



Fingerprint Authentication and Mobile App Based Monitoring of Vehicles Using IOT

Venkata Sai Kumar¹, Gunti Spandan², B Chakri³, Dinesh Babu⁴

¹ Student, Dept. of C.S.E, GITAM School of Technology, India, sareddyvenkatasai855@gmail.com

² Assistant Professor, Dept. of C.S.E, GITAM School of Technology, India, sgunti@gitam.edu

³ Student, Dept. of C.S.E, GITAM School of Technology, India, sirivelladineshbabu9@gmail.com

⁴ Student, Dept. of C.S.E, GITAM School of Technology, India, b.chakri222@gmail.com

ABSTRACT

Biometric and Vehicle Monitoring are main aspects to improve the Car Security. The paper incorporates a method of using finger impression sensor for unique mark validation, ringer sensor for flagging sound, GSM module for correspondence between a registering gadget or cell phone, GPS module for finding the area of vehicle, Wi-Fi module that can establish a connection between any microcontroller and Wi-Fi network, the vehicle security can be monitored through Blynk application So that Car Theft and Real Time monitoring Can be done.

Key words: Microcontroller, ATMEGA-328, GPS sensor, Blynk App.

1. INTRODUCTION

Vehicle robbery is potentially the quickest developing type of wrongdoing in India. Open space vehicle burglary: consistently, most vehicles are taken out and about (65 percent) or from the proprietor's home (15 percent). This type of vehicle burglary is called 'clean' vehicle robbery. Vehicle use is high because of an expansion in the populace so better wellbeing measures are required. Sending of on-board hostile to robbery frameworks may settle this issue, yet also includes additional venture for vehicle proprietors. A few people mount hostile to burglary gadgets in their vehicles to dissuade theft, for example, LoJack, ProScout, and TravelEyes2. A large portion of the gadgets joins remote availability and GPS restriction procedures [1].

Iot is the combination of systems and the capacity to create information over a system without human mediation. The IoT refers to the trillions of physical devices in the world that are linked to the Internet, most of which gather and even provide information. The prevalence of virtual devices makes it

feasible to transform something, from anything as tiny as a pill to anything as massive as a plane, into a fragment of IoT. The IoT is continuing to make the development of our physical environment more perceptive and progressively open, coordinating the programmable and physiological universes. Initially, IoT was primarily applicable to market and manufacturing, where its implementation is frequently referred to as machine-to-machine, The emphasis is currently on fitting our residences and workplaces with clever devices, transforming them into something that's suitable all around. The intermingling of innovation would achieve changes in the different segments, which would offer ascent to new chances

The developments of IoT look encouraging in the years ahead. IoT advances are probably going to be matched with other specialized advances, for example, computerized reasoning (AI) and self-ruling frameworks to give coordinated brilliant arrangements [9]. Normally, IoT advances will prepare billions of regular items with correspondence and insight. It has just been broadly executed in different fields, for example, wearables, savvy home applications, social insurance, shrewd urban communities, farming, modern mechanization. Certifiable models include IoT Sensors, IoT Data Analytics, IoT Monitoring and Control System, IoT Connected Plant, Smart Supply Chain Management, Smart Barcode Readers, Smart Grids, Connected HealthCare System, Smart Farming [8].

2. LITERATURE SURVEY

They're taking a shot at structuring and building up another vehicle against robbery notice and GPS beacon dependent on Android OS in a handheld correspondence terminal, according to the examination of Vehicle Anti-Theft System [1].

It expects to give vehicle insurance using the GSM module as appeared in the investigation of Wu Aiping. The objective of this paper is to give an Anti-Theft System Design dependent on GSM [2].

As per crafted by the Android App , they center around the advancement of procedures for the vehicle obligation and following framework progressively automobile. Paper focuses on the development of the Anti-Theft System for Fingerprint Sensors vehicles [3].

According to the examination of, Fingerprint Sensor For Vehicle Theft is giving an improved separation precision to an enemy of burglary cell phone application, the unit is outfitted with an accelerometer and GPS sensor framework that relays realtime. paper information position to the connected client around Distance Accuracy Improvement for Smartphone Anti-Theft Application [4].

Several more sophisticated devices, such as sensors, are mounted on the door handle. The anonymized fingerprint data is then analysed and administered to the unique mark controller inside the vehicle and to different frameworks, for example, the unique mark security framework for vehicles except for GPS and Radio Frequency Identification [5].

Radio Frequency Identification is utilized for the clever mechanized Anti-Theft control framework. The impediment here is that keyless RFID cards can without much of a stretch be the Auto Cop component, which is a video reconnaissance arrangement that can be coordinated to the vehicle. [7] The camera screens the activities in the going with vehicle consistently. The principle downside is that the camera won't identify unequivocally while there are changes in the lighting conditions inside the framework [6].

3. SYSTEM DESIGN

Numerous vehicles are encased with different security frameworks. We can discover beepers, alarm, entryways, and windows of most recent time, and individual wellbeing things. All things considered, every single such thing that is as of now accessible is exceptionally expensive. Our proposed framework comes when unapproved get to is made, a signal caution is activated and notice is sent to the proprietors of the cell phone.

Our key element is unique with different frameworks, for example, a brilliant entryway gets to gadget utilizing a unique mark module. The utilization of this framework is proposed to give access to just affirmed people. Both equipment and programming advances have been utilized to construct it. Crisis signal sound is given to make sure about the gadget by providing a notice when an unapproved individual enters the network. Motors are utilized to bolt and open the entryway. Furthermore, at any second, killing the vehicle's capacity flexibly by methods for a cell phone application, and different things, for example, finding the vehicle's area by GPS[10]. The WiFi module is utilized to give microcontroller connectivity to the WiFi network.

This study is a combination of latest technologies. One of the technologies used is the Fingerprint Sensor, which has more accuracy to provide security for authentication of the different customers to access the vehicle. The subsequent

innovation utilized is the Global Positioning System to decide the area of a vehicle on earth. It utilizes radio transmissions to trade data among satellites and GPS.

This IoT based vehicle checking framework additionally incorporates Buzzer caution to alarm the proprietor of the vehicle, if unapproved individual attempts to get to the vehicle, and a notice is sent to the proprietor, at whatever point the approved or unapproved individual gets to the vehicle. An inventive unit is incited in the framework, which is called as Engine Control Unit, which is utilized to slice the ability to the motor at whatever point a burglary of the vehicle occurs. This is the way security is given to vehicles.

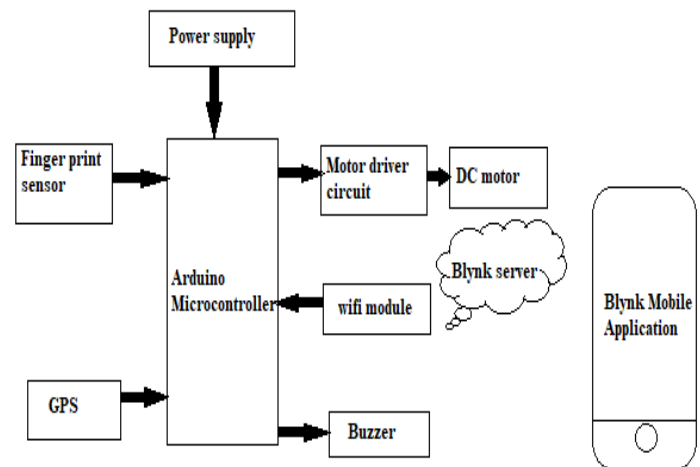


Figure 1: Block diagram of the Vehicle system

The square chart of our idea is found in the outline above (figure 1). The Arduino UNO micro-controller is used which is connected to wifi module, a GPS sensor and fingerprint sensor is connected to the micro-controller. From the micro-controller, the data is continuously transmitted to the Blynk server and the owner of the vehicle can monitor from the Blynk android application.

4. METHODOLOGY

In the proposed framework, we are not simply giving security to the vehicles by utilizing Fingerprint verification yet also, we give an observing framework to the vehicle proprietors with the assistance of a cloud-based application which is the Blynk App. The working procedure of the total framework is detailed clarified underneath.

The proprietor of the vehicle must get enlisted in the Blynk application giving the proprietor's subtleties like the name, telephone number, and the fingerprints to the Blynk Cloud. At that point, the proprietor can go about as an administrator to the Blynk application introduced on the portable.

As we have introduced the unique mark sensor on the entryway handle of the vehicle, one needs to embed their finger impression on the sensor to get passage to the vehicle.

Just enlisted individuals can get to the vehicle. If at all an unapproved individual attempts to get to the vehicle, effectively set bell gets enacted and sounds the caution to alarm the proprietor. Furthermore, since, we have set a GSM module, the proprietor gets an alarm message.

In case if the vehicle has been robbed by using any unethical events, still the owner can catch the location of the vehicle because of the GPS placed in the vehicle. By using a special feature of the proposed system the engine of the vehicle can be shut down with the help of EUC.

5. EXPERIMENTAL SETUP:

5.1 Arduino IDE

Arduino IDE is open-source software that is primarily used for coding and compiling programming to the Arduino machine. It's an approved Arduino program, rendering it so simple to compile an application so even an average citizen with little previous technological experience will get their feet wet in the learning method. It is comfortably, accessible to operational systems such as a MAC, Windows, Linux, and runs on the Java Platform. [11]



Figure 2:- Arduino Mega

5.2 GPS

Worldwide Positioning System is the viable Global Navigation System. The GPS utilizes an intensifying of somewhere in the range of 24 and 32 Medium Earth Orbit satellites turns in exact microwave flags that actuate the GPS beneficiaries to indicate your position, separation, heading, time. GPS beneficiary gets the signs from at any rate three satellites to figure separation and utilizations triangulation methods to register the two estimation positions or if nothing else four satellites to process the three estimation positions. PS is a key innovation for giving the gadget its place. It is initially utilized in military administrations however Early on permitted the framework accessible free for resident use as a typical decent. GPS has become broadly utilized to help to explore all-inclusive, and a significant strategy for mapping, looking over the land, exchange, and logical employments.



Figure 3: Global Positioning System

5.3 Fingerprint Sensor:

R307 Fingerprint Module comprises of optical unique finger impression sensor, fast DSP processor, superior unique mark arrangement calculation, high-limit FLASH chips and other equipment and programming creation, stable execution, straightforward structure, with finger impression section, picture preparing, finger impression coordinating, search and format stockpiling and different capacities.



Figure 4: Fingerprint sensor

5.4 GSM Module:

GSM device is a modified system that utilizes a SIM card and works with a network provider connection, much like a cell phone. GSM (Global Network System) requires a mechanism called a circuit swap. This form of contact enables a route to be formed between two machines. When the two computers are linked, a continuous stream of digital data is transmitted. GSM networks are of the central Switching Service (SS), Base Station (BSS), and Mobile Station (MS) services. [10]



Figure 5: GSM Module

5.5 NODE MCU:

ESP-MODULE 8266, which transfers the data from an Arduino to an IOT platform from which the user can access it. The Wi-Fi module is equipped with the TCP / IP protocol and has SOC in its own right. When connected to an Arduino board, ESP-8266 can easily provide wi-fi, as it has its own software sense. It acts fundamentally as a scaffold between wi-fi and existing microcontroller.



Figure 6: Node MCU

Below is the Fig. 7 which tells how the wiring diagram looks like in our project

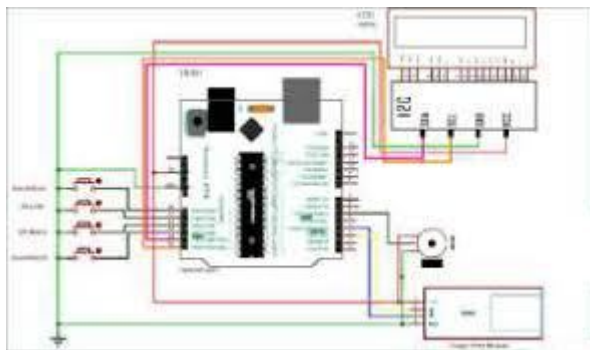


Figure 7: Wiring Diagram

6. SIMULATION RESULTS

The below figure shows the screenshots taken from the Blink App which shows us the following things i.e; the inserted fingerprint is matched and resulting the doors of the vehicle are unlocked.



Figure 8: Screenshot from led Display

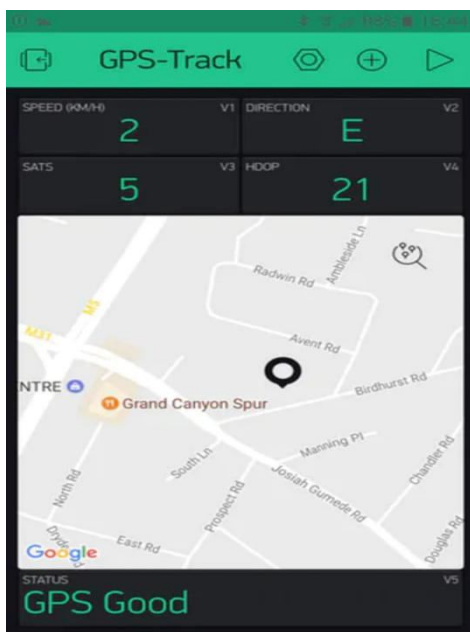


Figure 9: GPS Location

The above figure shows the screenshots taken from the Blink App which shows us the GPS location of the vehicle and also the speed at which it is travelling, the direction in which it is heading. So that the vehicle can be tracked easily.

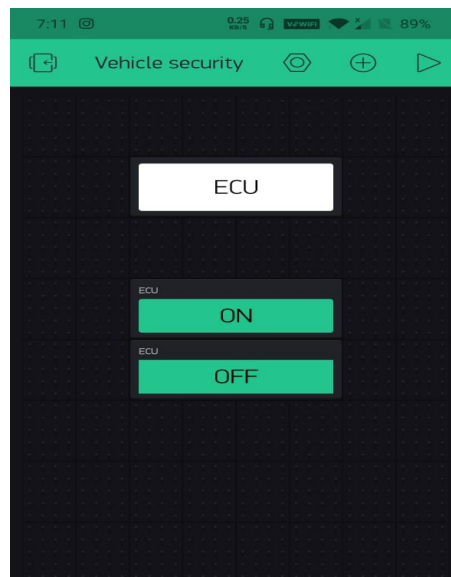


Figure 10: Engine on/Off Status

The above figure shows the screenshots taken from the Blink App which shows us the control unit of the ECU. Using this unit, we can cut the power supply to the engine.

Table 1:- Testing of the project device as a whole

| Testcase Description | Input Given | Output Expected | Actual Outcome | Observation |
|--|------------------------------------|--|----------------|-------------|
| When device is ON | Power is supplied to ON the device | LCD should display SYSTEM STARTS, send SMS, devices must blink | As Expected | Successful |
| GSM initialization | When device is ON | LCD displays GSM initialized | As Expected | Successful |
| Node MCU 8266 | Power is supplied to ON the device | Starts to blink | As Expected | Successful |
| Pairing of Node MCU 8266 with mobile App | ON mobile WIFI | Display WIFI is connected to the mobile | As Expected | Successful |
| If Fingerprint is matched | Power is supplied to ON the device | Vehicle doors are opened | As Expected | Successful |
| If Fingerprint is not matched | Power is supplied to ON the device | Sends an alert message to the owner | As Expected | Successful |
| GPS working | Power is supplied to ON the device | continuously sends the location coordinates | As Expected | Successful |

The table 1 provides the information about the reactions that occur for any action that is made in the system.

7. FUTURE ENHANCEMENT

In this paper, we have placed the Fingerprint sensor on the handle of the vehicle and we can monitor the location of the vehicle. But with further improvements like scanning the fingerprints from the mobile application itself which increases more security and monitoring ability can be increased by fixing cameras inside the vehicle on four corners which makes it a 360-degree monitoring system.

8. CONCLUSION

As referenced in this article, vehicle security and observing it assumes a significant job these days. The usage of IoT based Fingerprint confirmation and checking framework in the vehicles makes them increasingly secure and dependable. Putting resources into this framework will prompt simple getting to vehicles, observing them, and furthermore it keeps vehicles from getting looted.

This paper discloses the improved security to shield the vehicles from being gotten to by unapproved people with ease than different innovations.

In future improvements, fuel indicators, speedometers, rpm indicators, and fingerprint authentications can be added to the mobile application.

REFERENCES

1. Manyi Qian , Hailin Gao, Weihong Liu, **Android based Vehicle Anti-theft Alarm and Tracking System in Hand-held Communication Terminal** 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)
2. Wu Aiping, **Android based Vehicle Anti-Theft Alarm and Tracking System in Hand-held Communication Terminal** 2017 International Conference on Smart Grid and Electrical Automation.
3. Suvarna S Patil, AnandKumar, Harti,Praveena, PraveenKumar, H Lakshmitejaswani, **Anti-Theft System for Vehicles using FingerprintSensor** PROJECT REFERENCE NO: 41S_BE_1187.
4. Lee, S., Tewolde, G., & Kwon, J. (2014). **Design and implementation of vehicle tracking system using GPS/GSM/GPRS technology and smartphone application.**2014 IEEE World Forum on Internet of Things
<https://doi.org/10.1109/WF-IoT.2014.6803187>
5. Sathiyarayanan, M., Mahendra, S., & Vasu, R. B. (2018). **Smart Security System for Vehicles using Internet of Things (IoT).** 2018 Second International Conference on Green Computing and Internet of Things
<https://doi.org/10.1109/ICGCIoT.2018.8753073>
6. Sathiyarayanan, Mithileysh et al. **Smart Security System for Vehicles using Internet of Things (IoT).** 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT) (2018): 430-435.
<https://doi.org/10.1109/ICGCIoT.2018.8753073>
7. S. Prema, M. R. V. S. Deen, M. V. P. Krishna and S. Praveen, **Vehicle And License Authentication Using Finger Print** 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 737-740, doi: 10.1109/ICACCS.2019.8728402.
8. Jesudoss, A., and Muthuram BO. "**SAFE DRIVING USING IOT SENSOR.**" *International Journal of Pure and Applied Mathematics* 118.20 (2018): 3745-3750.
9. Wang, Gunawan, Natanael Alamas, and Marcelina Anggraeni. **The use of internet of things and big data to improve customer data in insurance company.** *International Journal of Emerging Trends in Engineering Research* 7.12 (2019): 756-761.
<https://doi.org/10.30534/ijeter/2019/047122019>
10. Panganiban,Edward(2019).**Microcontroller-base d Wearable Blood Pressure Monitoring Device with GPS and SMS Feature through Mobile App.** *International Journal of Emerging Trends in Engineering Research.* 7. 32-35.
<https://doi.org/10.30534/ijeter/2019/02762019>
11. Shelupanov, Aleksander & Konev, Anton. (2019). **Threat Model for IoT Systems on the Example of OpenUNB Protocol.** *International Journal of Emerging Trends in Engineering Research.* 283-290.
<https://doi.org/10.30534/ijeter/2019/11792019>