IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

Biometric Fingerprint-based Vehicle Ignition and Security System

Mr. Gaurav Bhoi, Ms. Mitali Kadu, Mr. Shrikant Hingole, Dr. Makrand M. Jadhav
Student, Department of Electronics and Telecommunication
Head Of Department, Department of Electronics and Telecommunication
NBN Sinhgad Technical Institute Campus, Pune, India

Abstract: *In the modern era of advanced technology, vehicle security has emerged as a critical concern due to increasing instances of vehicle theft and unauthorized access. Traditional security mechanisms such as mechanical keys and key fobs are often vulnerable to theft, loss, or duplication, thereby necessitating the development of more secure alternatives. This paper presents the design and implementation of a "Biometric Fingerprint-Based Vehicle Ignition and Security System," leveraging the NodeMCU ESP8266 microcontroller in conjunction with supporting hardware components, including a fingerprint sensor, keypad, LCD, DC motor, and buzzer.*

The system employs biometric fingerprint recognition as the primary authentication mode, offering a high level of security due to the uniqueness of individual fingerprints. Upon scanning, the fingerprint sensor transmits data to the NodeMCU, which verifies it against a pre-stored database of authorized users. Successful authentication triggers the vehicle ignition mechanism, represented by a DC motor, thereby granting access. In contrast, unrecognized attempts keep the system locked, denying unauthorized entry.

A keypad is incorporated as a secondary authentication method to enhance reliability. In cases where the fingerprint sensor fails to operate effectively due to environmental or technical factors, users may input a pre-set passcode. Real-time system status and prompts are displayed on an integrated LCD screen, ensuring a user-friendly interface and clear communication.

Additionally, a buzzer is used to alert users of security threats. Repeated failed authentication attempts activate the buzzer, serving as an audible alarm to indicate potential tampering or unauthorized access attempts. This multi-layered approach not only improves security but also increases the resilience and usability of the system.

The project demonstrates the practical advantages of integrating biometric technology into vehicle security systems. By replacing vulnerable traditional systems with biometric authentication, the proposed solution significantly elevates security standards. Future enhancements may include the incorporation of advanced biometric modalities such as facial or voice recognition, expanding the applicability of the system across various vehicle types and high-security domains.

Keywords: Fingerprint sensor, Vehicle security, Biometric ignition system, NodeMCU ESP8266

I. INTRODUCTION

Biometric Fingerprint-Based Vehicle Ignition and Security Systems represent a modern approach to enhancing automobile safety by integrating advanced authentication mechanisms with microcontroller technology. This project focuses on replacing conventional key-based ignition methods with a more secure and efficient fingerprint-based system. Utilizing the NodeMCU ESP8266 as the core processing unit, the system incorporates key hardware components, including a fingerprint sensor for primary biometric verification, a keypad for secondary authentication via passcode, an LCD for user feedback, a DC motor to simulate engine ignition, and a buzzer for alert notifications. The software algorithm manages fingerprint enrolment, matching, passcode verification, and secure control of the motor and alert subsystems. The uniqueness of fingerprint biometrics ensures reliable and non-replicable access, addressing the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

critical vulnerability of traditional vehicle ignition methods. Multi-layered authentication protocols enhance system robustness, while sound alarms help prevent unauthorized access.

II. METHODOLOGY

The fingerprint-based ignition system is a modern and secure solution designed to ensure that only authorized individuals can start a vehicle. This project aims to eliminate the risk of unauthorized access to vehicles, providing an advanced and user-friendly alternative to traditional key-based ignition systems. The system uses a Keypad, a fingerprint sensor, a NodeMCU ESP8266 microcontroller, and an LCD to perform a series of operations that authenticate users and control the vehicle's ignition. The NodeMCU ESP8266 microcontroller plays a central role in processing the data, making decisions, and controlling the flow of power to the ignition system.

The system starts with the fingerprint sensor, such as the R305 model, which captures the fingerprint of the user. This sensor works by scanning the fingerprint when the user places their finger on it. It then converts the scanned data into a digital format that can be sent to the NodeMCU ESP8266 via serial communication. The NodeMCU ESP8266, a low-cost microcontroller with Wi-Fi capabilities, processes the data received from the sensor and compares it with a pre-stored database of authorized fingerprints. This comparison is done using an algorithm that checks whether the scanned fingerprint matches one of the stored entries in the memory. The fingerprint data can be stored on the NodeMCU or an external memory module.

If the fingerprint matches one of the authorized users, the NodeMCU sends a signal to activate the vehicle's ignition system, allowing the engine to start. This ensures that only authorized users can start the vehicle, preventing unauthorized access. On the other hand, if the fingerprint does not match any authorized users, the system prevents the ignition circuit from being activated, and the vehicle will not start.

To make the system easier to use, an LCD screen is added to show important information to the user. The screen displays messages like "SYSTEM BOOTING," "DOOR UNLOCK," and "IGNITION ON." This helps the user know what's happening with the system and what to do next. The screen is connected to the NodeMCU using I2C communication, which makes the wiring simple and reduces the number of pins needed for the connection. This allows the system to work smoothly and efficiently.

Along with the LCD, a buzzer is included in the system to improve security and give alerts. When someone scans a fingerprint and it doesn't match the saved ones, the system keeps track of the failed attempts. If the wrong fingerprint is tried multiple times, the buzzer makes a loud noise. This helps to alert people nearby that someone might be trying to access the vehicle without permission. It also informs the user that the scan was not successful and they should try again with the correct fingerprint. This sound alert adds an extra layer of safety and makes the system more responsive.

The power management of the system is a crucial aspect to ensure stable operation, especially in a vehicle environment where fluctuating voltage levels are common. The system is powered by a 12V rechargeable battery, which is common in automotive applications. A converter is used to step down the 12V input to the required voltage levels, such as 5V for the NodeMCU ESP8266 and 3.3V for the fingerprint sensor.

In terms of the software architecture, the NodeMCU ESP8266 is programmed to handle various tasks, including reading the fingerprint data, comparing it with the authorized templates, and managing the display and buzzer outputs. The code is designed to execute these tasks sequentially and efficiently to avoid unnecessary delays or errors.

One of the main advantages of using the NodeMCU ESP8266 in this project is its built-in Wi-Fi capabilities. Overall, the fingerprint-based ignition system provides a modern, secure, and reliable method for controlling vehicle access. By combining biometric authentication, user feedback through the LCD and buzzer, and reliable hardware components like the Keypad, fingerprint sensor, and NodeMCU ESP8266, the system offers a highly effective solution to prevent unauthorized access. The power management system ensures that the vehicle's battery is not drained unnecessarily, while the modular design allows for future enhancements and additional features. This methodology provides a framework for building a practical and secure ignition system that can be easily adapted to different types of vehicles and integrated with future technologies.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

III. LITERATURE REVIEW

The reviewed studies offer various solutions that integrate biometric technologies, RFID, and additional sensors to enhance vehicle security. From [1], the use of multi-factor authentication through facial and fingerprint recognition emerged as a high-accuracy approach. Study [2] highlighted the significance of backup systems like RFID tags in cases of biometric failures, ensuring that the vehicle remains accessible to legitimate users. Lastly, [3] contributed to the discussion by exploring a dual-authentication method involving both RFID and fingerprints, with a focus on improving the overall user experience and security. Together, these studies demonstrate that the future of vehicle security lies in a combination of multiple authentication techniques to provide robust protection against unauthorized access.

The implementation of biometric authentication in vehicle ignition systems has gained traction due to its potential to enhance security, eliminate traditional keys, and simplify vehicle access. A variety of research has been conducted on the development of systems that utilize fingerprint recognition, among other biometric technologies, to secure vehicles and provide added protection from unauthorized use and theft.

The concept of a fingerprint-based ignition system revolves around replacing conventional keys with biometric data, ensuring that only authorized individuals can start the vehicle. These systems incorporate components such as microcontrollers, fingerprint sensors, GSM modules, and relays to establish a robust and reliable anti-theft mechanism [4]. The system typically functions by requesting a fingerprint from the user, comparing the scanned image with a stored fingerprint database, and allowing vehicle ignition only if a match is found [5]. This method is seen as a superior alternative to traditional ignition systems, which can be easily bypassed by physically tampering with the wiring.

Some prototypes have integrated additional functionalities like vehicle tracking and alert mechanisms. For instance, a system developed by researchers used GPS and GSM technologies to track the vehicle's location and notify the owner via SMS if unauthorized access was attempted [5]. These systems are versatile and can be applied to various vehicles, providing comprehensive security that includes tracking and monitoring features [6].

Despite the early successes of these systems, challenges remain in improving their reliability under adverse conditions. Fingerprint recognition systems have been shown to struggle in environments where the user's fingerprints are wet, oily, or dirty, with success rates dropping significantly in these conditions [6]. However, in controlled indoor environments, fingerprint-based systems have demonstrated promising success rates, with some systems achieving up to an 80% recognition rate when tested with clean fingerprints [6]. Future improvements could involve more advanced sensors or algorithms designed to improve accuracy, especially in real-world conditions.

One of the main benefits of fingerprint-based vehicle ignition systems is their user-friendliness and convenience. The absence of physical keys reduces the risk of theft and simplifies the user experience. Furthermore, some systems are capable of enrolling multiple fingerprints, allowing access to several authorized users, while also providing an option to change passcodes for added security [7][14]. Such systems offer flexibility, making them adaptable for various vehicles, and their user-friendly interfaces ensure broad applicability [19].

The combination of fingerprint authentication with other security measures like RFID (Radio Frequency Identification) technology has further strengthened vehicle security systems [9]. RFID tags allow for quick authentication alongside biometric data, enhancing the robustness of the security system. This dual-layered protection has been widely praised for reducing theft rates, especially in regions where vehicle theft is prevalent [5][9]. In addition to providing vehicle access, these systems notify the owner of any unauthorized entry attempts, providing real-time alerts and enhancing situational awareness [19][20].

Additionally, the use of OTP (One-Time Password) systems, in combination with fingerprint recognition, adds another layer of security to vehicle access. When the system is turned on, an OTP is sent to the owner's registered phone number, and vehicle ignition is only possible if the correct OTP is entered [10]. If an incorrect OTP is entered, an alert is immediately sent to the owner, indicating a potential security breach.

Research has shown that biometric systems, particularly fingerprint recognition, are reliable, cost-effective, and offer enhanced protection compared to traditional key-based systems. Moreover, these systems have been designed to withstand environmental challenges, such as bumpy roads or vehicle shocks, further validating their practicality [12]. They also have the potential for future expansion, including the integration of cloud computing for remote monitoring and the use of additional biometric data, such as facial or voice recognition, to further improve security [8][11].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

Although the technology offers numerous benefits, there are concerns regarding its implementation. Biometric systems can be expensive and require significant modifications to existing vehicle infrastructure. Additionally, issues with sensor accuracy in challenging environments, such as extreme weather or when the user is wearing facial coverings, could limit the effectiveness of facial or fingerprint recognition systems [18]. Nevertheless, continuous advancements in biometric technology are expected to overcome these challenges, potentially leading to more widespread adoption in the automotive industry in the near future.

In conclusion, fingerprint-based vehicle security systems are an effective and promising alternative to conventional ignition methods. They offer increased security, convenience, and flexibility while ensuring that only authorized users can start the vehicle. As biometric authentication technology becomes more refined, it is likely to play an even greater role in the future of automotive security, providing a reliable, cost-effective solution to prevent vehicle theft [16].

Block Diagram

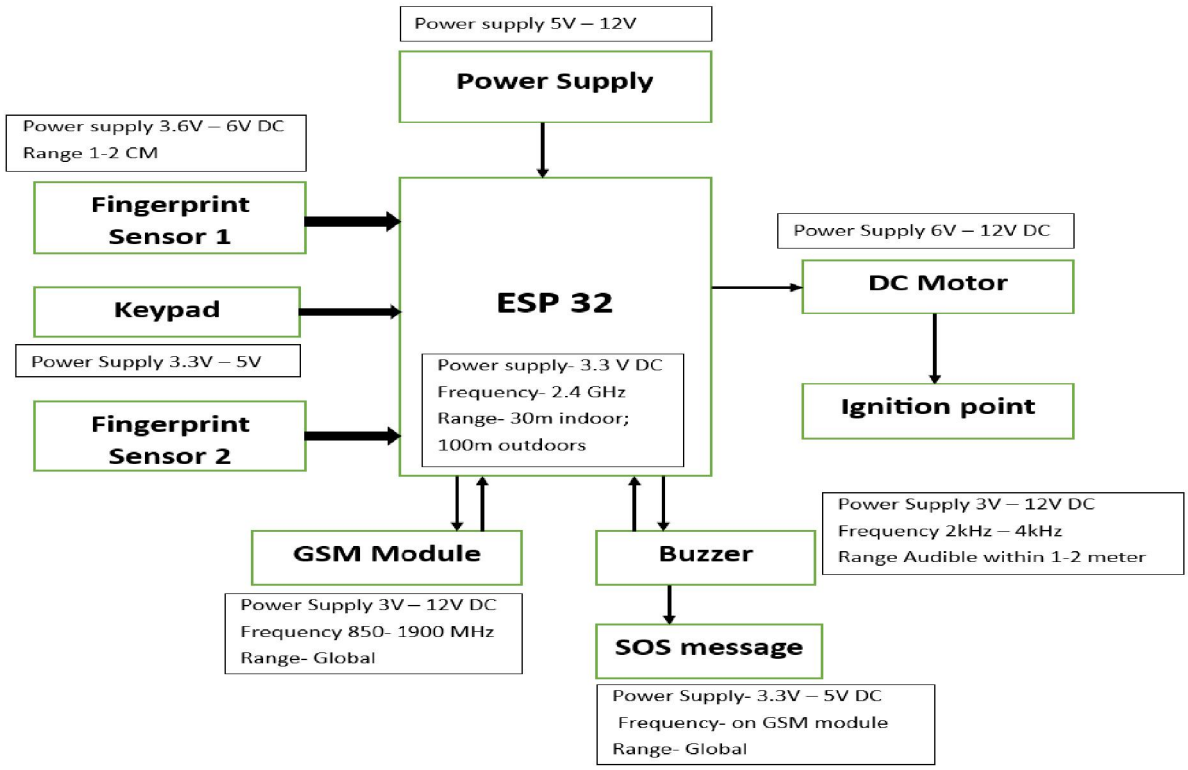

Figure No. 1. Block diagram of a Biometric fingerprint-based vehicle ignition and security system

IV. RESULTS

The developed prototype of the **Biometric Fingerprint-Based Vehicle Ignition and Security System** is shown in the figure below. The hardware implementation consists of a keypad, LCD module, DC motor, fingerprint sensor (internal), and supporting components mounted on a dual-board setup.

In this implementation:

The **keypad** is used as a backup authentication method in case fingerprint scanning fails or for additional passcode input.

The **16x2 LCD** provides real-time feedback such as "Access Granted," "Fingerprint Not Recognized," or "Enter Passcode."

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

The **DC motor** simulates the vehicle ignition system. When the correct fingerprint is scanned, the motor activates.
A **buzzer** (not visible) triggers during unauthorized access attempts.
The **fingerprint module**, though not visible externally in this image, is embedded within the structure and securely connected to the NodeMCU ESP8266 microcontroller.
This real-time demonstration verifies the proper integration and functionality of all components. The system successfully restricts ignition to only authenticated users, enhancing the overall security of the vehicle ignition process.

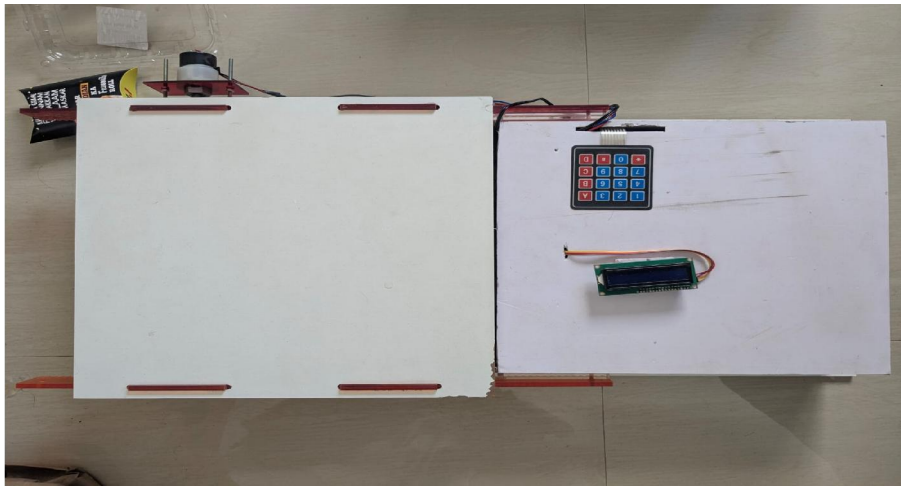

Figure No. 2: Working prototype of the ignition system

V. CONCLUSIONS

The Biometric Fingerprint-Based Vehicle Ignition System offers a modern and secure alternative to traditional key-based ignition methods. In this project, fingerprint authentication is combined with a keypad interface to enhance the security and user control of the vehicle. The system is built using a NodeMCU ESP8266, which manages all inputs and outputs efficiently. A fingerprint sensor ensures that only authorized users can start the vehicle, while the keypad can be used for additional input or manual override if required. Real-time feedback is provided through an LCD, keeping the user informed at each step, and a buzzer alerts users to any incorrect attempts or possible unauthorized access. By replacing conventional ignition systems with biometric technology, this project reduces the risk of vehicle theft and brings a higher level of safety and convenience. With its low cost, compact design, and ease of use, this system has strong potential in the automotive market as a practical and scalable solution for modern vehicle security.

ACKNOWLEDGMENT

This research was not funded by any grant.
We would like to express our sincere gratitude to all those who supported and guided us throughout the course of this project. First and foremost, we are thankful to our project guide, [Dr. M. M. Jadhav], for their invaluable support, technical insights, and continuous encouragement which played a crucial role in the successful completion of this work.

REFERENCES

[1]. Bhargav, B. A., Krishna, D. H., & Abudhagir, U. S. (2022).” Real Time Vehicle Security System Using Face Recognition and Finger Print.” Mathematical Statistician and Engineering Applications, 71(3s2), 1731-1744.
[2]. Sawant, N., Sutar, S., Ghumare, G., & Itole, M. D. (2021). “Fingerprint-Based Car Ignition System Using Arduino and RFID.” International journal, 6(5).
[3]. Al Halaseh, M. (2021). “Vehicle Ignition System Design Using Fingerprint Recognition and Radio Frequency Identification.”

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

[4]. Dasani, A. R. "Biometric Ignition and Vehicle Safety System-A Novel Approach to Reduce Vehicle Theft."
[5]. Jamshed, F. U. R. S. J., & Shaikh, K. A. Z. "Fingerprint Based Ignition System and Tracking of Vehicle."
[6]. Supriyono, H., Wijayanto, A. A., Jailani, R., & Tokhi, M. O. (2020). "Design, Implementation, and Evaluation of a Fingerprint-Based Ignition Key for Motorcycles." Automotive Experiences, 3(2), 68-80.
[7]. Rushikesh Vallakati, Ruturaj Kavitke, Rushikesh Deokar, Paresh Sawale, Prof. R. G. Janunkar, "Fingerprint Ignition System & Keyless Entry Via Fingerprint," Volume 9, Issue 4, 2021
[8]. Pranav PS, Hariharan G, Rajkamal J, Veeramani V, "Fingerprint Based Vehicle Security and Location Tracking System Using IoT," 07 Issue: 05 May 2020
[9]. A Vamshidar Reddy, L. Yashwanth, L. Nithin, M. Sai Dinesh, K. Ramya, "Fingerprint and RFID Based Bike and Car Ignition System," Volume 12 Issue IV Apr 2024.
[10]. Bh. Bhargavi, B. V. K. Padmaja, R. L. Mounika, K. V. K. S.S. Manikanta, N. Chandini, P. Sravani, "Anti-Theft System for Vehicle Security", 07 Issue: 06 June 2020.
[11]. Anshul Vashist, Romanch Kansal, Vaibhav Nijhawan, Zaid Zafar, "A Fingerprint-Based Ignition System in Vehicles," Volume 12, Issue 6, June 2021.
[12]. Amit Saxena, Sarthak Sharma, Shivam Gaur, Shubham Chauhan, Shantanu Varshney, "Ignition Based on Fingerprint Recognition," Volume 2 Issue 1 2022.
[13]. Gopu Priyanka, Bala Bhadruni Pranavi, Krishnamsetty Manaswini, A. S. R. Sai Srinivas, A. V. Rajan, "Fingerprint Based Vehicle Starter and Vehicle Tracking System," Volume-3, Issue-5, May-2020.
[14]. S. Jalaja, Aravinth. R., S. Hariharan, E.A. Herrick Linor, "Finger Print Sensing Vehicle Starter," Vol. 2(1), 2023.
[15]. Bindu B S, Darshini B S, Dhanushree M S, Tarun K P, Prasad A M, "Providing Security to the Vehicle Ignition System Using Fingerprint Technology and Driving License," Volume 8, Issue 2, February 2023.