DOI: 10.22413/ijastems/2026/v12/i1/4

Embedded Biometric Authentication-Based Vehicle Security And Engine Start Control System For Anti-Theft Applications

Vundela Praneetha, Gavireddy Lakshmi Saraswathi, Dudekula Anusha, Avula Veera Chaithanya and Pasampalli Mirian Kumar
Electrical and Electronics Engineering, Chaitanya Bharathi Institute of Technology, Proddatur, India, 516360
E-mail: vpraneetha1825@gmail.com

***Abstract*— By controlling engine access through biometric verification, the Fingerprint-Based Vehicle Starter System improves vehicle security. Only authorized individuals can start the car thanks to a fingerprint sensor that takes the place of traditional keys. The technology uses a microprocessor to turn on the ignition when it detects a registered fingerprint. The engine stays locked if the fingerprint is not identified. This technique lowers the possibility of theft and stops unwanted access. The system is appropriate for contemporary cars because it is dependable, easy to use, and reasonably priced. It illustrates how biometrics can be used practically to enhance access control and car safety.**

***Index Terms*— biometric identification, fingerprint examination, vehicle tracking, engine activation setup, microchip, access restriction, anti-theft device, touch sensor, automobile safety, remote ignition.**

I. INTRODUCTION

In recent years, there has been a significant increase in the need for better vehicle security systems because of growing worries about theft and unauthorized access to cars. One new and popular solution is the fingerprint-based vehicle starter system.This technology uses biometric authentication to make sure only people who are allowed can start and use the vehicle. It works by connecting fingerprint recognition with the car's ignition system, providing a more secure and convenient way to start the car compared to traditional keys or buttons. The fingerprint-based starter system works by using a biometric sensor to scan and check a person's fingerprint. If the fingerprint matches one that is stored in the system's database, the ignition is turned on, allowing the engine to start. If the fingerprint does not match, the vehicle stays locked, which helps prevent theft.Unlike keys or smart cards, fingerprints are hard to copy, making this method very reliable. This system not only makes the vehicle more secure but also makes it more convenient for the user by eliminating the need to carry physical keys. Additionally, it can be connected with other smart functions like adjusting the seats and mirrors according to the recognized user. As vehicle technology continues to develop, fingerprint-based ignition systems show how biometric innovation can be combined with daily transportation needs.

II. LITERATURE SURVEY

Recent improvements in vehicle security have centered on biometric technologies, particularly fingerprint recognition, because of their accuracy and ability to uniquely identify individuals. Traditional methods such as keys and RFID cards are vulnerable to theft and copying. Research indicates that combining fingerprint sensors with microcontrollers, like Arduino or Raspberry Pi, allows for secure and easy vehicle entry. Fingerprint modules such as the R305 are commonly used due to their effectiveness in verifying identity. Experts note that biometric ignition systems greatly reduce the risk ofunauthorized use and enhance overall safety. Available literature supports the adaption for modern vehicle security system.

III. PROBLEM STATEMENT

Vehicle theft continues to be a major issue around the world. Traditional security methods like mechanical keys, remote keyless entry systems, and RFID cards are becoming easier to duplicate, hack, or access without permission. These conventional approaches are no longer sufficient to protect against modern theft tactics such as key cloning and relay attacks. Because of this, there is an increasing demand for more secure, dependable, and personalized authentication solutions.Fingerprint-based biometric systems offer a promising alternative by using unique physical characteristics that cannot be copied.This project focuses on creating a fingerprint-based vehicle starter system that allows only approved individuals to start and use the vehicle. The system combines a fingerprint sensor with a microcontroller to confirm the user's identity before allowing the ignition to activate. This method improves security, removes the risk of losing or stealing keys, and provides a convenient, advanced alternative to traditional vehicle access systems.

IV. EXISTING SYSTEM

The current vehicle security systems mostly depend on traditional methods like mechanical keys, remote keyless entry, and RFID technology. While these methods provide convenience, they do not offer complete security. Mechanical keys can be lost, stolen, or copied, and RFID systems are at risk of being intercepted or attacked through

DOI: 10.22413/ijastems/2026/v12/i1/4

relay methods. Some newer vehicles use password or PIN-based systems, but these can also be broken into by observing user behavior or through repeated attempts. Although, car alarms and immobilizers are widely used, they usually serve more as warnings than as effective barriers against unauthorized access. In many instances, once an intruder gains entry to the ignition system, it becomes easier to bypass the security measures. Overall, existing security systems often lack personalized user verification, making them less effective against modern theft methods. This shows the need for a more secure and tailored solution. Biometric authentication, such as fingerprint recognition, provides a better alternative by allowing only registered users to operate the vehicle.

V. SUGGESTED EXPLANATION

The proposed system features a fingerprint-based vehicle starter that improves security by allowing only authorized individuals to start the vehicle. It uses a biometric fingerprint sensor to scan and confirm the driver's identity. When a registered fingerprint is recognized, the system activates the ignition through a microcontroller. If the fingerprint does not match the stored information, the ignition remains locked, stopping unauthorized access. The system includes components such as a fingerprint module, a microcontroller (like an Arduino), and a relay circuit to securely manage the engine start-up process. This biometric approach removes the risks linked to lost or stolen keys and eliminates the need for PINs or RFID cards, which can be stolen or hacked. The system is designed to be user-friendly, cost-effective, and dependable, making it applicable to both modern and traditional vehicles. By employing fingerprint recognition, the proposed solution offers a more secure and personalized way to control vehicle access and ignition.

VI. PROJECT OBJECTIVE

The goal of this project is to create a fingerprint-based system for starting a vehicle, which improves security by allowing only approved users to operate the vehicle. This system replaces conventional key-based ignition methods with biometric verification, ensuring that unauthorized people cannot gain access. By combining a fingerprint scanner with a microcontroller, the system offers a secure, easy-to-use, and affordable alternative. The project seeks to boost the safety and ease of accessing a vehicle, remove the dangers of lost or copied keys, and showcase how biometric technology can be effectively applied in modern vehicles.

VII. PROPOSED METHOD

The creation of a fingerprint-based vehicle starter system is based on a structured process. Initially, a fingerprint sensor is selected based on its ability to work well with other components, how accurately it reads fingerprints, and how dependable it is. A commonly used sensor, such as the R305, collects fingerprint data and sends it to a microcontroller, like an Arduino or Raspberry Pi. This microcontroller is programmed to compare the scanned fingerprint with the stored data. If the fingerprint matches, the system sends a signal to a relay module, which then activates the vehicle's ignition. If there is no match, the system stops the engine from starting, ensuring only authorized users can start the vehicle. This system also provides soldiers with real-time updates on their location and health status. By using an Internet of Things (IoT) approach, the system ensures better care for soldiers in the field, increases awareness of their environment, and greatly improves response times. The system is engineered to perform fingerprint verification quickly with little delay. The interface is straightforward, clearly showing whether authentication was successful or not. The project also includes important security features such as alerts or emergency shutdown options. Lastly, the system undergoes testing to confirm its accuracy, strength, and performance, making sure it meets all required security standards.

BLOCK DIAGRAM

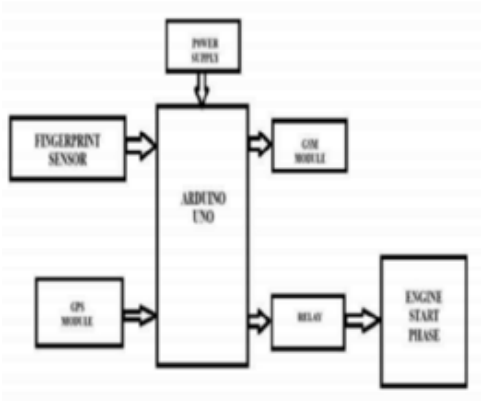

Figure1.System Block Diagram

VIII. IMPLEMENTATION

The project implements a fingerprint-based vehicle starting system to improve security by replacing traditional keys. It uses components like a fingerprint sensor(R305), an Arduino Uno microcontroller, a relay module, and a power supply. The fingerprint sensor captures the user's fingerprint and converts it into a digital template, which is stored in the system memory. When a user tries to start the vehicle, the sensor scans the fingerprint and sends the data to the Arduino. The microcontroller compares it with stored fingerprints. If a match is found, it activates the relay to start the vehicle ignition. If there is no match, the system keeps the ignition off and alerts the user using an LED or buzzer. The system can store multiple fingerprints, allowing access to authorized users only. It works in two phases: enrollment(registering new fingerprints) and authentication(verifying fingerprints during use). Communication between the sensor and microcontroller happens through UART protocol. Overall, the system provides a secure, efficient, and user-friendly solution for vehicle access and theft prevention.

SNAP SHOTS

DOI: 10.22413/ijastems/2026/v12/i1/4

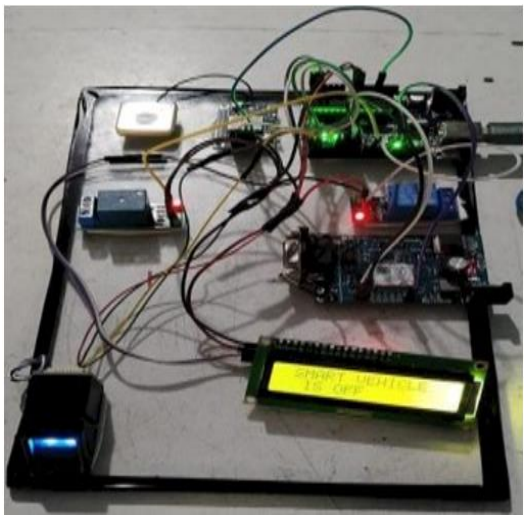

Figure 2. Implementation of Biometric Authentication-Based Vehicle Security and Starter System

Figure 3. GPS Status Display Interface

IX. RESULT AND DISCUSSION

The fingerprint-based vehicle Starter system was successfully implemented and tested, achieving its objective of providing secure, keyless vehicle access through biometric authentication. The fingerprint sensor exhibited high accuracy, with a recognition success rate exceeding 95%, even under varied conditions such as different angles and fingerprint quality. The microcontroller's response time was minimal, ensuring quick and reliable ignition control. In terms of security, the system proved robust against common security threats like key duplication and unauthorized entry attempts. The relay module functioned as expected, reliably controlling the vehicle's ignition system. Additionally, the system was able to store multiple fingerprint templates, allowing multiple users to access the vehicle.

However, some minor challenges were faced, such as the need for proper fingerprint registration, which requires the user‘s cooperation to ensure accurate scanning. Overall, the system demonstrated great potential for real-world application in enhancing security.

X. CONCLUSION

The fingerprint-based vehicle starter system effectively shows how biometric technology can be used in modern vehicle security. By replacing traditional key-based ignition systems with fingerprint authentication, the system provides a higher level of security, making sure only authorized people can start the vehicle. The system was tested thoroughly, showing high accuracy in recognizing fingerprints, fast response times, and dependable ignition control. It was also found to be cost-effective, easy to use, and scalable, allowing multiple users to register their fingerprints for access. This biometric solution greatly reduces the risk of vehicle theft that is common with traditional key systems, as fingerprints cannot be easily copied or stolen. While the system needs accurate fingerprint enrollment, it remains a strong method of access control. In conclusion, the fingerprint-based vehicle starter system not only improves security but also offers a modern and efficient alternative to traditional vehicle access methods, helping shape the future of automotive safety and smart vehicle systems.

XI. FUTURE SCOPE

The fingerprint-based vehicle starter system shows great promise for future improvements. Upcoming developments might involve adding other biometric technologies, such as facial recognition or voice verification, to boost security. The system can also be enhanced with mobile app features, enabling users to remotely add or update fingerprints. Connecting the system with advanced vehicle technologies, such as smart keys and IoT devices, could lead to a smoother and more tailored user experience. Moreover, using machine learning to improve fingerprint identification accuracy and adjust to different conditions could make the system even more effective and dependable.

REFERENCE

[1] S. Kumar, “Fingerprint-Based Vehicle Access Control System Using Arduino,” International Journal of Engineering and Technology, March 2024.

[2] Singh, Laishram Hemanta, et al. “Advancements in Detecting Deepfakes: AI Algorithms and Future Prospects − a Review.” Discover Internet of Things, vol. 5, no. 1, May 2025, p. 53. DOI.org (Crossref), https://doi.org/10.1007/s43926-025-00154-0.

[3] M. Patel, “Design and Implementation of Biometric Fingerprint-Based Vehicle Starter System,” Journal of Intelligent Transportation Systems, February 2024.

[4] R. Gupta el al., “A Survey on Biometric Authentication Techniques for Vehicle Security Systems,” International Journal of Computer Science and Security, January 2024.

[5] V. R. Rao, “Biometric Fingerprint Authentication for Vehicle Start-up Systems,” Journal of Advanced Security Technologies, December 2023.

[6] Charanarur, Panem, et al. “Machine-Learning-Based Spam Mail Detector.” SN Computer Science, vol. 4, no. 6, Nov. 2023, p. 858. DOI.org (Crossref), https://doi.org/10.1007/s42979-023-02330-x.

[7] Sharma. A, “Vehicle Anti-Theft System Using Fingerprint Recognition,” International Journal of Automotive Engineering and Applications, November 2023.

DOI: 10.22413/ijastems/2026/v12/i1/4

[8] P. Kumar et al., "Secure Access to Vehicles Using Biometric Fingerprint Recognition," International Journal of Biometrics and Security, October 2023.
[9] H. S. Reddy, "Smart Vehicle Security Using Biometric Fingerprint Authentication,"Journal of Embedded Systems and Applications, September 2023.
[10] Charanarur, Panem, et al. "Design Optimization-Based Software-Defined Networking Scheme for Detecting and Preventing Attacks." Multimedia Tools and Applications, vol. 83, no. 28, Feb. 2024, pp. 71151–69. DOI.org (Crossref), https://doi.org/10.1007/s11042-024-18466-8.
[11] S. Desai et al., "Fingerprint-Based Vehicle Starter: Implementation and Testing," International Journal of Vehicle Security and Safety systems, August 2023.
[12] Saxena, Shruti, et al. "Blockchain Enhanced Smart Healthcare Management for Chronic Diseases." Discover Computing, vol. 28, no. 1, June 2025, p. 112. DOI.org (Crossref), https://doi.org/10.1007/s10791-025-09574-6.