Volume 14, Number 2, 2021. pp. 117-128

Jordan Journal of Physics

ARTICLE

# Multifactor Authentication Car Tracking System Using Fingerprint Verification

**Ndianabasi. H. Valentine**[a], **Ogri J. Ushie**[b] and **Emmanuel I. Akaerue**[a]

[a] *Department of Physics, University of Calabar, Nigeria.*
[b] *Department of Electrical and Electronic Engineering, University of Calabar, Nigeria.*

***Doi:*** **https://doi.org/10.47011/14.2.3**
*Received on: 14/02/2020;* *Accepted on: 26/07/2020*

**Abstract:** The design of an intelligent system used to detect and locate vehicle theft has become a viable and sustainable tool in the security system globally. Multifactor authentication car tracking system works in a way that if an unauthorized person tries to steal the vehicle, the user and user's relatives and a registered police station will be notified with the GPS location. The fingerprint records are stored in the memory of the system. When the fingerprint matches with the stored ones, the microcontroller triggers and powers the circuit. The GPS module gets the location information from satellites in the form of location coordinates. The GSM module sends a short message service immediately to notify the owner in case of any theft action. The fingerprint test-scan results of approximately 100 percent competency level demonstrate that this technology has an enormous potential to enhance effective security and tracking technology in vehicles, objects and humans.

**Keywords:** Tracking system, GPS, Fingerprint, Module.
**PACS**: Electronic, 07.50.EK, 84.30.-r.

## Introduction

Global positioning system (GPS) trackers are portable devices that allow fleet managers, parents and vehicle owners of all kinds to monitor and track their cars and trucks. Real-time GPS trackers for cars are capable of providing instantaneous speed and location data, while less expensive options record this type of information for later use. With some GPS vehicle trackers, it is even possible to set up real-time alerts to go off whenever a driver speeds or deviates from a specific area.

The world population increase has led to a proportional increase in the demand of vehicles as a necessity of life in recent times. Improvement in science and technology has brought significant advancement in security measures to curb the menace of theft activities in vehicles. Car jackers have also developed higher techniques to bridge these measures; hence, a system with fingerprint innovation and tracking mechanism is needed to replace the existing vehicles' security structures. Vehicle Tracking Systems are important security measures that should be considered for ensuring life and vehicles, since they are equipped to keep the user informed about the vehicle's location through a telecommunication system [1-4].

The present work is focused on more secure tracking means for automobiles. The vehicles equipped with this device need to recognize the user's fingerprint before the engine is ignited. A limitation on the number of users is set, which makes the automobile more secure. Alongside, the device improves the security operation of

**Corresponding Author:** Emmanuel I. Akaerue **Emails**: emmanuelakaerue@unical.edu.ng; akaerueemmanuel@gmail.com

vehicles, measures the impact level of recent developed fingerprint engine starter systems and automobile starters and evaluates the unique difference of the acceptability level of the systems. Recently, fingerprint identification is one of the most important biometric technologies which have drawn an extensive amount of attention. The uniqueness of a fingerprint makes it acceptable and easy in modern-day technologies. Fingerprint biometrics provides a reliable, robust and full-proof personal identification. Fingerprint biometrics is one of the efficient, secure, cost-effective and easy to use technologies for user authentication [5-7]. Fingerprint authentication, like other biometric methods, requires the physical presence of the person to be identified. It potentially prevents unauthorized admittance to access control systems or fraudulent use of ATMs, Time and Attendance Systems, cellular phones, smart cards, desktop PCs, workstations, vehicles and computer networks. Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition [8-13].

## Research Methodology

The fingerprint Verification technology describes a high-security car tracking system with multi-factor authentication method using knowledge factor (password) through keypad, combined with an inherence factor (biometric) using fingerprint, which makes it more secure than the existing ones [6, 9-12]. The system features are: fingerprint module, GPS module, GSM module and 433MHz Ultra High Frequency (UHF), Radio Frequency (RF) transmitter and receiver modules, which are used for keyless access and control of the car. An output on the receiver is used to activate or deactivate the car in an event of car hijack.

The presented multifactor authentication car tracking system was designated and constructed into two sections: the transmitter section and the receiver section. The block diagrams of these sections are depicted in Fig. 1 and Fig. 2, respectively. The transmitter has a 4x3 matrix keypad and an acknowledge LED that briefly lights up each time one of the switches in the transmitter is pressed. Up to 16 separate transmitters can be used with one receiver in this design. The receiver on the other end combines the power of fingerprint, GPS and GSM module to add an extra security layer to the design.

Software is the key approach to this system; basically, three types of software were adopted for this design. These include Dip Trace which is a schematic capture program used in the designing of the schematic diagram, Proteus which is a simulation package used in the simulation of the finished design and Atmel Studio which is an Integrated Development Environment (IDE) used in the writing and compilation of the needed program for the work. In the design, a microcontroller was used to accomplish the task of monitoring and controlling of the system instead of a handful of digital integrated circuits (ICs) and other hardware to keep the component count low while maximizing the number of ways in which the design can be matched to real-life requirements. Adopting this approach gives room for the addition of new features and advancing functionality. This approach also makes the implementation far easier. The method used in the design is unique, due to the fact that wireless technology involves the combination of GPS, GSM and RF wireless transmitter and receiver modules. The hard-ware parts are combined with the power of software to archive the entire work, with the software being the key driving power. Using this method allows certain new features to be implemented easily through the configuration of the software instead of changing the hardware.

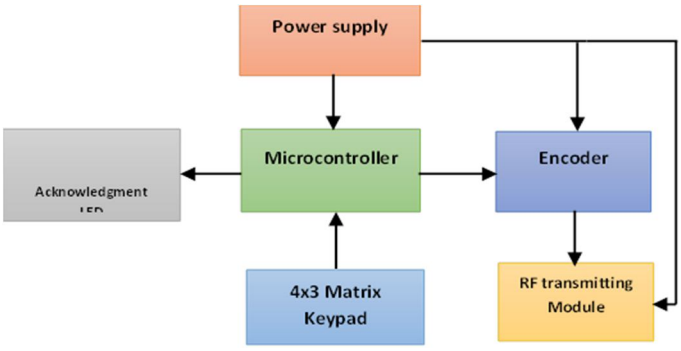


FIG. 1. Block diagram of transmitter section.

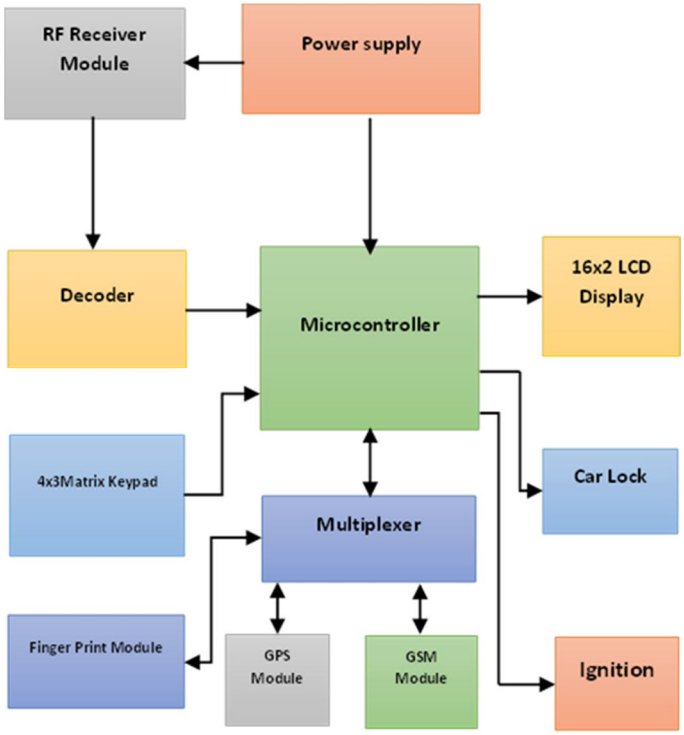


FIG. 2. Block diagram of receiver section.

The core of the tracking system is based on ATmega16 microcontroller, the responsibility of which is to monitor and manage the tracker. In the transmitter, the controller receives data from the keypad and transmits the received data *via* 433MHz transmitting module *via* HT12E encoder integrated circuit. In the receiver, the controller receives the transmitted data *via* HT12D decoder integrated circuit and initializes the system to begin operation. The signal received from the fingerprint module is also sent to the microcontroller for processing. The circuit diagrams of the transmitter and the receiver sections are shown in Fig. 3 and Fig. 4, respectively.

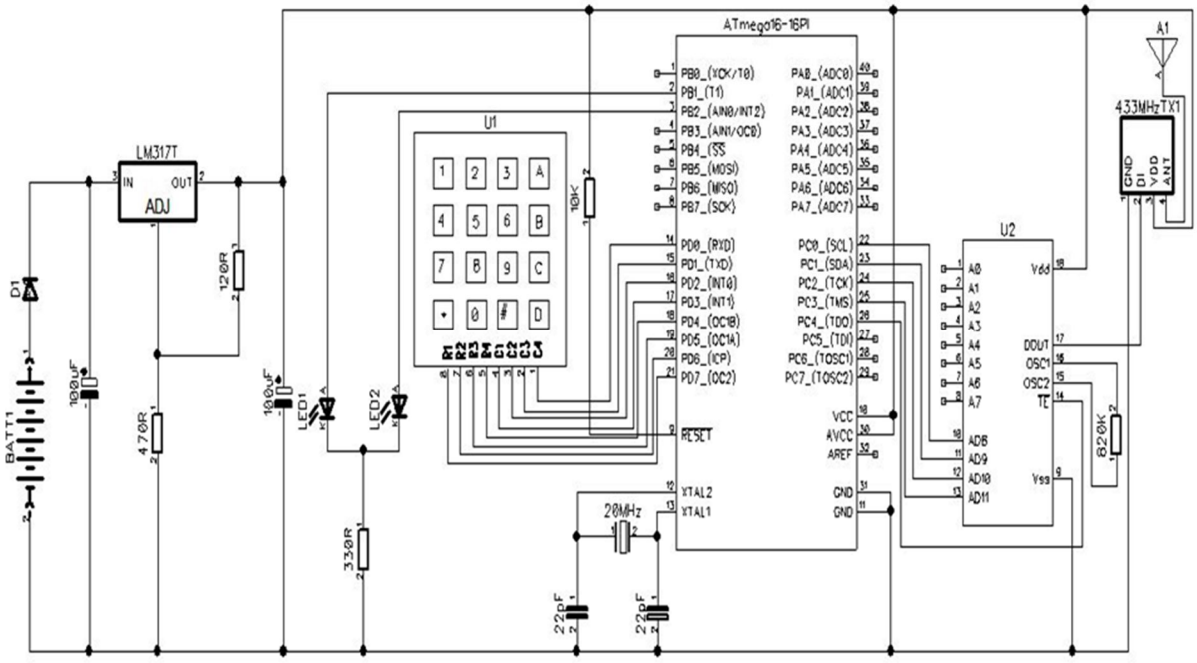


FIG. 3. Circuit diagram of transmitter section.

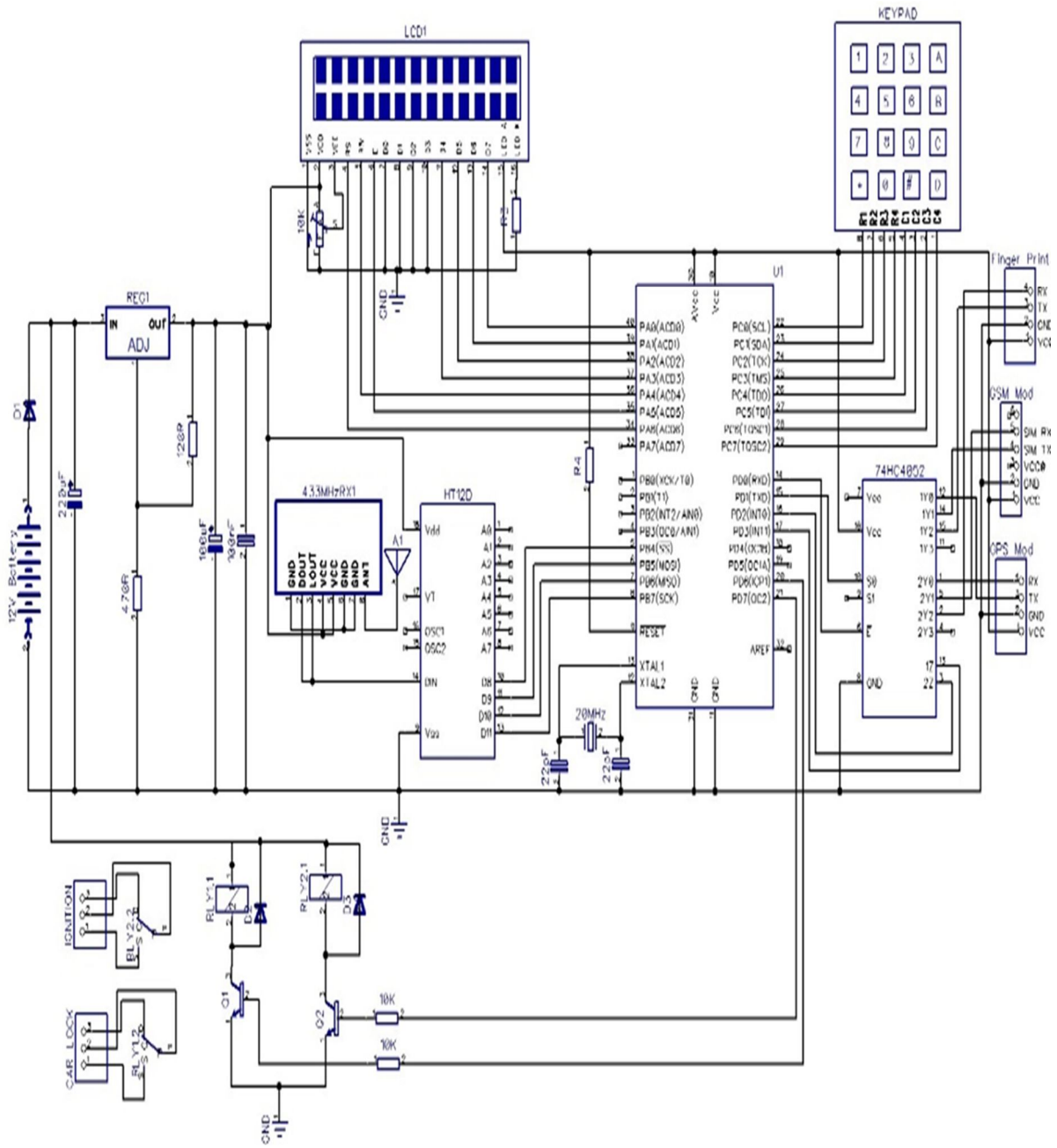


FIG. 4. Circuit diagram of receiver section of multifactor authentication car tracking system.

## Stage-by-stage Breakdown of the System

The entire car tracking system is made up of seven major units as follows:

(i) Power supply unit (ii) Receiver and decoder/remote control unit (iii) Microcontroller/data processing unit (iv) Authentication unit/data acquisition and management (v) LCD display unit (vi) Switching unit (vii) Communication unit/GPS and GSM modules.

***The power supply unit*** is the general supply that supplies power to the entire system. Power for the circuit is derived from the car's 12V battery. The DC output from the car battery is fed to a positive adjustable voltage regulator type LM317 the responsibility of which is to supply constant +5V DC from +12VDC car battery for the microcontroller, RF transmitter and receiver modules, GSM, GPS, fingerprint module and LCD display, as shown in Fig. 5. The capacitors are responsible for decoupling the power supply line from ripple [14].

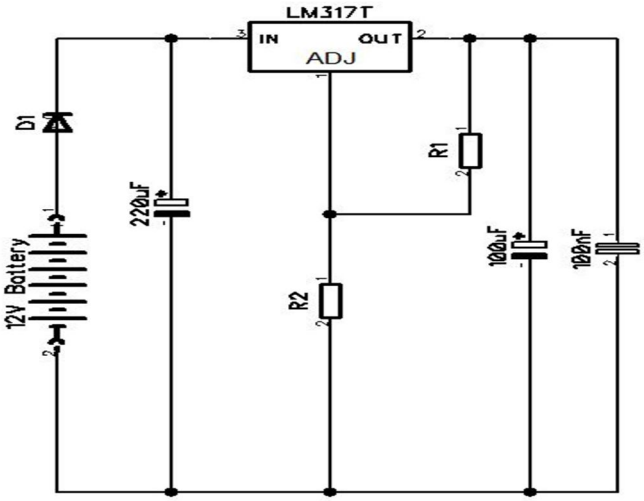


FIG. 5. Power supply unit of the car tracking system.

***Receiver and decoder (remote control unit)*:** This unit consists of a 433MHz Radio Frequency (RF) receiver and a decoder, with the function to receive the transmitted data that is sent from the transmitter and decode it back into binary data, before sending it to the microcontroller for processing. During operation, the decoder decodes back the signal from the data in pin (DIN) into binary information (digital information) and then sends the information that it decodes to the microcontroller. The circuit diagram of the receiver and decoder section is shown in Fig. 6 [15].

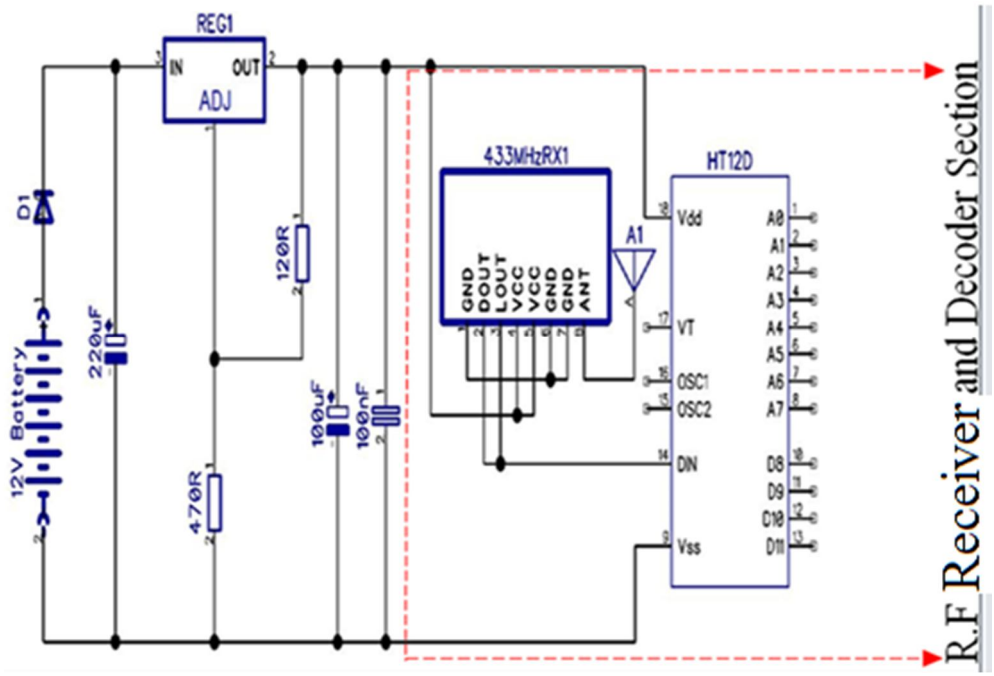


FIG. 6. Circuit diagram of the receiver and decoder section.

***Microcontroller (data processing unit):*** This unit consists of an ATmega16 microcontroller, crystal oscillator and its loading capacitors. In spite of the seemingly complex operation of the work, the circuit itself is really very simple. Most of the intelligence is done by the microcontroller through a firmware program hidden inside the controller, which is really the heart of the circuit shown in Fig. 7. The microcontroller runs at 20MHz using a crystal oscillator as its time base. In operation, the microcontroller monitors and manages every data and the signal that is coming from input devices (GPS, GSM, fingerprint module, RF transmitter and receiver modules) at the designated ports of the microcontroller, respectively [16].

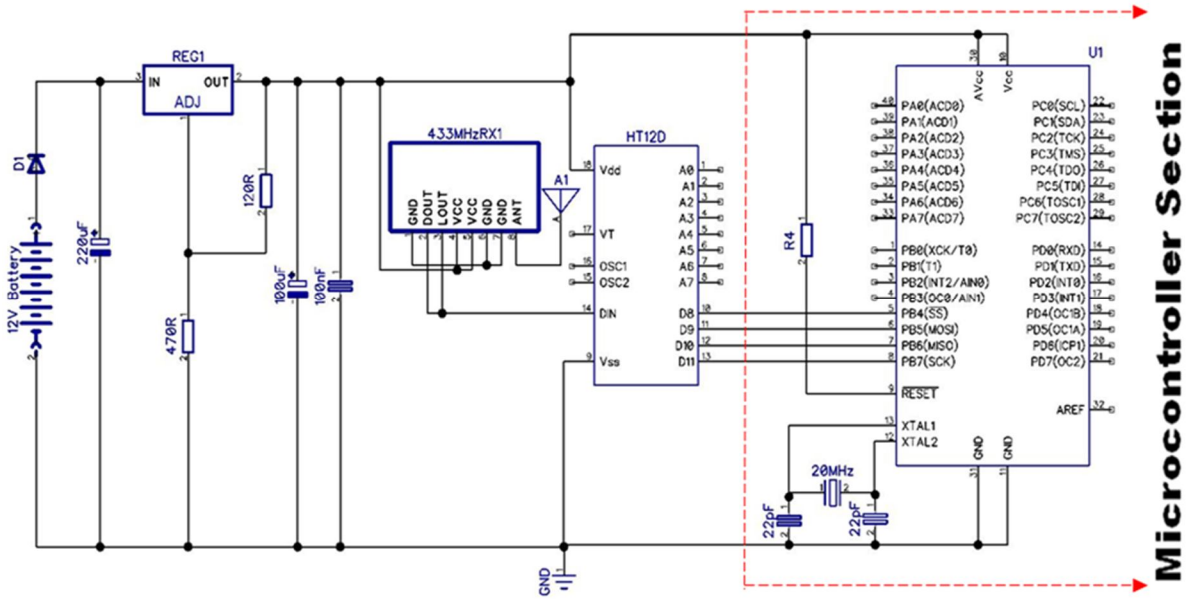


FIG. 7. Circuit diagram of the microcontroller section.

***Authentication unit (data acquisition and management):*** Shown in Fig. 8, this unit is comprised of the keypad, fingerprint, GPS, GSM module and multiplexer. The functions of these modules are to receive and send data to the microcontroller for processing. When there is a change in any of these input devices, it causes a change in the designated ports of the microcontroller to which they are connected and the controller in turn reads and interprets these values before executing the action in which it is being programmed to do [17].

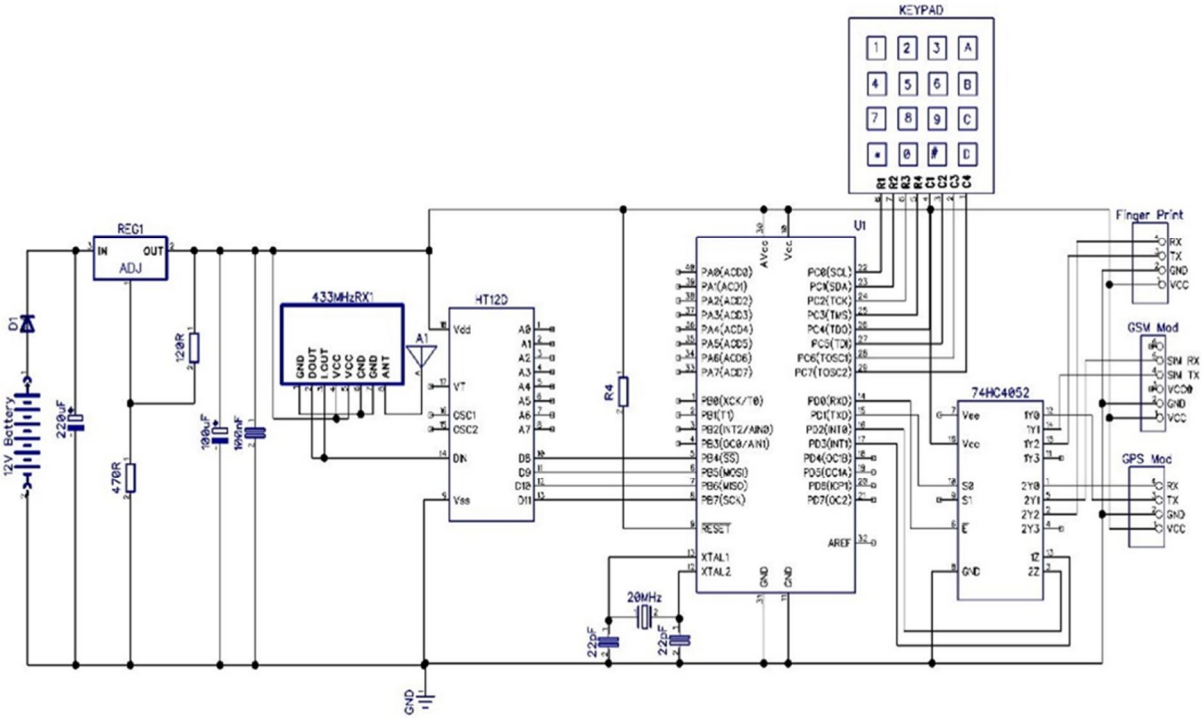


FIG. 8. Schematic diagram of the car tracking system with authentication unit.

***The liquid crystal display (LCD) unit*:** It is a collection of a variable resistor and a current-limiting resistor for the LCD backlight. The display unit uses a standard 16-character by 2-line display wired in 4-bit mode to display the functionality, condition and status of the car tracking system performance, as shown in Fig. 9. The displayed data is *processed* by the microcontroller before being sent to the display unit for display. The display data enables the user to know the status of the system [18].

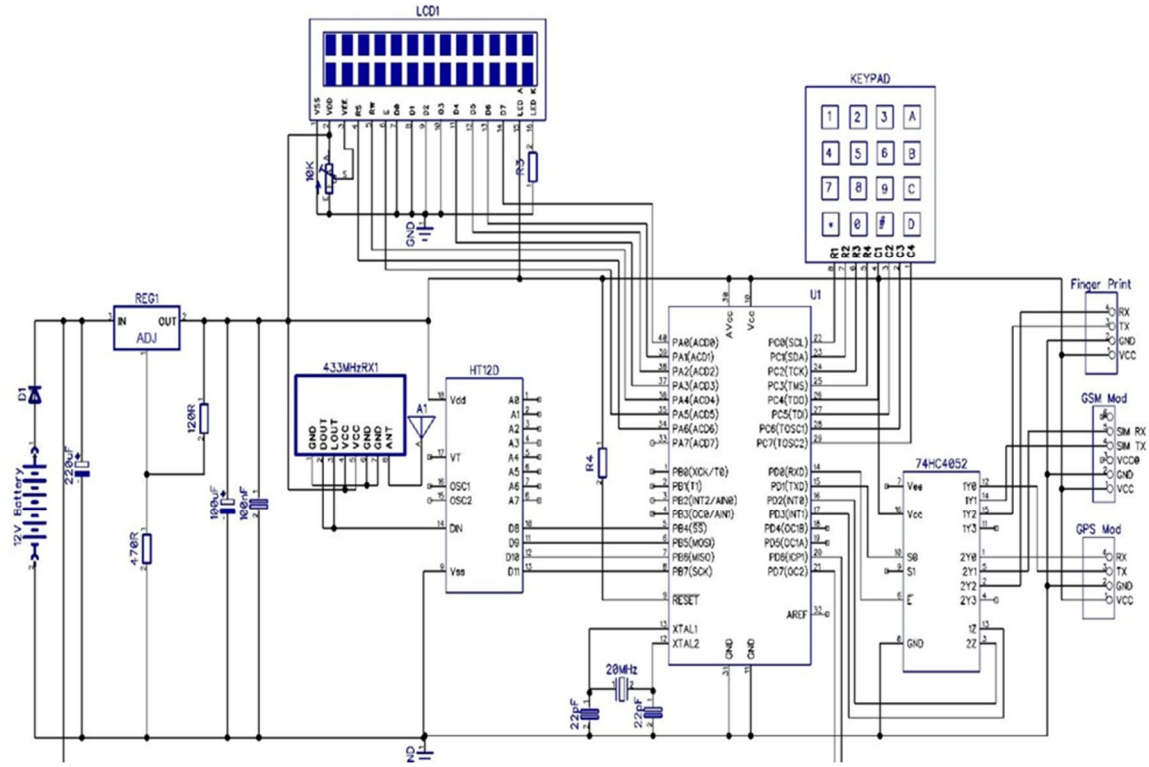


FIG. 9. Schematic diagram of the car tracking system with the display unit.

***The switching and activation unit:*** It is saddled with the responsibility of engaging and disengaging the car when there is a change in the data received by the microcontroller through the respective input devices (keypad, fingerprint module, GPS and GSM modules). This section, as shown in Fig. 10, is comprised of two transistors, two relays and diodes the function of which is to protect the transistors from getting damaged when there are occurrences of back Electromotive Force (EMF) during the operation of the system [19].

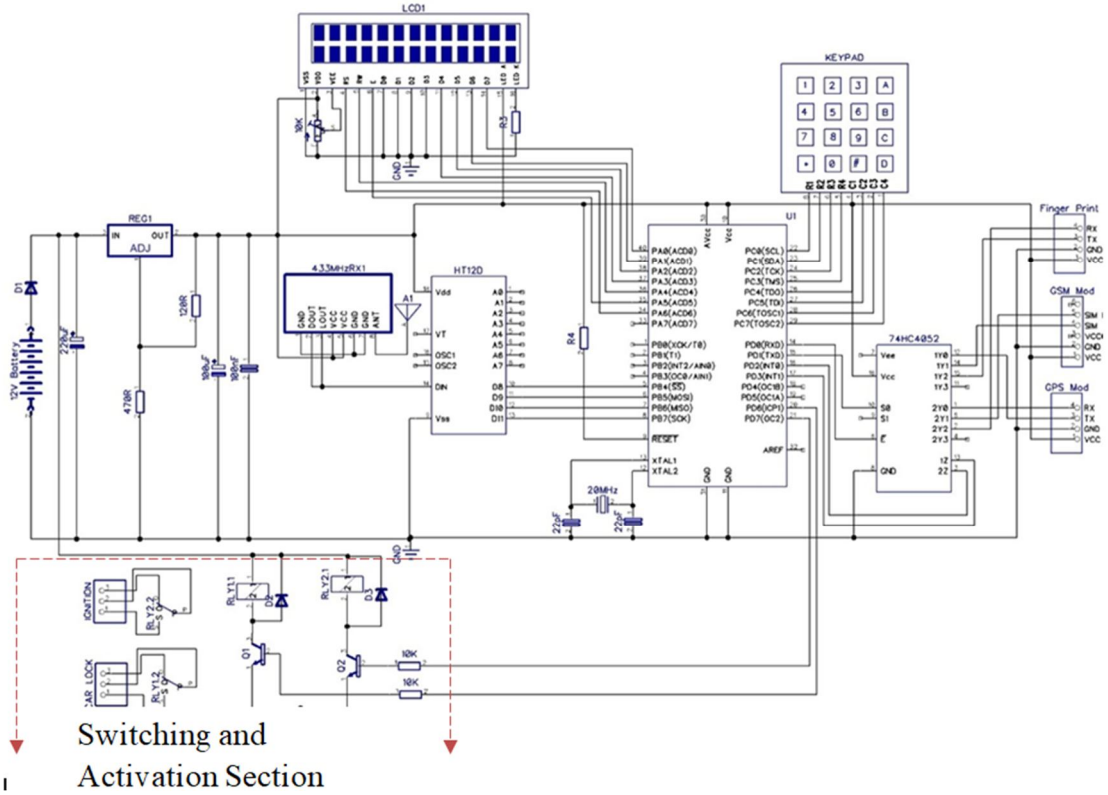


FIG. 10. The switching and activation unit of the car tracking system.

***Communication unit /GPS and GSM module:*** GPS contains a serial port interface with the microcontroller. It receives and sends location data to the microcontroller and the microcontroller receives the data and transmits it to the user using GSM.

GSM module is interconnected with the microcontroller. The receiver pin of the microcontroller is wired with the transmitter pin of GSM modem and the transmitter pin of the microcontroller is wired with the receiver pin of GSM modem. The module uses the attenuation commands to select the mode in transferring and receiving messages and other functions, like calls, … etc. It also uses time division multiple access technology. GSM/GPRS modem used in this work is SIM800 which is interfaced to the system to track and keep the coordinates of the car as well as sending an SMS text message to the user when unauthorized persons get access to the car. With the GSM and GPS modules, the user can track and control the car remotely. The modem also communicates and sends a text message to a dedicated security phone numbers when a wrong code or invalid fingerprint is detected in the system as well as the location (latitude and longitude) of the vehicle.

## Results

The technique of this system is to use scan cues to determine the changes of the state of the phase voltage value. The difference in phase voltage instructs the microcontroller to switch to activate the lock and ignition switching system. When the system is switched on, it checks to get the current status of the user in terms of fingerprint pattern; during this period, if this does not match the one stored in the system data EEPROM, the microcontroller takes over and activates the lock disengaging the ignition system of the car and then sends an SMS to the car owner notifying him/her of possible car theft with the location of the car. This system covers all the theoretical and practical areas specified for this research work. It helps in providing additional security measures by demanding the vehicle owner's fingerprint after a three minutes' drive, after three failed attempts by the system to recognize the fingerprint of the user. The steps below discuss the results of the system and its working conditions.

**Step I. Access to the car using a handheld transmitting device (first-level authentication)**

This is the separate unit of this research work and can also be called a handheld device. The test for this was first used to activate the car by inputting the 4-digit admin password (0124) in order to activate the vehicle; the red LED blinks at each input and a verification of the inputted pin saved in its EEPROM will be activated. If correct, it will send an RF signal to the car which in turn activates the car door in order to allow the user's access to the car. In the event of correct password entered by the user, the car doors unlock for the user to gain access to the car and a display (WELCOME CAR HAS BEEN ACTIVATED) appears, as shown in Fig. 11.


FIG. 11. Result for inputting the correct password combination.

**Step II. Access to the car ignition system (second-level authentication)**

However, the second-level authentication is carried out while the user is in the car and demands the fingerprint verification before the ignition is activated. The system demands that the right thumb of the user's finger be placed in the fingerprint module so as to authenticate the fingerprint recognized by the system. This is displayed in Fig. 12, as (SCANNING FP., PLS. PUT YOUR THUMB). Fig. 13 is an indication that the fingerprint module is carrying out a verification process to ascertain that the finger placed in the fingerprint module is recognized by the system and the scanning process is completed. Then, the system will display the recognized fingerprint code with a predetermined identification number, ID NO: 000. Then, the system instructs the microcontroller to switch on the relay to activate the ignition switching system of the car for the user to start the car with the key. Fig. 14 shows that the finger placed in the fingerprint module is not recognized by the system.

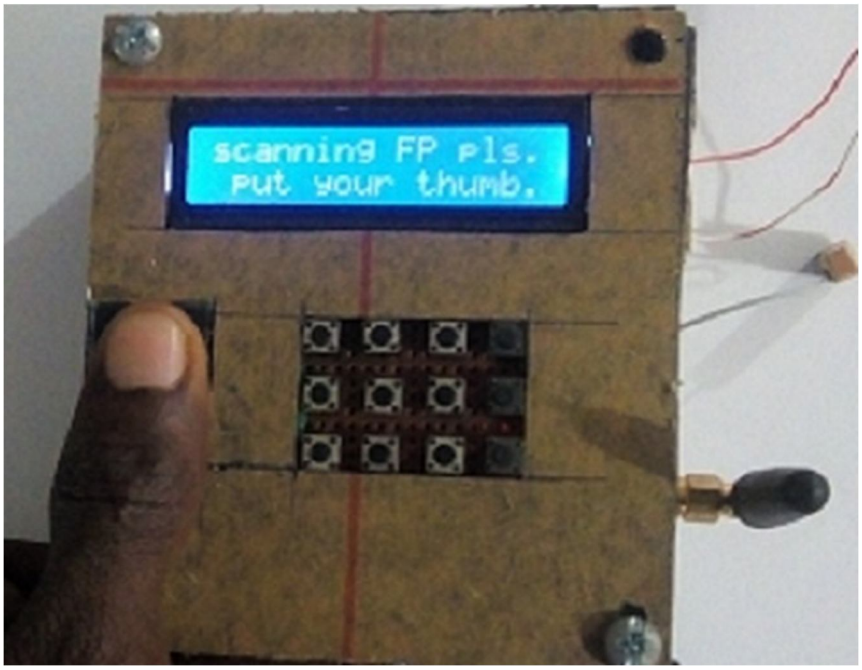


FIG. 12. Result requesting to put the user's finger.


FIG. 13. Result showing scanning the correct finger.


FIG. 14. Result showing scanning a wrong finger.

**Step III. Verifying that the car is not used by an intruder (third-level authentication)**

In order to verify this level of authentication, a test was carried out on a car while on motion. The system demands the fingerprint within a 3-5 minutes' drive to accertain the authenticity of the user for three times. After three failed attempts by the system to recognize the fingerprint while the car is still on motion, it demands for the thumb to be placed once again in the fingerprint module. This is an additional security measure to ensure that the car is driven by the owner whose fingerprint was verified and recognized by the fingerprint module in the system.

**Step IV. Communication/ Tracking**

This process shows a pop-up message as shown in Fig. 15 by sending a responder message to the car owner, relative and security agency's cell phone number as predefined in the system for tracking. On the receipt of this message, as shown in Fig. 16, the owner or either of the predefined phone numbers recognized by the system can now forward a programmed code message **"@STOP"** to the system to track the car by disengaging the car ignition system, thus confining the intruder inside the car by initiating the central lock system. Then, the system will automatically send the location and the coordinates of the car through GPS/GSM *via* S.M.S. for recovery.


FIG. 15. Result showing SMS sent to the designated mobile phone.


FIG. 16. Result showing an alert message sent to the user's mobile phone.

**Step V. Fingerprint authentication/ evaluation**

For an extra authentication, fingerprint module is interfaced with the system in order to grant access to the user when required. When the fingerprint is inputted, the system then registers the fingerprint pattern and then prompts the user to start the car. After the verification of the fingerprint pattern, the microcontroller receives the control command and energizes the ignition relay. Table 1 demonstrates the fingerprints test-scan of correct thumbs and wrong thumbs of users. The reliability test, as shown in Table 1, is a clear indication that the proposed system is a high-security car tracking system with approximately 100 percent competency level.

TABLE 1. Fingerprint test result and evaluation

| S/No. | Input | Output (Result) | No. of Times Tested |
|---|---|---|---|
| 1 | Correct fingerprint identification | Image found with ID No: 000 | 12 |
| 2 | Wrong fingerprint rejection | Image not found in the database | 12 |
| 3 | Correct fingerprint rejection | None | 8 |
| 4 | Wrong fingerprint acceptance | None | 8 |

## Conclusion

The main aim of this research work had been accomplished as described in the technical description of this work. It is satisfactory to say that there are several methods in which one can design a tracking system with intelligent security features that can be used in both domestic and industrial applications. With the above proposed type of system, the cost of paying insurance companies to manage and insure cars would be eliminated. The design specifications were established from an examination of related work and the demand for tracking system applications. These criteria were critical in creating a work that met with the original objectives. Thus, having constructed a device that successfully met these specifications calls for future improvements in the area of other device compatibility as needed, as well as security camera integration. Miniaturization of the system is also recommended for future enhancement in the field of tracking technology.

## References

[1] Kodavati, B. and Raju, V.K., IJERA, 3 (1) (2012) 616.

[2] Yang, D.K., Cai, B.G. and Yuan, Y.F., IEEE Symposium on Intelligent Transportation Systems, 2 (2003) 1246.

[3] Joshi, R.R., Proceedings, IEEE on Intelligent Vehicle Symposium, (2002) 36.

[4] Deepika, V., Suneel, M., Chiranjeevi, M., Satya, V. and Swamy, T., IJACSCC, (2013).

[5] Win, Z.M. and Sein, M., SICE Annual Conference, Waseda University, Tokyo, Japan, (2011) 13.

[6] Saraswat, C., IJCSE, 2 (2) (2010) 264.

[7] Rishabh, M. and Prashant, T., Thesis: National Institute of Technology Rourkela, Orissa-India, (2011), (Published).

[8] Adeoye, T.O., JWCSIT, 4 (6) (2014) 76.

[9] Ushie, O.J., Valentine, N.H., Ekong, I.B., Etido, M.G. and Bassey, J.U., JAET, 9 (2) (2019) 30.

[10] Ahmed, A.E. and Mohammed, K., Open Comput. Sci., 10 (2020) 17.

[11] Asmita, S.U. and Sankpal, S.S., IJITEE, 8 (10) (2019) 65.

[12] Mounika, A. and Chepuru, A., IJRTE, 8 (2) (2019) 2399.

[13] Power Supply Units: https://en.wikipedia.org/wiki/Power_supply_unit_(computer) [Accessed 31 January 2020].

[14] Wireless transmitter and receiver RF modules: https://www.electronicshub.org/wireless-transmitter-and-receiver-using-rf-module. Retrieved30th January 2020.

[15] Darko, H. and Bojan, G.A., Sensors, 14 (6) (2014) 9755.

[16] Naveen, K.V., Sujana, T., Likith, S.D. and Ramesh, C.G., IJSR, 4 (8) (2013) 419.

[17] Liquid Crystal Display Device: https://en.wikipedia.org/wiki/Liquid_crystal_display. [Retrieved 30th, January, 2020].

[18] Pressman, A.I., Billings, K. and Morey, T., "Switching Power Supply Design", 3rd edn., (McGraw-Hill, ISBN 0-07-148272-5p, 2009).

[19] Aliyu, S., Abdullahi, U., Pomam, M., Hafiz, M., Sanusi, A. and Akanmu, S., 3rd Intern. Eng. Conf., Federal University of Technology, Minna, Nigeria, (2019).