Automatic Locking System for Locker at Brail Stores

Rifqi Amalya Fatekha S.ST., MTR.T.[1] Selvia Nabila Nurhayati[1]

[1]Jurusan Teknik Elektro, Prodi Teknik Rekayasa Elektronika, Politeknik Negeri Batam, Batam, Indonesia

[*]Email: sselvianabilanurhayati@gmail.com

Received on 14-01-2026 | *Revised on 14-01-2026*

***Abstract*— This research develops an automatic locking system using fingerprint biometric authentication for the Brail component store at Batam State Polytechnic to address inefficiencies in manual inventory operations, including chaotic tracking and material misappropriation. The system employs the ADDIE model (Analysis, Design, Development, Implementation, and Evaluation) integrating an ESP32 microcontroller, fingerprint sensor, 4-channel relay module, and 12V solenoid locks. The system was tested with 25 registered users and 150 registered fingerprint records as the authentication database. Testing involved 150 locker unlocking attempts to evaluate system efficiency and detection accuracy. Results showed that out of 150 attempts, 125 attempts (83.33%) successfully unlocked the locker while 25 attempts (16.67%) failed. Detailed analysis of system response conditions revealed that 110 data (73.33%) successfully detected fingerprints and activated the solenoid lock, 25 data (16.67%) detected fingerprints but experienced actuator failure preventing lock activation, and 15 data (10.00%) failed to detect fingerprints resulting in no system response due to sensor reading failures. The measurement method used average opening time per 30 openings to assess system performance. These results confirm effective system operation, successfully transforming manual processes into a controlled digital system with enhanced security and accountability. The ESP32 effectively manages biometric authentication and relay control for electromagnetic lock actuation. Future improvements include fingerprint sensor calibration optimization, solenoid actuator stability enhancement, and signal handling refinement to minimize detection failures. This research demonstrates practical embedded systems application for inventory management and security in educational institutions.**

Keywords: fingerprint biometric, automatic locking system, ESP32 microcontroller, inventory management, ADDIE model

INTRODUCTION

The implementation of Problem-Based Learning (PBL) as a pedagogical paradigm at Politeknik Negeri Batam is significantly influenced by the availability and efficiency of logistical support, particularly that provided through the on-campus component store [1]. However, reliance on the current manual operational system creates significant inefficiencies that undermine the responsive and structured principles essential to the PBL process. It has been observed that recurring operational issues include the following: the absence of integrated inventory

supervisor (e.g., lab assistant). This integration ensures that

tracking mechanisms; the wastage of resources due to irregular retrieval patterns of materials; and the misuse of components that has the potential to lead to disputes among student groups [2]. It is evident that these conditions have a detrimental effect on the learning process, thereby reducing the efficacy of collaborative learning experiences. In response to these challenges, this study proposes the development of an integrated, digitally-supported smart locker system [3][4]. The core design integrates a dedicated web-based management portal with a set of physically connected lockers equipped with electronic access control [5][6].The operational mechanism employs strict conditional access protocols, whereby each locker remains digitally locked until a user's online material request is verified and approved by an authorised supervisor, such as a laboratory assistant or logistics coordinator [1]. The integration of digital authorisation and physical retrieval ensures the smooth distribution of materials and creates a transparent, traceable audit trail for each transaction [7][5]. It is evident that the proposed system has the capacity to transform Warung BHP from an open manual operation into a controlled, digital logistics ecosystem [8][9]. It is anticipated that this transformation will enhance material-use accountability, optimise component inventory management, and ultimately strengthen the logistical foundation supporting the achievement of academic objectives within PBL implementation at the polytechnic.

I. METHOD

The Research and Development (R&D) method using the ADDIE model approach is the most suitable research method for automatic locker locking system projects because it involves a systematic and structured technology product development process. The ADDIE model consists of five main stages that are interrelated and sequential, starting from Analysis, Design, Development, Implementation, to Evaluation.

1. Analysis

   During the analysis phase, security weaknesses in conventional lockers at Brail stores were identified, particularly the risk of component loss and unauthorised access. A literature review was conducted on fingerprint biometric systems, ESP32 microcontrollers, relay modules, and solenoid locks. User requirements were also gathered through observation and interviews with store managers to determine locker quantity, usage duration, and security expectations[10]. Based on this analysis, a fingerprint-based automatic locking system was proposed, allowing access only to registered users and employing a sequential locking mechanism to prevent simultaneous locker access.

2. Process Design

During the design phase, the overall system architecture was conceived, incorporating the ESP32 as the primary controller, a fingerprint sensor for authentication input, a 4-channel relay as a switch, and a solenoid lock as an actuator. The design encompasses the creation of block diagrams, comprehensive circuit diagrams with GPIO pin configurations, and algorithm flowcharts that regulate program logic.

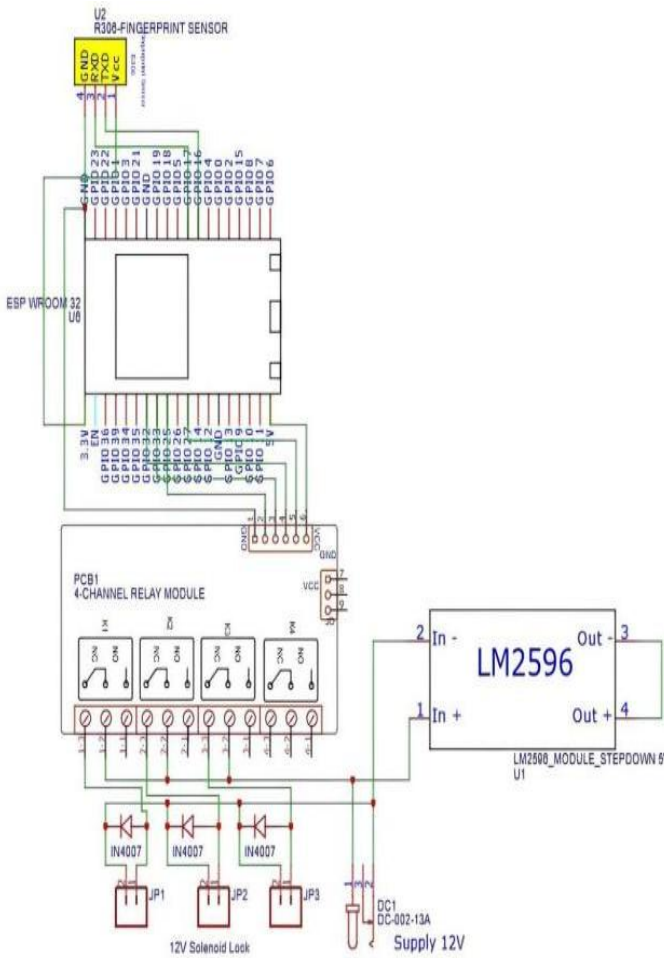

Figure 1. Schematic Design

These flowcharts. initiate with fingerprint detection, proceed to user verification, and culminate in sequential relay activation and auto-off timers. Furthermore, a biometric database was designed to store fingerprint data and user experience aspects, such as new fingerprint registration procedures and a step-by-step tap mechanism for opening lockers.

3. System Development

The system development process commences with system design, encompassing the design of the architecture, workflow, and the primary components of the system. The overarching objective of this design is to furnish stakeholders with a comprehensive representation of the system ahead of its implementation.

3.1 Software

Warung BHP website is a web-based platform with separate user and administrator interfaces. The system implements authentication and authorization mechanisms, restricting access to registered users only. New user registrations require administrator approval before full system access is granted. Role-based access control (RBAC) differentiates access levels between regular users and administrators to maintain data integrity and security.Hardware Components

3.2 Hardware Components

The hardware specifications used in the development of this system are as follows:

a). ESP32 Microcontroller

Acts as the main controller, processing biometric data, managing authentication, and controlling relay outputs. Integrated Wi-Fi/Bluetooth enables remote monitoring and configuration

Figure 2. ESP32 Microcontroller

b). Fingerprint Sensor

Captures and processes fingerprint images with onboard feature extraction. Communicates authentication results to ESP32 via UART interface.

Figure 3. Fingerprint Sensor

c). Channel Relay Module

Provides electrical isolation between ESP32 (3.3V/5V logic) and 12V solenoid locks, protecting the microcontroller from current surges. Controls up to three locker doors independently.

Figure 4. Channel Relay Module

d) LM2596 Step-Down Converter

Converts 12V input to regulated 5V output for ESP32 power supply with high efficiency and minimal heat generation.

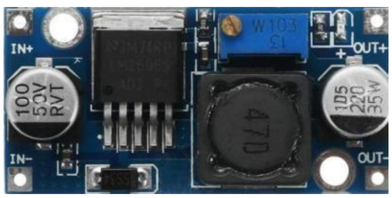

Figure 5. LM2596 Step-Down Converter

e) 12V Solenoid Lock

Electromagnetic actuator that unlocks when powered (12V DC) and locks when de-energized via internal spring mechanism. Three units control individual locker doors.

Figure 6. 12V Solenoid Lock

f) DC Power Supply

Provides 12V DC to solenoid locks and LM2596 converter with sufficient current capacity for simultaneous lock activation.

Figure 7. DC Power Supply

The system development process commences with system design. This stage focuses on defining the system architecture, hardware configuration, and control flow required to ensure proper system functionality. The flowchart below represents the system deployment procedure.

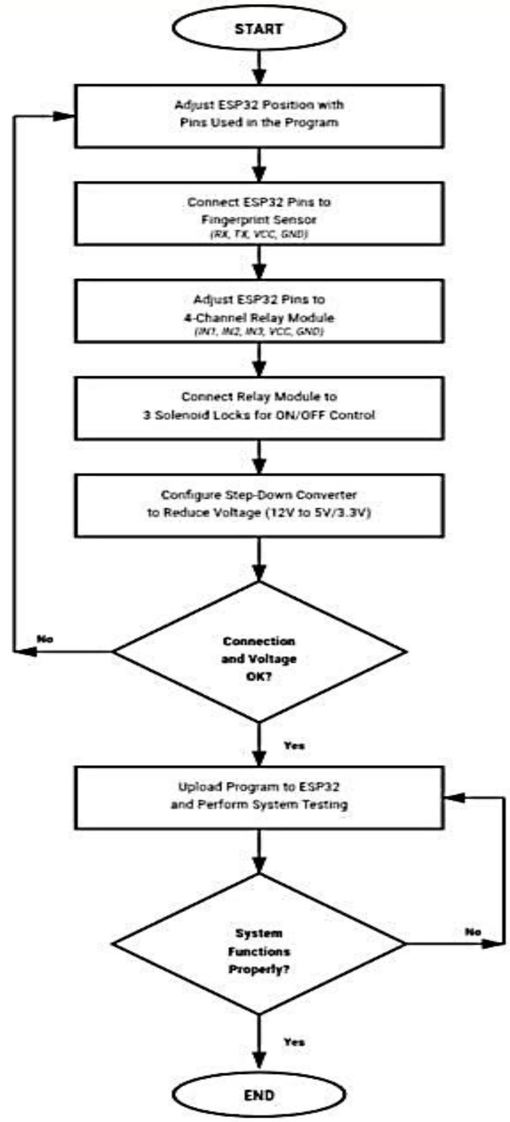

Figure 8. flowchart System Deployment Procedure

The ESP32 must be configured, and the pins that will be utilised in the program must be specified. The installation of the fingerprint sensor is to be initiated with the connection of the RX, TX, VCC and GND cables to the ESP32. The installation of the relay necessitates the connection of four relay channels (IN1-IN4, VCC, GND) to the ESP32.

In order to establish a connection to the solenoid lock, it is necessary to connect the relay to three solenoid locks in order to control the door.

In order to set up the converter, it is necessary to install a step-down converter in order to reduce the voltage from the 12V adapter to 5V and 3.5V.

Testing Stage: It is imperative to undertake a thorough examination of the connections to ensure that all cables and voltages are correct. In the event that this proves to be an inadequate solution, it is advisable to return to the initial stage of the process.The upload program should be initiated if the response is positive. Following this, the code should be uploaded to the ESP32 and the system should be tested (i.e.

fingerprint → relay → lock).

The function must be checked to ensure that the system is operating correctly. In the event of encountering any issues, it is necessary to re-upload the program.The process has been completed. Provided that all systems are functioning correctly, the system is ready for utilisation.
[1].

4. System Implementation

This flowchart illustrates the implementation workflow of a fingerprint-based access control system controlled by an ESP32 microcontroller.

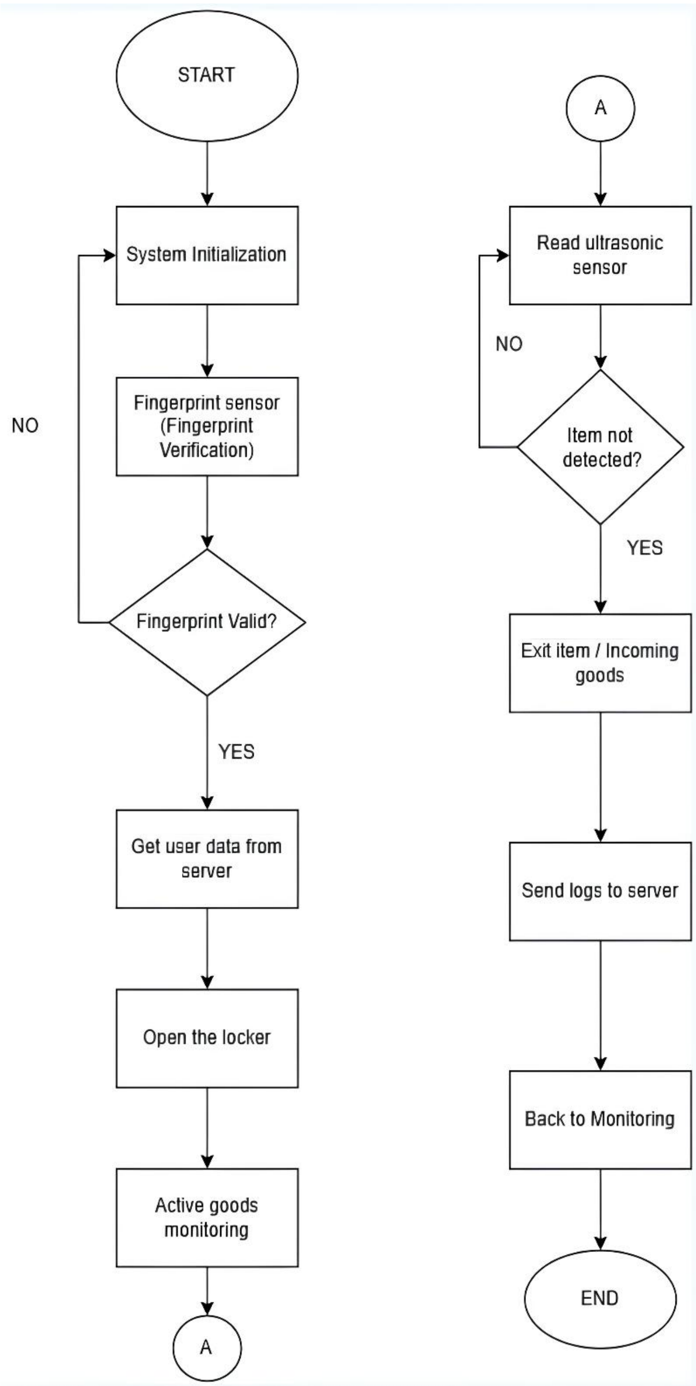

Figure 9. Flowchart Illustrates the Implementation Workflow

The process starts with fingerprint acquisition and verification against the registered fingerprint database. Upon

II. Result and Discussion

This table presents the testing results of the fingerprint-based locker system, including the number of registered users, total fingerprint data, unlocking attempts, and the overall success rate of the system during the testing phase.

A. Result

1. Fingerprint-Based Locker System Testing Results

This section presents the results of the experimental evaluation conducted on the fingerprint-based automatic locker system. The analysis focuses on system detection, accuracy, actuator response, and operational reliability. The quantitative results and testing parameters are summarized in. **Table 1**, which serves as the basis for further discussion of system performance.

Table 1. Fingerprint-Based Locker System Testing Results

Testing Parameters	Data Quantity	Successful Results	Unsuccessful Results	Remarks
Registered Users	25 users	-	-	Only User With Registered Allowed
Total Registered Finger Print Data	150 records	-	-	Used Authentication Databased
Locker Unlocked Attempts	150 attempts	125 attempts	125 attempts	The Locker Open When a Valid finger Print is detected
Unlocking success	-	83.33%	16.37%	Based on 150 attempts

A comprehensive evaluation of the system's performance under restricted test conditions was obtained from the test data of the fingerprint-based biometric verification system for locker opening. The test comprised an authentication database containing 150 fingerprint records from 25 registered users, which showed that only individuals who had registered their fingerprints were permitted to access the system. During the testing phase, 150 attempts were made to open lockers. Of these attempts, the system successfully authenticated and opened lockers in 125 instances, while the remaining 25 attempts were unsuccessful. The outcomes of this investigation yielded an initial success rate of 83.33%, accompanied by a failure rate of 16.67%. These figures indicate that the system functions well in the majority of cases, but there is still room for improvement in terms of reliability, given the number of unsuccessful attempts that may have been caused by factors such as suboptimal finger placement, initial recording quality, or sensor sensitivity. This data provides a foundation for preliminary evaluation of the reliability of biometric authentication systems in the context of personal locking.

2. Response of the Fingerprint Sensor to the Solenoid Lock

Following the overall performance evaluation presented in **Table 1**, this section further examines the internal response of the system components during the authentication process. Specifically, the analysis focuses on the relationship between fingerprint detection by the sensor and the corresponding activation of the solenoid lock. The detailed system response under various operational conditions is summarized in **Table 2**, providing deeper insight into the sources of successful operation and system failure.

Table 2. Response of the Fingerprint Sensor to the Solenoid Lock

System Response Condition	Number of Data	Percentage (%)	Remarks
Fingerprint detected and solenoid lock activated	110 data	73.33%	Successfully unlocked
Fingerprint detected but solenoid lock not activated	25 data	16.67%	Actuator Failure
Fingerprint not detected and no system respond	15 data	10.00%	Sensor reading failure

the conclusion of this study that, based on the results of testing the system's response to fingerprint authentication attempts, a more detailed picture of the performance of the mechanical and sensor subsystems was obtained. Of the total 150 attempts analysed, the system responded by activating the key solenoid in 110 attempts, equivalent to an operational success rate of 73.33%. However, two categories of failure were identified: firstly, in 25 attempts (16.67%), the fingerprint was detected correctly but the solenoid was not activated, indicating a failure in the actuator or its control circuit.

Secondly, in 15 attempts (10.00%), the system did not respond at all due to a failure in the fingerprint sensor reading. These results confirm that, in addition to the accuracy of biometric recognition, the reliability of the actuation components and the stability of the sensor reading are critical factors that significantly affect the overall performance of the system. These findings underscore the necessity for further evaluation of the interface design between the sensor module, signal processor, and actuator to enhance the robustness of the system in real operational conditions further evaluation of the interface design between the sensor module, signal processor, and actuator to enhance the robustness of the system in real operational conditions

3. Automatic Locker Opening Time Data Description

To complement the system performance evaluation discussed in the previous sections, this study further analyzes the temporal characteristics of the automatic locker opening process. The analysis focuses on the system response time during repeated unlocking operations, including both successfully detected and undetected attempts. The descriptive attributes of the dataset used for this evaluation are presented in **Table 3**, which summarizes the automatic locker opening time data.

Table 3. Automatic Locker Opening Time Data Description

Variable	Category	Description
Observed system	System	Automatic locker opening system
Total observations	Count	150 opening attempts
Successful openings (detected)	Count	115 attempts
Undetected openings (failed detection)	Count	35 attempts
Measurement focus	Parameter	Time required for the locker to open
Number of openings per trial	Count	30 openings
Data type	Type	Quantitative (continuous time data)
Unit of measurement	Unit	Seconds
Data aggregation method	Method	Average opening time per 30 openings
Purpose of data	Objective	Performance evaluation of system efficiency and detection accuracy

System performance evaluation data obtained from 150 authentication attempts was analysed to categorise operational responses into three main conditions. The initial condition, involving the detection of the fingerprint and the subsequent activation of the key solenoid, occurred in 110 cases, constituting 73.33% of the total attempts. This outcome signifies a complete success in the opening process. The second condition manifested in 25 data points (16.67%), where the fingerprint was successfully recognised but the key solenoid was not activated. This failure was attributed to a malfunction of the actuator or its control circuit. The third condition, characterised by the absence of fingerprint detection and system response, occurred in 15 data points (10.00%), attributable to a sensor reading failure. The findings indicate that the system demonstrated an overall functional success rate of 73.33%, with the remaining 26.67% representing failures attributable to two critical points: the unreliability of the actuator module (16.67%) and the limitations of the sensor in reading biometric data (10.00%). These findings emphasise the necessity of enhancing the reliability of mechanical-electrical components and optimising sensor accuracy to achieve higher operational success rates in real-world applications.

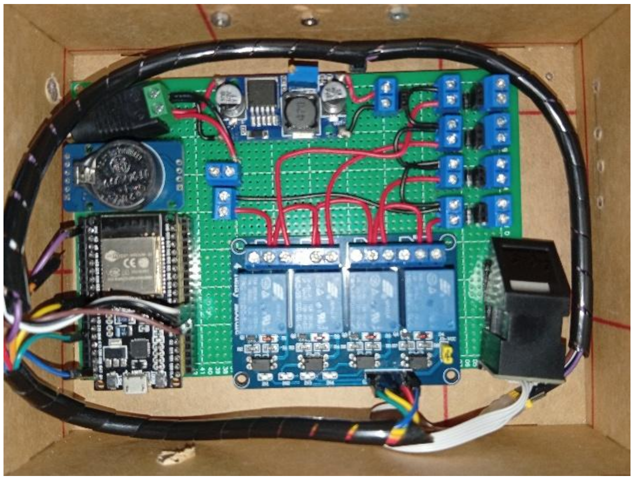

Figure 10 . Result Product

Additionally, the temporal analysis of the automatic locker opening time indicates that the system response generally complies with the predefined operational timing specified in the system implementation flowchart. These results confirm that the system performs consistently in terms of authentication success, actuator response, and timing behavior.

B. Discussion

The results indicate a strong correlation between the implemented system workflow and the observed experimental performance. The success rates obtained in Table 1 align with the fingerprint verification logic defined in the flowchart, where registered fingerprints trigger actuator activation. The component-level failures identified in Table 2, including actuator and sensor detection issues, correspond to critical stages in the system flow, particularly during fingerprint recognition and solenoid lock control.

Furthermore, the opening time analysis in Table 3 supports the intermediate conclusion that the system's timing logic is correctly implemented within the ESP32-based control architecture. However, the presence of undetected fingerprint events and actuator failures suggests that system reliability can be further improved through enhanced sensor calibration, improved actuator control stability, and optimized signal handling.

III. Conclusion

The analysis of the test data indicates that the fingerprint-based locker unlocking system demonstrated a recognition success rate of 83.33%, with 125 out of 150 attempts resulting in successful locker unlocking. However, a subsequent analysis of the system's response conditions revealed that only 73.33% of trials resulted in solenoid lock activation following fingerprint detection. Meanwhile, 16.67% of trials exhibited actuator failure, and 10% were attributed to sensor failure. The system response time was measured quantitatively using continuous data in seconds, showing that the system was able to operate with acceptable efficiency. However, there was still room for improvement in actuator reliability and sensor detection accuracy. Consequently, the implementation of this system is viable, contingent upon the enhancement of the mechanical actuator and sensor calibration to minimise the failure rate.

References

[1] S. Chakkaravarthy Sethuraman, A. Mitra, K. C. Li, A. Ghosh, M. Gopinath, and N. Sukhija, "Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets," *IEEE Access*, vol. 10, no. November, pp. 112721–112730, 2022, doi: 10.1109/ACCESS.2022.3216665.

[2] D. Aswini, R. Rohindh, K. S. Manoj Ragavendhara, and C. S. Mridula, "Smart Door Locking System," *2021 Int. Conf. Adv. Electr. Electron. Commun. Comput. Autom. ICAECA 2021*, pp. 1–5, 2021, doi: 10.1109/ICAECA52838.2021.9675590.

[3] H. Rama Moorthy, Shrinivasa, R. Chetan, M. Deepak Rao, N. J. Avinash, and N. S. Krishnaraj Rao, "Biometric Authentication for Safety Lockers Using Cardiac Vectors," *ICPECTS 2020 - IEEE 2nd Int. Conf. Power, Energy, Control Transm. Syst. Proc.*, pp. 2–6, 2020, doi: 10.1109/ICPECTS49113.2020.9336976.

[4] M. Shanthini, G. Vidya, and R. Arun, "IoT enhanced smart door locking system," *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 92–96, 2020, doi: 10.1109/ICSSIT48917.2020.9214288.

[5] J. A. J. Alsayaydeh, M. F. Yusof, S. Mamchenko, R. A. Hamzah, and S. G. Herawan, "Design and Evaluation of a Biometric IoT-Based Smart Lock System with Real-Time Monitoring and Alert Mechanisms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 7, pp. 349–362, 2025, doi: 10.14569/IJACSA.2025.0160737.

[6] S. Chandrappa, Prithviraj, H. Aditya Pai, I. S. Rajesh, R. Manjunath Sargur Krishnamurthy, and R. Sneha Shetty, "Smart Locker 2.0: Leveraging IoT and Machine Learning for Secure, User-Friendly Public Storage," *2025 Int. Conf. Artif. Intell. Data Eng. AIDE 2025 - Proc.*, pp. 696–700, 2025, doi: 10.1109/AIDE64228.2025.10987522.

[7] R. S. Sabeenian, M. Kawin, S. Akshayasri, P. M. Dinesh, M. Alagarsamy, and G. P. Lakshmi, "IoT-Based Data Logging System for Authenticated Bank Locker Access to Ensuring Security," *Int. Conf. Intell. Innov. Pract. Eng. Manag. 2024, IIPEM 2024*, no. Iipem, pp. 1–5, 2024, doi: 10.1109/IIPEM62726.2024.10925690.

[8] J. Sa-Ngiampak *et al.*, "LockerSwarm: An IoT-based smart locker system with access sharing," *5th IEEE Int. Smart Cities Conf. ISC2 2019*, pp. 587–592, 2019, doi: 10.1109/ISC246665.2019.9071664.

[9] K. R. Umadi, A. Aishwarya, J. E. Narendramath, S. M. Inchara, and P. P. P. Dharishini, "Smart E-Locker System using IoT," *IDCIoT 2023 - Int. Conf. Intell. Data Commun. Technol. Internet Things, Proc.*, no. IDCIoT, pp. 41–45, 2023, doi: 10.1109/IDCIoT56793.2023.10053507.

[10] X. Yang, S. Yang, J. Liu, C. Wang, Y. Chen, and N. Saxena, "Enabling Finger-Touch-Based Mobile User Authentication via Physical Vibrations on IoT Devices," *IEEE Trans. Mob. Comput.*, vol. 21, no. 10, pp. 3565–3580, 2022, doi: 10.1109/TMC.2021.3057083.