

IoT-Based Smart Door Lock Design for Multi-Stage Locking in Sterilization Rooms

Muhammad Danny Setiawan^{1*}, Miftahur Rohman².

^{1,2} Department of Electrical Engineering, Faculty of Engineering, Universitas Negeri Surabaya
A5 Building Ketintang Campus, Surabaya, 60231, Indonesia

Email: ¹muhammaddanny.21011@mhs.unesa.ac.id, ²miftahurrohman@unesa.ac.id

Abstract –This research presents the design and development of an Internet of Things (IoT)-based Smart Door Lock system implemented in a sterilization room with a step-by-step locking mechanism. The system is designed to improve security and ensure that sterilization procedures are carried out according to standards, where doors can only be accessed sequentially as predetermined. The hardware consists of an ESP32 microcontroller connected to a fingerprint sensor for user authentication and a solenoid door lock as the door actuator. The system is also integrated with an IoT-based server, enabling real-time monitoring of door status through a mobile application. Experimental results show that the system functions properly, allowing doors to open only according to the specified sequence, while access data can be stored and monitored online. Therefore, this Smart Door Lock system provides an effective solution to support both security and operational efficiency in sterilization rooms.

Keywords: Smart Door Lock, IoT, ESP32, sterilization room, step-by-step locking.

I. INTRODUCTION

Doors are the main route used to enter and exit a room. Through doors, access to a room can be controlled with the help of a locking system. In general, the locking system used today is still conventional, consisting of a physical key, which is widely used in homes, warehouses, and buildings. However, this traditional method has limitations in terms of additional security, such as the lack of the ability to record who has accessed the door or how often the door is used [1]. Along with technological developments, especially in the field of industrial electronics, innovations such as smart door locks have emerged. These systems allow digital locking and unlocking with higher security levels and can be integrated with the Internet of Things (IoT) for real-time monitoring and control [2].

In production environments that require sterile conditions, such as cleanrooms, access control becomes more critical. The two-door system is commonly implemented to prevent outside air from directly entering sterile rooms. However, in practice, violations often occur due to human negligence, such as opening both doors simultaneously, which increases the risk of contamination [3]. In addition, the absence of an integrated security system still allows unauthorized access.

Several previous studies have examined smart door lock designs with multi-sensor integration [4]. developed a

prototype using RFID, keypad, and magnetic switch sensors, while [5] designed a system with fingerprint, keypad PIN, and RFID modules. These studies show that smart door locks can provide higher security compared to conventional systems, but their application in sterile room environments has not been widely explored.

Based on these considerations, this research proposes the design of a smart door lock system with a staged locking mechanism integrated with IoT technology. The system is built using an ESP32 microcontroller as the main controller, supported by fingerprint sensors and keypad for dual authentication, PIR sensors for sterilization activation, and buzzer alarms. The two-door sequential mechanism is implemented to maintain sterile conditions, while data integration with cloud services (Google Spreadsheet) and notification via Telegram enables real-time monitoring. This design is expected to improve the accuracy, efficiency, and security of access control in sterile production rooms.

II. METHODS

The research method applied in this study is Research and Development (R&D) based on the Sugiyono model with a design-based approach. This method was chosen because the study aims to produce a product in the form of an IoT-based smart door lock system with a staged locking mechanism for sterile rooms, as well as to improve previous studies on multi-

sensor locking systems. R&D serves as a bridge between basic research and applied research, enabling the development of innovative and applicable products. In this study, the developed system integrates IoT technology to allow real-time monitoring of door locking status and to automatically store user access data in a database. The recorded data can then be used for further analysis and evaluation of system performance.

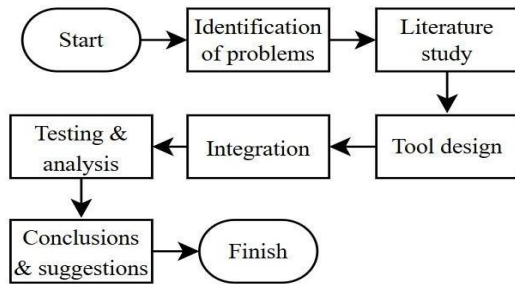


Figure 1 Research Flowchart

In Figure 1, a flowchart illustrates the stages of the research process from beginning to end, starting with problem identification and ending with the preparation of conclusions and recommendations. The research must follow the sequence outlined in the diagram to ensure it runs in a systematic and well-structured manner. This study was conducted during the even semester of the 2024/2025 academic year, while the collection of reference materials took place in the odd semester of the same academic year. The research activities were carried out in Building A8, at the Microprocessor Laboratory, which was selected as the location because it provides complete facilities to support the design and development of the research tools.

Hardware Design System

In Figure 3.2, the design of the IoT-based smart door lock system is presented, where the selection of each hardware component is carried out by considering performance, reliability, and ease of integration. The ESP32 microcontroller is used as the main controller because it is equipped with Wi-Fi and Bluetooth connectivity, a dual-core processor, and multiple GPIO pins that support a variety of input and output functions, making it highly suitable for IoT applications. The fingerprint sensor is employed as the primary authentication method due to its ability to provide accurate and real-time user identification, while the 4x4 keypad functions as an additional authentication method for PIN input and access control. A buzzer is integrated into the system as an audio feedback indicator to notify the success or failure of the authentication process.

To maintain the sterile condition of the room, a humidifier is included as a sterilization device that can be automatically activated when user presence is detected by the PIR sensor. The PIR sensor plays an important role in motion detection and is directly connected to the ESP32 to trigger the sterilization process. A relay module is used as an electronic switch to

control high-voltage devices, such as the solenoid door lock and humidifier, while maintaining safe isolation from the microcontroller. For cloud-based data management, Google Spreadsheet is employed as the storage medium, which is integrated through Google App Script to enable real-time recording and monitoring of access activities. This combination of hardware and software components ensures that the system operates comprehensively, providing a reliable and efficient IoT-based access control solution for sterile environments.

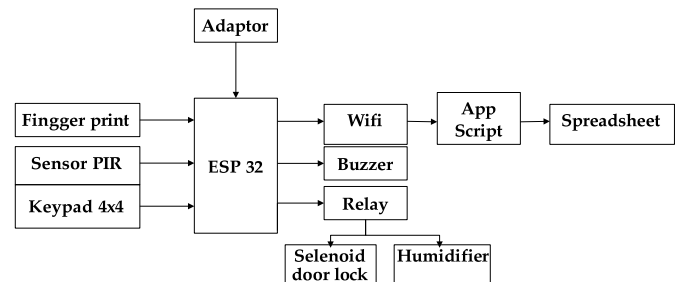


Figure 2 System block diagram

At this stage, the designed hardware and software are implemented into a single integrated operational system. The goal of this integration is to ensure that every component, both hardware and software, operates in a synchronized and efficient manner. The process involves hardware assembly, software configuration, internet network setup, and the integration of several components, including the ESP32 microcontroller, fingerprint sensor, 4x4 keypad, buzzer, solenoid door lock, PIR sensor, and humidifier, along with supporting platforms such as Google Sheets and Google App Script. The circuit schematic of the hardware system is illustrated in the following figure.

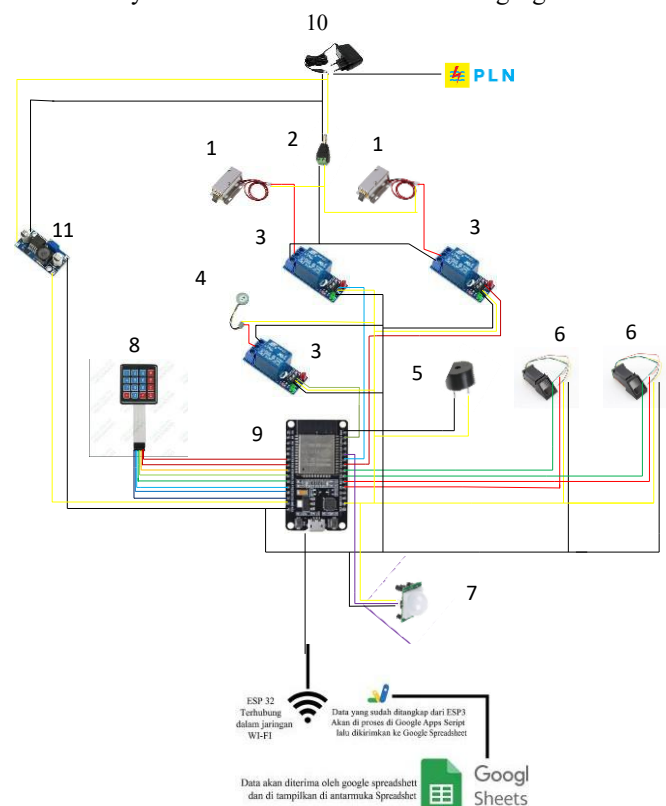


Figure 3 Wiring designing hardware

Software Design System

In Figure 4 presents the software flowchart of the Smart Door Lock system implementing a step-by-step locking method to regulate entry and exit in the sterilization and production rooms which describe in figure 5. The system utilizes biometric authentication (fingerprint), keypad, PIR sensor, and humidifier, all of which are integrated with a cloud-based automatic logging platform (Google Spreadsheet).

For entry access, users must authenticate via Fingerprint 1 or the keypad. If authentication fails, the buzzer emits an intermittent tone and access is denied. If successful, the buzzer emits a long tone, the sterilization room door opens, and the PIR sensor detects user presence. Once detected, the humidifier is activated for 5 seconds as part of the air sterilization protocol before the production room door unlocks. All activities are automatically recorded in Google Spreadsheet.

For exit access, authentication is performed via Fingerprint 2 in the production room. If authentication fails, the buzzer emits an intermittent tone and exit access is denied. If successful, the buzzer emits a long tone, the production room door unlocks first, followed by the sterilization room door. This activity is also logged automatically into Google Spreadsheet.

The step-by-step locking method ensures that only one door can be opened at a time, thereby enhancing security and maintaining the integrity of the sterile environment. The entire process operates automatically, in an integrated manner, and in real time.

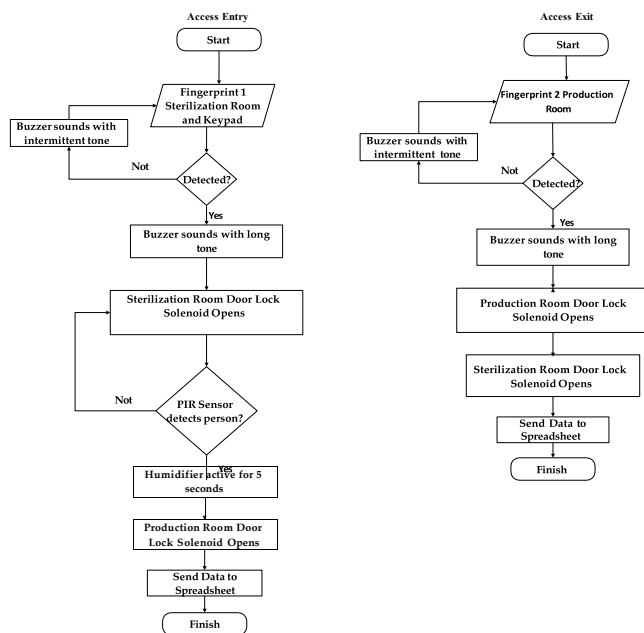


Figure 4 Programming Flowchart



Figure 5 Step-by-Step Locking Smart Door Lock System

III. RESULT AND DISCUSSION

Fingerprint Testing

Based on the test results presented in Table 1, all fingerprint data were successfully detected by the fingerprint sensor, achieving a 100% recognition rate. However, when assessed in terms of reading quality, only 16 out of 20 trials produced a confidence value of ≥ 70 . Thus, the effective quality success rate can be considered 80%, indicating that although the sensor is able to capture all fingerprint data, the reliability of the recognition process still depends on the confidence value obtained.

Table 1 Testing fingerprint confidence value

| Testing No. | ID Fingerprint | Status | Fingerprint | Confidence | Notes |
|-------------|----------------|----------|-------------|------------|----------------|
| 1 | 1 | Detected | Inner Door | 84 | Successful |
| 2 | 2 | Detected | Inner door | 82 | Successful |
| 3 | 3 | Detected | Inner door | 102 | Successful |
| 4 | 4 | Detected | Inner door | 89 | Successful |
| 5 | 5 | Detected | Inner door | 53 | Low confidence |
| 6 | 1 | Detected | Outer door | 81 | Successful |
| 7 | 2 | Detected | Outer door | 93 | Successful |
| 8 | 3 | Detected | Outer door | 67 | Successful |
| 9 | 4 | Detected | Outer door | 93 | Successful |
| 10 | 5 | Detected | Outer door | 144 | Successful |
| 11 | 6 | Detected | Inner door | 212 | Successful |
| 12 | 7 | Detected | Inner door | 129 | Successful |
| 13 | 8 | Detected | Inner door | 124 | Successful |
| 14 | 9 | Detected | Inner door | 97 | Successful |
| 15 | 10 | Detected | Inner door | 74 | Successful |
| 16 | 6 | Detected | Outer door | 244 | Successful |
| 17 | 7 | Detected | Outer door | 140 | Successful |
| 18 | 8 | Detected | Outer door | 52 | Low confidence |
| 19 | 9 | Detected | Outer door | 53 | Low confidence |
| 20 | 10 | Detected | Outer door | 63 | Low confidence |

The confidence values obtained during testing ranged from 52 to 244, which reflects the sensor's certainty level in matching fingerprint data with the stored template. This variation is influenced by several factors, including finger placement position, applied pressure during contact with the sensor, cleanliness of both the finger and sensor surface, as well as the quality of the initial fingerprint enrollment.

The analysis yielded a mean confidence value of 103.8, which indicates that, in general, the sensor demonstrates a relatively high level of certainty. Nevertheless, the standard deviation of 50.77 reveals considerable variability in the data relative to the mean. This suggests that while the sensor is effective in reading fingerprints, the reading quality is not yet fully consistent across all trials.

These findings emphasize the importance of considering both recognition rate and confidence stability when evaluating biometric systems, particularly for applications requiring high

levels of security and reliability [6].

Table 2 Fingerprint testing positions

| Fingerprint Position | status | confidence |
|-------------------------|---------------------------|------------|
| Finger Straight 0° | Detected | 112 |
| | Detected | 129 |
| | Detected | 166 |
| | Detected | 110 |
| | Detected | 180 |
| Finger Facing Right 90° | Detected (low confidence) | 55 |
| | Detected (low confidence) | 54 |
| | Detected (low confidence) | 74 |
| | Detected (low confidence) | 59 |
| | Detected (low confidence) | 52 |
| Finger Facing Down 180° | Detected (low confidence) | 52 |
| | Detected (low confidence) | 65 |
| | Detected (low confidence) | 61 |
| | Detected (low confidence) | 58 |
| | Detected | 73 |

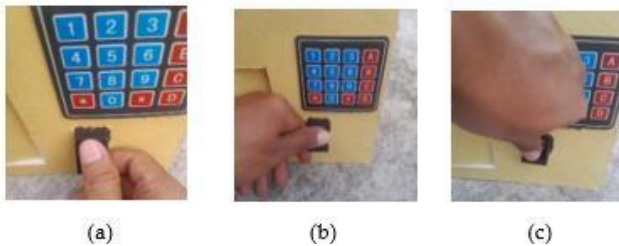


Figure 6 Fingerprint Testing with positions

Table 4.2 presents 15 fingerprint tests using the author's thumb with three sensor orientations. The results show that confidence values decrease as the finger rotation angle increases. The straight parallel position (0°) yielded the highest confidence (110–180, mean 139.4), making it the most optimal orientation. In contrast, the right-facing (90°) and downward-facing (180°) positions produced much lower confidence values (means of 58.8 and 61.8, respectively). These findings indicate that larger rotation angles reduce the sensor's ability to capture fingerprint ridge and valley patterns accurately, with the straight orientation (0°) recommended for optimal performance.

Based on the test results in Table 3, nine trials were conducted using the author's thumb under three surface conditions: wet, dusty, and clean. The results indicate that finger surface conditions significantly affect both reading success and confidence values. Out of nine trials, only six were successfully detected, giving a total success rate of 66.7%. The overall mean confidence value was 57.0 with a standard deviation of 50.75, indicating a wide data spread and inconsistent readings. These findings suggest that finger cleanliness is a key factor in biometric system accuracy, where wet conditions often cause detection failure, dusty conditions

reduce confidence quality, and clean fingers are recommended to achieve optimal results.

Table 3 Fingerprint Testing under Different Fingerprint Conditions

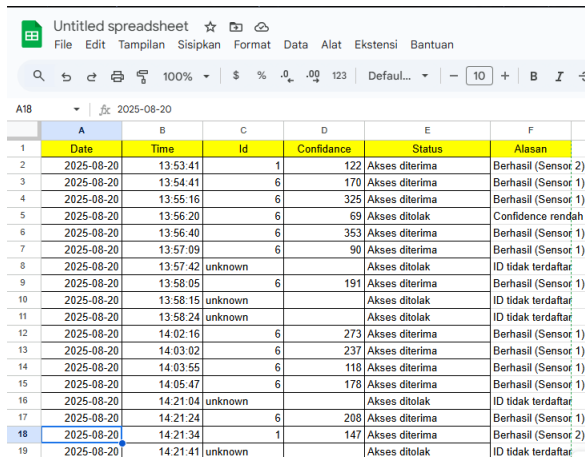
| Fingerprint Condition | Status | confidence |
|-----------------------|---------------------------|------------|
| Wet | Not Detected | - |
| Wet | Not Detected | - |
| Wet | Not Detected | - |
| Dusty | Detected (low confidence) | 56 |
| Dusty | Detected (low confidence) | 42 |
| Dusty | Detected (low confidence) | 50 |
| Clean | Detected | 120 |
| Clean | Detected | 105 |
| Clean | Detected | 140 |

Table 4 Testing of Data Transmission

| Experiment No. | Fingerprint User ID | Data Status | Data Transmission Time (s) |
|----------------|---------------------|-------------|----------------------------|
| 1 | Id 1 | Sent | 3,67 |
| 2 | Id 2 | Sent | 3,55 |
| 3 | Id 3 | Sent | 3,49 |
| 4 | Id 4 | Sent | 4,14 |
| 5 | Id 5 | Sent | 4,27 |
| 6 | Id 1 | Sent | 5,51 |
| 7 | Id 2 | Sent | 3,3 |
| 8 | Id 3 | Sent | 3,94 |
| 9 | Id 4 | Sent | 4,8 |
| 10 | Id 5 | Sent | 4,47 |
| 11 | Id 6 | Sent | 5,45 |
| 12 | Id 7 | Sent | 3,88 |
| 13 | Id 8 | Sent | 3,69 |
| 14 | Id 9 | Sent | 3,88 |
| 15 | Id 10 | Sent | 3,96 |
| 16 | Id 6 | Sent | 5,26 |
| 17 | Id 7 | Sent | 5,05 |
| 18 | Id 8 | Sent | 3,75 |
| 19 | Id 9 | Sent | 4,8 |
| 20 | Id 10 | Sent | 4 |

Based on the test results in Table 4, all trials showed that data were successfully transmitted with complete status, with delivery times ranging from 3.30 seconds to 5.51 seconds. The fastest transmission was recorded in trial 7 at 3.30 seconds, indicating efficient system performance under stable network

conditions. The longest time, 5.51 seconds, was likely caused by network fluctuations during testing. The average transmission time to Google Spreadsheet was 4.24 seconds, with a standard deviation of 0.68 seconds, suggesting relatively small variation and stable system performance. Overall, the system achieved a 100% success rate in data transmission, demonstrating high reliability and effective hardware–software integration under normal network conditions.



| | A | B | C | D | E | F |
|----|------------|----------|---------|------------|----------------|---------------------|
| | Date | Time | Id | Confidence | Status | Alasan |
| 1 | 2025-08-20 | 13:53:41 | 1 | 122 | Akses diterima | Berhasil (Sensor 2) |
| 2 | 2025-08-20 | 13:54:41 | 6 | 170 | Akses diterima | Berhasil (Sensor 1) |
| 3 | 2025-08-20 | 13:55:16 | 6 | 325 | Akses diterima | Berhasil (Sensor 1) |
| 4 | 2025-08-20 | 13:56:20 | 6 | 69 | Akses ditolak | Confidence rendah |
| 5 | 2025-08-20 | 13:56:40 | 6 | 353 | Akses diterima | Berhasil (Sensor 1) |
| 6 | 2025-08-20 | 13:57:09 | 6 | 90 | Akses diterima | Berhasil (Sensor 1) |
| 7 | 2025-08-20 | 13:57:42 | unknown | | Akses ditolak | ID tidak terdaftar |
| 8 | 2025-08-20 | 13:58:05 | 6 | 191 | Akses diterima | Berhasil (Sensor 1) |
| 9 | 2025-08-20 | 13:58:15 | unknown | | Akses ditolak | ID tidak terdaftar |
| 10 | 2025-08-20 | 13:58:24 | unknown | | Akses ditolak | ID tidak terdaftar |
| 11 | 2025-08-20 | 14:02:16 | 6 | 273 | Akses diterima | Berhasil (Sensor 1) |
| 12 | 2025-08-20 | 14:03:02 | 6 | 237 | Akses diterima | Berhasil (Sensor 1) |
| 13 | 2025-08-20 | 14:03:55 | 6 | 118 | Akses diterima | Berhasil (Sensor 1) |
| 14 | 2025-08-20 | 14:05:47 | 6 | 178 | Akses diterima | Berhasil (Sensor 1) |
| 15 | 2025-08-20 | 14:21:04 | unknown | | Akses ditolak | ID tidak terdaftar |
| 16 | 2025-08-20 | 14:21:24 | 6 | 208 | Akses diterima | Berhasil (Sensor 1) |
| 17 | 2025-08-20 | 14:21:34 | 1 | 147 | Akses diterima | Berhasil (Sensor 2) |
| 18 | 2025-08-20 | 14:21:41 | unknown | | Akses ditolak | ID tidak terdaftar |

Figure 7 Data in the spreadsheet

Figure 7 shows the data logging system stored in Google Spreadsheet. The spreadsheet records important information in real time, including the date, time, user ID, confidence value, access status, and reason. This automated data recording feature ensures that every access activity, whether accepted or rejected, is documented accurately for further monitoring and analysis.

IV. CONCLUSION

This research successfully developed an IoT-based smart door lock with a stepwise locking mechanism, integrating fingerprint and keypad authentication, real-time data storage using Google Spreadsheet, and ESP32 connectivity. The system achieved a 100% fingerprint recognition rate, with an effective reliability of 80% due to variations in finger position, pressure, and sensor cleanliness. Data transmission testing confirmed system stability, with an average delay of 4.24 seconds, demonstrating fast and responsive performance.

Despite these promising results, the system still presents limitations. The fingerprint recognition reliability shows significant variance, as indicated by a high standard deviation, suggesting the need for further optimization in sensor calibration and algorithm robustness. In addition, reliance on Google Spreadsheet as the primary database may pose scalability and security challenges in real-world applications. Future studies are recommended to integrate more secure and scalable cloud platforms, enhance multi-factor authentication, and expand the system's adaptability for broader industrial and institutional use.

ACKNOWLEDGMENT

The author sincerely extends gratitude to Miftahur Rohman, S.T., M.T., for the valuable guidance, insightful feedback, and encouragement provided throughout the research and completion of this work. Appreciation is also expressed to all lecturers and staff of the Electrical Engineering Department for their knowledge and support during the academic journey. The author would also like to convey heartfelt thanks to family, friends, and especially to dear friend GAN, for their continuous encouragement, support, and prayers that have greatly contributed to the completion of this study.

REFERENCES

- [1] D. Adidrana, H. Suryoprago, dan A. R. Hakim, "Perancangan Sistem Smart Door Lock Menggunakan Internet of Things (Studi Kasus: Institut Teknologi Telkom Jakarta)," *J. Informatics Commun. Technol.*, vol. 4, no. 2, hal. 102–108, 2023.
- [2] I. Maulana, E. Azriadi, dan J. Musrido, "Rancang Bangun Sistem Smart Door Lock Menggunakan Mikrokontroler Esp32 Berbasis Internet Of Things (Iot) dan Smartphone Android," *J. Tek. Ind. Terintegrasi*, vol. 6, no. 1, hal. 195–208, 2023.
- [3] F. F. Iman, "Purwarupa Iman, F. F. (2017). Purwarupa Smlman, F. F. (2017). Purwarupa Iman, F. F. (2017). Purwarupa Smart Door Lock Menggunakan Multi Sensor Berbasis Sistem Arduino. Fakultas Teknologi Informasi Dan Elektro Universitas Teknologi Yogyakarta, 1–7.Smart Doo," *Fak. Teknol. Inf. dan Elektro Universitas Teknol. Yogyakarta*, hal. 1–7, 2017.
- [4] Abdul Hakim Prima Yuniarto, Y. Lestiyanti, M. F. Asrori, N. Laela, dan A. Nurcholis, "Perancangan Smart Door Lock System dengan Multi Sensor untuk Sistem Keamanan Rumah," *Techné J. Ilm. Elektrotek.*, vol. 22, no. 2, hal. 333–342, 2023.
- [5] S. Wahyuning, *Dasa-Dasar Statistik*, Yayasan Prima Agus Teknik, Semarang. 2021.
- [6] A. H. P. Yuniarto, Y. Lestiyanti, M. F. Asrori, N. Laela, dan A. Nurcholis, "Perancangan Smart Door Lock System dengan Multi Sensor untuk Sistem Keamanan Rumah," *Techné Jurnal Ilmiah Elektroteknika*, vol. 22, no. 2, pp. 333–342, 2023.
- [7] R. Husein, "Rancang Bangun Smart Door Lock Menggunakan ESP32-CAM sebagai Monitoring Keamanan Berbasis IoT pada Ruang Dosen Laboratorium Elektronika," *Politeknik Negeri Sriwijaya*, 2023.
- [8] M. Derbali., "Toward Secure Door Lock System: Development IoT Smart Door Lock Device," *Authorea Prepr.*, 2023.
- [9] M. Melinda, "Smart Door Locking System for Children Using HC-SR04 and IoT Integration," *J. Nas. Tek. Elektro*, vol. 14, no. 2, pp. 1293, 2025.
- [10] A. H. P. Yuniarto, Y. Lestiyanti, M. F. Asrori, N. Laela, dan A. Nurcholis, "Perancangan Smart Door Lock System dengan Multi Sensor untuk Sistem Keamanan Rumah," *Techné J. Ilm. Elektrotek.*, vol. 22, no. 2, pp. 333–342, 2023.
- [11] R. F. Rizky et al., "Sistem Smart Door Lock Menggunakan Voice Recognition Berbasis Arduino," *BIT J. Ilm. Teknol. Inf. dan Komput.*, vol. 6, no. 3, 2023.