ISSN No:-2456-2165

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:- This research paper presents an effective anti-theft vehicle security system which integrates Global Positioning System (GPS), Global System for Mobile Communication (GSM) and Biometrics technologies (i.e. fingerprint) for user identification and authentication. Theft security of vehicles in common parking places has become a matter of great concern Thus, a system capable of identifying and tracking the geographical location of a remote vehicle, which requires constant surveillance of the vehicle is needed. 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. GPS and GSM modules were utilized to prevent theft and to determine the exact location of vehicle and a fingerprint reader module to identify authorized persons and thus start the engines. The GSM modem enables a two-way communication between the user and the system. The microcontroller was programmed using embedded C/C++. The fingerprint readings and also SMS commands will be used to immobilize and demobilize the vehicle via relay, thus protecting the cars from theft and unauthorized users.

I. INTRODUCTION

Vehicle theft has been a persisting problem around the world. Currently, there is a rapid increase in vehicle theft in this part of the world and this is a universal problem. As a result of the rising number of stolen or vandalized vehicles, vehicle tracking system is currently gaining vast popularity especially in unsecured locations. The security standard such as alarm based security provided by the manufacturers of vehicles is regarded as being ineffective and unable to prevent vehicle theft [1]. Due to the alarming situation of vehicle theft, people have already started to use theft control systems like immobilizers in their vehicles. But they are outdated methods which can be hacked easily and also these antitheft vehicle systems are very expensive. Also, the high cost of vehicles, commercially available anti-theft vehicular systems, insurance, and deductibles and the potential waiting periods for insurance settlements create a significant financial hardship for many victims. Once a vehicle is stolen, it becomes hard to track it, which considerably decreases the chances of recovering it.

To resolve these problems, there is a need to have a system that monitors and communicates with the device owner. This paper presents the development of an antitheft vehicle security system using Global Positioning System (GPS), Biometrics and mobile communication protocol that will monitor, protect and secure vehicles. Data transfer between the user and the proposed system are achieved through a short message services (SMS) protocol available in the cellular phone. The proposed system is interfaced with an immobilizer which uses Biometric (i.e. Fingerprint) authentication to turn on the engine and to 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. This satellite technology has made it easy to identify the vehicles location. The importance of this proposed project cannot be over emphasized since it will help to reduce the rate of vehicle theft in our society. This paper attempts to proffer a lasting solution by exploring GPS, Biometrics and GSM technologies coupled with some other digital control techniques as possible remedy.

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.

❖ *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 as follows;

[3] 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 consists 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 user.

[4] proposed a reliable multi- tracking system for multiple vehicles using GPS and GSM. It 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 is used for live vehicle tracking by sending short messages to turn the vehicle ignition on.

[5] proposed a vehicular identification and authentication system based on Zigbee communication technology for security monitoring in a campus setting. 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 consists 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.

[6] 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 is used to view the current location and status of each vehicle. The objective of this system is 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.

[7] designed and implemented a low-cost car anti-theft security system using microcontroller and thus, ensured maximum security for car or any kind of automobiles. 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 as long as 400 foot in free space but it was less in the case of obstacle in the way. So, it cannot cover a long distance. This length coverage problem is one of the major restrictions of this work. As a result of this the system cannot be accessed over distant locations.

[8] designed and constructed a vehicle anti-theft system which can be remotely controlled through GSM network. Communication between the user and the vehicle sub-system was via SMS (Short Messaging Service). SMS commands were sent to the GSM/GPRS Modem Module. The system was designed to be accessed from a remote/distant location where there is GSM coverage and also monitor, control and initiate the vehicle immobilizer relay when the vehicle has been stolen. This system does not integrate an authentication system to identify the user of the vehicle, thus it can be hot wired and due to the drawback of inconsistence in the availability of GSM network in some areas, the vehicle will not be protected from theft.

As a result of the annual increase in the number of stolen vehicles [9] developed a system to prevent vehicle theft by creating a controllable system that can display the location of a vehicle using GPS to get the actual location of the vehicle and GSM as a communication medium with the vehicle for ease of finding after theft attempt. The authors used an interrupt program was used to combine the program of both modules into a single program. After carrying out several tests, the results concluded that the system can provide standard GPS coordinate when requested via Short Message Service (SMS) and can also be used to control an actuator. The system did not utilize Cell Tower Triangulation in its programming so if the signal was lost, there was no assisting system to pin point the coordinate without the signal of the satellite. Thus, the system is considered not reliable.

The design and development of a cost effective and reliable Internet of things (IoT) framework which consists 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 of the high speed expressway was presented in [10]. In this system, the velocity of the vehicle was approximated in the real-time environment using Euler's algorithms. In this work, 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 can be generated. If the vehicle crosses the limit then the driver can be notified using the web applications along with that the highway traffic authority can 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.

[11] depicted a Vehicle Theft Detection, Locking and Tracking System which would be able to get the exact location of the vehicle if it was stolen so that the owner can track it. This system can also turn off the engine of the vehicle remotely by immobilizing its engine and sends the tracking data over through an SMS. The limitation of this

system is the inability to distinguish between the user and an intruder due to the lack of an authentication system.

[12] described a project which help to find the location of a theft vehicle by using GSM and GPS at any period and also this device stored the message by the application in the mobile. In the system they used GSM modules and several components, the owner or the user of the vehicle was alerted with a message at the time of occurrence of theft. It sent the messages to the owner via SMS. When the owner sent a message to the system the microcontroller received and processed the message. It would send the location of the vehicle with a time gap to get current/present location. Here the disadvantage is that does not include an authentication unit.

[13] developed a low-cost vehicle theft control scheme using a microcontroller and with usage of GPS and GSM technology. They also integrated an accident detection feature to the system which sends an emergency alert message to police and ambulance along with exact location, in case the vehicle is met with an accident. They used a keypad protection system to secure the vehicle from theft since it was password protected. The device tracks the location of vehicle it was connected to and sent it to users mobile in form of SMS. The arrived data, in the form of latitude and longitude was used to locate the Vehicle on the Google. Authentication was also provided so that only the authorized users can access the vehicle. A wide future scope guarantees that an enhancement to this device finds a great importance in real time system.

➢ *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 demobilize the system by sending SMS commands and also receive location. The system is also 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. 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 cases of unavailability of power due to the depletion of the vehicle battery.

III. MATERIAL AND METHODS

The antitheft system is divided into two main sections which consists of the system hardware and system software.

A. 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 ensures 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/Transmitter) 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 obtains better and 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.

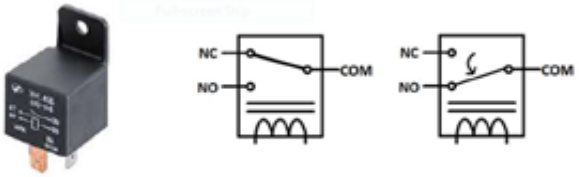

Fig 7:- Immobilizer Relay and Symbol

➢ *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.*

ISSN No:-2456-2165

IV. BLOCK DIAGRAM OF THE SYSTEM

This section handles the systematic process of designing the system. Figure 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.

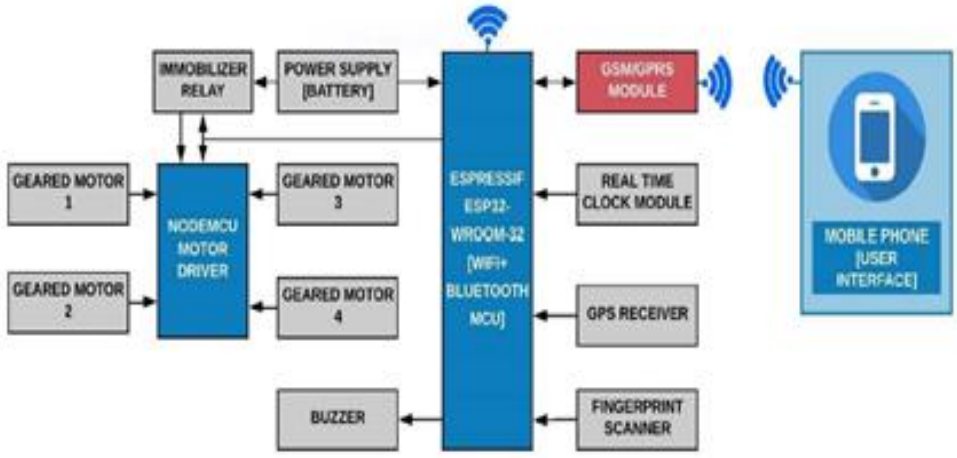

Fig 8:- Block Diagram of the System

A. Software System

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 is developed using Android Studio Integrated Development Environment (IDE) for Google's Android operating system. The Android applications are 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 are downloaded and installed from the Android platform. The basics of the environment was studied from the Android Studio Documentation, thus understanding its architecture and features. On running Android Studio on the OS, it automatically detects Java and it downloads some of the build tools. The Graphical User Interface (GUI) that enables the user to interact with the application, controls the vehicle chassis for test purposes and registers new users to the system is designed using Java programming language after the complete build-up of the application and setup.

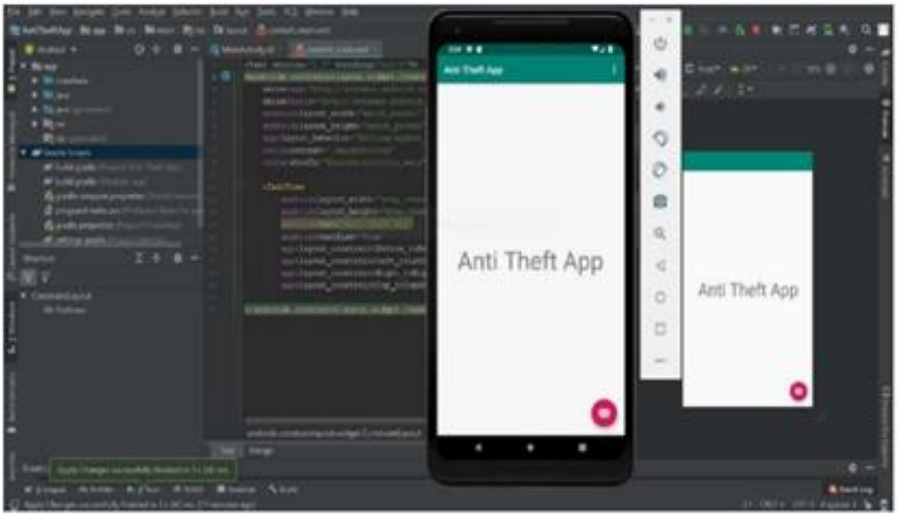

Fig 9:- Android Studio Integrated Development Environment

ISSN No:-2456-2165

➢ *Algorithm and Flow chart of the system*

The algorithm of the Anti-Theft Vehicle Security System consists of the overall system design algorithm which segments into GSM Control Subroutine. The algorithm is generated using C++programming language and are graphically represented using flowcharts. The main purpose of the flowchart is to analyze the different processes of the program. The Anti-theft Vehicle Security 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, FP 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 data base. 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 FP entry.
Step 7: Check for GSM/GPRS 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

Table 1:- Anti-theft Vehicle Security System Algorithm

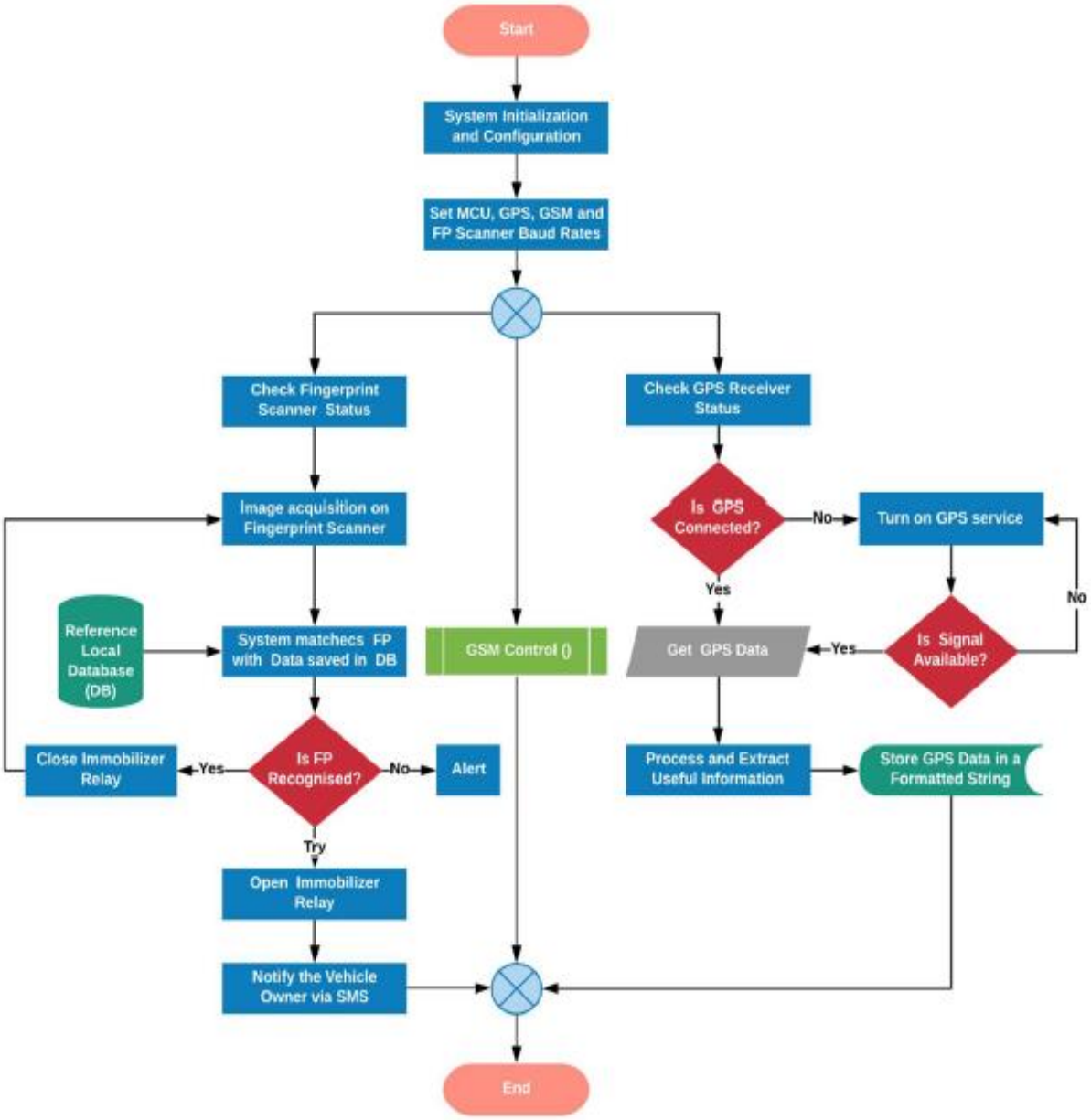

Fig 10:- System flowchart

V. REESULT AND DISCUSSION

Various tests were done to observe the functionality and performance of the system. They were carried out on several stages which involves the validation of several independent modules of the system 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 include validation of GSM/GPS/GPRS Module, NodeMcu ESP32S, Optical Fingerprint Scanner and GPS Receiver. In optical fingerprint validation, several tests were carried out on the biometric sensor which include power test, connectivity test, capturing/extraction and fingerprint comparison test. The sensor is powered from the NodeMcu and observed if the scanner light of the sensor is on. Sensor connectivity between the fingerprint scanner and NodeMcu is established using serial communication. A test program is uploaded to send a command packet containing the open command and non-zero command parameter. This causes 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 and efficiency of the scanner. Checks were also done 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 11-13 below.

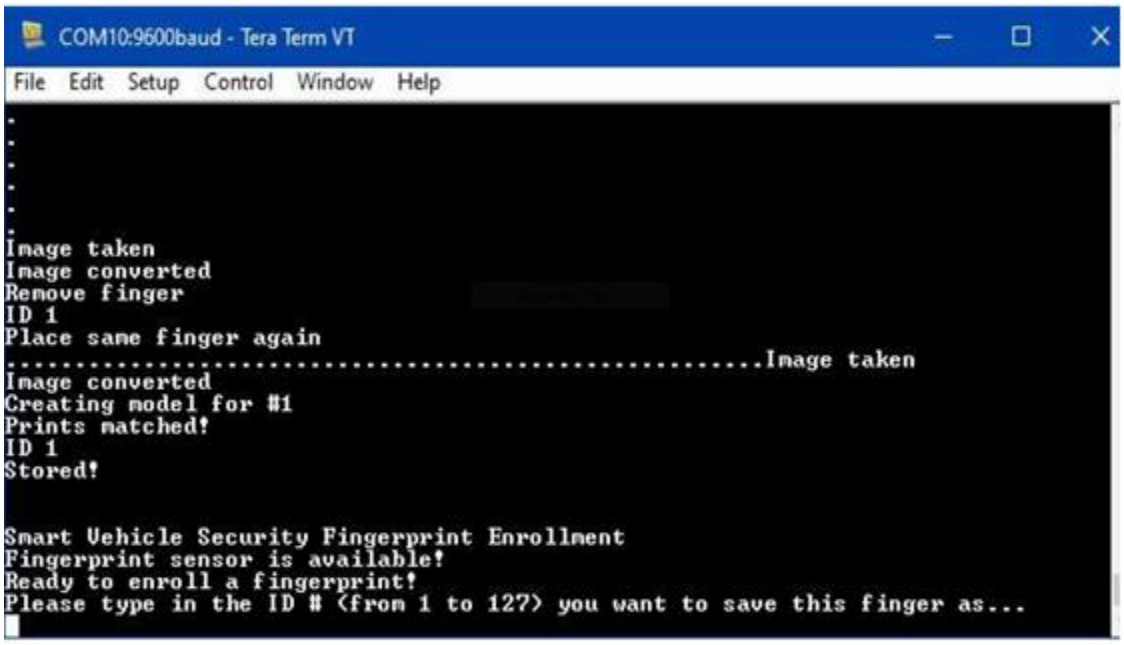

Fig 11:- Fingerprint Capture and Enrollment Test Result

Figure 12 depicts the system matching confidence. It is the degree of comparison between the user print in the local database and the currently scanned print.

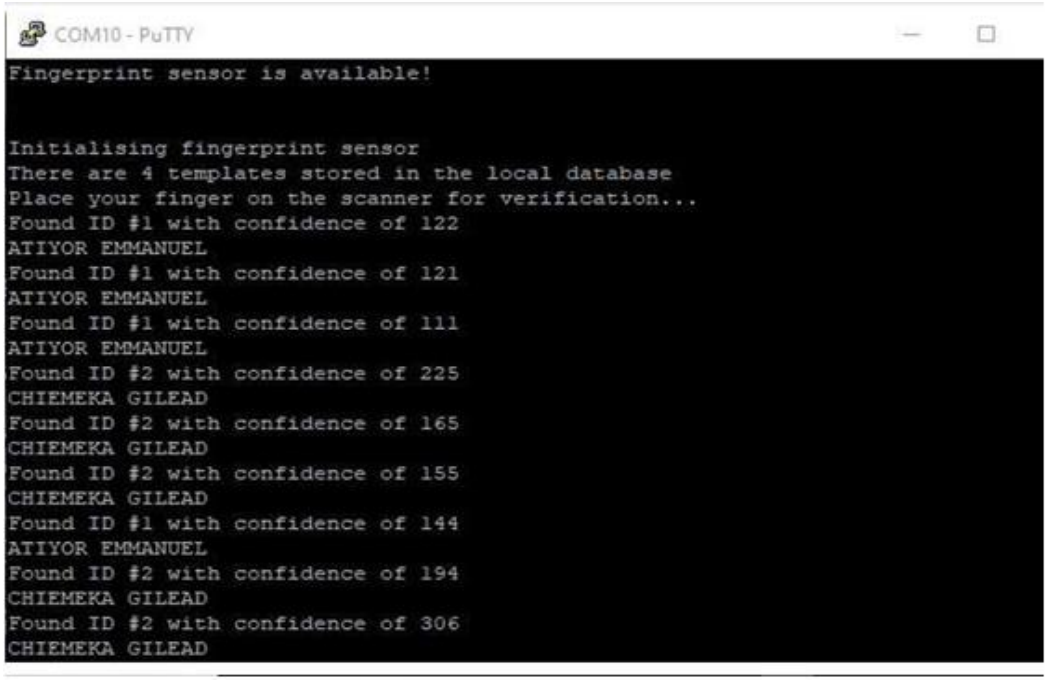

Fig 12:- Fingerprint Matching Results using PuTTY as Terminal Emulator

It shows from observation that, the higher the confidence of a matched print, the greater its matching efficiency.

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

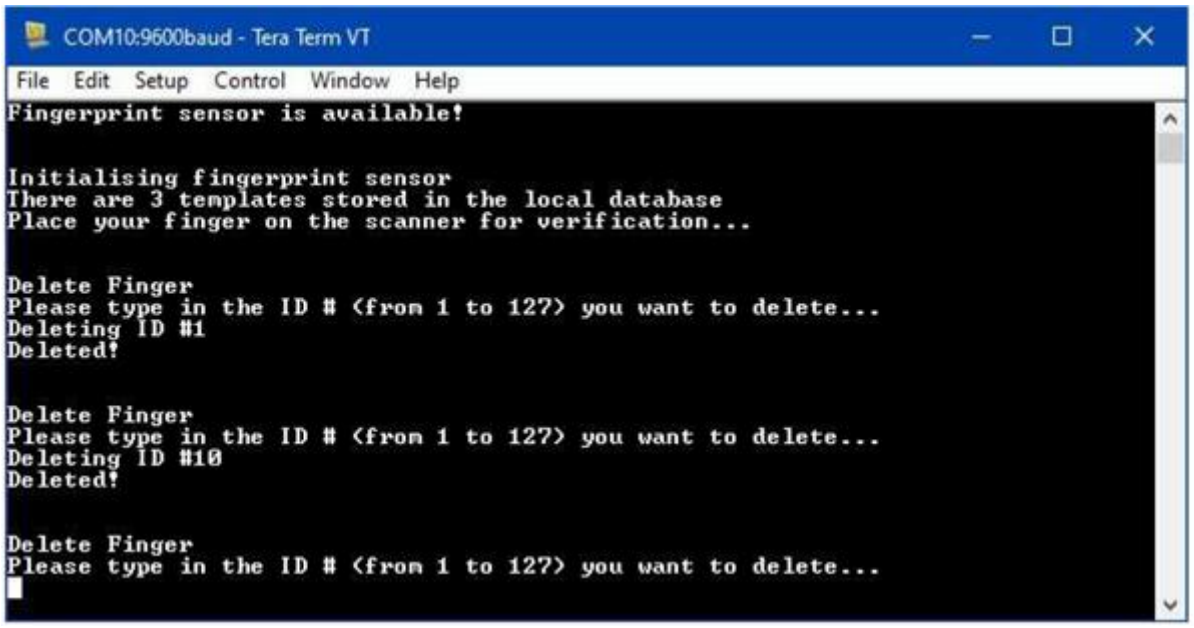

Fig 13:- Fingerprint Removal Results

In GPS Receiver Validation, a test program was uploaded to also record the connection status and also the capability of the receiver to remotely connect with available satellites. The program is structured to obtain the number of satellites connected to and also the geographical location of 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 is of close proximity with actual result. Figure 14 shows the geographical positioning of obtained from the receiver using google maps platform.

Fig 14:- GPS Receiver Test Position using Google Maps Platform

For experimental purposes, the system was mounted on a 4WD Smart Robotic Car Chassis, thus mobility test is required. The wheels were tested individually by powering its terminals using a 9V lithium battery and also 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. During the web-based android development process, a lot of errors were identified and handled. The programs were tested using the Pixel 2 XL API 22 contained in the Android Virtual Device Manager (AVD). After the software development process, the web-based android application was tested in order to check its functionality. The application was designed using

a navigation drawer and hosted on a Cloud platform. Data from the application are synchronized in real time to the Cloud Real Time Database which were later received through the internet by the NodeMcu and vice versa. The Navigation drawer is made up of several fragments such as Maps Fragment, Control Fragment, Tools Fragment etc. The integration of Google Maps to the application enable real time tracking of the system.

Table 2 shows the control commands and results of the system after test and also its functionality. The Enable 1,2 and Enable 3,4 pins of the motor shield are always kept HIGH to enable the motors connected to both sides of the driver. During implementation test phase, the system was mounted on a Smart car chassis and the commands from Table was passed on to the system. After a durable test on the system, it was observed that the system functions as expected. The system connected automatically to the available wireless network and authenticates with the cloud through Access Point (AP) internet providers network. After connection was established, the vehicle read and to the real time database. A biometric print is required for user authentication in order to start the vehicle.

Buttons	Function	MCU I/O response				Observation
		IN1	IN2	IN3	IN4	
FWD	Forward	0	1	0	1	The chassis is moves forward
BWD	Backward Reverse Turn	1	0	1	0	It moves in a reverse direction
FRT	Forward Right Turn	0	1	0	0	The chassis is turned in a Clockwise direction
FLT	Forward Left Turn	1	1	1	0	Turns in an anti-clockwise Direction
BRT	Reverse Right Turn	1	0	1	1	Reverse turn in an anticlockwise Direction
BLT	Reverse Left Turn	0	0	0	1	Reverse turn in a clockwise Manner
LIGHT	Light Switch	HIGH-ON, LOW-OFF				Toggles the vehicle light on and off on state change
DEM.	Demobilize or Mobilize	HIGH-Mobilize, LOW-Demobilize				Remotely turns on and shutdown vehicle
GET LOC	Get GPS Location	get Value()				Retrieve GPS data from cloud and parse location
RT.	Real Time Tracking	Async. GET request				Multiple route location in real Time
GET USER	Get Vehicle User	get Value()				Retrieve vehicle user data or information from cloud
REG	Register Location	set Value()				Stores the user information in real time database
SMS Commands to the Device using GSM Link						
GET	Sends Location	get Value()				Stores the user information in real time database
DEM.	Demobilize	set Value()				Shutdown the vehicle from a remote location
MOB.	Mobilize	set Value()				Starts the vehicle remotely

Table 2:- Overall System Control and Observation

VI. CONCLUSION AND RECOMMENDATION

The development of a smart vehicle security using GPS, Fingerprint authentication and GSM technologies was tested and result showed that it functions as expected. The system is controlled by a web-based android mobile application developed by Java programming language in Android Studio IDE. With the application of the cloud-hosted real time database to the C-Secure application of the security system, data from the vehicle are streamed to the database in real time and in occasions where there is no network coverage in the tracking region, the vehicle last location data can be retrieved from the database and the vehicle approximate locations can be estimated.

The test carried out on the system proved that the user of the device can remotely demobilize the vehicle in real time using SMS commands and Mobile application through cellular network and internet respectively. In cases of hijacking, the vehicle user can leave the car safely, and then he/she could use any phone to send out some commands and remotely cut off power supply, so as to stop the vehicle from moving and thus get it back. The location of the vehicle could be found out accurately when the latitude and longitude values obtained and passed into Google Map Fragment in the C-Secure Application interface developed for the system, the location of the vehicle could be found out accurately. With the integration of the fingerprint authentication unit, the vehicle security was improved due

to the fact that only authorized users can start the vehicle. The ability to be able to reduce the random occurrence of vehicle theft in our society is of utmost importance for protection of vehicles in our society.

One of the improvements done to previous works was the integration of an authentication system and the use of the real time cloud database for data storage. The incorporation of this protection system alerts the user by sending a text message and can use GPS for parsing the strings, Latitude and Longitudinal information of the vehicle for the purpose of tracking it and send a text message for the purpose of stopping it will enhance safety and security. Also, the integration of fingerprint authentication unit and server-less control mechanism helps to regulate the access of intruder, thus there is difficulty in starting the car. This will prevent the car from theft and time wastage due to tracking of stolen vehicles.

The smart anti-theft security 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]. Khairul, H. B, Development of GSM-Based Vehicle Anti-Theft System, 2006.
[2]. Y. Soweon, Fingerprint Recognition: Models and Applications, 2014.
[3]. 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.
[4]. 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.
[5]. 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.
[6]. 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.
[7]. 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.
[8]. 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.
[9]. 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.
[10]. B. P. Rahul and P. Tasgaonkar, An IoT Framework for Intelligent vehicle monitoring System. International Conference on Communication and Signal Processing, 1694-1696., 2019.
[11]. N. Kaushik, M. Veralkar, P. Parab, and K. Nadkarny, Anti-Theft Vehicle Security System. International Journal for Scientific Research and Development, vol.5(5), pp 1477-1480, 2017.
[12]. M. Geetha, T. Priyadarshini, B. Sangeetha, and S. Sanjana, Anti-theft and tracking mechanism for vehicles using GSM and GPS. International Conference on Science Technology Engineering & Management (ICONSTEM), pp 252-255, 2017.