Fingerprint Based Ignition and Door lock System

Maizatul Alice Meor Said[1*], Mohamad Harris Misran[1], Mohd Azlishah Othman[1], Noor Azwan Shairi[1], Zahriladha Zakaria[1], Siti Normi Zabri[1], Azahari Salleh[1], Mohd Zahid Idris[2]

[1]Centre for Telecommunication Research & Innovation (CeTRI), Faculty Technology dan Kejuruteraan Elektronik dan Computer (FTKEK), University Technical Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100, Durian Tunggal, Melaka, Malaysia.

[2]Marine Engineering and ETO, Abu Dhabi Maritime Academy, 6th Streeet, Musaffah M-14, Abu Dhabi, United Arab Emirates

[*]Corresponding Author

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000803

Received: 12 August 2025; Accepted: 18 August 2025; Published: 30 October 2025

ABSTRACT

The integration of security features in vehicles has become a critical concern due to the increasing incidents of vehicle theft. Traditional vehicle ignition and door lock systems, which rely on physical keys or remote devices, are susceptible to unauthorized access. This paper presents a fingerprint-based ignition and door lock system for vehicles, leveraging the PIC16F877A microcontroller. The proposed system aims to enhance vehicle security by implementing biometric authentication, ensuring that only authorized individuals can start the engine or access the vehicle. The primary problem addressed by this study is the vulnerability of conventional vehicle locking systems, which can be bypassed through key duplication, remote hacking, or physical tampering. Current solutions, though effective to some extent, still lack a reliable, tamper-proof, and user-specific method for securing vehicles. The solution proposed in this study utilizes fingerprint recognition technology as a means of secure authentication, offering an advanced and personalized approach to vehicle security. The methodology involves interfacing a fingerprint sensor with the PIC16F877A microcontroller, which processes and verifies the fingerprint data against pre-registered templates stored in the system. The microcontroller controls the door lock and ignition system based on the outcome of the fingerprint verification. The proposed system is designed to be low-cost, reliable, and easily integrable into existing vehicle systems. The system's performance demonstrates its practicality for real-world applications, offering an innovative solution to improve vehicle security.

INTRODUCTION

The security of vehicles has become an increasingly critical issue as the incidence of vehicle theft and unauthorized access continues to rise. Traditional methods of securing vehicles, such as using physical keys, remote key fobs, and transponder keys, while effective to some extent, have significant limitations. These systems are vulnerable to key duplication, hacking, or physical tampering. For instance, thieves can easily replicate physical keys or exploit weaknesses in remote entry systems, making it easier to gain unauthorized access. Additionally, the loss of a key fob or the hacking of a keyless entry system may lead to potential breaches of vehicle security. These weaknesses highlight the need for more advanced and secure methods of vehicle access and ignition. In this context, biometric authentication systems have gained attention as a more secure, personalized solution. Among various biometric techniques, fingerprint recognition has proven to be a reliable and highly effective method due to its uniqueness, accuracy, and ease of implementation in security systems.

Fingerprint-based biometric systems are already widely used in various applications such as smartphone security, banking, and government identification systems due to their inherent security advantages. These systems work by capturing the fingerprint of the individual, which is unique to each person, making it difficult for unauthorized individuals to bypass the system. As a result, researchers have begun to investigate the potential of fingerprint recognition systems for automotive applications, aiming to address the shortcomings of traditional vehicle security systems. Recent studies have shown promising results for fingerprint-based vehicle access and ignition

systems, where only authorized users can access the vehicle. For example, Srivinas proposed an innovative fingerprint-based vehicular access system, emphasizing the reliability of fingerprint recognition in preventing unauthorized access and ensuring ease of use for authorized individuals [1].

In recent years, advancements in fingerprint recognition technology have also made their way into vehicle security systems. Tappari designed a cost-effective fingerprint-based vehicle security system that integrates an optical fingerprint sensor with a microcontroller, thus eliminating the need for physical keys while improving security and convenience. Their system reduces the risk of unauthorized access due to key duplication or signal interception [4]. Moreover, Hajare developed a fingerprint-based ignition system that integrates seamlessly with vehicle electrical systems. Their approach offers a tamper-resistant solution by ensuring that only authorized users can start the engine, addressing the vulnerabilities of traditional ignition systems [2].

The results from these studies have sparked further interest in adopting fingerprint-based security systems within the automotive industry. These studies suggest that fingerprint recognition technology holds great potential in providing higher security and more personalized vehicle access. Janunkar further reinforced the idea that incorporating fingerprint recognition can significantly enhance vehicle security by addressing challenges such as optimizing recognition speed, improving accuracy, and maintaining minimal power consumption in automotive applications [3].

Fingerprint recognition technology, although highly secure, faces several challenges. One of the main hurdles is integrating the fingerprint authentication system with existing vehicle mechanisms, such as ignition and door lock systems. Researchers have explored various ways to achieve seamless integration between biometric sensors, microcontrollers, and mechanical actuators that control the vehicle's security features. Additionally, the scalability of these systems for mass production remains a significant consideration. While systems tested in controlled environments have shown impressive results, real-world applications of these systems in vehicles require adjustments for factors such as sensor positioning, user interface, and overall robustness under different environmental conditions [9][10].

Furthermore, ensuring the robustness of fingerprint-based systems against spoofing attacks is a critical challenge that researchers have been addressing. Spoofing attacks, where fake fingerprints are used to deceive the system, present a major concern. Recent advancements in fingerprint recognition algorithms have focused on improving the accuracy and reliability of fingerprint matching, reducing the chances of false positives and negatives. Several studies have also explored the integration of multimodal biometric systems to enhance security further. For example, integrating fingerprint recognition with facial recognition or voice recognition could significantly reduce the likelihood of spoofing or fraud, as it would require multiple factors to match before access is granted [5][6].

In addition to spoofing protection, researchers have also focused on developing systems that can function in diverse environmental conditions. Factors such as dirty or damaged fingerprint sensors can significantly hinder system performance, making it important to improve sensor durability and robustness. Advanced algorithms designed for feature extraction and fingerprint matching play a critical role in overcoming these challenges by improving the system's ability to handle various fingerprint conditions, including smudges, cuts, or skin injuries [7][8]. Furthermore, vehicle ignition and access systems must be designed to handle environmental factors such as temperature, humidity, and dirt, ensuring the reliability of the system in diverse conditions [11][12].

While significant progress has been made in the development of fingerprint-based vehicle security systems, several challenges still hinder their widespread adoption. These challenges primarily relate to the integration of fingerprint recognition technology with existing vehicle architectures, system reliability under real-world conditions, and ensuring robustness against environmental factors such as dirty or damaged sensors. Furthermore, the systems need to be optimized to minimize false positives, false negatives, and spoofing attacks while maintaining low power consumption. Ensuring that these systems are scalable for mass production in the automotive industry, without significant redesigns to the vehicle’s infrastructure, remains a critical gap that needs to be addressed. While laboratory results have shown promising performance, the transition to real-world applications requires additional refinement, particularly in addressing the challenges posed by environmental factors, such as dirt on sensors and varying finger positions, as well as ensuring resistance to hacking and spoofing attempts [13][14][15].

METHODOLOGY

The methodology for developing a fingerprint-based vehicle security system involves several critical steps, including circuit design, fabrication, component soldering, and system testing. Each stage is integral to ensuring that the system functions efficiently and reliably, providing an advanced security solution for modern vehicles. The process is broken down into four major phases: circuit design using Proteus, fabrication, soldering of components, and testing and troubleshooting.

1. Circuit Design Using Proteus

The first step in the development of the fingerprint-based vehicle security system is the design of the electronic circuit. Proteus, a widely used circuit simulation and PCB design tool, is employed to create the circuit schematic. The primary components in this design include the microcontroller, fingerprint sensor, LCD display, motor driver for the door lock mechanism, and relay for controlling the vehicle's ignition system.

Figure 1: Proteus Design Suite Software

The microcontroller is the heart of the system, responsible for processing the fingerprint data and controlling the ignition and door-lock mechanisms. In this case, the PIC16F877A microcontroller is selected due to its versatility, sufficient I/O pins, and compatibility with the required sensors. The microcontroller will handle tasks such as interfacing with the fingerprint sensor, controlling the output devices (ignition relay and motor driver), and displaying system status on the LCD.

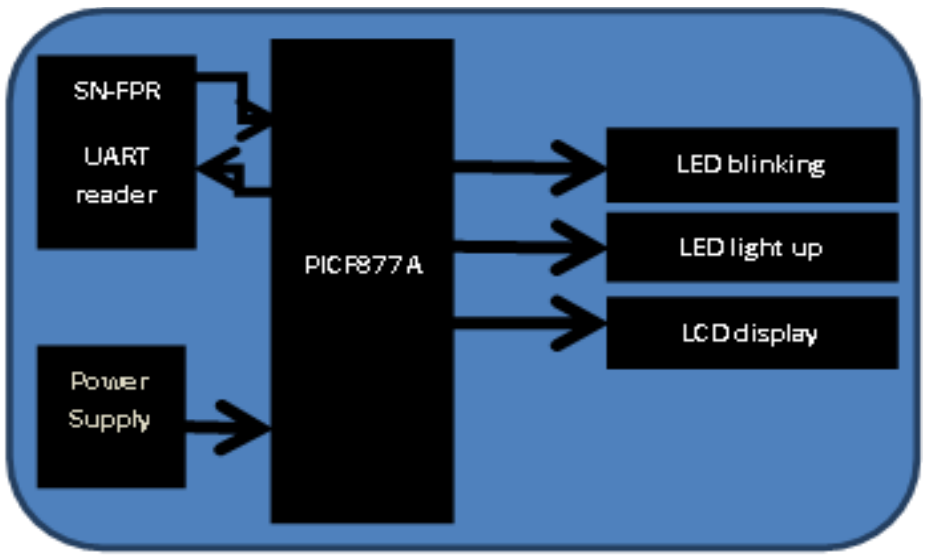

Figure 2: System framework

The microcontroller is programmed to execute a sequence of steps:

1. Initialize the fingerprint sensor and LCD display.
2. Capture the fingerprint data from the sensor when a user places their finger on the sensor.
3. Verify the fingerprint data by matching it with the stored templates in memory.
4. Control the ignition relay and the door lock motor depending on the result of the authentication process.

The fingerprint sensor is connected to the microcontroller via serial communication (UART), using a communication protocol such as RS232 or TTL-level UART. The sensor will capture a fingerprint and convert it into a template, which will then be sent to the microcontroller for verification. The fingerprint data is compared with stored templates, and based on the match, the system either grants or denies access.

Two main output devices are integrated into the system: the motor driver for controlling the vehicle door locks and the ignition relay for starting the vehicle. The motor driver controls the actuator that locks or unlocks the vehicle doors. The ignition relay is responsible for starting the vehicle when the authorized fingerprint is recognized.

The motor driver and relay are controlled via the microcontroller's digital output pins. When a correct fingerprint is verified, the microcontroller activates the relay for ignition or sends a signal to the motor driver to unlock the doors. When an incorrect fingerprint is detected, the system denies access and no action is performed.

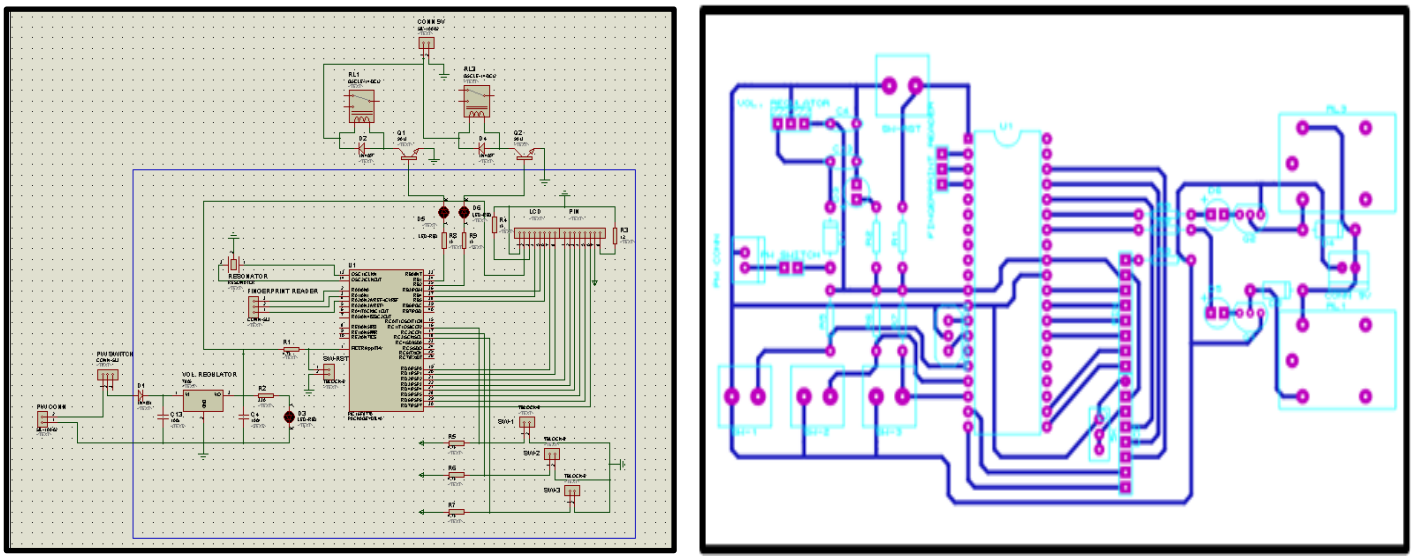

Figure 3: Proteus Software Interface

After designing the circuit schematic in Proteus, the system undergoes simulation within the Proteus environment. This simulation step allows for early detection of errors and verification of the system's functionality before physical implementation. During simulation, the behavior of the fingerprint sensor, microcontroller, motor driver, and relay is tested. The system is checked for fingerprint recognition accuracy, correct door lock operation, and ignition system control.

2. Fabrication of the Circuit

Once the circuit design is confirmed and tested in the simulation environment, the next step is to fabricate the physical circuit. This involves generating a printed circuit board (PCB) based on the circuit schematic.

The PCB is designed using PCB design software, such as EAGLE or KiCad. The circuit schematic from Proteus is imported into the PCB design software, where the components are placed, and the traces are routed to connect them. The PCB layout is carefully designed to ensure that the signals from the fingerprint sensor, microcontroller, and output devices are routed efficiently and without interference. The power supply circuit is designed to provide stable voltage levels for all components, including the microcontroller, fingerprint sensor, and actuators.

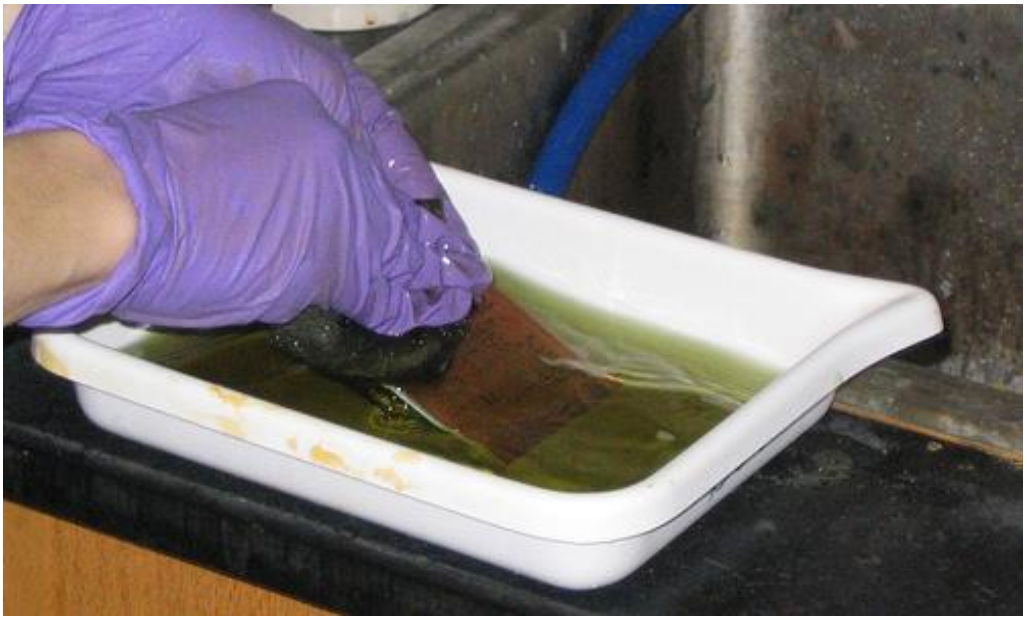

Figure 4: Fabrication process of PCB Board

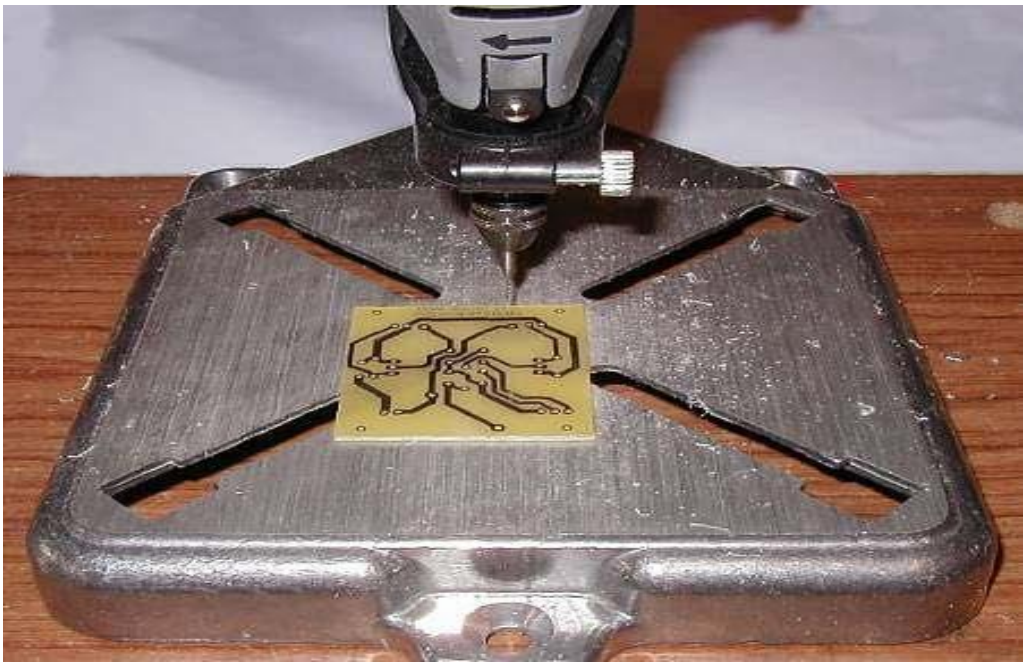

Figure 5: Drilling Process on PCB Board

After finalizing the PCB design, the board is sent to a PCB manufacturer for fabrication. The PCB is typically fabricated using FR4 material, which is a standard and cost-effective material for most electronics. The PCB is fabricated with solder mask, silkscreen, and copper traces to form the electrical connections between components. The board is then inspected for any design flaws before proceeding with component assembly.

3. Soldering Components onto the PCB

With the PCB fabricated, the next step is to assemble the system by soldering the electronic components onto the board. This requires both manual and automated soldering techniques to ensure reliable connections and minimal risk of errors.

Before soldering, all components (microcontroller, fingerprint sensor, motor driver, relay, and passive components) are placed onto the PCB. Each component's pins are aligned with the pads on the PCB to ensure correct placement. The microcontroller, fingerprint sensor, and motor driver are typically surface-mount devices (SMD), while other components like resistors, capacitors, and LEDs are through-hole devices.

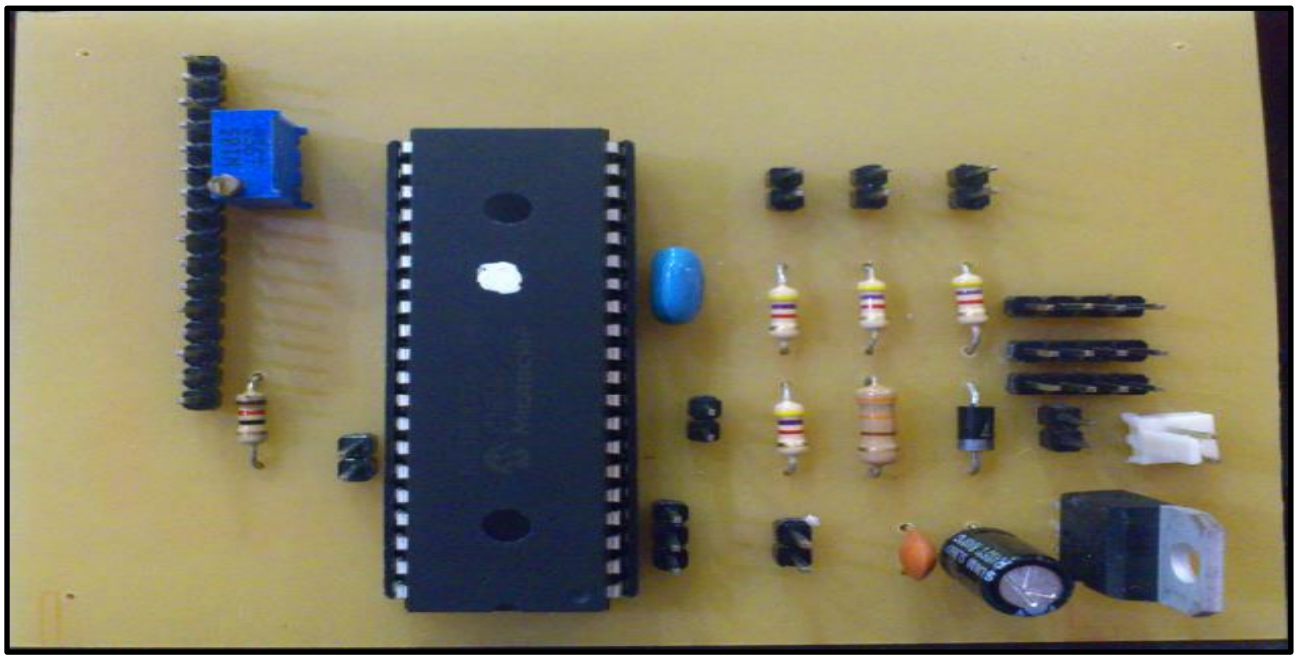

Figure 6: Installation of component on PCB board

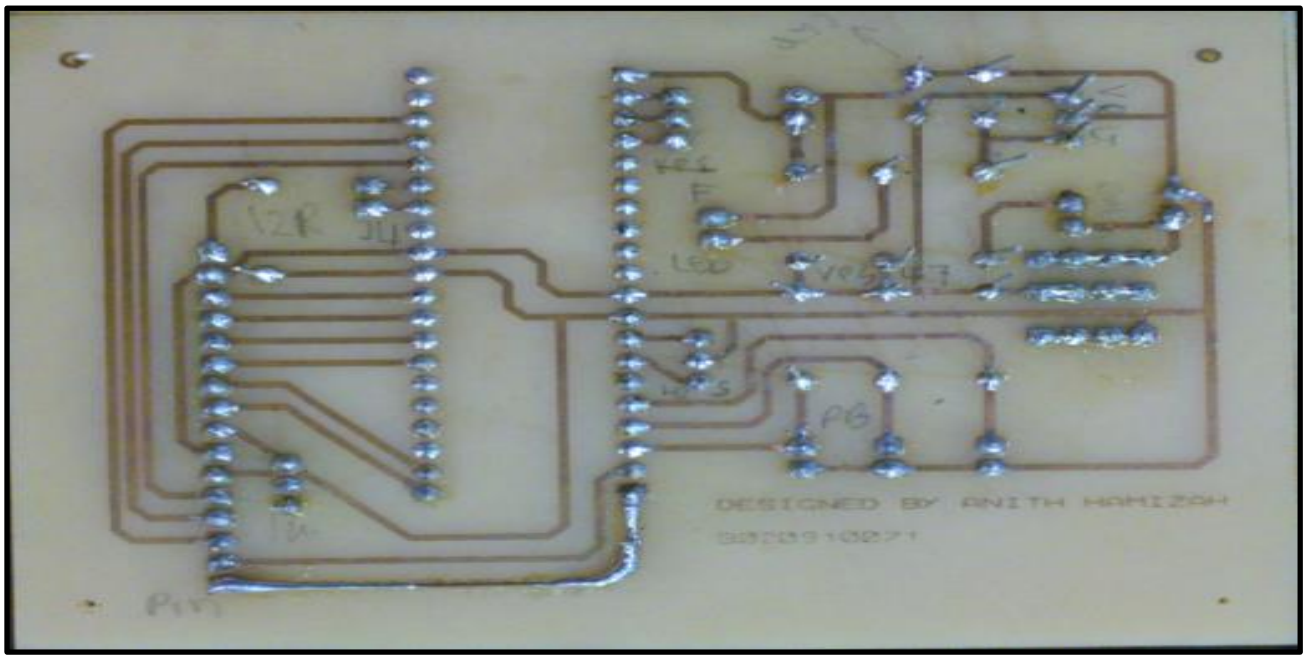

Figure 7: Soldering Process

The soldering process begins with the microcontroller and fingerprint sensor. These components are the most delicate and require careful attention to avoid overheating. The soldering iron is used for precise soldering of the leads, with a temperature-controlled soldering station employed to prevent component damage. The motor driver and relay are then soldered onto the PCB, followed by the passive components like resistors and capacitors.

For the best results, flux is applied to the component leads to ensure proper soldering. The soldering iron tip is carefully moved along the pins of each component to create a strong, reliable connection. After completing the soldering, a magnifying glass or microscope is used to inspect each solder joint to ensure that there are no shorts or cold solder joints.

4. Testing and Troubleshooting

After completing the soldering process, the system undergoes a rigorous testing and troubleshooting phase. This step ensures that the system is functioning as expected and that any potential issues are addressed.

The first step in the testing process is to apply power to the system. Using a multimeter, the voltage levels across the various components are checked to ensure that they are within the required operating ranges. The fingerprint sensor, microcontroller, and output devices are all tested to ensure they receive proper power and are ready for operation.

Once power is confirmed, the system is tested for functionality. The fingerprint sensor is calibrated to ensure it correctly reads and processes fingerprint data. A test fingerprint is enrolled into the system, and the microcontroller's response to the fingerprint authentication process is observed. The LCD display is used to provide feedback during this process, showing messages such as "Access Granted" or "Access Denied."

The motor driver is tested by activating the system's door lock control mechanism. The motor is commanded to unlock or lock the doors, depending on the fingerprint verification result. The ignition relay is also tested by attempting to start the vehicle. If the fingerprint is recognized as valid, the system sends a signal to the relay to start the vehicle's ignition system.

During testing, any issues encountered are carefully diagnosed and addressed. For example, if the fingerprint sensor is not reading correctly, the sensor's connections or power supply are checked. If the motor does not activate, the relay or motor driver connections are inspected for errors. If the microcontroller fails to match fingerprints, the programming code is reviewed to ensure correct logic.

Software debugging is done using tools like debuggers and serial monitors to monitor communication between the microcontroller and the fingerprint sensor. The system's firmware is updated to resolve any performance issues, ensuring that the fingerprint matching process is quick and accurate.

RESULT

Figure 8 shows a fingerprint verification system prototype built on a custom-designed PCB. The board includes various components such as resistors, capacitors, and potentiometers, which are essential for the circuit's operation. The microcontroller unit serves as the brain of the system, processing signals from the fingerprint sensor and controlling other components.

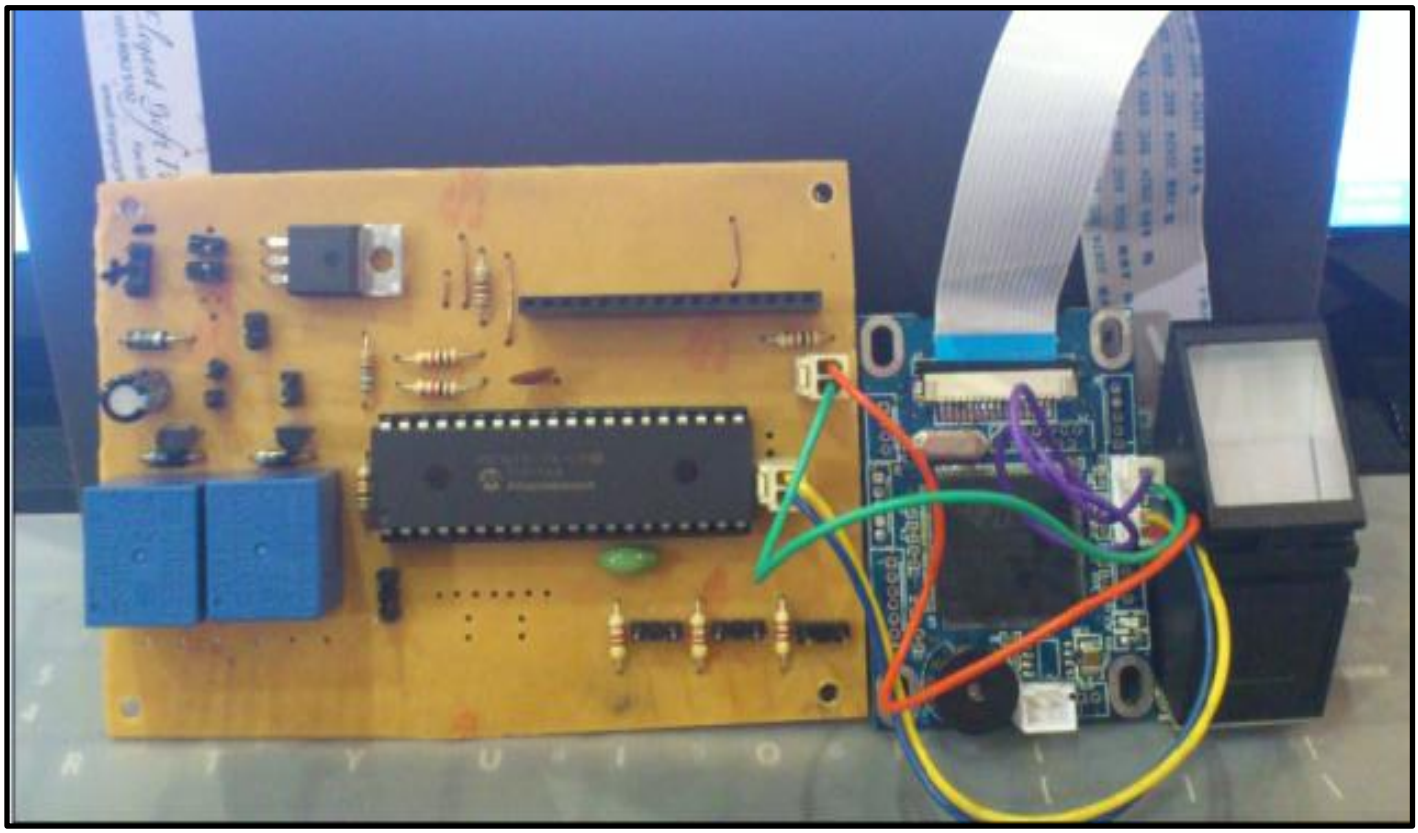

Figure 8: System Prototype

The fingerprint sensor module, visible on the right side, is used to capture and verify fingerprints. The wiring suggests that the fingerprint sensor is connected to the microcontroller, likely using a serial interface, allowing the system to scan and compare fingerprints with a stored database. The coloured wires indicate connections to the microcontroller for power and data transfer. Additionally, two blue blocks appear to be push buttons, which might serve as user input for the system, perhaps for Enrollment or activation. The system is powered via a DC jack, indicating its standalone operation.

The provided flowchart in Figure 9 outlines two fingerprint verification processes, each with distinct objectives: starting the engine and unlocking the door. Both processes begin with the fingerprint scanning and verification stages, where the user's fingerprint is compared against a database of authorized users. If the fingerprint matches an authorized user, the system proceeds; otherwise, it halts the process and alerts the user. For the engine-starting process, once a user's fingerprint is verified, the system enables ignition and displays a message, "Start your engine." The user is given a 60-second window to start the engine, and if they do not, the system re-enables ignition after the time has passed. If the user is authorized but fails to start the engine within this time frame, the system simply ends the process without starting the engine.

In the case of door unlocking, the system plays an auditory cue, Tone 1, if the fingerprint is authorized, unlocking the door afterward. If the fingerprint does not match an authorized user, Tone 2 sounds, indicating a failed attempt, and the door remains locked. In both cases, data is recorded for audit purposes, especially during successful verifications. This process ensures that only verified users can perform critical actions like starting the engine or unlocking the door, using secure fingerprint biometrics for authentication. The system's feedback includes both visual cues (messages on a display) and auditory cues (tones) to guide the user through the verification process.

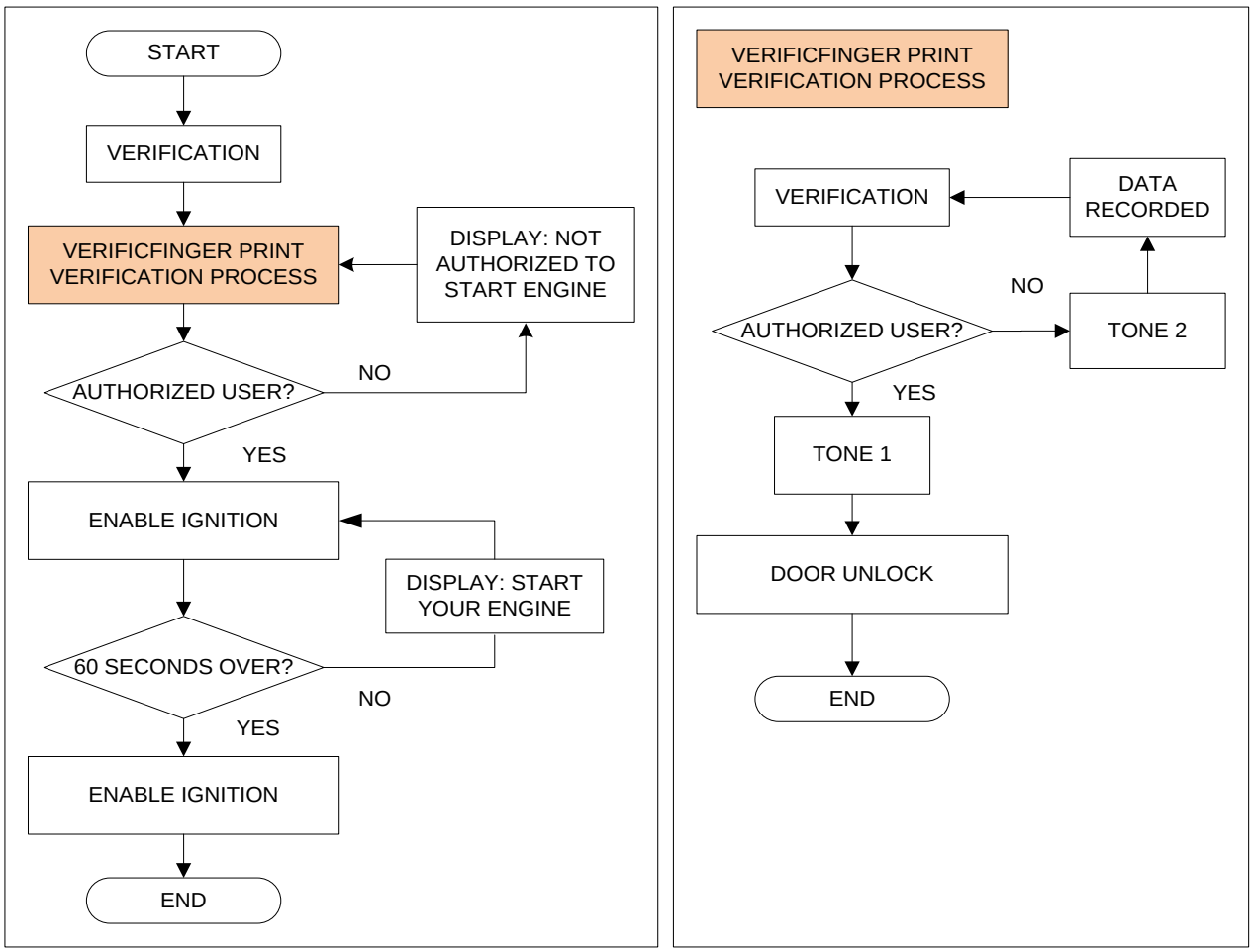

Figure 9: System Flowchart

The system begins with a welcoming display that prompts the user to “Please touch your finger” for fingerprint verification as shown in Figure 10. Upon pressing their finger on the fingerprint scanner, the system captures the

fingerprint image and processes it to match it with the stored data in the database of authorized users. This step is crucial for ensuring that only those with proper authorization can gain access to the system's functions. Referring to Figure 11, if the fingerprint matches an authorized user, the system proceeds by granting access, allowing the user to start the engine and open the door. To indicate successful verification, a blinking LED light is activated. This blinking LED acts as a visual cue for the user, signaling that the fingerprint has been accepted, and they can now proceed with starting the engine and unlocking the door.

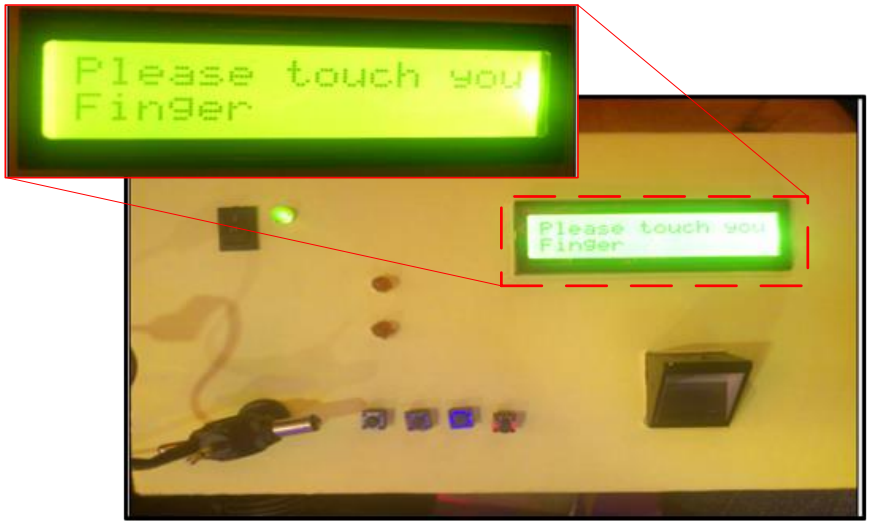

Figure 10: Please touch your finger Display

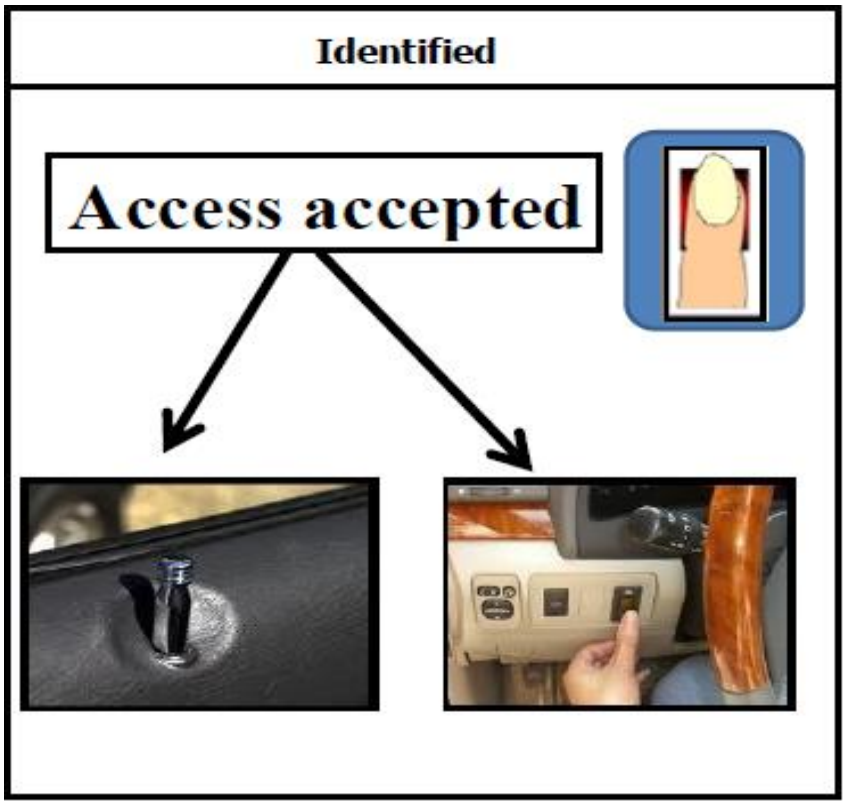

Figure 11: Authorization identified

However, if the fingerprint does not match any authorized entry in the system's database, the system will deny access. In this case, an alarm will sound as an immediate notification to the user, indicating that the verification process has failed and that the user is not authorized to proceed. In Figure 12, the alarm serves both as an auditory signal for the user and as a deterrent for unauthorized access attempts. At this point, the system also records the failed attempt, storing relevant data such as the time of the attempt and the fingerprint scan for later review. This data logging helps in tracking unauthorized access attempts, providing a level of security and traceability.

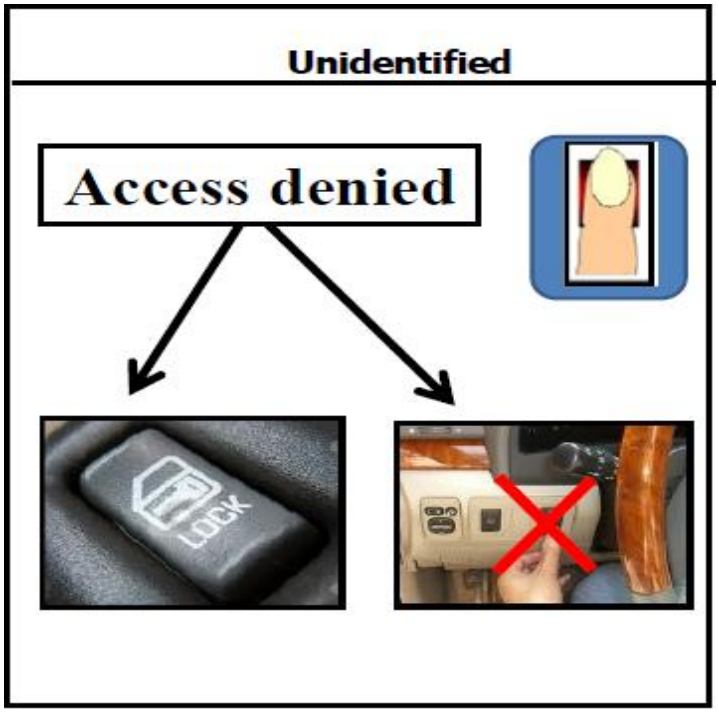

Figure 12: Authorization unidentified

When access is denied, the system ensures that the engine remains locked, preventing any unauthorized person from starting the vehicle. Similarly, the door remains locked, adding an extra layer of security. These mechanisms are in place to safeguard the vehicle or secure area from being accessed by an individual without proper authorization. The system, therefore, balances user convenience with high security, allowing seamless access for authorized individuals while simultaneously protecting against unauthorized entry.

In summary, this biometric authentication system enhances security by using fingerprint recognition to control access to critical systems like the engine and door. The visual and auditory indicators make the process clear for the user, while the data recording ensures that failed access attempts are properly logged for future review. The combination of LED indicators, alarms, and data recording makes the system highly secure and user-friendly, providing an effective solution for sensitive access control applications.

CONCLUSIONS

In conclusion, the fingerprint-based access control system offers a highly secure and user-friendly method of authentication for critical functions such as starting an engine and unlocking doors. By utilizing biometric verification, the system ensures that only authorized individuals are granted access, effectively minimizing the risk of unauthorized use. The system's design includes essential features like real-time feedback through visual (blinking LED) and auditory (alarm) indicators, which not only guide the user through the verification process but also alert them to any security breaches in the form of failed attempts. The integration of data recording further enhances the security of the system, as it logs failed access attempts along with important information, such as the time of the attempt and the fingerprint scanned. This data can be reviewed later to monitor for patterns of unauthorized access attempts, contributing to better overall security management. The system also ensures that when access is denied, both the engine and door remain locked, preventing any unauthorized person from using the vehicle or secure area.

From a practical standpoint, this biometric solution streamlines the process of access control by eliminating the need for traditional keys or PINs, offering a faster, more secure alternative. Its application is vast, ranging from vehicle security to access control in restricted areas, making it a versatile and valuable solution in the field of modern security systems. Overall, this fingerprint authentication system demonstrates an effective blend of security and convenience, ensuring that access is granted only to those with proper authorization, while safeguarding sensitive areas and functions against unauthorized use. The system's reliability, combined with its ease of use, makes it an ideal choice for any application requiring secure access control.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Centre for Research and Innovation Management (CRIM) and University Technical Malaysia Melaka (UTeM) for their invaluable support throughout this project. Their resources, guidance, and encouragement played a crucial role in the successful development and implementation of this fingerprint-based access control system.

REFERENCE

1. Y. Srinivas, V. K, L. Vamsi M, A. M, R. M, H. N, "Fingerprint Based Vehicle Anti-Theft Detection and Alerting System," 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 929-934, 2023. DOI: 10.1109/ICECA58529.2023.10395660
2. P. Hajare, "Fingerprint Recognition System," International Journal of Research and Engineering, vol. 3, pp. 18-21, 2016. DOI: 10.48175/ijsrem15929
3. R. G. Janunkar, "Fingerprint Ignition System & Keyless Entry via Fingerprint," 2021. DOI: 10.55041/ijsrem44498
4. S. Tappari, "Fingerprint-Based Smart Vehicle," International Journal for Research in Applied Science and Engineering Technology, 2023. DOI: 10.22214/ijraset.2023.54650
5. M. P. Vijayan, "Fingerprint & Passcode Based Anti-Theft Vehicle System," 3rd International Conference on Artificial Intelligence for Internet of Things (AIIoT), 2024, pp. 1-6. DOI: 10.1109/AIIoT58432.2024.10574591
6. P. More, A. Lingayat, V. Masudge, S. Singar, "Biometric Vehicle Access and Ignition System Using Fingerprint Recognition," 2021. DOI: 10.48175/IJARSCT-1469
7. K. Vinod Kumar, "Improving the Security System for the Vehicle by Using the Driving License and Fingerprint Automation," International Journal of Scientific Research in Engineering and Management, vol. 10, pp. 7296-7304, 2024. DOI: 10.55041/ijsrem29633
8. M. S. Agrawal, "Vehicle Safety System Using Fingerprint Scanner and Driving License Data," International Journal of Scientific Research in Engineering and Management, vol. 19, pp. 591-606, 2021. DOI: 10.1007/978-981-15-9678-0_51
9. P. R. Sharma, "Security for Vehicle Ignition System by Fingerprint Technology," International Journal of Advanced Research in Science, Communication and Technology, 2022. DOI: 10.48175/ijarsct-7770
10. R. Sreenivasulu, "Fingerprint-Based Vehicle Starter," International Journal of Scientific Research in Engineering and Management, 2022. DOI: 10.55041/ijsrem15929
11. M. Reddy, B. Muni Bhavana, A. Dimple, K. K. Surya Prathap Reddy, "Security for Vehicle Ignition System by Finger Print Technology," International Journal of Advanced Research in Science, Communication and Technology, 2022. DOI: 10.48175/ijarsct-7770
12. S. P. Smitha, "Vehicle Theft Authentication System," INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 2024. DOI: 10.55041/ijsrem34089
13. S. Agrawal, S. Bhardwaj, R. Tyagi, V. Rastogi, "Driving License Management System Using Finger Print Sensors with Seat Belt Monitoring System," International Journal for Research in Applied Science and Engineering Technology, vol. 11, pp. 591-606, 2021. DOI: 10.1007/978-981-15-9678-0_51
14. P. Padma, G. Shalini, L. Hrushitha, A. Srinidhi, D. Sathvika, "Fingerprint Vehicle Starter Using Arduino," International Journal of Scientific Research in Engineering and Management, 2023. DOI: 10.55041/ijsrem15929
15. P. Ramana, "Fingerprint & Passcode Based Anti-Theft Vehicle System," INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 2025. DOI: 10.55041/ijsrem44498