**Journal of Global Engineering Research & Science (J-GERS)**
Vol. 02, No. 02, December 2023, pp. 79-85
ISSN: 2830-5906, *e*-ISSN: 2830-5418, DOI: 10.56904/j-gers.v2i2.77

# Implementation of Motorcycle Security System Using Fingerprint R503

**Martoni Darusman[1], Arisa Olivia Putri[1], Legenda Prameswono Pratama[1,*]**
[1]Department of Electrical Engineering, Faculty of Engineering and Computer Science, Jakarta Global University, Depok 16412, Indonesia

**Article Info**

***Article history:***

Received September 23, 2023
Revised November 16, 2023
Accepted December 04, 2023

***Keywords:***

Internet of Things (IoT)
Security system
ESP32
Motorcycle
Biometric authentication

**ABSTRACT** (10 PT)

Motorcycles are a widely used mode of transportation across diverse populations in both urban and rural areas. However, the increasing prevalence of motorcycle theft has become a major public concern, highlighting the urgent need for more advanced and reliable security solutions. In response, this study proposes the development of a motorcycle security system based on the Internet of Things (IoT) that integrates biometric authentication technology to enhance safety and prevent unauthorized access. The system is built using the R503 fingerprint sensor for biometric verification, the ESP32 microcontroller for processing and connectivity, and Telegram as a real-time notification medium. Additional components such as a relay module and buzzer are used to control the ignition system and provide audible alerts when unauthorized access attempts are detected. The system only grants access to users whose fingerprints have been pre-registered, ensuring personalized and secure authentication. A series of functional tests, including initialization, fingerprint recognition, and system response, were conducted to evaluate performance. Testing on five users demonstrated a high accuracy rate of 98%, with only a 2% error rate, indicating the system's reliability in real-world scenarios. Furthermore, the integration with Telegram enables remote monitoring, providing immediate alerts to users when suspicious activity occurs. These features collectively enhance vehicle safety and user convenience. In conclusion, the developed system offers a promising solution for modern motorcycle security by leveraging IoT and biometric technologies, and it has the potential to be integrated into broader smart transportation and vehicle monitoring ecosystems.

***Corresponding Author:***

Legenda Prameswono Pratama
Department of Electrical Engineering, Faculty of Engineering and Computer Science, Jakarta Global University, Depok 16412, Indonesia
Email: legenda@jgu.ac.id

## 1. INTRODUCTION

Fingerprint recognition has become a prominent solution in the field of biometric authentication, widely applied in systems requiring secure, fast, and reliable identity verification. Its advantages such as uniqueness, permanence, and ease of use, make fingerprint biometrics ideal for access control, financial transactions, mobile computing, and other security system [1], [2]. The development of secure and private fingerprint-based authentication protocols continues to evolve, incorporating methods such as visual secret sharing, homomorphic encryption, and bio-cryptographic models to protect data integrity and user privacy [3], [4]. Despite these advancements, fingerprint systems still face challenges such as spoofing and template protection, prompting researchers to explore various approaches including odor-based fake fingerprint detection and image enhancement techniques [5], [6].

Previous studies implemented fingerprint-based vehicle security systems and embedded authentication modules [7], [8]. It also applies ideas from related works on home energy security and mobile device integration with biometric systems [9], [10]. In addition, IoT-based system architectures distribution control using

*e*-ISSN: 2830-5418, *p*-ISSN: 2830-5906

photometric sensor frameworks have demonstrated how sensor integration and remote monitoring can enhance system efficiency and reliability [11]. Although previous research has demonstrated the potential of biometric authentication for enhancing vehicle and home security, gaps remain in the development of real-time, low-cost, and IoT-integrated fingerprint systems tailored specifically for motorcycles. Most studies have focused on broader applications such as cars, smart homes, or cloud service access, often overlooking the practical constraints and needs of two-wheeled vehicle users [12], [13]. Additionally, concerns regarding system vulnerability, user acceptance, and effective multimodal integration highlight the need for more secure and user-friendly implementations [14].

The research aims to design a secure motorcycle system that leverages IoT and biometric technology for enhanced real-time security and monitoring. The security system using a fingerprint sensor is integrated with a Telegram application. This system is expected to address the shortcomings of previous studies, such as improving the sensor's resilience to environmental factors and adding remote notification features for real-time monitoring.

## 2. METHOD

This research employs an experimental design to develop a motorcycle security system based on a fingerprint sensor integrated with the Telegram application. The research process begins with data collection through literature reviews and interviews to identify existing security issues and gather user requirements. Next, the system design is developed, including an algorithm for the authentication process, represented in pseudocode: initializing the fingerprint sensor, waiting for user input, and sending a notification to Telegram while unlocking the motorcycle upon successful fingerprint detection, or displaying an error message otherwise. Telegram is used for its ease of integration and general use. The implementation uses the ESP32 microcontroller to connect the sensor and the application. ESP32 is used in this study due to the processing capability and easy to develop built-in Wi-Fi. Testing is conducted under various conditions to evaluate the system's reliability and accuracy, focusing on fingerprint recognition success rates and notification delivery speed. The effectiveness of telegram notifications testing was conducted through interviews and surveys with potential users. The interviews involved 10 respondents, consisting of parking attendants and online motorcycle drivers

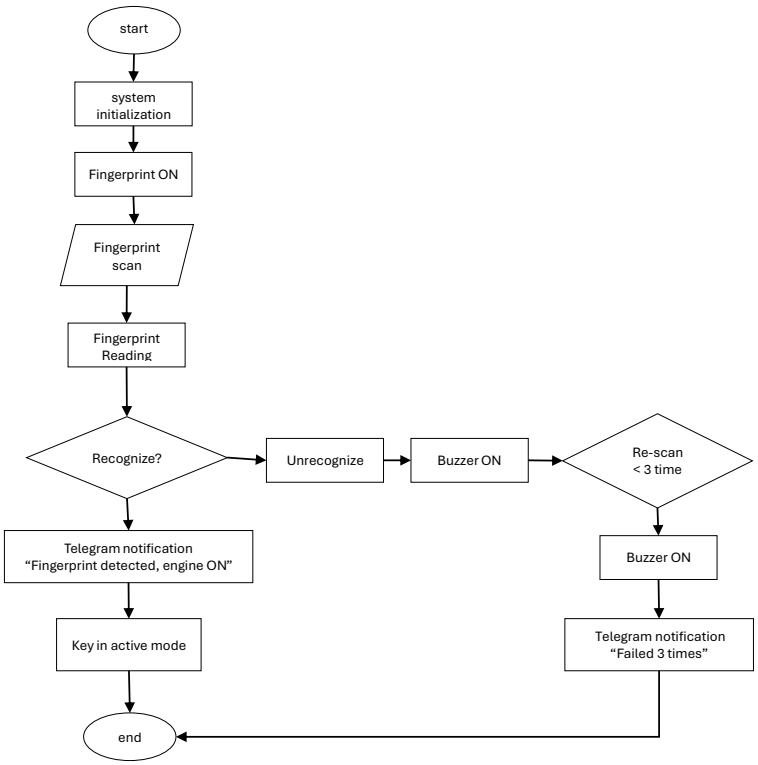



**Figure 1.** System Process Flowchart for IoT-Based Motorcycle Security

The flowchart in figure 1 describes a fingerprint-based engine ignition system. The process starts with system initialization, followed by turning on the fingerprint sensor. The user is prompted to scan their

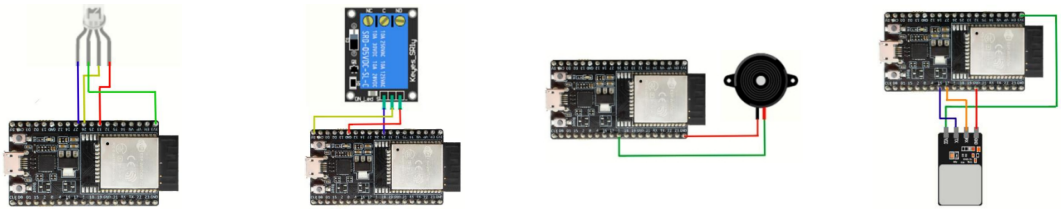
fingerprint, which is then read by the system. If the fingerprint is recognized, a Telegram notification is sent stating “Fingerprint detected, engine ON,” and the system enters active key mode to enable the engine. If the fingerprint is not recognized, a buzzer is activated, and the system checks if the number of scan attempts is less than three. If so, the user is allowed to retry. If the user fails three times in a row, the buzzer activates again, and a Telegram notification is sent with the message “Failed 3 times.” This flow ensures both secure access control and real-time failure alerts.

The hardware requirements for the fingerprint-based engine control system are implemented using several key components. First, a laptop with Intel Core i5-7200U, 8 GB RAM, Windows 10 Pro, is used for programming, configuration, and monitoring the system. Second, an Oppo A5 2020 smartphone with processor Snapdragon 665, 4 GB RAM, 128 GB storage serves as the medium for receiving notifications via Telegram. Third, an ESP32 development kit functions as the microcontroller, operating at 3.3V and supporting various digital and analogue I/O operations. It features 4 MB flash memory and runs at a clock speed of 240 MHz Next, a relay module is used to control power to the motorcycle's ignition system, capable of switching loads up to 250V AC or 30V DC at 10A. A fingerprint sensor in model R503 is employed for biometric authentication, offering capacitive sensing, a 200-fingerprint capacity, and communication via UART/TTL. For feedback and alerts, a 5V buzzer is integrated into the system. Finally, the Spykar F-2015 motorcycle operates as the output device, powered by a 12V battery and controlled through the relay based on fingerprint recognition results.

## 3. RESULTS AND DISCUSSION

### 3.1. Tool Design

Based on Figure 2a, there is a functional connection between the ESP32 input pins (number 26, 27, and 33) and the connected LEDs. Specifically, pin 27 of the ESP32 is linked to the red LED, meaning that when this pin is activated, the red LED will illuminate. Similarly, pin 26 is connected to the green LED, so activating this pin will turn on the green LED. Furthermore, pin 33 is associated with the blue LED, which will light upon activation. All these LED pins are connected to a 3V3 power source, providing the necessary voltage to enable LED operation. In figure 2b, the connection between the ESP32 and the relay is established through pin 25, which serves as the control signal for the relay. When pin 25 is activated, the signal is transmitted to the relay, prompting it to change its state, thereby switching the connected device on or off. The 5V power supply is connected to the relay's VCC pin, ensuring the necessary power for its operation. Additionally, the system's GND pin plays a crucial role in maintaining proper functionality. With this configuration, the ESP32 effectively controls the output through the relay. Figure 2c illustrates the connection between the ESP32 and the buzzer demonstrates how these components operate together within the system. The GND pin on the ESP32 serves as the grounding path, connecting to the negative (-) terminal of the buzzer, while pin 5 on the ESP32 functions as the output pin that links to the positive (+) terminal of the buzzer. When pin 5 is activated through programming, the buzzer receives sufficient electrical current to produce sound. The generated sound may serve various purposes, including alarms, notifications, or specific tones, depending on the application's requirements. Furthermore, the tone configuration of the buzzer can be modified by adjusting the frequency transmitted through pin 5 of the ESP32. This configuration is widely implemented in numerous IoT projects to develop effective alert systems. Figure 2d describes the connection between the ESP32 pins and the fingerprint module that defines their functional relationship within the system. The GND pin on the fingerprint module is connected to the GND pin on the ESP32, serving as the grounding path for the circuit. The 3V3 power supply is linked to the VCC pin on the fingerprint module, providing the necessary voltage for its operation. Additionally, pin 16 on the ESP32 is connected to the TX (transmit) pin of the fingerprint module, enabling data transmission from the ESP32 to the fingerprint sensor. Similarly, pin 17 functions as the RX (receive) pin, receiving data from the fingerprint module. This configuration facilitates serial communication between the ESP32 and the fingerprint module, allowing the ESP32 to send commands and process fingerprint data for authentication.



(a) (b) (c) (d)

**Figure 2.** schematic (a) LED, (b) relay, (c) Buzzer, (d) fingerprint

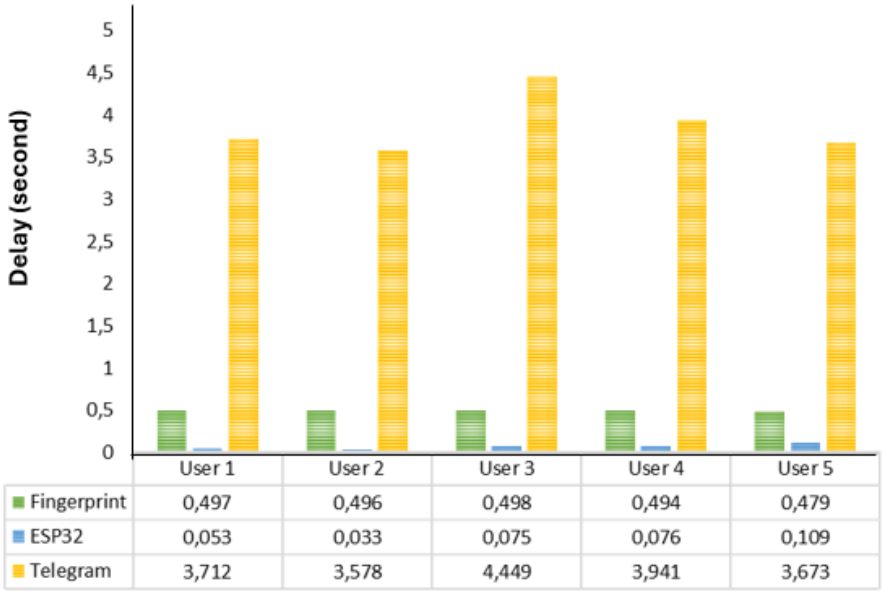
*e*-ISSN: 2830-5418, *p*-ISSN: 2830-5906

Based on the result, it can be concluded that all external components, namely the LED, relay, buzzer, and fingerprint sensor operate effectively in accordance with their designated functions. The ESP32 microcontroller serves as the central control unit, exhibiting reliable performance and the capability to manage multiple peripherals simultaneously, while maintaining stable power distribution and connectivity. These results indicate that the circuit configuration is functional and suitable for practical implementation.

### 3.2. Performance Testing Results

At the performance testing stage of the security system, delay measurement was the primary focus to assess how quickly the system responds to input and generates output. The system's delay was measured from fingerprint scanning to motor activation, as well as the time taken to send notifications to users. This analysis aims to ensure that the system operates within a specific time frame, which is crucial for maintaining security and user experience. In the context of IoT-based system development, response speed is a key element determining the operational success of the system. Based on previous studies and references, the ideal time standards for each component in this IoT security system are as follows:

- Fingerprint Sensor: Ideal detection time ≤ 1 second.
- ESP32 Microcontroller: Data processing time ≤ 0.5 seconds.
- Telegram Notification Transmission: Ideal delay ≤ 2 seconds for real-time communication.




| | User 1 | User 2 | User 3 | User 4 | User 5 |
|---|---|---|---|---|---|
| Fingerprint | 0,497 | 0,496 | 0,498 | 0,494 | 0,479 |
| ESP32 | 0,053 | 0,033 | 0,075 | 0,076 | 0,109 |
| Telegram | 3,712 | 3,578 | 4,449 | 3,941 | 3,673 |

**Figure 3.** Delay Comparison Graph for Each User

The fingerprint detection delay ranges from 0.479 seconds to 0.498 seconds, fully meeting the ideal standard of ≤1 second. Detection times across all users are highly consistent, with User 5 recording the fastest detection time at 0.479 seconds, while User 3 exhibited a slightly slower response at 0.498 seconds. Regarding data processing within the ESP32 component, performance remains highly efficient, with processing times ranging between 0.033 seconds and 0.109 seconds. User 2 achieved the fastest processing time at 0.033 seconds, whereas User 5 exhibited a slightly longer processing duration of 0.109 seconds. These results indicate that the ESP32 component operates optimally, with a delay time well below the standard threshold of ≤ 0.5 seconds. Meanwhile, the delay time for Telegram notification transmission exhibits a considerable range, between 3.578 seconds and 4.449 seconds. User 2 recorded the fastest transmission time at 3.578 seconds, whereas User 3 experienced the slowest transmission at 4.449 seconds. According to real-time communication standards, the ideal delay should be within ≤ 2 seconds. The higher delay observed can be attributed to several factors, primarily the instability of the internet connection. Therefore, further optimization of the system is required to enhance notification transmission efficiency and align with real-time communication standards.

Overall, this security system demonstrates very good performance, especially in local components such as the Fingerprint and ESP32, which have small and consistent delay times across all tests. Compared to previous research, this system has met or even exceeded the established ideal time standards. However, the delay in sending notifications via Telegram can still be further improved to achieve more consistent and

efficient times under various conditions. With high performance in response speed and efficiency. Notification delivery this system is suitable to be implemented as an IoT-based security solution, with room for improvement in the notification delivery components.

### 3.2.1. Accuracy Level Testing

This test aims to evaluate the accuracy level of the fingerprint system used as a security system mechanism. In this test, it was conducted by 5 users who performed 20 trials each. The following test results can be seen in Table 1. Based on testing conducted with five participants, each performing 20 trials, the fingerprint sensor demonstrated reliable performance. The sensor achieved an accuracy rate of 98%, with no instances of misidentification or cross-recognition between User 1 and other participants. These findings indicate that the fingerprint sensor operates with a high degree of precision. Moreover, the 98% accuracy rate positions the sensor as a competitive and dependable biometric authentication tool when compared to results reported in previous studies.

**Table 1.** Accuracy Level Testing

| No | User | Test No. | | | | | | | | | | | | | | | | | | | | Error |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | (%) |
| 1 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 0 |
| 2 | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 0 |
| 3 | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 0 |
| 4 | 4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 5 |
| 5 | 5 | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 5 |

### 3.2.2. Buzzer Testing

This test was conducted to determine how the buzzer responds when an unregistered fingerprint attempts to access this system. Each user performed 3 trials. The results of the buzzer testing can be seen in Table 2.

**Table 2.** Unregistered Fingerprint Buzzer Detection Testing

| No | User | Unregistered Fingerprints | Trial Number | Ringing/ No Ringing | Time (s) |
|---|---|---|---|---|---|
| 1 | 1 | Right Thumb | 1 | Ringing | 00,67 |
| | | | 2 | Ringing | 00,55 |
| | | | 3 | Ringing | 02,33 |
| 2 | 2 | Right Index Finger | 1 | Ringing | 00,58 |
| | | | 2 | Ringing | 00,68 |
| | | | 3 | Ringing | 02,86 |
| 3 | 3 | Right Middle Finger | 1 | Ringing | 00,66 |
| | | | 2 | Ringing | 00,53 |
| | | | 3 | Ringing | 02,70 |
| 4 | 4 | Left Thumb | 1 | Ringing | 00,56 |
| | | | 2 | Ringing | 00,62 |
| | | | 3 | Ringing | 02,94 |
| 5 | 5 | Left Index Finger | 1 | Ringing | 00,47 |
| | | | 2 | Ringing | 00,43 |
| | | | 3 | Ringing | 02,90 |

Table 2 shows that the buzzer detection system works according to the design. In the first and second trials, when an unregistered fingerprint was detected, the buzzer sounded, indicating that the system did not provide excessive audio warnings. However, in the third trial, after two consecutive failed attempts, the buzzer sounded longer than in the first and second trials, providing a clear signal that access was denied. This system is designed to provide clear and sufficient warnings to users after three failed attempts, increasing user awareness of authentication status and avoiding disturbances from the buzzer sounding too frequently. Thus, the buzzer functions effectively to enhance system security through context-appropriate audio feedback during authentication trials.

*e*-ISSN: 2830-5418, *p*-ISSN: 2830-5906

### 3.2.3. Power Consumption Calculation

In the power consumption calculation test, it was conducted to determine the consumption. Energy Used by the System During Idle and Active Conditions.

**Table 3.** Power Consumption Calculation.

| No | Condition | Voltage (V) | Current (A) | power (W) | Time (Minute) | Energy (Wh) |
|---|---|---|---|---|---|---|
| 1 | Idle | 3.25 | 0,27 | 0,8775 | 1 | 0.014625 |
| 2 | Used | 3.3 | 0,57 | 1,881 | 1 | 0.03135 |

Table 3 shows that in idle condition, the system voltage is 3.25 V, with an average current of 0.27 A, resulting in a power consumption of 0.8775 W per minute. The total energy used for 1 minute is 0.014625 Wh. When in use, the voltage increases to 3.3 V, with an average current of 0.57 A, resulting in a power consumption of 1.881 W per minute. The total energy used for 1 minute is 0.03135 Wh.

### 3.2.4. Effectiveness Of Telegram Notifications

Testing was conducted through interviews and surveys with potential users. The interviews involved 10 respondents, consisting of parking attendants and online motorcycle drivers. The results show that most respondents (90%) consider mobile-based technology very important in daily life, while 70% consider digital security very crucial. Regarding acceptance of the Telegram-based security system, 60% of respondents stated they agree to use it, while 40% strongly agree. The main factors supporting this acceptance are security aspects, flexibility, and ease of access.

In a survey on the use of this system, 60% of respondents admitted to frequently using vehicle security technology, while 80% strongly agree with the existence of this system. However, there are challenges in notification speed, where 90% of respondents rated notifications as having a delay of 3 to 5 seconds, while 10% stated more than 5 seconds. This factor can be associated with the ESP32 internet connection affecting real-time message delivery. Many respondents (70%) rated this system as easy to use, while 30% considered it very easy. However, 30% of respondents experienced slight difficulties in understanding the Telegram interface as the main medium of this security system. This indicates the need for further education regarding the use of the Telegram application in motorcycle security systems.

From the aspect of notification acceptance, 50% of respondents sometimes experience difficulties in receiving or responding to notifications, while 30% do not experience difficulties. Network connectivity factors contribute to this delay. Overall, 90% of respondents feel satisfied with this system. With a high satisfaction level, the fingerprint and Telegram-based security system has great potential to be implemented as a modern and efficient vehicle security solution.

### 3.2.5. Analysis Of Field Test Results

This field test was conducted to evaluate the reliability of the fingerprint sensor-based motorcycle security system under actual operational conditions. The 1st test started at 12 PM until it ended on the 3rd day at 12 PM, with data conducted every 6 hours. The parameters observed in this test include sensor status (functioning or not) and vehicle status (safe or missing). The main objective of the test is to ensure the stability of the system in various environmental conditions and to measure its effectiveness in preventing unauthorized access. Based on the test results obtained, data can be seen in Table 4 as follows:

**Table 4.** Field Test Results.

| No | Day, Time | Sensor (Work/ not work) | Motorcycle (Safe/Lost) |
|---|---|---|---|
| 1 | 1st day, 12:00 PM | Work | Safe |
| 2 | 1st day, 18:00 PM | Work | Safe |
| 3 | 2nd day, 00:00 AM | Work | Safe |
| 4 | 2nd day, 06:00 AM | Work | Safe |
| 5 | 2nd day, 12:00 PM | Work | Safe |
| 6 | 2nd day, 18:00 PM | Work | Safe |
| 7 | 3rd day, 00:00 AM | Work | Safe |
| 8 | 3rd day, 06:00 AM | Work | Safe |
| 9 | 3rd day, 12:00 PM | Work | Safe |

Based on the test results listed in Table 4, the fingerprint sensor functions well in each testing session without experiencing failure. During the testing period, the security system showed stable and consistent performance in reading and verifying user fingerprints. In addition, no cases of lost vehicles were found, indicating that this system can provide optimal protection for motorcycles. The high reliability of the sensor also shows that this device works efficiently and responsively without experiencing technical disruptions.

## 4. CONCLUSION

Based on the research conducted on the Motorcycle Security System Prototype, it can be concluded that:

1. The motorcycle security system using the R503 fingerprint sensor, ESP32 microcontroller, and relay module has been successfully designed to detect valid and invalid fingerprints. This system has potential for integration into smart vehicles ecosystems, offering a scalable, real-time security solution.
2. The performance of the fingerprint-based security system shows an accuracy level of 98%, with an average delay time of 2.5 seconds from fingerprint scanning to the motorcycle being active. In addition, the system has low power consumption, which is 0.014625 Wh in idle conditions and 0.03135 Wh when the system is operated, making it efficient for use in motor vehicle applications.
3. The effectiveness of notifications through the Telegram application has been tested and shows high reliability in providing authentication information in real-time. Notifications were successfully sent with an average delivery time of 3 seconds, and include information on authentication success, unauthorized access attempts, and the overall system status. Thus, this feature allows users to monitor vehicle security directly and take quick action in suspicious situations.
4. For future work, the system can be enhanced by integrating facial recognition technology or implementing multi-factor authentication methods, such as combining fingerprint scanning with PIN codes or smartphone verification, to provide a higher level of security and prevent unauthorized access more effectively.

## ACKNOWLEDGEMENTS

The author thanks the robotic laboratory of Jakarta Global University for the facilities provided for this research.

## REFERENCES

[1] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "BioSec: A Biometric Authentication Framework for Secure and Private Communication Among Edge Devices in IoT and Industry 4.0," *IEEE Consum. Electron. Mag.*, vol. 11, no. 2, pp. 51–56, Mar. 2022, doi: 10.1109/MCE.2020.3038040.

[2] S. C. Dass, "Fingerprint-Based Recognition," *Int. Stat. Rev.*, vol. 81, no. 2, pp. 175–187, Aug. 2013, doi: 10.1111/insr.12017.

[3] A. ARAKALA, "SECURE AND PRIVATE FINGERPRINT-BASED AUTHENTICATION," *Bull. Aust. Math. Soc.*, vol. 80, no. 2, pp. 347–349, Oct. 2009, doi: 10.1017/S0004972709000665.

[4] W. Yang, S. Wang, K. Yu, J. J. Kang, and M. N. Johnstone, "Secure Fingerprint Authentication with Homomorphic Encryption," in *2020 Digital Image Computing: Techniques and Applications (DICTA)*, IEEE, Nov. 2020, pp. 1–6. doi: 10.1109/DICTA51227.2020.9363426.

[5] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis," 2005, pp. 265–272. doi: 10.1007/11608288_36.

[6] S. Alsharif, A. El-Saba, and R. Stripathi, "Improving the recognition of fingerprint biometric system using enhanced image fusion," S. S. Agaian and S. A. Jassim, Eds., Apr. 2010, p. 77080D. doi: 10.1117/12.853061.

[7] P. Rivandi, A. Winda, D. Satrio, and M. I. Solihin, "Automotive Start–Stop Engine Based on Fingerprint Recognition System," *E3S Web Conf.*, vol. 130, p. 01022, Nov. 2019, doi: 10.1051/e3sconf/201913001022.

[8] Z. Brijet, B. S. Kumar, and N. Bharathi, "Vehicle Anti-Theft System Using Fingerprint Recognition Technique," *Open Acad. J. Adv. Sci. Technol.*, vol. 1, no. 1, pp. 36–41, 2017, doi: 10.33094/5.2017.11.36.41.

[9] A. A. N. A. Nusantar, I. A. E. Zaeni, and D. Lestari, "Home Energy Security Prototype using Microcontroller Based on Fingerprint Sensor," *Front. Energy Syst. Power Eng.*, vol. 1, no. 2, p. 19, Jul. 2019, doi: 10.17977/um049v1i2p19-29.

[10] C. Chen, C. Lee, and C. Hsu, "Mobile device integration of a fingerprint biometric remote authentication scheme," *Int. J. Commun. Syst.*, vol. 25, no. 5, pp. 585–597, May 2012, doi: 10.1002/dac.1277.

[11] R. R. Al Hakim *et al.*, "IoT-based pesticide distribution control system with photometric sensor frameworkIoT-based pesticide distribution control system with photometric sensor framework," *J. Glob. Eng. Res. Sci.*, vol. 1, no. 2, Aug. 2024, doi: 10.56904/jgers.v1i2.23.

[12] N. Kiruthiga, L. Latha, and S. Thangasamy, "Real Time Biometrics Based Vehicle Security System with GPS and GSM Technology," *Procedia Comput. Sci.*, vol. 47, pp. 471–479, 2015, doi: 10.1016/j.procs.2015.03.231.

[13] P. Ruiu, G. Caragnano, G. L. Masala, and E. Grosso, "Accessing Cloud Services through Biometrics Authentication," in *2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, IEEE, Jul. 2016, pp. 38–43. doi: 10.1109/CISIS.2016.76.

[14] Z. Wu, J. Yang, J. Zhang, and H. Yue, "Multibiometric Fusion Authentication in Wireless Multimedia Environment Using Dynamic Bayesian Method," *Secur. Commun. Networks*, vol. 2018, pp. 1–12, Nov. 2018, doi: 10.1155/2018/5783976.