Is GPS Connected?
No
Turn on GPS service
Yes
No
Reference Local Database (DB)
System matchecs FP with Data saved in DB
GSM Control ()
Get GPS Data
Yes
Is Signal Available?
Close Immobilizer Relay
Yes
Is FP Recognised?
No
Alert
Process and Extract Useful Information
Store GPS Data in a Formatted String
Try
Open Immobilizer Relay
Notify the Vehicle Owner via SMS
End

Figure 9: System flowchart

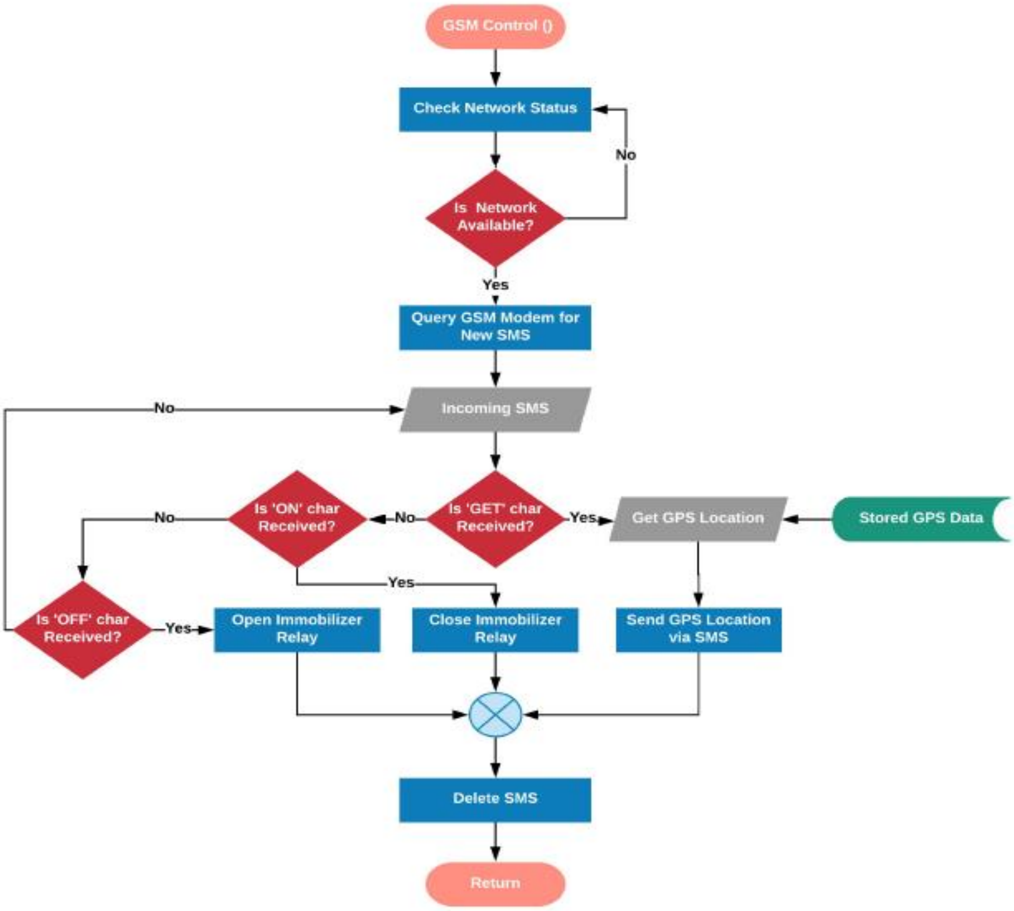


Figure 10: GSM Control Subroutine flowchart

- *Proposed System*

The proposed system is made up of a biometric authentication unit (i.e. fingerprint scanner) which is used for verifying the users of the vehicle by matching the captured fingerprint with predefined fingerprints in the database. Registration of users is done using the android based user interface. GPS receiver receives the location data like latitude, altitude and longitude of a vehicle and stores it in the EEPROM of the NodeMcu which can be accessed remotely via wireless transfer protocol. This data can be transmitted to the mobile device or the user through GSM network or Wi-Fi. Also, through the Graphical User Interface (GUI), functions such as control, registration of users and monitoring of the system. The GUI connects to the system through a unique Internet Protocol (IP) address which is obtained from the serial monitor of the NodeMcu through programme. Apart from long distance data transmission, the GSM modem is also used to remotely immobilize the system by sending SMS commands and also receive location. The 4WD double layer smart car chassis is a basis for which the prototype of the system will be tested since it provides mobility. The power supply unit provides a backup power for the system in case of unavailability of power due to the depletion of the vehicle battery.

IV BLOCK DIAGRAM OF THE SYSTEM

This section handles the systematic process of designing the system. Figure 11 is the block diagram of the anti-theft vehicle security system using GPS and GSM technology with fingerprint authentication. It is seen from the block diagram that the system is made up of two parts viz the anti-theft vehicle security system and the user interface (mobile phone) which communicates via a wireless connection. It also shows how several independent modules are interfaced with the microcontroller. The system consists of a power supply, GPS receiver, GSM/ GPRS module, optical fingerprint scanner/reader module, RTC module, vehicle immobilizer relay and the NodeMcu ESP32S development board and also a mobile phone for interacting with the system.

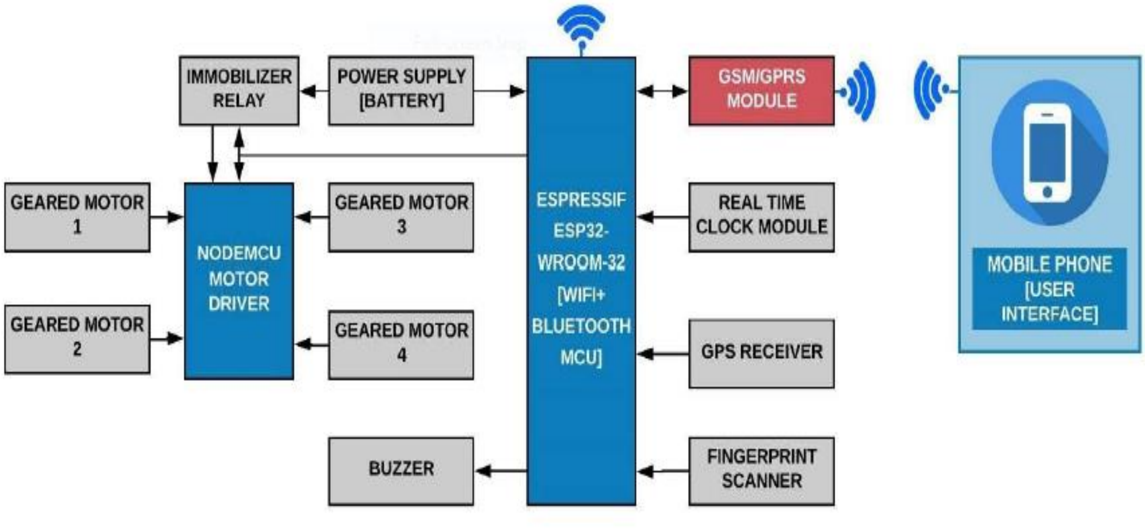


Figure 11: Block Diagram of the System

- *Design of Electronic Hardware*

The design of the electronic hardware of the system was done using Fritzing, an open-source hardware initiative software. The graphical representation of the electronic circuit of the system is shown in Figure 12.

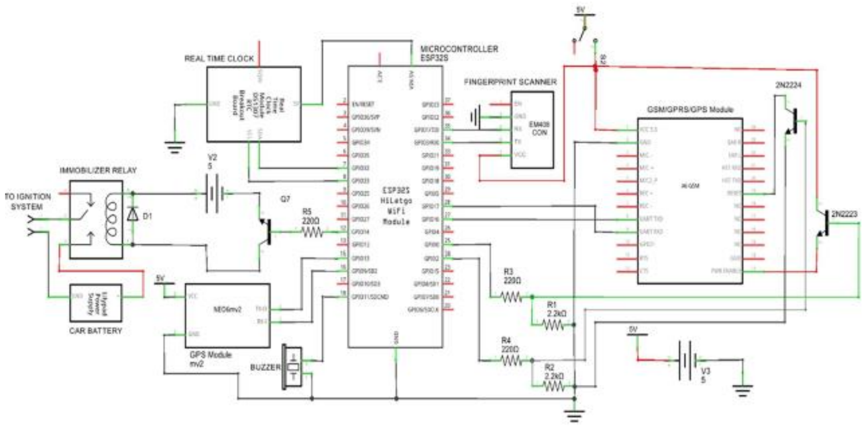
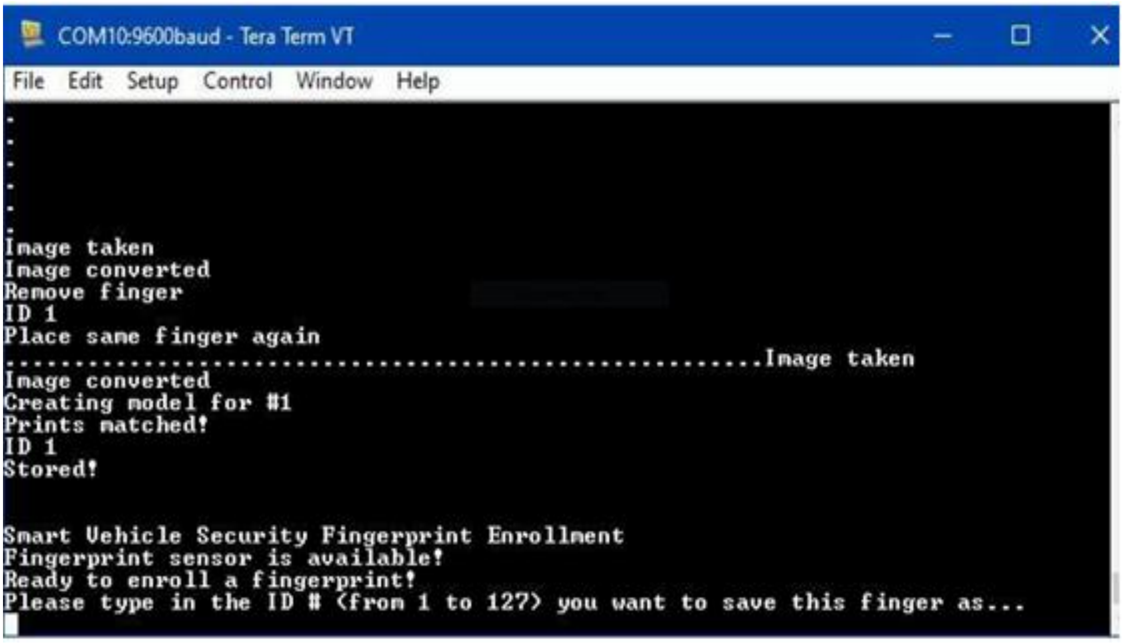


Figure 12: Schematic of The Anti-Theft Security System

IV. REESULT AND DISCUSSION

Various tests were done out to observe the functionality and performance of the system. They were carried out on several stages and also after its integration to make the entire system. Also, hardware checks and software debugging were done to enable an overall effective performance of the system. Some of the tests performed on the independent modules of the system before integrating as a unit were validation of GSM/GPS/GPRS Module, NodeMcu ESP32S, Optical Fingerprint Scanner and GPS Receiver. In optical fingerprint validation, several tests such as power test, connectivity test, capturing/extraction and fingerprint comparison test were carried out on the biometric sensor. The sensor was powered from the NodeMcu and observed if the scanner light of the sensor was on. Sensor connectivity between the fingerprint scanner and NodeMcu was established using serial communication. A test program was uploaded to send a command packet containing the open command and non-zero command parameter. This caused a fully functional optical sensor to send back a data packet containing the devices static information such as firmware version and serial number. Also, tests were carried on the scanner to check the capture and capturing capability, efficiency of the scanner and to observe its override (read/write) tendencies to its local database. The results from the fingerprint enrolment, match/capturing and removal were visualized and analysed in the windows console application using PuTTY as illustrated in figures 13-15. The figure 13 depicts the degree of comparison between the user print in the local database and the currently scanned print. This was the system matching confidence. It was observed that the higher the confidence of matched print, the greater its matching efficiency.

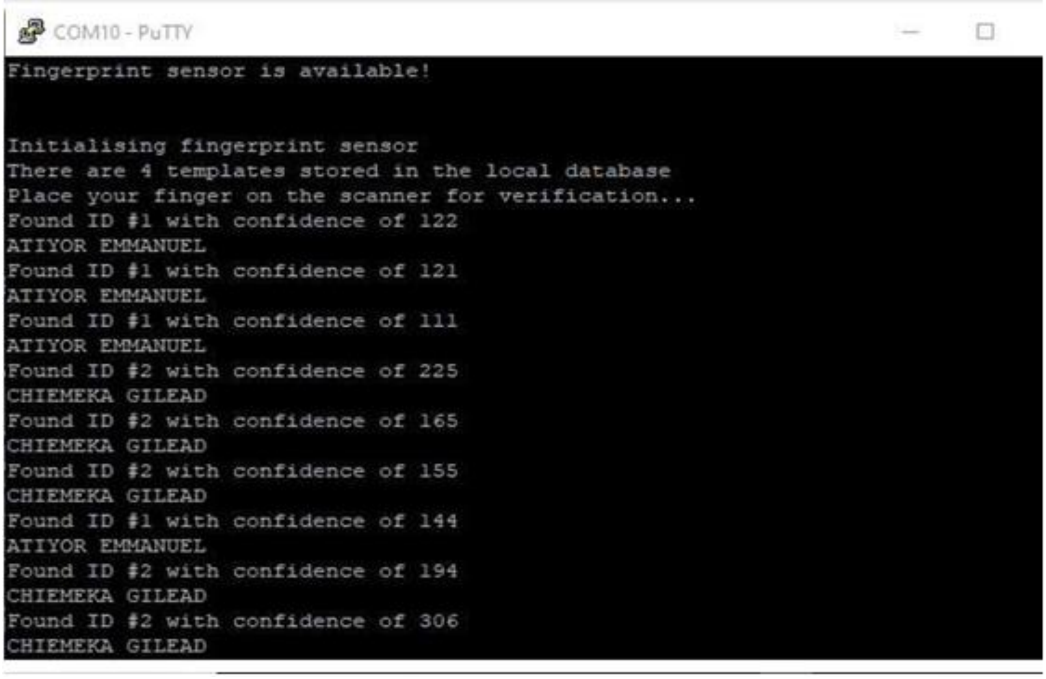

COM10:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
.
.
.
.
.
.
Image taken
Image converted
Remove finger
ID 1
Place same finger again
.......................................................Image taken
Image converted
Creating model for #1
Prints matched!
ID 1
Stored!

Smart Vehicle Security Fingerprint Enrollment
Fingerprint sensor is available!
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Fig 13:- Fingerprint Capture and Enrollment Test Result

Figure 14 depicts the system matching confidence. It is the degree of comparison between the user print in the local database and the current scanned print. The following snapshot illustrates the fingerprint removal result tested during the implementation phase of this work. The fingerprint removal algorithm helped to improve the authentication system security as print not authorized after enrollment was deleted or removed from the system.

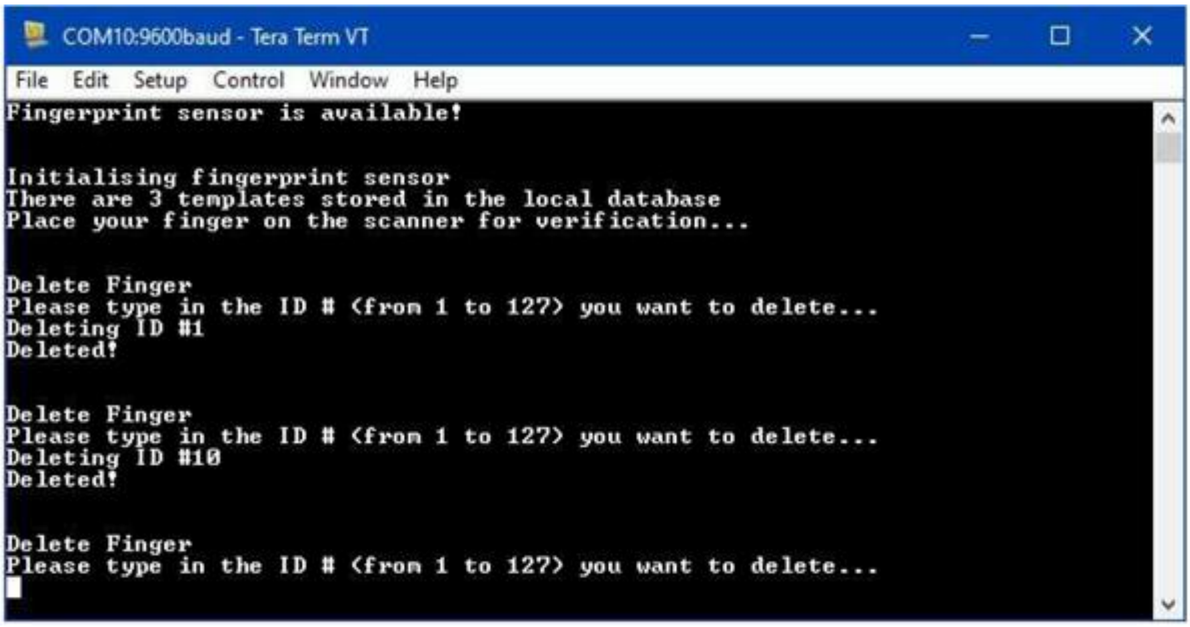


```
Fingerprint sensor is available!


Initialising fingerprint sensor
There are 4 templates stored in the local database
Place your finger on the scanner for verification...
Found ID #1 with confidence of 122
ATIYOR EMMANUEL
Found ID #1 with confidence of 121
ATIYOR EMMANUEL
Found ID #1 with confidence of 111
ATIYOR EMMANUEL
Found ID #2 with confidence of 225
CHIEMEKA GILEAD
Found ID #2 with confidence of 165
CHIEMEKA GILEAD
Found ID #2 with confidence of 155
CHIEMEKA GILEAD
Found ID #1 with confidence of 144
ATIYOR EMMANUEL
Found ID #2 with confidence of 194
CHIEMEKA GILEAD
Found ID #2 with confidence of 306
CHIEMEKA GILEAD
```

Fig 14:- Fingerprint Matching Results using PuTTY as Terminal Emulator

The following snapshot illustrates the fingerprint removal results as tested during the implementation phase of this work.



```
Fingerprint sensor is available!

Initialising fingerprint sensor
There are 3 templates stored in the local database
Place your finger on the scanner for verification...

Delete Finger
Please type in the ID # (from 1 to 127) you want to delete...
Deleting ID #1
Deleted!

Delete Finger
Please type in the ID # (from 1 to 127) you want to delete...
Deleting ID #10
Deleted!

Delete Finger
Please type in the ID # (from 1 to 127) you want to delete...
```

Fig 15:- Fingerprint Removal Results

The GPS module was powered on by the rated acceptable supply and physically inspected if the indicator LED was turned on as expected. The receiver was connected to the microcontroller and then the windows PC through a serial communication link. In GPS Receiver Validation, a test program was uploaded to record the connection status and the capability of the receiver to remotely connect with available satellites. The program was structured to obtain geographical location and the number of satellites connected to the receiver. The data received was analyzed to observe if the module was in a working condition and also to note the extent of its deviation from actual location. The accuracy of the data obtained from the receiver was confirmed by checking the latitudinal and longitudinal positioning of the receiver using the google maps platform. This check confirmed that the accuracy of the sensor was high owing to the fact that the result obtained was of close proximity with actual result. Figure 16 shows the geographical positioning obtained from the GPS receiver using google maps platform.

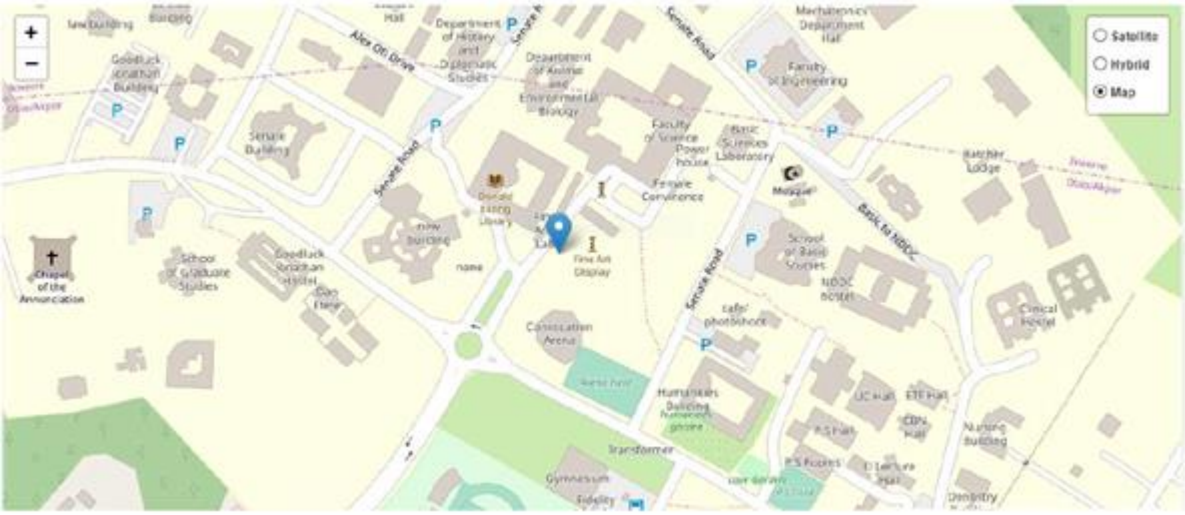


Fig 16:- GPS Receiver Test Position using Google Maps Platform

For experimental purposes, mobility test was carried out on the system mounted on a 4WD Smart Robotic Car Chassis. The wheels were tested individually by powering its terminals using a 9V lithium battery. A wheel directional test was accomplished using a NodeMcu Motor driver built on the L293D hybrid bidirectional motor driver chip. The NodeMcu motor driver was powered using an external power source and the status LED was checked if turned on. The motors were connected to the socket of the driver and a test program was uploaded to the NodeMcu to test the bidirectional tendencies of the L293D dependent motor board. The supply voltage to the motor was also varied to observe an increase in the speed of the motor. Due to the complexity of the system, a web-based user interface was designed using the android platform to render a better experience to the user.

V. CONCLUSION AND RECOMMENDATION

Vehicle security is essential as the vehicle theft is increasing and becoming the most common crime in the recent years. The paper presents the development of an anti-theft vehicle security system using GPS and GSM technologies with fingerprint authentication. The anti-theft system is controlled by a web based android mobile application developed using Java programming language in Android Studio IDE. One of the improvements done to previous works is the integration of fingerprint authentication system and the use of the real time cloud database for data storage. The authentication unit only helps to regulate the access of intruders. Alert messages are sent to the car owner via SMS or mobile app to notify him of any illegal access. The vehicle can be remotely immobilized in real time even in a GPS denied environment. Thus, preventing vehicle theft and time wastage in tracking stolen vehicle. In cases of hijacking, the vehicle user can leave the car safely, and then use any phone to send out some commands. Data from the vehicle are streamed to the database in real time and the vehicle approximate location can be estimated by retrieving the vehicle last location from the database. The vehicle owner remotely immobilizes the vehicle and cut off power supply, so as to stop the vehicle from moving and thus get it back.

The smart anti-theft system can be made more efficient and secured by incorporating other biometric identification systems like Face Recognition alongside the fingerprint authentication feature for more secureness. Additional technology like Radio Frequency (RF), Camera and some touch screen-based application can also be adopted. The system is not only limited to vehicle security, it can find real time application in shipment or courier service companies for cargo monitoring, transportation companies and petroleum distribution truck. The web-based android application tracking fragment can be modified for individual tracking, thus people can keep track of their loved ones.

REFERENCES

[1] Nagaraja B.G, Ravi Rayappa, M Mahesh, Chandrasekhar M P and Manjunath T.C, Design and Development of a GSM-Based Vehicle Anti-Theft Control System, IEEE International Conference on Advanced Computer Control, pp 148-12, 2009

[2] Y. Soweon, Fingerprint Recognition: Models and Applications, Ph.D Dissertation 2014.

[3] Zhigang L, Anqi Z and Shaojun L, Vehicle Anti-Theft Tracking System Based on Internet of Things, IEEE, pp 48- 52, 2013.

[4] D. Mrinmoy D, M. Akteruzzaman and M.D Mahmud, Anti-Theft Protection of Vehicle by GSM and GPS with Finger Print Verification, IEEE International Conference on Electrical, Computer and Communication Engineering, 2017.

[5] V.M Pradip and Chile R H, Real Time Vehicle Tracking System Based on ARM7 GPS and GSM Technology, IEEE India Conference, 2015, pp 2517-2522.

[6] 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.

[7] 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.

[8] 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. [9] 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.

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

[12] B. P. Rahul and P. Tasgaonkar, An IoT Framework for Intelligent vehicle monitoring System. International Conference on Communication and Signal Processing, 1694-1696., 2019.