



FINGER PRINT VEHICLE STARTER AND THEFT CONTROL USING GPS

ARUN BATI¹, SRUSHTI V C², PRIYANKA G³, AKASH R⁴, Prof. GAGANAMBHA⁵

¹Student(4VM19EE402), ELECTRICAL AND ELECTRONICS ENGINEERING, VVIET, MYSORE, INDIA

²Student(4VM18EE074), ELECTRICAL AND ELECTRONICS ENGINEERING, VVIET, MYSORE, INDIA

³Student(4VM18EE054), ELECTRICAL AND ELECTRONICS ENGINEERING, VVIET, MYSORE, INDIA

⁴Student(4VM18EE002), ELECTRICAL AND ELECTRONICS ENGINEERING, VVIET, MYSORE, INDIA

⁵Faculty, ELECTRICAL AND ELECTRONICS ENGINEERING, VVIET, MYSORE, INDIA

Abstract: Fingerprints are amongst the oldest and most changed biometric systems, and they are frequently employed in biometric forms of identification. Vehicle safety has become a serious problem as the frequency of crime has increased. Vehicle keys are a big concern these days since they are easily forgotten or lost when carried. A system that uses a fingerprint authentication method to start a car. The operator can use the fingerprint reader to start the car with this technology. At start, this technology lets the customer to authenticate by scanning their unique fingerprint. To start the car, they might register several fingerprints. When a user scans their fingerprint in monitoring mode, if the framework does not recognize or memorize the fingerprint, or if the unknown person scans, the device alerts the security and turns off the ignition by having turned off the petrol nozzle in the event of a breach using GPS when the IC is relocated by an unrecognized user. This provides a safe and worry-free way to begin the engine or automobile. This is due to the system's usage of an ATmega 328 microcontroller, which includes an LCD screen, as well as pushbuttons and a starting motor. Another potential is a seamless and quick start for an identifiable user.

Keywords— Fingerprints, Vehicle safety, GPS, ATmega 328, LCD screen.

I. INTRODUCTION

Only individuals whose fingerprints are pre-stored in the database can use fingerprint authentication equipment. Though in the case of a total power outage or battery loss, registered fingerprints are kept. This minimizes the need to keep records of keys or memorise a passcode or PIN sequence. As there are no credentials or sequences that can be duplicated or pirated, or lock that can be selected, it can only be accessed when an authorised person is detected. As a result, the fingerprint-based lock is an excellent solution to commonly encountered problems. In contrast to the traditional practise of utilising keys, this paper concentrates on using fingerprints to access locks. Passwords and other pattern-based security mechanisms have recently been employed to restrict illegal access to such systems. Password-based authorization, on the other hand, has an inherent flaw in password leaking. The patterns are simple to copy and duplicate. In this research, we provide an indirect authentication strategy that adds a security layer to the password patterns. Biometric technologies have shown to be effective security methods in a variety of settings.

The vehicle tracing system was created and deployed to always track the position and activity of any equipped vehicle. The gadget is implanted within an automobile whose location is to be calculated and monitored in real-time, and it uses GPS coordinates and global system for mobile information sharing packet radio service advanced technologies. The GSM & GSM/GPRS components are controlled by a microprocessor. At periodic intervals, GPS module obtain geographical information, and a GSM/GPRS module is utilised to communicate and maintain the vehicle's position to the dataset.

A GPS tracking module is an instrument that utilizes the Global Positioning Technique to identify the accurate position of a car, person, or other object which is linked to and stores the location at frequent interim. The gathered location information is retained in the tracing device or transferred via cellular network to a central position database or an internet-connected PC (GPRS). This enables the position of the object to be demonstrated against a geographical backdrop in real-time or afterwards when analysing the route employing customised software. The development's main goal is to keep the car safe from any theft. We are adding protection by including biometrics, such as a fingerprint, to do this. Initially, the car owner must store their own fingerprint in the fingerprint module. To transmit or receive data to or from the user, the GSM module is needed. During the programming, the operator's cell phone number must be fixed.

The permitted fingerprint must be entered to start the four-ignition wheelers. If an unauthorized fingerprint is entered, the user will instantly receive notice and the local security device will be activated. We can also track the four-wheeler to avoid burglary by calling the GSM module that is included into the equipment. Then real-time monitoring commences, and the vehicle's GPS position is communicated to the operator through SMS. The first step is to examine your fingerprint with a biometric scanner. The next step is verification, which involves checking the database for permission. If it is validated, the ignition will turn on or an

alert will sound, depending on the biometric system. Biometrics are mostly used to provide safety for two-wheelers. Face identification, voice identification, fingerprint identification, and eye (iris) recognition are all examples of biometrics. When compared to other types of identification, fingerprint identification is the least expensive. Fingerprint verification is now used for all security purposes in businesses, ATMs, banks, and other places. The fingerprint reader is coupled to the biometrics unit, which is linked to the ignition switch. When we touch the fingerprint scanner, it compares it to the current one and, if it matches, the engine starts. The major goal of this study is to create a two-wheeler anti-theft technology. As a result, we've created fingerprint identification for two-wheeler starters. The owner's and other authorised people's fingerprints are kept in the database, and when the car is started, the scanned fingerprints are compared to the database.

II LITERATURE SURVEY

Sayantam Sadhukhan, Aritra Acharyya, and Rajendra Prasad (2017) describe the relevance of IoT with mobile applications in their essay "Car Security System employing Fingerprint Scanner and IOT", released in Indian Journal of Science and Technology. They go on to say how crucial it is to maintain our automobiles as safe as we maintain our cell phones. The team discusses how to utilise a biometric auto entry system to keep your vehicle safe. It only permits numerous people to utilise the automobile if they have been given permission. The employment of a mobile application is advantageous in this case. When the automobile is robbed, it sends a notification to the owner. Rajeev Velikkal (2019) outlines the demonstration of a keyless automobile entry system in his project, which was published in the Indian Journal of Science and Technology. He created this unit with the help of an Arduino kit, which he drew and programmed. Simple programming languages are used to create the design.

As per a 2013 research paper titled "Fingerprint based locking system," the author created this work specifically to increase the bike's safety. The objective of this work is to investigate and comprehend the notion of the Fingerprint Module. Fingerprint Unit, Relay, Buzzer, and Arduino Module are all used in this application. The proposal also employs the usage of a buzzer as a signalling device. The owner of the bike can add or remove fingerprints, permitting or disallowing anyone to ride the motorcycle. [2] The biggest drawback of this idea is that once the battery runs out, the device will not operate. In addition, because the ignition system is built for several purposes, the cost of the system is still inexpensive. As per a 2013 research paper titled "Fingerprint based locking system," the author created this work specifically to increase the bike's safety. The objective of this work is to investigate and comprehend the notion of the Fingerprint Module. Fingerprint Unit, Relay, Buzzer, and Arduino Module are all used in this application. The proposal also employs the usage of a buzzer as a signalling device. The owner of the bike can add or remove fingerprints, permitting or disallowing anyone to ride the motorcycle. [2] The biggest drawback of this idea is that once the battery runs out, the device will not operate. In addition, because the ignition system is built for several purposes, the cost of the system is still inexpensive.

"Fingerprint Sensor-Based Anti-Theft System for Vehicles" The use of microcontrollers and GSM modem to avoid automobile burglary, as well as biometrics, such as fingerprints, to ensure security. "Fingerprint sensor takes fingerprint pictures, compares the originality of each print detected by the scanner, and relates it to the one recorded in its unit or local database server," says the author of a fingerprint-based verification and surveillance features based on GSM and GPS technology. A Biometric Method for Vehicle Security Employing Fingerprint Identification vehicle surveillance system utilizing person detection methods. The study emphasizes on the most common methods for automated person identification, such as fingerprint recognition and different existing car security systems. "Vehicle Security with a Smart Anti-theft System" Security, particularly car theft security in public parking lots, has been a source of worry. Using an embedded system coupled with the Global Positioning System (GPS) and the Global System for Mobile Communication, an effective anti-theft car security system is built (GSM). In the car, precautionary measures such as engine ignition cut-off, gasoline supply cut-off, and electrical shocks mechanism are fitted and operated by the user or owner's GSM phone. With the use of SMS, the owner may lock or unlock their vehicle.

III PROBLEM STATEMENT

An alternate design that integrates a fingerprint scanner with the Arduino microcontroller has been suggested to enhance the device's security mechanisms. The suggested concept provides a more comprehensive solution to system control. The schematic diagram of the suggested design is shown in Fig.5.1. To monitor the equipment and allow access to a user in a distant region, the suggested technique utilizes a GSM/GPS-based unit. The best technique to safeguard a car from numerous sorts of theft is to use a vehicle locking system. It is the vehicle safety device that provides a more comprehensive along with luxurious insurance for one's automobile. A fingerprint authentication device is included in the design, which offers excellent security and authentication characteristics. This unit, coupled with the GSM and GPS modules, enables us to identify and rectify numerous flaws in the equipment more quickly.

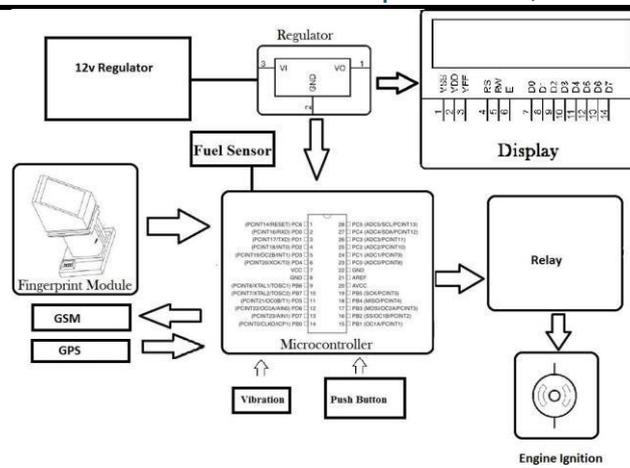


Fig 3.1: Block Diagram of the Vehicle Ignition System

The subsequent sections discuss the various necessary components for this design execution.

1. GSM module
2. GPS module
3. Arduino Micro controller
4. Fingerprint Scanner
5. Liquid Crystal Display
6. Relay Circuit

GSM Module:

The GSM module makes it easier to transmit and receive information on a cell phone. The GSM module has an antenna for accepting network signals via the user's mobile phone. For interaction, this GPS system is configured with AT instructions. The Transmitter (TX) and Receiver (RX) pins which is employed to communicate serially with the microcontroller. SIM state, signal strengthening, and connectivity are all checked via AT instructions.



Fig. 3.2

GPS Module:

GPS stands for Global Positioning System, and it is a navigation process that monitors the precise location of the device or a location. GPS enables us to pinpoint the exact position of the gadget, reducing the risk of robbery.



Fig. 3.3

Arduino Micro controller:

The suggested architecture makes use of an Arduino Mega 2560 microcontroller module, which is depended on the ATmega 2560 microprocessor. The microcontroller controls all the modules and works as a reason in achieving the expected result.

**Fig. 3.4****Fingerprint Module:**

A fingerprint sensor device is connected to and operated by an Arduino uno board in this setup. The consumer can register his fingerprint in the ATmega2560 microcontroller using the Arduino IDE.

**Fig. 3.5****Liquid Crystal Display (LCD):**

An LCD is a graphical show technology that uses the capabilities of light fluctuation to display the result. In this concept, an LCD is required to demonstrate different messages to the consumer, making the gadget handier. A welcome message, an approach request text, or a permit authorized notification are examples of different sorts of communications.

**Fig. 3.6****Relay circuit:**

A relay is an electrical device that acts as a switch, allowing one signal to operate many circuits. For real-time execution of the suggested architecture, a junction box was employed in this work. The junction box is associated with several appliances, all of which run on AC electricity.

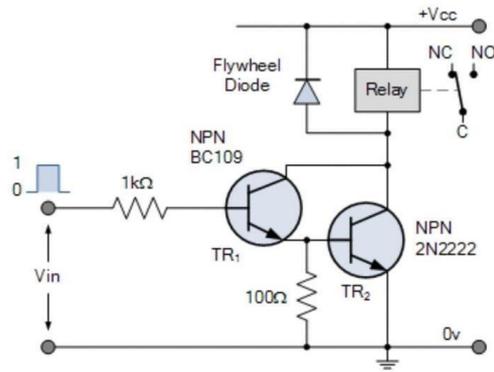


Fig. 3.7

The vehicle's operator is required to store their own fingerprint in the fingerprint module. During the coding, the owner's cellphone number should be fixed. The permitted fingerprint must be entered to activate the four-ignition. wheeler's If an unauthorized fingerprint is entered, the user will instantly receive notice and the regional security system will be activated. The vehicle's GPS location is then communicated to the user through SMS, allowing for real-time surveillance. Alerts to the device can also be used to regulate the vehicle's ignition. There are two serial ports in use. One is for GSM modems, while the other is for GPS modems. The gadget is attached to the vehicle. The cell phone, which provides a wireless link between the car tracking system and the user, is used to supervise the complete gadget. A GSM SIM card is put into the vehicle tracking device's specific SIM card slot to receive and transmit SMS. The user may send an SMS from his cell phone, find out where his car is, and utilize the feature to secure it.

IV RESULT

The setup of the LCD and GSM module is the first step in the implementation procedure. After all the elements have been set up, the user may operate the gadget directly by sending text messages. This system also enables a person who is close to the system to access it if the authorized user grants access. The person who is close to the system terminal places his finger on the fingerprint sensor. If the fingerprint is a legitimate picture, a notification requesting access permission will be transmitted to owner's device. If the system's owner transmits an access allowing message, anybody within range of the device can manually operate it. If the fingerprint picture is deemed to be unknown, the LCD will display "invalid user" and the person will be denied entry. Several permitted and illegal requests to login to the system are part of the testing circumstances for this work.



Fig. 3.8

THESE INCLUDES THE FOLLOWING:

- Authorized login, which entails using a verified fingerprint to get access to the device. Unauthorized access, i.e., a fingerprint that hasn't been authorized.
- A vehicle is towed for a set period.
- The user's notification to enable and disable the device.

Fingerprint recognition enhances the safety of a vehicle by limiting access to only authorized personnel. Future improvements in terms of effectiveness and accuracy can be made by either enhancing the technology used to record the picture or using picture enhancement techniques.

V CONCLUSION

Because everyone's fingerprint is distinctive and only authorised users may access the car, the predicted effect of adopting this approach upon the vehicle is that only the authorised person will be able to start it. The car will not ignite for everyone who has a key. The data of the individual will be compared to that of the database, and only if there is a match, the vehicle will be used. Thus, by installing this very inexpensive and widely accessible technology on a car, significantly higher safety and uniqueness may be achieved than with a traditional lock and key. The construction of a smart car surveillance system based on GPS, fingerprint authentication, and GSM technology was sorely tested, and the findings confirmed that it works as predicted. The system is administered using a web-based Android application created in the Android Studio IDE using the Java language. When the cloud-hosted real-time database is used in conjunction with the surveillance system's C-Secure application, information from the vehicle is broadcasted in real time to the database, and if there is no cellular service in the tracking province, the vehicle's last location information can be recovered from the dataset and the vehicle's approximate areas can be predicted.

The system's test revealed that the device's owner may demobilise the vehicle remotely in real time utilizing SMS instructions and a mobile application via cellular network and the internet, respectively. In the event of a hijacking, the vehicle owner may safely exit the vehicle and then use any phone to transmit orders and remotely turn off ability to stop the automobile from driving and thereby reclaim it. When the longitude and latitude data obtained and sent into Google Map Segment within C-Secure Application programming interface established for the device, the vehicle's position could be determined precisely. The car security has been increased with the incorporation of the fingerprint recognition device, as only authorised users may start the vehicle. The capacity to limit the frequency of vehicle theft on a widespread selection in our culture is critical for the security of automobiles in our community. Incorporation of an authentication method and the usage of a real-time cloud database for information storage were two of the advancements made to prior efforts. This security process will enhance security and safety by sending a text message to the user and using GPS to parse the string, Longitude and Latitude information of the vehicle for monitoring it and sending a text message to the user for the purpose of halting it. In addition, the integration of a fingerprint identification device and a server-less control mechanism aids in regulating intruder accessibility, making it harder to begin the automobile. This will protect the automobile from robbery and save time due to stolen vehicle monitoring.

REFERENCES

- [1] Joel Sachin, Kiran Rana Gill, "Anti-Theft System For Vehicles Using Fingerprint Sensor", International Journal Of Scientific & Engineering Research, Volume 7, Issue 7, July-2016 1436 ISSN 2229-5518.
- [2] K.Dineshkumar, G. Nirmal, S.Prakash, S.Raguvaran, "A Review of Bike Security System Using Fingerprint GSM&GPS", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2015.
- [3] Karan Siyal and G. Gugapriya, "Anti-Theft Vehicle Locking System using CAN", Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/105307, December 2016 ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645.
- [4] Mrs.shubhangi mali, professor J.A.shaikh, "Fingerprint based authentication and security system using GSM and GPS technology", International Journal of Engineering Trends and Technology (IJETT)
- [5] Volume- 45 Number8 -March 2017.
- [6] Kiran Rana Gill, Joel Sachin, " Vehicle ignition using fingerprint sensor", IJIRST – International Journal for Innovative Research in Science & Technology | Volume 2 | Issue 12 | May 2016 ISSN (online): 2349-6010.
- [7] Pankaj Verma , J.S Bhatia, "Design and development of GPSGSM based Tracking system with googlemap based Monitoring", International Journal of Computer Science, Engineering and Applications (IJCSA) Vol.3,No.3, June 2013.