IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Vehicle License Authentication Using Fingerprint

[1]N. Babi, [2]H. Tirupathi Rao, [3]V. Jaya Sri, [4]K. Laxmi Sourya, [5]Mr. P. Vyasa Omkar

[1,2,3,4]B Tech Student, [5]Assistant Professor

[1,2,3,4,5]Department of Electronics and Communication Engineering,

[1]Godavari Institute of Engineering & Technology(Autonomous), Rajahmundry, AP, India.

***Abstract*** *:* The aim of this project is to develop a fingerprint identification-based vehicle license authentication system with the goal of improving security. The system is developed on the basis of an Arduino Mega as the microcontroller, and an fingerprint sensor is used as the biometric authentication module. Switches are used in controlling fingerprint operation so that the vehicle can be opened only by the licensed persons. A NodeMCU module is used for control of vehicle entry and notification for both scenarios: successful authentication of the licensed persons and unauthorized persons attempting to utilize the vehicle. An LCD is used for real-time feedback purposes in the form of authentication and vehicle status and vehicle information. GPS is utilized for vehicle tracking purposes, whereas direction of motion of the vehicle is controlled with the help of a motor driver. A buzzer is utilized for providing feedback in the form of successful authentication as well as unsuccessful authentication for making a secure and user-oriented system for a vehicle access.

**Index Terms** : Arduino mega, Node MCU, GPS, fingerprint sensor

## 1. INTRODUCTION

Personal and commercial vehicle protection has become highly significant with technological advancement. Age-old physical keys, RFID, and PIN remain the same technology that has been in use for decades but could be hacked into, stolen, and copied. The vulnerabilities of these are utilized by criminals with relay attacks, RFID scanning, and copying keeping vehicles at high risk of being stolen. Accordingly, stronger means of authentication to safeguard cars against unapproved entrance with increased simplicity have been proposed.

Fingerprint-based vehicle authentication is increasingly becoming popular as a highly secure method. Compared to conventional methods that use outside devices, fingerprint recognition employs individual-specific biometric data. Fingers cannot be duplicated, which makes this means of securing cars tamper-proof. By applying fingerprint verification with car control systems, only those with the access right can utilize and drive the car. This erases the dangers of stolen or misplaced keys with a guaranteed smooth user experience. Fingerprint authentication application consists of various components brought together for secure access. The door panel or dashboard contains a built-in fingerprint sensor where the users place their fingerprint to open the entrance.

The machine is utilized to scan and match the fingerprint data against a registered database. When a match is found on verification, the entry is activated, and one is able to drive the vehicle. Unauthorized entry, if it is found, will prevent entry and is able to initiate security features like alarms or remote alert to inform the owner. User friendliness and reliability of fingerprint authentication is one of the greatest strengths. Fingers can never go missing as compared to PIN codes or keys that get either lost or misplaced, and even no unauthorized individual can easily reproduce them. Current fingerprint sensors have been developed with the ability to operate effectively against all kinds of conditions prevailing out there, ranging from maximum precision at extreme temperatures of weather conditions. These therefore are perfectly designed for vehicle protection where there should be maximum reliance.

Apart from security, fingerprint identification is also handy. Compared to key-based systems, the users are not required to store keys or memorize passwords. Fingerprint scanning is speedy and handy. Several users can also be registered, which enables family members or authorized personnel to drive the car without extra keys. The fingerprint login can further be coupled with live tracking to increase security. Upon illegal access, instant notification may be sent to the mobile of the owner. GPS tracking provides vehicle location monitoring in case of theft and has complete authority on security and entry.With advancing automobile technology, fingerprint authentication will be the most noticeable automobile security feature in the future. With the integration of biometric identification with IoT and AI, automobiles can also customize settings such as climate control and seat positions for various users. Even though there are issues of cost and accuracy, advancing developments are reducing the cost and improving accuracy of fingerprint verification, determining the future of automobile security.

## 2. LITERATURE REVIEW

Raj, K., & Gupta, P. [2023] and Patel, M., & Sharma, R. [2022] also suggested a fingerprint system for secure vehicle entry. Only authorized users can access a vehicle through the system. It does not support the use of regular keys, thus limiting theft and chances of unauthorized entry. The process consists of mainly three major steps: fingerprint verification, access control, and user authentication. In the initial step, a fingerprint sensor module reads and verifies the user's fingerprint. The system verifies whether the vehicle can open and start up with only the registered fingerprints, offering a singular and secure vehicle access. Through the process explained by Rao, K., & Deshmukh, P. [2019], significant security is improved as it prevents unauthorized individuals from taking over the vehicle. The second stage, access control, is where the fingerprint module interfaces with the car's ignition system. After verification of the fingerprint, the system makes the car ready to be started. This is similar to the electro-mechanical car immobilizer Sharma, N., & Joshi, R. [2020] proposed, where the engine will not be started unless a valid fingerprint is given. The third step, identifying who the users are, allows the system to maintain records of usage to ensure that only persons authorized have accessed the vehicle. This concept builds on the study of Mehta, P., & Bose, T. [2021], which researched intelligent vehicle security systems that incorporate fingerprint authentication and remote monitoring. The research supports that fingerprint-based authentication systems work in an efficient way and are more trustworthy compared to RFID-based systems, states Singh, A., & Verma, N. [2022]. There is a limitation, however, as it lacks real-time tracking using GPS, states Chandra, V., & Mishra, R. [2021]. It would be more improved if it had tracking technology built in for complete vehicle safety.

## 3. PROBLEM DEFINITION

Current car security systems such as keys and RFID cards are easily stolen or hacked, leaving cars vulnerable. The project will implement a vehicle license system based on fingerprint identification with Arduino Mega as the controller. It will include a fingerprint sensor, NodeMCU, GPS, LCD, motor driver, and buzzer. The

system only allows authorized persons to drive and use the vehicle and offers real-time tracking and security notifications. This enhances car safety, prevents unauthorized use, and enhances overall security efficiently.

## 4. EXISTING SYSTEM

Conventional car security systems like keys, RFID, and PINs are easy to steal, copy, or hack. They do not have real-time tracking and GPS, and hence a theft cannot be detected. As security threats are changing, conventional methods are not enough, and hence advanced solutions like fingerprint identification and instant alerts are needed for better car security.

### 4.1 Disadvantages of Existing System

1. Physical keys and RFID systems can be easily duplicated or stolen.

2. RFID-based systems are vulnerable to hacking and unauthorized cloning.

3. Conventional systems do not provide instant alerts for unauthorized access attempts.

4. Many traditional security systems lack GPS, making it difficult to locate stolen vehicles.

5. Most traditional systems lack additional security layers like biometrics or OTP verification.

6. Older systems do not allow remote access or vehicle control via mobile applications.

## 5. METHODOLOGY

### 5.1 PROPOSED SYSYTEM

The proposed model applies a fingerprint identification system to validate vehicle licenses for increased security. An Arduino Mega operates the system and communicates with an R307 fingerprint sensor to verify users. A NodeMCU module provides notifications when an individual attempts to gain access, enabling tracking of where the vehicle is. A motor driver assists in controlling movement, and an LCD indicates whether access is granted or not. A buzzer provides sounds for access attempts. The system applies fingerprint security, real-time tracking, and monitoring for efficient vehicle access control.

### 5.2 Advantages of Proposed System

1. Only authorized users can access the vehicle.

2. Alerts notify users of access attempts instantly.

3. Enables real-time location tracking for theft recovery.

4. LCD displays authentication status and messages clearly.

5. Vehicle starts only after successful authentication.

6. Buzzer notifies users of authentication success or failure.

7. Wi-Fi sends alerts for security monitoring remotely.

8. Fingerprints ensure unique and secure authentication.

9 Biometric system is durable and requires less maintenance.

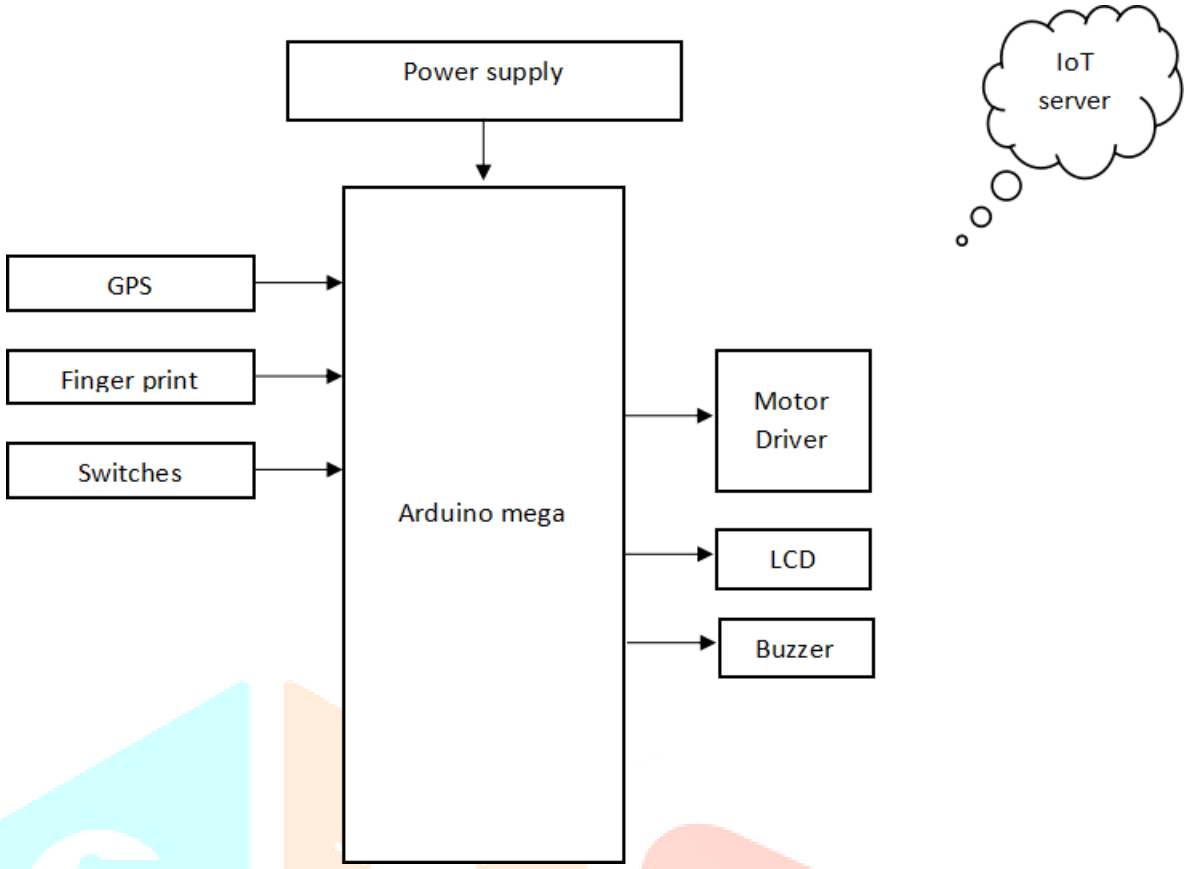
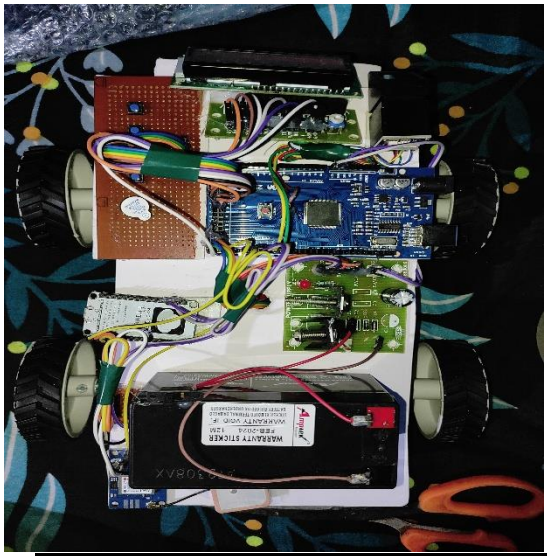



**Fig.1 Block Diagram**

## 6. RESULTS AND DISCUSSION

### 6.1 Testing and Evaluation

This sub-section discusses performance of Vehicle License Authentication System using Fingerprint Recognition. More significant aspects include authentication in identification, speed of real-time alarm, wireless stability, and security reinforcement. Comparison indicates the biometric authentication advantage over conventional key-based systems. Experimental findings support enhanced automobile security using fingerprint authentication and GPS positioning location tracking. The system provides quick response and wireless communication and thus is applicable to contemporary security. Cloud storage can increase data availability, and encryption can increase security. The only minor disadvantage is wireless reliance for real-time notifications, but reliability is not lost. Upgrades in the future include cloud-based history storage and sensor calibration for better accuracy. Although Bluetooth has limited range, the system is still reliable, secure, and efficient for vehicle access control.



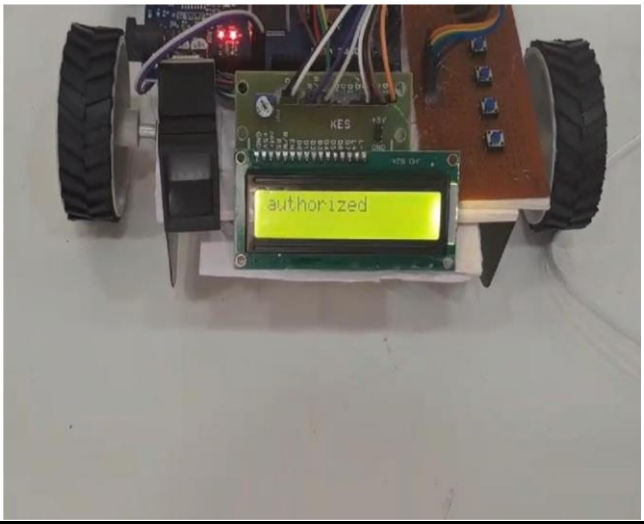


Fig.2 Developed circuit

Fig.3 For Authorized Person


Fig.4 For Unauthorized Person

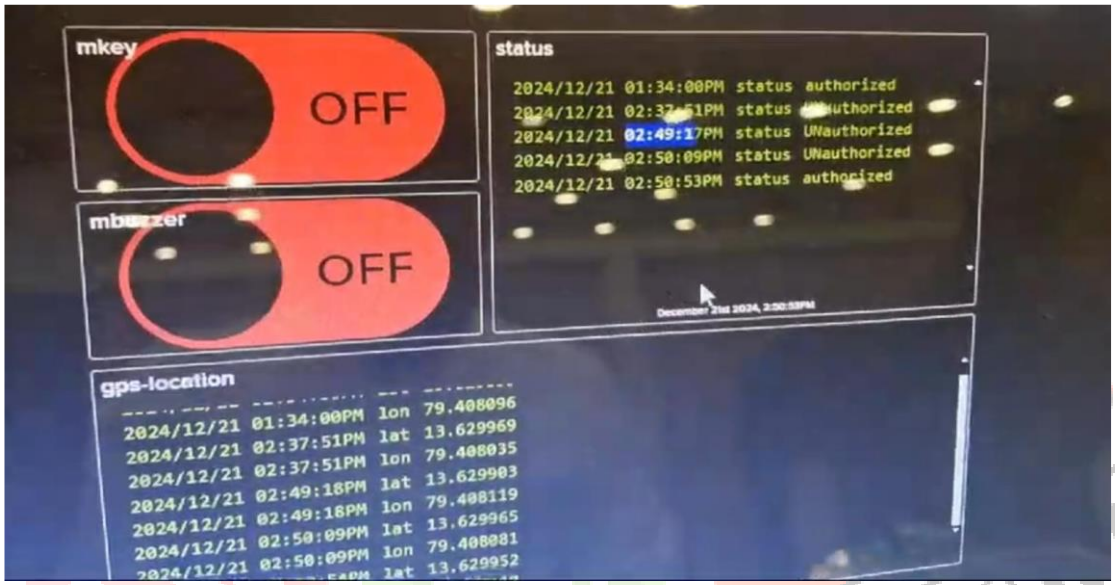



Fig.5 Final Output in Adafruit IO Server

## 7. CONCLUSION & FUTURESCOPE

The "Vehicle License Authentication Using Fingerprint" system secures vehicles with fingerprint verification, location tracking in real time, and GPS location. It ensures that only the correct individual is driving the vehicle and sends notifications upon location tracking to respond instantly in the event of theft or misuse. The system addresses weaknesses in existing security systems by utilizing the application of IoT technology. Future upgrades include face recognition for enhanced security, mobile authentication through smartphone apps, and AI for detecting suspicious activity. Geofencing controls where vehicles go, and blockchain logs secure authentications. Cloud monitoring gives immediate access to security information. These upgrades make the system an intelligent security solution via AI and IoT, which makes vehicles safer, simpler to operate, and more resistant to theft.

## REFERENCES

[1] K. RAJ AND P. GUPTA (2023), "FINGERPRINT-BASED VEHICLE ACCESS SYSTEM FOR ENHANCED SECURITY, "IN PROC. IEEE INT. CONF. ON SECURE VEHICLE TECHNOLOGIES (SVT), PP. 1-6.

[2] A. SINGH AND N. VERMA (2022), "STANDALONE RFID-BASED VEHICLE SECURITY SYSTEM," IN PROC. IEEE INT. CONF. ON SMART ACCESS CONTROL (SAC), PP. 1-5.

[3] V. Chandra and R. Mishra (2021), "GPS-Based Vehicle Tracking System for Real-Time Security," in Proc. IEEE Int. Conf. on Vehicle Monitoring (VM), pp. 1-7.

[4] H. Desai and S. Kulkarni (2020), "Vehicle Theft Prevention System Using Mechanical Locks and Alarms," in Proc. IEEE Int. Conf. on Automotive Security (AS), pp. 1-4.

[5] M. Patel and R. Sharma (2022), "Hybrid Biometric and RFID-Based Vehicle Access Control System," in Proc. IEEE Int. Conf. on Biometric Access Technologies (BAT), pp. 1-6.

[6] S. Kumar and D. Agarwal (2020), "Voice-Controlled Vehicle Security System Using Speech Recognition," in Proc. IEEE Int. Conf. on Intelligent Vehicle Authentication (IVA), pp. 1-5.

[7] P. Mehta and T. Bose (2021), "IoT-Based Smart Vehicle Security Using Mobile App and Biometric Authentication," in Proc. IEEE Int. Conf. on IoT and Smart Mobility (IoTSM), pp. 1-6.

[8] K. Rao and P. Deshmukh (2019), "Electro-Mechanical Vehicle Immobilizer Controlled by Biometric Authentication," in Proc. IEEE Int. Conf. on Vehicle Security Systems (VSS), pp. 1-6.

[9] N. Sharma and R. Joshi (2020), "NFC-Based Vehicle Access Control System Using Mobile Authentication," in Proc. IEEE Int. Conf. on Smart Transportation (ST), pp. 1-4.