SMART MULTIFACTOR AUTHENTICATION SYSTEM FOR SECURITY OF VEHICLE

[1]Prof. P. R. Bhole, [2]Sejal Yogesh Sonar, [3]Bhagwati Machhindra Patil, [4]Shubham Shravan Pawar, [5]Aniket Mahesh Chaudhari

[1]Assistant Professor, Electronics and Telecommunication Engineering Department, R. C. Patel Institute of Technology, Shirpur, associated with Dr. Babasaheb Ambedkar Technological University, Lonere, and Maharashtra, India

[2,3,4,5] U.G. Student, Electronics and Telecommunication Engineering Department, R. C. Patel Institute of Technology, Shirpur, associated with Dr. Babasaheb Ambedkar Technological University, Lonere, and Maharashtra, India

Abstract*—The increasing incidence of vehicle theft has highlighted the limitations of traditional vehicle security mechanisms such as mechanical locks, single-key systems, and basic electronic access control. Many existing systems rely on a single rigid authentication technique, which often compromises either security or user convenience. To address these issues, this paper presents a Smart Vehicle Protection System using Multiple Authentication Techniques, designed to provide flexible yet secure vehicle access. The proposed system integrates fingerprint-based biometric authentication, RFID-based authentication, and PIN-based keypad authentication using an ESP32 microcontroller as the central control unit. Unlike conventional multi-step authentication systems, the proposed design allows authorized access to the vehicle using any one valid authentication method, thereby improving usability while maintaining security. Each authentication module operates independently, and successful verification from any single module enables vehicle unlocking through an electronic locking mechanism. The system is implemented using low-cost, readily available hardware components, making it suitable for both modern and legacy vehicles. Experimental testing demonstrates that the system reliably authenticates authorized users while preventing unauthorized access attempts. Additionally, the use of the ESP32 enables future expansion toward IoT-based features such as remote monitoring, alert notifications, and access logging. The proposed solution offers a balanced approach between security, convenience, and cost-effectiveness, making it a practical enhancement over traditional vehicle security systems.

I. INTRODUCTION

The continuous growth in the number of vehicles worldwide has increased the demand for reliable and intelligent vehicle security systems. Vehicle theft and unauthorized access remain serious concerns, especially with the widespread use of conventional locking mechanisms such as mechanical keys, single-key ignition systems, and basic electronic access controls [1]. These traditional security solutions are often insufficient to address the evolving security requirements of modern vehicles, highlighting the need for smarter and more adaptable protection mechanisms [7].

Recent advancements in embedded systems and digital authentication technologies have enabled the development of electronic vehicle security solutions. Authentication methods such as biometric fingerprint recognition, Radio Frequency Identification (RFID), and Personal Identification Number (PIN)–based keypad systems have gained attention due to their ability to provide controlled and user-specific access [5]. These techniques enhance vehicle protection by ensuring that access is granted only to authorized users while also improving operational convenience.

In this context, integrating multiple authentication techniques into a single vehicle security system has emerged as an effective approach to enhance access flexibility and reliability [9]. By offering more than one authentication option, users are provided with alternative methods to unlock the vehicle, ensuring seamless access in varied usage scenarios. Such systems improve the overall user experience while maintaining secure access control [10].

This paper presents a Smart Vehicle Protection System using Multiple Authentication Techniques, designed to provide secure and flexible vehicle access. The proposed system integrates fingerprint-based biometric authentication, RFIDbased authentication, and PIN-based keypad authentication, all managed by an ESP32 microcontroller [8]. Each authentication method functions independently, and successful verification from any one method enables the vehicle unlocking mechanism. This design approach enhances ease of use while maintaining a robust security framework.

The system is implemented using cost-effective and readily available hardware components, making it suitable for deployment in both modern and existing vehicles. The ESP32 microcontroller works as a control unit, that provides processing capabilities for wireless communication support [4]. This allow the system to extend easily for future IoT based functionalities such as remote access, notification alerts [6].

II. LITERATURE SURVEY

Vehicle security is the major issue of research due to the increasing rate of car theft and unauthorized access.Researchers have investigated various authentication techniques and methods to enhance vehicle protection. The literature section is on RFID-based access systems, biometric authentication, PIN-based systems, multi-authentication techniques, embedded controller platforms and Internet of Things enabled car security solutions is reviewed in this part.

A. RFID-Based Vehicle Access Systems

Radio Frequency Identification (RFID) technology has been widely used in vehicle access and keyless entry systems due to its contactless operation and low implementation cost [3]. Researchers have suggested RFID based vehicle security systems where a RFID card works as a digital key, and the vehicle unlocks only after the card is verified.As compared to mechanical keys, the RFID system is more convenient and simple to install. RFID is common option for safety systems due to its simplicity and low power requirements

.

B. Biometric Authentication for Fingerprint Recognition

Biometric authentication is a fingerprint recognition device used in vehicle security research due to its user specific and non transferable nature [2]. Many studies shows the integration of fingerprint sensors with microcontrollers to control vehicle door locks and ignition systems. Fingerprint-based systems verifies the users by matching their unique fingerprints, which makes the access control more secure and reliable. Research prototype shows that fingerprint authentication can be easily used in embedded systems with the available fingerprint sensors, thus making it suitable for real-time vehicle access.

C. PIN and Keypad-Based Authentication Systems

PIN based authentication system uses numeric keypads which is commonly used in home and automotive applications for access control [3]. In this PIN based authentication system vehicle opens only when the users enter the correct password on a keypad. These system is simple, low cost and easy to use which makes value for a system. Keypad authentication is often used as alone or as a backup with other security methods, gives more flexibility to users to access the system.

D. Multi-Authentication and Hybrid Access Control Systems

To enhance security and usability, researchers have proposed multi-authentication and hybrid access control system. that combines multiple authentication methods [5], [9]. Some studies focus on multi-factor authentication, where users must pass multiple verification such as RFID , biometric authentication. Other works propose multi-option authentication systems in which access is granted if any one of the authorized authentication methods is successfully verified. These designs aim to improve user convenience while maintaining a secure access framework, especially in embedded and automotive applications.

E. Microcontroller-Based Implementations

Embedded microcontrollers plays a crucial role in modern vehicle security systems. Platforms such as Arduino and ESP32 are widely used in research and prototype development due to their flexibility, processing capability, and support for multiple peripheral interfaces [4], [8]. Several studies demonstrate the integration of RFID readers, fingerprint sensors, keypads, and electronic locking mechanisms using these controllers. ESP32 microcontroller, in particular, is favored for its built in Wi-Fi and Bluetooth support, enabling future scalability towards connected and intelligent vehicle systems.

F. IoT-Enabled Vehicle Security Systems

With the advancement of Internet of Things (IoT) technologies, vehicle security systems are increasingly being extended with remote monitoring and alert features [1], [6]. Researchers have explored that IoT-based vehicle protection solutions can provide real-time notifications, access logs, and remote control through mobile or cloud platforms [11]. These systems typically combine embedded controllers with wireless communication modules to transmit security events such as unauthorized access attempts. IoT integration enhances system functionality and supports intelligent transportation applications.

G. Summary of Existing Research

The literature shows that RFID, biometric fingerprint authentication, and PIN-based systems each offer different advantages for vehicle security. Embedded microcontroller platforms enable effective integration of these authentication methods into compact and cost-effective systems. Recent research trends emphasize combining multiple authentication techniques to improve flexibility and reliability [7]. These findings provide strong motivation for designing a smart vehicle protection system that integrates multiple independent authentication methods using a single embedded controller, with scope for future IoT-based enhancements.

III. METHODOLOGY

This section explains how the proposed Smart Vehicle Protection System is designed and implemented, including the system design, main hardware parts, circuitry, and how the system works.

A. System Design Overview

The proposed system offers a secure and flexible way to access a vehicle using more than one authentication method [9]. An ESP32 microcontroller acts as the main control unit. It manages authentication requests and controls the vehicle's locking mechanism. The system includes three separate authentication modules:

1. Fingerprint-based biometric authentication
2. RFID-based authentication
3. PIN-based keypad authentication

Unlike traditional multi-step authentication systems where all steps must be completed, this design allows access if any one valid authentication method is successful. Each module works on its own. Once authentication is successful, the ESP32 will activate the electronic lock to open the car door. If authentication fails, the system stays locked but allows the user to retry.

B. Hardware Components

Below are the main hardware parts used in the proposed system:

1. ESP32 Microcontroller: The ESP32 is the core processing unit of the whole system [4]. It connects to all the authentication modules, runs the authentication logic, and controls the electronic lock. The ESP32 is chosen because it has high processing power, low energy use, many GPIO pins, and built-in wireless communication features.

2. Fingerprint Scanner: The fingerprint scanner captures and checks fingerprint patterns for biometric authentication [2]. The scanned fingerprint is compared with stored templates. If they match, the scanner sends a signal to the ESP32 for further processing.
3. RFID Module: The RFID module lets the system use contactless authentication with RFID cards or tags [3]. Each authorized user gets an RFID tag. When a valid tag is read, the RFID reader sends the ID to the ESP32 to verify it.
4. Keypad Module: The keypad allows PIN-based authentication. The user enters a numeric code. The ESP32 checks the entered PIN against stored valid codes. If the PIN matches, access is granted.
5. Electronic Locking Mechanism: This is an electronic device such as a relay, solenoid, or motor actuator that locks or unlocks the vehicle door [10]. The ESP32 controls this mechanism using a digital signal when authentication succeeds.
6. Power Supply Unit: A rechargeable battery is used to power the entire system. Voltage regulation circuits are added to make sure that the ESP32 microcontroller and all connected components receive a stable and reliable power supply.

C. Circuit Diagram Description

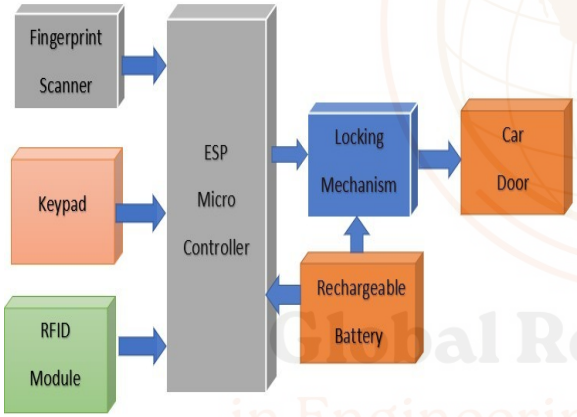

Fig. 1: Block Diagram: Smart Multifactor Authentication System for Security of Vehicle

The fingerprint sensor and RFID module are connected to the ESP32 using serial communication. The keypad is connected to the digital GPIO pins in a matrix form. The electronic locking system is controlled through a relay or motor driver circuit connected to the ESP32. Proper isolation and protection components are used to ensure safe and reliable operation of the locking system.

D. Methodology Summary

The proposed system combines multiple authentication methods into a single embedded system [5]. The ESP32 microcontroller manages authentication and locking operations efficiently. The modular design improves reliability and allows easy future upgrades. Overall, the system provides a secure, flexible, and cost-effective solution for vehicle access control.

E. Flowchart Description

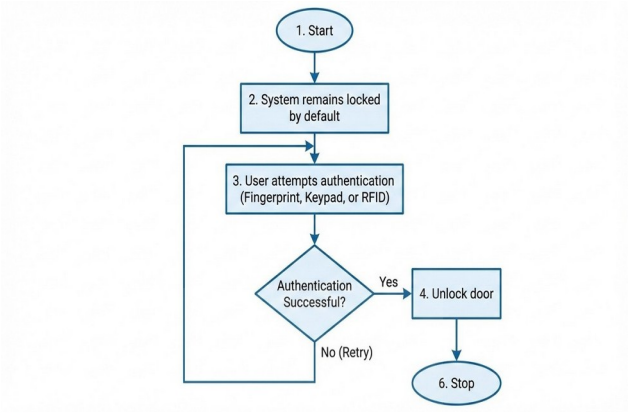

Fig. 2: Flow chart

The working flow of the system is as follows:

1. The system starts and remains locked by default.
2. The user tries to authenticate using fingerprint, RFID, or keypad.
3. The system checks the entered authentication details.
4. If authentication is successful, the ESP32 activates the electronic lock to unlock the vehicle door.
5. If authentication is fails, the system stays locked and allows the user to try again.
6. After unlocking the system the process stop

IV. WORKING PRINCIPLE

The Smart Vehicle Protection System works on the principle of flexible authentication [8]. Access to the vehicle is granted when any one authorized authentication method is successfully verified. By default, the system remains in a locked and secure state while continuously monitoring user inputs.

When the system is powered ON, the ESP32 initializes all connected modules such as the fingerprint scanner, RFID reader, keypad, and electronic lock. The vehicle door remains locked until a valid authentication request is detected. The user may initiate authentication using any one of the available methods: fingerprint authentication, RFID-based authentication, or PIN-based keypad authentication.

In the case of fingerprint authentication, the fingerprint scanner captures the user's fingerprint and compares it with the stored templates [2]. If a match is detected, a success signal is transmitted to the ESP32. For RFID authentication, the RFID reader scans the presented RFID tag and sends the unique identification number to the microcontroller, which verifies it against authorized records [3]. For keypad authentication, the user enters a predefined PIN, which is validated by the ESP32 against stored credentials.

The ESP32 processes the authentication result from each module independently. If any one of the authentication methods is successfully verified, the microcontroller generates a control signal to activate the electronic locking mechanism. This action

unlocks the vehicle door, allowing authorized access. Once unlocked, the system completes the operation cycle.

If authentication fails, the ESP32 does not trigger the locking mechanism, and the vehicle remains in the locked state. The system then allows the user to retry authentication without requiring a system reset. This continuous monitoring and verification process ensures secure and reliable vehicle access.

The use of a rechargeable power supply ensures uninterrupted system operation, while the ESP32 microcontroller provides efficient processing and scalability. The working principle emphasizes a balance between security and user convenience, making the system suitable for real-world vehicle protection applications with potential for future IoT-based enhancements [1], [6].

V. CONCLUSION

This paper presented a Smart Vehicle Protection System using multiple authentication techniques to provide secure and flexible access control for vehicles [9]. The proposed system integrates fingerprint-based biometric authentication, RFIDbased authentication, and PIN-based keypad authentication using an ESP32 microcontroller as the central control unit. By allowing vehicle access through any one valid authentication method, the system achieves an effective balance between security and user convenience. The modular design of the system ensures reliable operation, as each authentication method functions independently while contributing to a unified access control decision. The system remains locked by default and unlocks the vehicle only after successful authentication, thereby preventing unauthorized access. Experimental implementation confirms that the proposed design performs consistently and accurately in authenticating authorized users [7]. The use of low-cost and readily available hardware components makes the system suitable for both modern and existing vehicles. Furthermore, the selection of the ESP32 microcontroller provides scalability and opens possibilities for future enhancements such as IoT-based monitoring, access logging, and remote alert notifications [11].
Overall, the proposed Smart Vehicle Protection System offers a practical, cost-effective, and efficient solution for improving vehicle security. The system successfully addresses the growing need for intelligent vehicle access control and serves as a strong foundation for future advancements in smart automotive security technologies.

VI. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Prof. P. R. Bhole, Assistant Professor, Department of Electronics and Telecommunication, R. C. Patel Institute of Technology, Shirpur, for their valuable guidance, support, and encouragement throughout this project. We also extend our thanks to the laboratory staff and peers who provided assistance during the design, testing, and implementation phases of the Smart Multifactor Authentication System for Security of Vehicle.

Finally, the authors acknowledge the support of R. C. Patel Institute of Technology, Shirpur, India, for providing the necessary resources and facilities to successfully carry out this work.

VII. REFERENCES

[1] S. Kumar, A. Sharma, and R. Singh, “Smart Vehicle Security System Using IoT and Multifactor Authentication,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, no. 6, pp. 45–50, Jun. 2020.

[2] M. Alenezi and K. Almustafa, “A Biometric-Based Vehicle Access Control System Using Fingerprint Recognition,” IEEE Access, vol. 8, pp. 223456–223465, 2020.

[3] P. Patil, S. Jadhav, and A. Kulkarni, “RFID and Keypad Based Advanced Vehicle Security System,” International Journal of Engineering Research and Technology (IJERT), vol. 10, no. 4, pp. 312–317, Apr. 2021.

[4] R. Gupta and N. Verma, “Design and Implementation of Smart Car Locking System Using ESP32,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 10, no. 8, pp. 88–93, 2021.

[5] A. A. Khan, M. H. Rehman, and T. Saba, “Multifactor Authentication in Embedded and IoT-Based Systems: Security Challenges and Solutions,” Journal of Network and Computer Applications, vol. 168, pp. 102760, 2020.

[6] S. R. Bhagat and P. S. Bangare, “IoT-Based Vehicle Security and Tracking System Using GSM, GPS, and Biometric Authentication,” International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 5, no. 7, pp. 1–6, 2021.

[7] J. Lee, H. Kim, and S. Park, “Secure Access Control for Smart Vehicles Using Multi-Layer Authentication,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 4, pp. 2876–2886, Apr. 2022.

[8] A. Mishra and S. Yadav, “ESP32-Based Smart Lock System with Biometric and RFID Authentication,” International Journal of Computer Applications, vol. 174, no. 22, pp. 12–18, 2021.

[9] Y. Zhang, X. Chen, and L. Wang, “A Secure Multifactor Vehicle Access System Based on Embedded Controllers,” Sensors, vol. 22, no. 9, pp. 3412, 2022.

[10] V. Chavan and D. Patil, “Electronic Vehicle Door Lock System Using IoT and Multifactor Authentication,” International Research Journal of Engineering and Technology (IRJET), vol. 10, no. 1, pp. 1120–1125, Jan. 2023.