FINGERPRINT VEHICLE STARTER

Yashwant Shankar Jadhao
Department of Instrumentation and control engineering
Vishwakarma Institute of Technology
Pune, Maharashtra, India
yashwant.jadhao24@vit.edu

Prof Jitendra.Gaikwad
Department of Instrumentation and control engineering
Vishwakarma Institute of Technology Pune, Maharashtra, India
Jitendra.Gaikwad@vit.edu

Sanika Pramod Ghute
Department of Instrumentation and control engineering
Vishwakarma Institute of Technology
Pune, Maharashtra, India
sanika.ghute24@vit.edu

Abstract*:- *In order to make sure that only authorised users can start a car, this paper presents a clever and secure ignition system that uses fingerprint authentication. The system has a GSM module that, after five unsuccessful fingerprint attempts, notifies the car owner via SMS to increase security. Furthermore, a mobile application has been created that enables the owner to remotely grant access to reliable people when necessary. The suggested system provides a workable and dependable answer to the current problems with vehicle security by fusing biometric authentication, real-time alerts, and remote access control.

Keywords — ***Fingerprint Authentication, Vehicle Security, GSM Module, IoT, Mobile App Control, ESP32, Biometric System***

1.INTRODUCTION

This paper presents a clever and secure fingerprint authentication ignition system that ensures only authorised users can start a car. To improve security, the system has a GSM module that sends an SMS to the car owner after five failed fingerprint attempts. Additionally, a mobile application has been developed that allows the owner to remotely grant access to trustworthy individuals when needed. By combining remote access control, real-time alerts, and biometric authentication, the proposed system offers a practical and reliable solution to the present issues with vehicle security.

In this regard, biometric authentication technologies have begun to garner interest as a potent substitute for automobile security. Fingerprint recognition stands out among other biometric methods due to its precision, individuality, and user-friendliness. A fingerprint is specific to each person and difficult to duplicate, unlike a physical key or card that can be lost, stolen, or shared. A dependable and customised method of preventing unwanted access is to use fingerprints as a digital key. These factors have led to the development of a number of fingerprint-based ignition systems in recent years. The majority of these current systems are still quite simple, though. They don't offer extra security features like owner notifications, logs of illegal attempts, or remote access control; they only permit fingerprint verification and vehicle ignition. This project suggests an Advanced Fingerprint Vehicle Starter System that does more than merely use fingerprint verification to start the car in order to fill these gaps. It presents two significant improvements that improve the system's intelligence, security, and usability for daily tasks. The addition of a GSM module to the system is the first improvement.

The addition of a GSM module to the system is the first improvement. This makes it possible for the system to instantly send SMS alerts to the registered owner's phone in the event of a suspicious activity. For instance, the system will automatically identify a potential intrusion attempt if someone tries to start the car five times in a row without success. At that point, it immediately notifies the owner via SMS of the unsuccessful attempts and potential illegal access [2], [11], [12]. Even when the owner is not physically present, this feature makes sure they are always informed about what is happening with their car. It turns the system into an active monitoring system instead of just a passive lock.

The second improvement emphasises flexibility and user convenience. The registered vehicle owner can remotely grant or deny access to others through a mobile application created with MIT App Inventor [4]. This eliminates the need for the owner to manually register their fingerprint or give the keys to a trusted friend or family member who needs to use the car while they are away. Alternatively, they can just authorise ignition for that individual via the app. Without sacrificing safety, the app offers a simple and safe method of controlling vehicle access.

Depending on how the hardware is configured, either Bluetooth or the Internet is used to communicate between the mobile app and the car system. The ESP32 microcontroller, which is

especially well-suited due to its integrated Wi-Fi and Bluetooth capabilities, is used in the system to enable this [3], [6]. As the system's brain, the ESP32 controls fingerprint authentication, sends GSM notifications, and interacts with the mobile application.

The system securely stores fingerprint data in EEPROM for storage [9]. This guarantees that the stored fingerprints are still accessible for authentication even in the event that the system is shut down. To make coding and system operation easier, a number of Arduino libraries were incorporated during development. These include LiquidCrystal_I2C [10], [19] for displaying system information on an LCD screen, the Adafruit Fingerprint Sensor Library [15] for controlling fingerprint operations, and ArduinoJson [8] for handling data exchange. Furthermore, the system was able to share data for real-time monitoring and analysis through the use of platforms such as ThingSpeak [7] for IoT integration.

When combined, these enhancements turn the fingerprint ignition system from a simple security device into a complete smart car security system. In addition to making sure that only authorised individuals can start the car, the system actively looks for intruders, alerts the owner right away, and provides them with the ability to control access from a distance. Owners of private vehicles will benefit from increased security against theft and abuse. The system can be expanded to handle numerous vehicles for commercial fleet operators, guaranteeing controlled access and lowering operational risks.

As a result, the Advanced Fingerprint Vehicle Starter System provides a more dependable and useful answer to contemporary vehicle security issues by integrating biometric authentication, GSM-based alerts, Internet of Things communication, and mobile app control. By providing remote control, personalised access, and real-time monitoring, it surpasses both conventional and even simple fingerprint ignition systems. This makes it a useful strategy for both individual users and larger applications in sectors where controlled access and vehicle security are essential.

2. Literature Survey

Prior studies on car security have mostly concentrated on RFID-based authentication, keyless entry systems, and simple biometric techniques. Although these methods offer a certain amount of automation and convenience, they frequently fall short when it comes to more complex security requirements. Typically, features like remote access control or real-time owner alerts are absent.

A fingerprint-based car ignition system, for instance, was introduced by Kumar et al. [1] and verifies the driver before letting the car start. Even though this method makes sure that only authorised users can start the car, it lacks additional safeguards like SMS alerts for unsuccessful attempts or remote authorisation through a mobile app. Similar to this, despite their popularity, RFID-based systems have their own disadvantages. For example, RFID tags are easily copied or faked, leaving cars open to theft.

Since IoT technologies are developing so quickly, researchers have begun looking into more intelligent solutions. Few systems provide a comprehensive package that integrates biometric access, GSM-based alerts, and mobile app control in a single, dependable, and reasonably priced setup. Some recent systems have improved monitoring by adding GPS tracking and mobile alerts.

Our suggested system combines several technologies into a single platform to close these gaps. A SIM800L GSM module [2] notifies the owner via SMS whenever there are repeated attempts at unauthorised access, and a fingerprint sensor is used for biometric authentication. The system's central component is an ESP32 microcontroller [3], which was selected for its integrated Bluetooth and Wi-Fi capabilities, enabling seamless communication with a unique Android application created with MIT App Inventor [4].

Combining mobile app control, GSM alerts, and biometric security creates a hybrid smart system that is both safe and useful for daily use. It solves the drawbacks of previous systems and provides a more dependable option for contemporary car security by offering both real-time monitoring and remote access.

3.METHODOLOGY

By fusing wireless communication, remote control functionality, and biometric authentication into a single integrated platform, the suggested system is intended to offer a clever and dependable vehicle ignition solution. To make sure that only authorised users can start the car, the system uses fingerprint authentication in addition to more conventional techniques like keys or RFID cards. Hardware and software collaborate harmoniously to accomplish this, and the overall architecture is

split into three interrelated components: a mobile application that enables remote access and control, a GSM-based alert and communication module, and a fingerprint-based biometric authentication unit.

The ESP32 microcontroller, which was chosen in particular due to its integrated Wi-Fi and Bluetooth capabilities, small size, and adaptability to connect with external peripherals, coordinates all of these components. The fingerprint unit, which manages the enrolment and authentication procedures, is essential to security. The system saves a user's fingerprint upon registration and verifies the action by displaying a message like "Fingerprint Saved." If the user's fingerprint is already stored, it displays "Fingerprint Already Exists." When a legitimate fingerprint is scanned during normal operation, the system authorises the vehicle to start by activating a relay module; unsuccessful attempts are rejected with a warning message. The system has an intrusion detection mechanism to further improve security.

When an unauthorised individual attempts to start the car five times in a row, the system instantly reacts by displaying "Unauthorised User" on the LCD screen, sounding a buzzer to warn onlookers, and using the SIM800L GSM module to send the registered vehicle owner an SMS notification with a timestamp. This guarantees that the owner is notified of any suspicious activity right away. This system, which combines several layers of protection, is a sensible and clever approach to contemporary car security since it not only prevents unwanted access but also gives the owner real-time information and control.

4.BLOCK DIAGRAM

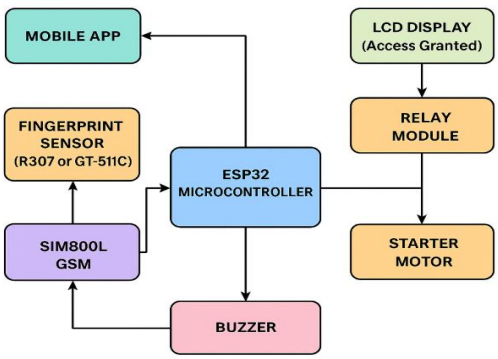


Fig.1.Block digram of a system

5.PROPOSED SYSTEM

The suggested system is intended to be a cutting-edge and safe platform for vehicle ignition that enhances user convenience and safety by integrating mobile app control, SMS alerts, and fingerprint authentication. This system makes it much harder for trespassers to enter the car by limiting who can start it, unlike conventional locking techniques like keys, RFID tags, or key fobs. A biometric fingerprint sensor, which is used to authenticate registered users and enrol new ones, is at the heart of the design. Unregistered people cannot access the vehicle because only stored fingerprints can turn on the ignition.

The system's brain is an ESP32 microcontroller, which processes fingerprint sensor inputs, connects to a mobile application for remote control, communicates with the SIM800L GSM module to send SMS alerts, and controls the relay module to regulate ignition. The system has an intrusion alert feature to bolster security: the GSM module immediately notifies the car owner of a potential breach if an unidentified fingerprint is scanned five times in a row. Because of its direct connection to the ignition system, the relay module only permits the starter motor to start when a legitimate fingerprint is found.

The system also incorporates an LCD display for user interaction, which shows updates and clear instructions like "System Locked," "Access Granted," and "Place Finger to Start." By alerting those in the vicinity when repeated unauthorised attempts are detected, a buzzer serves as an extra layer of local security. A mobile application that allows the vehicle owner to remotely grant or deny access has been developed in order to increase the system's flexibility. For instance, the owner can use the app to grant permission for a trusted friend or family member to use the car without physically giving them the keys or requiring them to register their fingerprints beforehand.

This system offers the car owner more convenience and control, even when they are not there, in addition to robust protection against theft by integrating fingerprint-based authentication, real-time alerts, and mobile-based remote access.

6.CIRCUIT DIGRAM

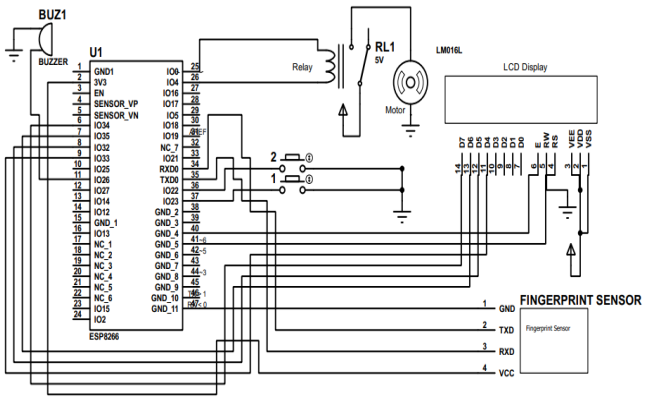
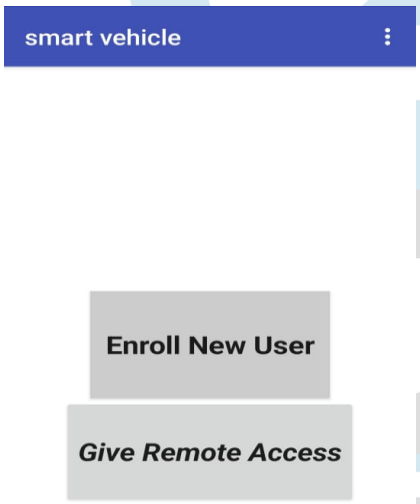


Fig.2. circuit of hardware part

7. Mobile Application Interface



The mobile application designed for the Smart Vehicle System serves as the primary interface between the user and the fingerprint-based vehicle starter hardware. The home screen of the application provides access to two essential functions:

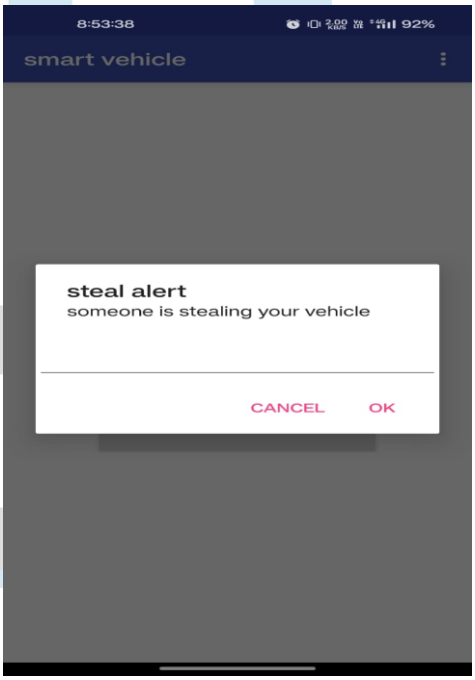
1. Enroll New User

This feature allows the administrator or vehicle owner to enroll new users into the system by registering their fingerprint. The enrolled fingerprints are securely stored via communication with a microcontroller (such as ESP32), which handles the fingerprint data acquisition and authentication logic. This function is intended for adding trusted individuals such as family members or other authorized drivers.

2. Give Remote Access

This feature provides the user with the ability to remotely access and control the vehicle. Through this option, actions like unlocking, starting, or disabling the vehicle can be performed remotely. It is implemented using a cloud-based backend such as ThingSpeak**,** Firebase**,** or a custom IoT platform. This feature is particularly useful in situations where physical access is not possible, allowing secure control of the vehicle from anywhere via the mobile network.

8. NOTIFICATION

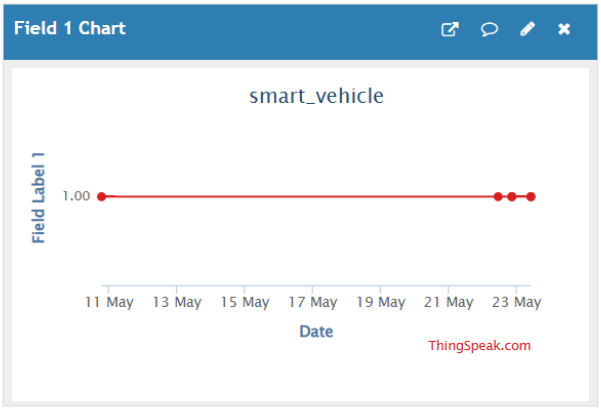


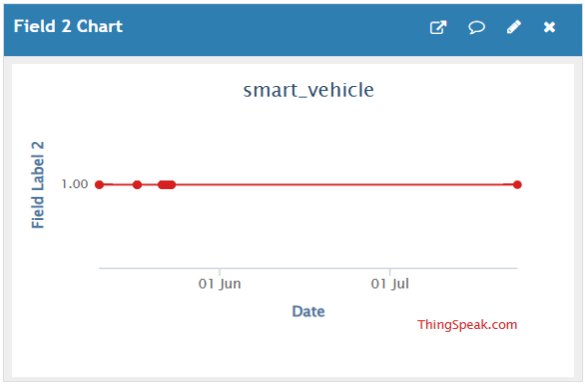
To enhance the security of the vehicle, the Smart Vehicle mobile application includes a real-time Theft Alert Interface that is activated in the event of unauthorized access. As illustrated in Fig. Y, this interface displays a high-priority alert titled "steal alert" with the message:"Someone is stealing your vehicle."

This screen is triggered when the system detects multiple failed fingerprint authentication attempts—typically after five unsuccessful tries**,** which suggests a possible intrusion attempt. This functionality is enabled by the fingerprint sensor module and microcontroller (e.g., ESP32), which continuously monitor authentication requests and detect anomalies.

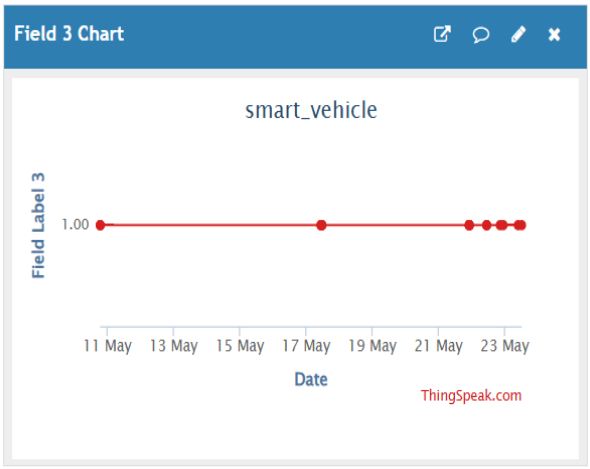
Upon receiving this alert, the user is presented with two action options:

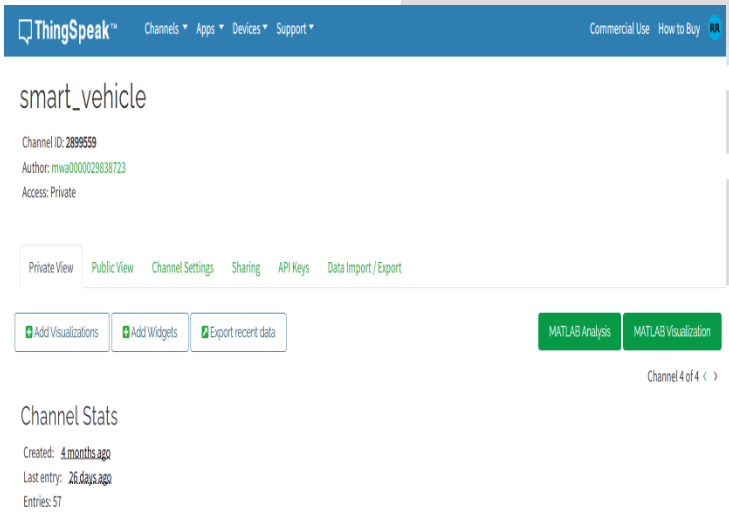
- **OK**: Selecting this option acknowledges the alert and may trigger pre-programmed countermeasures such as locking the ignition system, activating a buzzer, or sending an emergency alert to a registered contact or server.
- **CANCEL**: This option simply dismisses the alert without initiating any further action.





9.THINK SPEAK DATA





- **THINGSPEAK DATA ANALYSIS FOR FINGERPRINT VEHICLE STARTER:**

The proposed Advanced Fingerprint Vehicle Starter with GSM Alert and Mobile App Control was integrated with the ThingSpeak IoT cloud platform to record and monitor real-time data from the system. The ESP32 microcontroller uploads system states to ThingSpeak at regular intervals, allowing remote visualization and analysis of the vehicle's ignition and authentication events.

Three primary data fields were defined in the channel named "smart_vehicle", each representing a key operational parameter of the system:

1.Field (Authentication Status):

This field stores the output of the fingerprint authentication process.

A value of `1.0` indicates that a valid, registered fingerprint was detected and the vehicle ignition was authorized.

A value of `0.0` would represent an invalid or unauthorized attempt.

In the collected data, most values remain at `1.0`, showing that all recorded attempts during testing were successful authentications.

2.**Field (Relay/Ignition Status):**

This field corresponds to the state of the relay module that controls the vehicle's ignition.

A value of `1.0` means the relay is active, and the ignition circuit is ON.

A value of `0.0` means the relay is inactive, keeping the ignition OFF.

The flat line observed in the chart indicates that once authentication was granted, the ignition stayed ON during testing.

3.**Field (System/GSM Alert Status):**

This field is used to log the overall system state or GSM alert trigger.

A value of `1.0` shows that the system was functioning normally without unauthorized access attempts crossing the alert threshold.

If repeated failures had occurred, this value would drop to `0.0` or trigger changes, indicating that the GSM module had sent an alert message.

9. CONCLUSION

The developed fingerprint vehicle starter system enables only registered fingerprints to start the ignition, making it a more intelligent and dependable method of protecting automobiles. This makes it far safer than conventional key or RFID-based systems since it prevents unauthorised people from accessing or abusing the vehicle. To make sure the owner is always aware of potential threats, the system incorporates real-time SMS alerts that notify them immediately if multiple unauthorised attempts are made. Additionally, a mobile application adds flexibility without sacrificing security by enabling owners to conveniently grant or deny access to trusted individuals remotely. This system, which is safe, affordable, and simple to use, can be used for both private automobiles and commercial fleets, providing a useful and contemporary answer to today's vehicle problems.
vehicle security challenges

.10.Future Scope

By limiting ignition to registered fingerprints, the developed fingerprint vehicle starter system offers a more intelligent and dependable method of vehicle protection. This makes it far safer than conventional key or RFID-based systems since it prevents unauthorised people from accessing or abusing the vehicle. To make sure the owner is always aware of potential threats, the system incorporates real-time SMS alerts that notify them immediately if multiple unauthorised attempts are made. Additionally, a mobile application adds flexibility without sacrificing security by enabling owners to conveniently grant or deny access to trusted individuals remotely. This system, which is appropriate for both private automobiles and commercial fleets, is made to be safe, affordable, and simple to use. It provides a practical and modern solution to today's vehicle security challenges.

11.REFERENCES

1. A. Kumar et al., "Biometric-based vehicle ignition system," IEEE Trans. Veh. Tech., vol. 68, no. 2, pp. 1001–1007, 2020.

2. SIM800L GSM Module Datasheet, Available: https://cdn.sparkfun.com/datasheets/GSM/GPRS_SIM800.pdf

3. ESP32 Technical Reference Manual, Espressif Systems, https://docs.espressif.com/projects/esp-idf/en/latest/esp32/

4. MIT App Inventor, https://appinventor.mit.edu

5.https://learn.adafruit.com/adafruit-optical-fingerprint-sensor

6.https://arduino-esp8266.readthedocs.io/en/latest/

7.https://www.mathworks.com/help/thingspeak/

8.https://arduinojson.org/

9.https://www.arduino.cc/en/Reference/EEPROM

10.https://github.com/johnrickman/LiquidCrystal_I2C

11.https://www.electronicshub.org/fingerprint-based-vehicle-starter-project/

12.https://circuitdigest.com/microcontroller-projects/fingerprint-based-vehicle-ignition-

system-using-arduino

13.https://randomnerdtutorials.com/esp8266-fingerprint-sensor/

14.https://maker.pro/arduino/projects/fingerprint-based-security-system-using-nodemcu

15.https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library

16.https://github.com/esp8266/Arduino/tree/master/libraries/ESP8266HTTPClient

17.https://github.com/esp8266/Arduino

18.https://github.com/bblanchon/ArduinoJson

19.https://github.com/fdebrabander/Arduino-LiquidCrystal-I2C-library

20.https://www.youtube.com/watch?v=_NGXB4i-cKY

21.https://www.youtube.com/watch?v=8AMwFUSMN_o

22.https://www.youtube.com/watch?v=J3n_dUvEyPY

23.https://www.youtube.com/watch?v=1Rcglg8RT30

24.https://www.youtube.com/watch?v=B3K-Hy69iCQ