Journal of Deep Learning, Computer Vision and Digital Image Processing
E-ISSN: 2986-8939 P-ISSN: 2986-8920
Vol. 4, No. 1, March 2026
DOI. https://doi.org/10.61255/decoding.v4i1.1522

Design and Evaluation of an ESP32-Based Smart Helmet Locker Using Student Identity Card Authentication

Muhammad Fathur Rachman ✉
(Universitas Negeri Makassar, Makassar, Indonesia)

Haripuddin
(Universitas Negeri Makassar, Makassar, Indonesia)

Satria Gunawan Zain
(Universitas Negeri Makassar, Makassar, Indonesia)

Jumadi M. Parenreng
(Universitas Negeri Makassar, Makassar, Indonesia)

Sanatang
(Universitas Negeri Makassar, Makassar, Indonesia)

OPEN ACCESS

ARTICLE HISTORY
Received: 25 January, 2026
Revised: 23 February 2026
Accepted: 17 March, 2026

KEYWORDS
ESP32;
ISO/IEC 25010;
RFID;
Student identity card;
Smart locker.

ABSTRACT

Purpose – To develop and evaluate an ESP32-based smart helmet locker using student identity card (KTM) authentication.

Methods – Development followed the ADDIE model. The prototype integrated RFID authentication, a solenoid lock, Google Sheets logging, and Telegram notifications. Controlled tests addressed selected ISO/IEC 25010 quality characteristics, and 24 students completed a study-specific usability questionnaire.

Findings – Functional and repeated-operation tests each achieved 100% success under the defined conditions. Mean card-detection, LCD-response, and Telegram-notification times were 1.85, 3.55, and 3.25 seconds. The questionnaire's mean raw total was 45.00 out of 50; because negative items were not reverse-scored, this value is not a validated overall usability or feasibility score.

Research implications – The prototype supports controlled locker access and monitoring in the tested scenarios. A single prototype, internet dependence, and limited user data constrain generalizability. Helmet-theft reduction, comprehensive security, and long-term field reliability were not established.

Originality – The study integrates established authentication, control, logging, and notification technologies for a campus helmet-locker application.

Correspondence Author: ✉ fathur21rachman@gmail.com
To cite this article : Rachman, M. F., Haripuddin, Zain, S. G., Parenreng, J. M., & Sanatang. (2026). Design and evaluation of an ESP32-based smart helmet locker using student identity card authentication. *Journal of Deep Learning, Computer Vision and Digital Image Processing*, *4*(1), 41-70. Doi. https://doi.org/10.61255/decoding.v4i1.1522

This is an open access article under the CC BY-SA license

INTRODUCTION

Motorcycles have become the most widely used mode of transportation in Indonesia due to their affordability, flexibility, and operational efficiency. The increasing use of motorcycles among students has made helmets an essential component of daily mobility activities [1]. In addition to complying with traffic regulations, helmets function as protective equipment designed to reduce the risk of serious head injuries and fatalities resulting from traffic accidents [2], [3]. Despite their importance, helmet security remains a common issue in many university environments. Students frequently leave helmets on motorcycle mirrors, under seats, or in other unsecured locations while attending lectures [4]. Such practices increase the likelihood of theft and unauthorized use. The absence of dedicated storage facilities and limited supervision within parking areas further contribute to this problem [5].

A preliminary survey conducted among students of the Department of Informatics and Computer Engineering, Universitas Negeri Makassar, revealed that more than 92% of respondents use motorcycles as their primary transportation mode. Furthermore, approximately 96% of respondents reported having experienced, witnessed, or heard about helmet theft incidents within the campus environment. Most respondents identified the lack of secure storage facilities as one of the primary causes of helmet theft. These findings indicate the need for a technology-based storage solution that may support more controlled helmet storage and reduce exposure to theft risks. The rapid development of Internet of Things (IoT) technology has opened opportunities for implementing intelligent security systems capable of providing automated access control, real-time monitoring, and centralized data management [6], [7]. IoT-based systems have been widely adopted in various fields because they enable communication between devices through internet networks, resulting in improved efficiency, accessibility, and monitoring capabilities [8], [9]. One potential implementation of IoT technology is the development of smart locker systems that integrate authentication technologies and cloud-based monitoring services [10], [11].

Several previous studies have explored the implementation of smart locker technologies using various authentication mechanisms. Abdahu et al. (2024) developed a Smart Helmet Cabinet that utilized mobile QR Code authentication, ESP32-CAM for user credential scanning, and ESP32 NodeMCU for controlling the locker access mechanism. Their study demonstrated that digital authentication could be integrated with an electronic locker system to identify authorized users and manage access to secure helmet storage [12].

Similarly, Rozy and Fahruzi (2022) proposed a locker security system utilizing RFID/NFC technology through the PN532 module. Their findings showed that RFID/NFC authentication successfully controlled locker access, although the system performance was influenced by reading distance and environmental conditions [13]. Amin et al. (2022) further developed an RFID-based locker system integrated with Android notifications. The proposed system utilized electronic identity cards and demonstrated the potential of combining authentication mechanisms with monitoring services to improve locker security [14].

More recently, Nugraha et al. (2024) developed a smart keyless locker system utilizing Bluetooth Low Energy (BLE) and ESP32. Their research demonstrated fast response times and successful Telegram-based notifications. However, system performance was affected by physical barriers and BLE communication limitations. Previous studies indicate that RFID, NFC, and BLE technologies can effectively support locker security systems. Nevertheless, most existing implementations focus primarily on access control and local authentication mechanisms without fully integrating cloud-based data management and centralized monitoring features [15].

Although numerous studies have explored smart locker development, several limitations remain. First, most existing systems focus only on authentication mechanisms and do not provide centralized data storage capabilities. Second, only a limited number of studies integrate cloud databases, real-time notifications, and student identity cards within a single IoT ecosystem. Third, several systems require dedicated access cards or mobile applications, increasing implementation complexity and operational costs. Therefore, there is still a need for a more integrated smart locker system that utilizes existing student identity infrastructure while simultaneously supporting cloud-based management and real-time monitoring. Accordingly, the contribution of this study lies in the practical integration of established technologies rather than in a new algorithm or communication protocol.

This study aims to design and develop an IoT-based smart helmet locker utilizing ESP32 and RFID-enabled Student Identity Cards (KTM) as authentication credentials. Furthermore, the developed prototype is evaluated using selected quality characteristics informed by ISO/IEC 25010, focusing on functional suitability, performance efficiency, reliability, and usability.

The proposed smart locker system is expected to support controlled helmet storage through RFID-based authentication, cloud-based data management, and real-time monitoring services. Prototype performance is assessed against predefined operational criteria associated with the selected quality characteristics; the evaluation does not represent formal or complete conformity with ISO/IEC 25010.

METHOD

Research Design

This study employed the Research and Development (R&D) method to develop and evaluate an IoT-based smart helmet locker utilizing ESP32 and RFID-enabled Student Identity Cards (KTM) as an authentication mechanism. The ESP32 is a microcontroller developed by Espressif Systems. Its main advantage lies in the integration of Wi-Fi and Bluetooth modules, which simplifies the development of IoT systems requiring wireless connectivity [16]. Meanwhile, RFID is a technology that uses radio waves to automatically identify objects or individuals [17], [18]. The development process adopted the ADDIE model, which consists of Analysis, Design, Development, Implementation, and Evaluation stages. The ADDIE model was selected because it provides a systematic and iterative framework that supports the development, implementation, and assessment of technology-based products [19]. Schematically, the stages of the research procedure for the ESP32-Based Smart Locker with KTM using the ADDIE development model are illustrated in Figure 1.

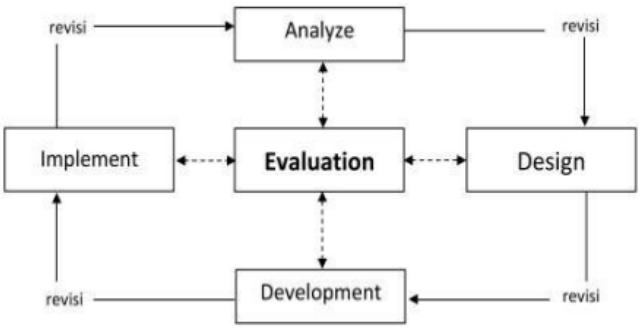

Figure 1. ADDIE Development Model

The product was designed as a prototype intended to address the identified helmet-storage problem by integrating RFID authentication, cloud-based data management, and real-time notification services into a single smart locker system.

System Architecture

The proposed system consists of hardware and software components integrated through Internet of Things (IoT) technology. The hardware subsystem includes an ESP32 microcontroller, RFID RC522 module, relay module, solenoid door lock, LCD display, and power supply unit. ESP32 functions as the main controller due to its built-in Wi-Fi capability, low power consumption, and suitability for IoT applications [20].

RFID technology was employed as the authentication mechanism because it enables automatic identification using radio-frequency communication without requiring physical contact [21]. The RFID-enabled Student Identity Card (KTM) serves as the access credential, allowing students to utilize an existing campus identification medium without requiring an additional authentication card [22], [23].

The software subsystem consists of Arduino IDE, Google Sheets, Google Apps Script, and Telegram Bot. Google Sheets serves as a cloud database, while Google Apps Script facilitates communication between ESP32 and the cloud database through web-based services [24]. Telegram Bot provides real-time notifications whenever locker access activities occur. The system architecture is shown in Figure 2.

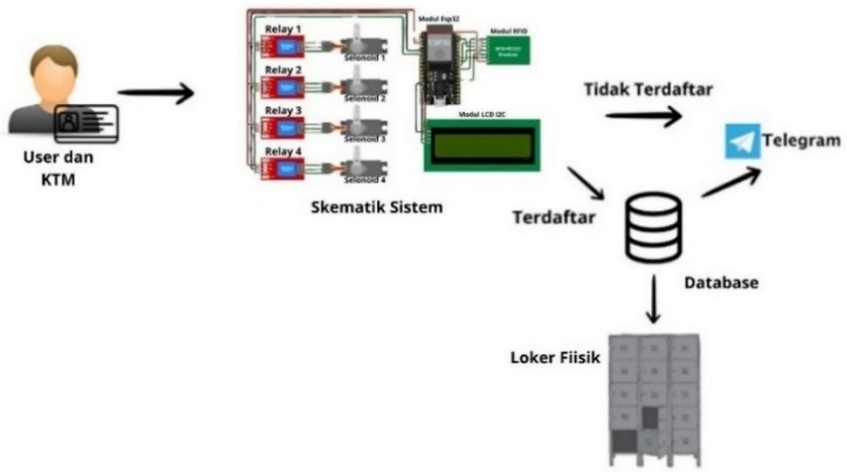

Figure 2. System Architecture

System Workflow

The operational workflow begins when a user places an RFID-enabled KTM card near the RFID reader. The RFID RC522 reads the unique identifier (UID) embedded within the card and transmits the data to ESP32 [25]. The ESP32 then verifies the UID against records stored in Google Sheets through Google Apps Script. If the UID is recognized, the system activates the relay and solenoid door lock, granting access to the locker. Simultaneously, user information and access records are stored in the cloud database, and a notification is sent through Telegram. Conversely, if the UID is not registered, the system denies access and displays an error message on the LCD. The system flowchart is shown in Figure 3.

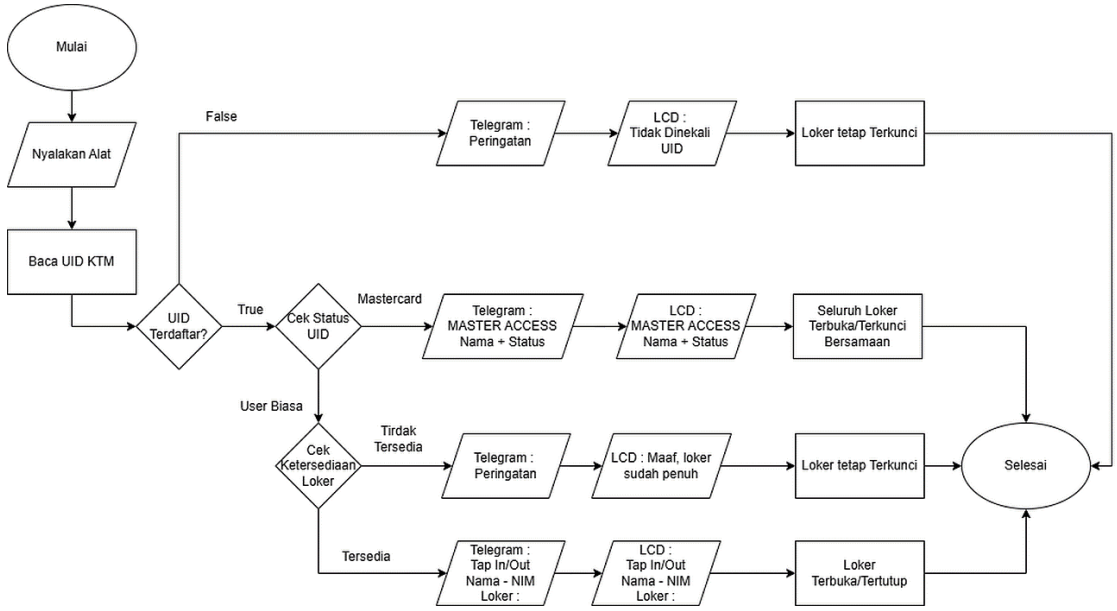

Figure 3. System Flowchart

Hardware and Software

The system consists of hardware and software developed to support authentication, access control, and monitoring functions. Table 1 presents the primary hardware components utilized in this study.

Table 1. Hardware Components

Component	Function
ESP32	Main controller
RFID RC522	User authentication
Relay Module	Electronic switching
Solenoid Door Lock	Locker locking mechanism
LCD Display	User information display
KTM RFID Card	Authentication medium

The software was developed using Arduino IDE as the programming environment. Google Sheets was integrated as a cloud-based data-storage and access-logging platform, while Telegram Bot was used to deliver real-time notifications regarding system activities [26]. In the developed system, Google Apps Script functioned as the web-based intermediary that received requests from the ESP32 and processed data before recording it in Google Sheets.

Table 2. Software Components

Software	Function
Arduino IDE	Firmware development
Google Sheets	Cloud database
Google Apps Script	Data processing and communication
Telegram Bot	Real-time notification

Google Sheets was used as the prototype's cloud-based access-logging layer, while Google Apps Script provided the web-based service that received and processed data transmitted by the ESP32. A comparable RFID access-control system implemented real-time access logging through Google Sheets via Google Apps Script to support lightweight and centralized monitoring [24].

Participants

The usability evaluation involved 24 students from the Department of Informatics and Computer Engineering, Universitas Negeri Makassar, selected purposively because they represented the intended user group of the developed smart locker. Before completing the questionnaire, participants received an explanation of the study purpose and operating procedure and interacted directly with the prototype by performing the available KTM-based access workflow and observing the LCD and Telegram responses. Prior experience with RFID-based systems was not used as a selection criterion and was not separately analyzed. The evaluation was conducted after institutional permission had been obtained from the relevant academic unit at Universitas Negeri Makassar. Participation was voluntary, informed consent was obtained before testing, and respondent identities were reported using anonymous codes.

Instruments

Testing was conducted through a series of experiments to determine whether the system functioned in accordance with its intended design objectives. All research instruments, including the hardware and software testing protocols and the 10-item usability questionnaire, were submitted to expert validators and validated before data collection. The validators were the research supervisors, who reviewed the clarity, relevance, coverage, and alignment of each instrument with the study objectives. The tests included evaluating the system's ability to detect KTM access cards, verify database records, operate the locking mechanism, and send notifications to Telegram.

ESP32 Testing

Testing focused on the basic functions of the main hardware component, the ESP32, which serves as the system control center. The purpose of this testing was to ensure that all major components function optimally and are well integrated to support the smart locker system. The aspects tested are shown in Table 3.

Table 3 presents the tested aspects, including Wi-Fi connectivity, database integration, port functionality, data input reading from RFID and other sensors, and real-time data processing capabilities of the ESP32.

Table 3. ESP32 Testing Protocol

No.	Testing Aspect	Test Condition	Expected Result
1	Wi-Fi Connectivity Function	Connecting the ESP32 to a Wi-Fi network	Functioning / Not Functioning
2	Database Connectivity Function	Connecting the ESP32 to the database	Functioning / Not Functioning
3	Port Response Function	Connecting the ESP32 to supporting devices	Functioning / Not Functioning

System Functionality Testing

This test aims to evaluate every functional feature of the Student ID Card (KTM)-based security system. The aspects tested include the system's ability to read and distinguish between registered and unregistered KTMs, display the appropriate information on the LCD screen, send notifications when a locker is in use, and ensure that lockers can only be opened if the KTM's UID is registered in the database. The testing instruments are shown in Table 4.

Table 4. System Functionality Testing Protocol

No.	Testing Aspect	Test Condition	Expected Result
1	KTM Detection	Reading UID from the KTM card	Functioning / Not Functioning

No.	Testing Aspect	Test Condition	Expected Result
2	Database Matching with KTM UID	Comparing registered and unregistered KTM cards	Match / No Match
3	LCD Text Display	Testing with registered and unregistered KTM cards	Functioning / Not Functioning
4	Relay and Solenoid Activation	Automatic locker opening	Opened / Not Opened
5	Telegram Notification	Notification message sent to Telegram	Sent / Not Sent

System Accuracy Measurement Testing

Accuracy testing evaluated whether the prototype correctly detected student identity card (KTM) unique identifiers (UIDs), matched them against database records, and delivered the expected notifications. Table 5 presents the tested aspects.

Table 5. System Accuracy Measurement Protocol

No.	Testing Category	Number of Trials	Number of Correct Detections	Number of Incorrect Detections	Accuracy Percentage (%)
1	KTM UID Detection	--	--	--	--%
2	UID Matching Accuracy with the Database	--	--	--	--%
3	Real-Time Notification Delivery	--	--	--	--%

Performance Efficiency Testing

The purpose of this testing is to evaluate the system's performance in terms of response speed and technical capabilities under various operational conditions.

Table 6 lists the timing measures for card detection and notification delivery, together with the card-reading distance and card-condition checks. For this study, a mean response time of 5 seconds or less was adopted as the efficiency criterion. The tested distances and conditions describe the prototype evaluation and do not establish the reader's maximum operating range.

Table 6. Performance Efficiency Testing Protocol

No.	Testing Parameter	Response Time	Unit
1	KTM Detection Time	(s)	Seconds
2	LCD Notification Delivery Time	(s)	Seconds
3	Telegram Notification Delivery Time	(s)	Seconds
4	KTM Detection Distance	(cm)	Centimeters

Reliability Testing

The purpose of this testing is to evaluate the system's reliability in consistently performing its functions under various operational conditions. The main focus of the testing includes the stability of KTM UID detection, the success rate of notification delivery, and the system's ability to operate continuously without experiencing disruptions. The aspects tested are presented in Table 7.

Table 7. Reliability Testing Protocol

No.	Test Type	Number of Trials	Successful	Failed	Accuracy (%)
1	Student ID Card UID Detection	40	-	-	-
2	Notification Delivery Operation	40	-	-	-
3	Continuous Operation Test (12 Hours)	5	-	-	-

Usability Testing

The usability evaluation employed a study-specific questionnaire consisting of 10 statements rated using a five-point Likert scale. The questionnaire included five positively worded and five negatively worded statements designed to capture users' perceptions of intended use, ease of operation, ease of learning, system functionality and consistency, confidence, and the need for assistance when interacting with the developed smart locker system. Before administration, the complete questionnaire was content-validated through expert judgment by the research supervisors. The instrument structure is summarized in Table 8.

Table 8. Usability Questionnaire Structure

No.	Variable	Indicator	Number of Items	Attribute	Scale
1	Usefulness	Benefits and usefulness of the system	2	Positive	Likert 1–5
2	Ease of Use	Ease of operating the system	2	Mixed	Likert 1–5
3	Ease of Learning	Ease of understanding the system	2	Mixed	Likert 1–5
4	User Satisfaction	User comfort and confidence	1	Positive	Likert 1–5
5	System Complexity	Level of system complexity	1	Negative	Likert 1–5
6	System Inconsistency	Consistency of features and functions	1	Negative	Likert 1–5
7	Need for Assistance	Dependence on technical assistance	1	Negative	Likert 1–5

For transparency, the questionnaire items were as follows: (1) I think I would frequently use this smart locker to store my helmet; (2) I find this smart locker system unnecessarily complicated to use, particularly during the KTM tapping process; (3) I find the smart locker system very easy to use; (4) I think I would need assistance from another person or a technician to use this smart locker; (5) I

find that the smart locker features, including KTM reading, Telegram notifications, and the LCD display, function very well; (6) I find many inconsistencies in the operation of the smart locker system; (7) I think other users would learn how to use this smart locker very quickly; (8) I find the procedures for using this smart locker very confusing; (9) I feel confident and secure when using this smart locker; and (10) I would need to learn many things before I could use this smart locker effectively. Each statement was rated using a five-point Likert scale ranging from Strongly Disagree to Strongly Agree. Responses were retained in their original coding direction. Consequently, the questionnaire results are interpreted descriptively at the item level as preliminary user perceptions, and the raw combined total is retained only for transparency rather than treated as a standardized usability or feasibility score.

Security Testing

This test aims to assess the system's security in protecting access and preventing unauthorized actions. The evaluation focuses on the system's ability to distinguish between registered and unregistered users, manage potential abuses such as duplicate access (spam scans), and maintain a locked state during manual intrusion attempts. The aspects of this evaluation are presented in Table 9.

Table 9. Security Testing Protocol

No.	Test Scenario	Expected Result	Successful	Failed
1	Registered Student ID Card (KTM) Access	Locker opens successfully	-	-
2	Unregistered Student ID Card (KTM) Access	Locker remains locked	-	-
3	Multiple Access Attempts (Spam Scan)	Each UID can only perform Tap-in and Tap-out alternately	-	-
4	Manual Tampering Test (Physical Break-in Attempt)	System remains locked	-	-

Data Analysis Techniques

The study used descriptive quantitative analysis supported by qualitative interpretation of operational observations. Quantitative procedures included functional success percentages, accuracy rates, repeated-operation success rates, mean response times, variability statistics, and descriptive Likert scores. Operational observations from abnormal-condition and security tests were interpreted qualitatively to explain prototype behavior and limitations. The evaluation was informed by selected quality characteristics associated with ISO/IEC 25010 - functional suitability, performance efficiency, reliability, and usability - and does not claim complete conformity with the standard.

Functional Suitability Analysis

The analysis was conducted using the function success rate method based on the results of black-box testing. The suitability calculation was performed using the formula shown in Equation (1).

$$\text{Functional Suitability (\%)} = \frac{\textit{number of succesfull features}}{\textit{number of features designed}} \times \mathbf{100}\% \quad (1)$$

Accuracy Analysis

Accuracy is used to measure the overall success rate of the system in correctly recognizing KTMs. Accuracy is calculated using the formula shown in Equation (2).

$$\text{Accuracy (\%)} = \frac{\textbf{Number of correct results}}{\textbf{Total number of trials}} \times \mathbf{100}\% \quad (2)$$

Performance Efficiency Analysis

Performance analysis was conducted by calculating the average response time from several trials, as shown in Equation (3).

$$\textbf{\textit{Mean response time}} = \frac{\sum t_i}{n} \quad (3)$$

Where:

ti = response time in the i-th experiment

n = number of experiments

For this study, a mean response time of ≤ 5 seconds was classified as efficient.

Reliability Analysis

Reliability is measured by the system's success rate when run repeatedly. Reliability is calculated using the formula shown in Equation (4).

$$\textbf{\textit{Reliability}}(\%) = \frac{\textbf{\textit{Number of successful trials}}}{\textbf{\textit{Total number of trials}}} \times \mathbf{100}\% \quad (4)$$

≥ 95%: Highly Reliable

80% to < 95%: Fairly reliable

< 80% : Not Very Reliable

Usability Analysis

The questionnaire responses were analyzed descriptively using their original five-point Likert scores, as presented in Table 10. Because the positively and negatively worded statements were retained in their original response direction, item-level results were emphasized and the combined respondent totals were not treated as a standardized overall usability score.

Table 10. Usability Analysis

Likert Scale	Raw Score	Response Meaning
Strongly Agree (SA)	5	Strong agreement
Agree (A)	4	Agreement
Neutral (N)	3	Neutral response
Disagree (D)	2	Disagreement
Strongly Disagree (SD)	1	Strong disagreement

Each response was tabulated by respondent and statement. Statement-level totals were retained to show the distribution of responses to each questionnaire item, while respondent totals and the overall raw total were presented only for transparency. The mean raw respondent total was calculated by dividing the sum of the respondent totals by the number of respondents, as shown in Equation (5). No standardized feasibility cutoff was applied to this raw mixed-polarity total.

$$\textbf{\textit{Mean raw score}} = \frac{\textbf{\textit{Total questionnaire score}}}{\textbf{\textit{Number of respondents}}} \quad (5)$$

The resulting questionnaire values were interpreted descriptively as preliminary user perceptions of the prototype. Because the instrument was study-specific and the mixed-polarity responses were retained in their original scoring direction, labels such as "Highly Eligible" or "Highly Feasible" were not used as standardized conclusions.

Scope and Limitations

This study focused on the development of a prototype smart helmet locker utilizing ESP32 and RFID-enabled Student Identity Cards. The evaluation was limited to selected functional suitability, performance efficiency, reliability, and usability characteristics informed by ISO/IEC 25010; it did not establish complete conformity with the standard. The developed system was implemented as a single-locker prototype and depended on internet connectivity for cloud database synchronization, UID verification, and Telegram notification services. This internet dependency is a core operational limitation because unstable or unavailable Wi-Fi can prevent database verification and normal locker access. Long-term environmental durability under weather exposure, electromagnetic interference, and component degradation was not evaluated. Prior RFID experience and detailed participant demographics were not separately analyzed, and the study-specific questionnaire findings are interpreted only as preliminary user perceptions. The study also did not measure actual reductions in helmet theft or changes in campus security outcomes. Therefore, the findings represent controlled prototype validation and may not fully represent large-scale or long-term field deployment.

RESULTS AND DISCUSSION

Results

Physical Description of the Prototype

The prototype's control components were assembled in a box mounted above the locker.

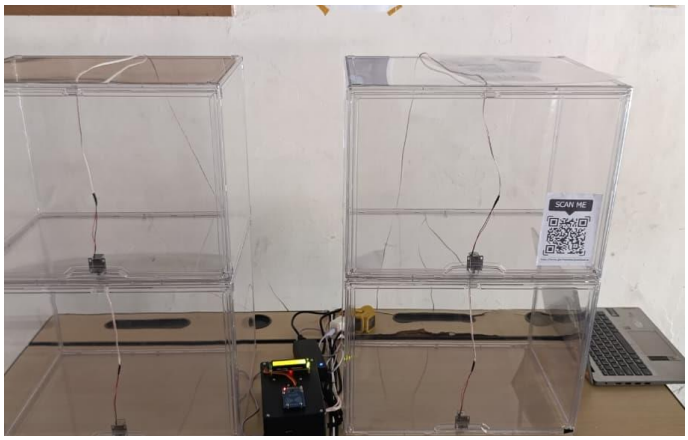

Figure 4. Physical Components of a Helmet Locker

Figure 4 shows the relay, RFID reader, and solenoid door-lock components. The reader was positioned above the locker for KTM tap-in and tap-out operations, and the solenoid lock was mounted inside the door. The prototype used a 5 V input supply for the ESP32 board and a separate 12 V supply for the solenoid locks. Board input voltage must be distinguished from the operating voltage of the ESP32 logic and connected peripherals.

System Test Results

Hardware Test Results (ESP32)

The purpose of this test is to ensure that the main hardware component, the ESP32, and its peripherals function properly to support the system requirements. The results are summarized in Table 11.

Table 11 presents the results of basic functionality testing of the main hardware component, the ESP32. These tests were conducted to validate the device's readiness prior to the implementation of more complex algorithms. The test results indicate success in all three aspects of the testing.

Table 11. ESP32 Device Test Results

No.	Testing Aspect	Test Condition	Test Result
1	Wi-Fi Connectivity Function	Connecting the ESP32 to a Wi-Fi network	Functional
2	Database Connectivity Function	Connecting the ESP32 to the database	Functional
3	Port Response Function	Connecting the ESP32 to peripheral devices	Functional

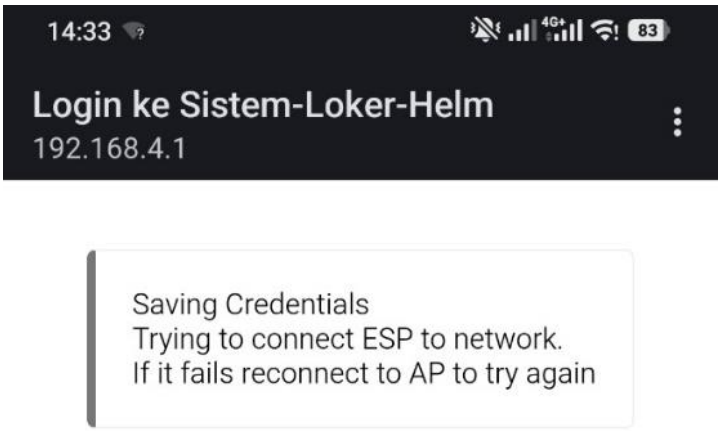

Figure 5. The Device Has Successfully Connected to Wi-Fi

Figure 5 shows that the device has successfully connected to the Wi-Fi network. This figure documents the success of the initial hardware testing, in which the system was able to connect to the Wi-Fi network that will be used for sending notifications to Telegram and accessing the database in the form of spreadsheets.

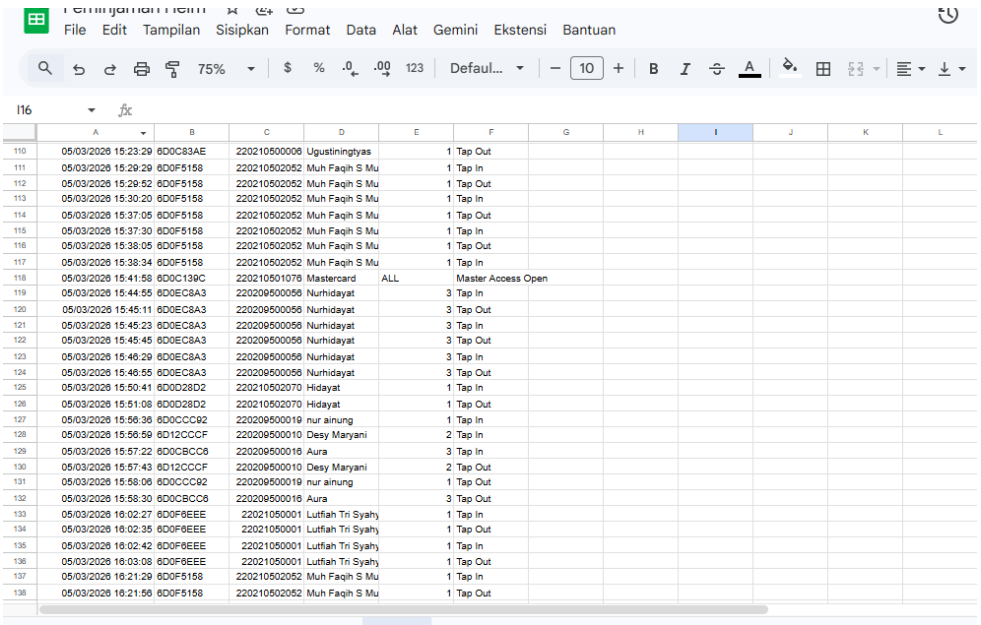

Figure 6. The Device Has Successfully Connected to the Database

Figure 6 shows that the device has successfully connected to the database that was created. This figure demonstrates that the ESP32 device has successfully accessed the connected database and is able to send and receive data from it.



Figure 7. The Devices and Ports Have Successfully Connected to Each Other

Figure 7 shows that the ESP32 device and its ports have successfully detected other supporting devices.

As shown in Table 11 and supported by the documentation in Figures 5, 6, and 7, all three aspects of the ESP32 hardware are functioning successfully with a "Functioning" status. The ESP32 has successfully connected to the Wi-Fi network. The device also successfully accessed the database to accurately send and receive data. Thus, this table confirms that the system's hardware testing was successfully completed.

System Functionality Test Results

Functionality testing was conducted to ensure that all key features of the security system operate in accordance with the design and specifications. This testing covered the system's ability to identify KTMs, store data, perform verification, send warning notifications, and activate alarms. The results of the system's functionality testing are presented in Table 12.

Table 12 presents a summary of the system verification results from the functionality testing. This testing aimed to ensure that the entire system workflow, from the detection process to the system response, operated as expected. All five tested functions completed 15 trials without an observed failure under the controlled test conditions. This result confirms successful integration of the hardware components (ESP32, RFID reader, and relay) and the software components (database and Telegram Bot) within the defined test scenarios, but it should not be interpreted as evidence of complete stability across broader environmental and operational conditions.

Table 12. ESP32 System Functionality Results

No.	Testing Aspect	Test Condition	Number of Trials	Successful	Failed	Conclusion
1	Student ID Card (KTM) Detection	Reading the UID from the student ID card	15	15	0	Functional
2	Database Matching with Card UID	Comparing registered and unregistered card UIDs	15	15	0	Compliant
3	LCD Text Display	Testing with registered and unregistered student ID cards	15	15	0	Functional
4	Relay and Solenoid Activation	Automatic locker unlocking	15	15	0	Opened Successfully
5	Telegram Notification	Notification message sent to Telegram	15	15	0	Delivered Successfully

However, it should be noted that these tests were conducted within certain operational constraints, such as connectivity dependencies, environmental conditions, card quality, and so on.



Figure 8. The System Successfully Detected the KTM UID

Figure 8 shows that the system successfully detected the UID from the KTM access card. This test represents the results of a functionality test to verify the system's ability to read the KTM UID.

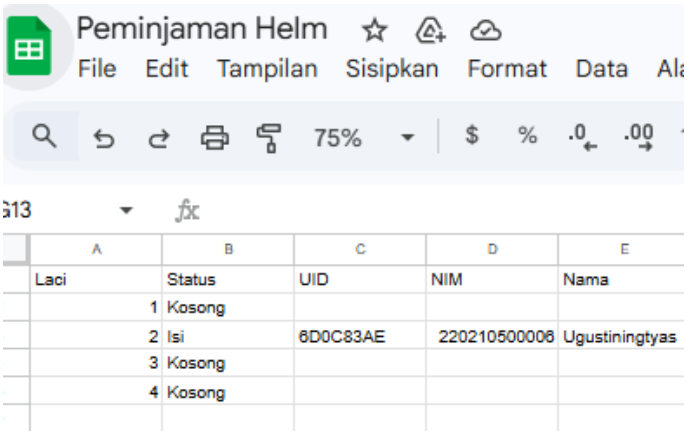

Figure 9. The System Successfully Sent Data to the Database

Figure 9 shows that the system successfully sent data to the database and received feedback from the database. These results confirm the system's ability to read every detected KTM and then compare the read UID data with the UIDs registered in the database.

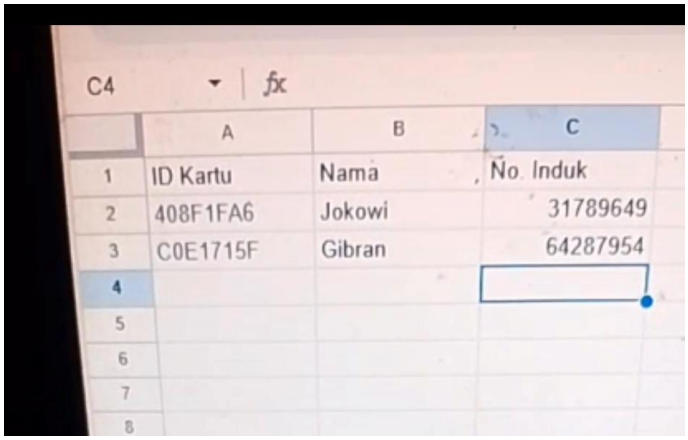

Figure 10. The System Successfully Reads and Matches UID Data

Figure 10 shows that the system successfully reads the UID and matches the data, then sends a notification to the user in the form of text displayed on the LCD.



Figure 11. Relay and Solenoid System Successfully Opens Locker

Figure 11 shows the relay and solenoid activation test to verify the system's ability to automatically control the locker opening mechanism. The test results show that when the relay is activated, the solenoid operates as commanded, allowing the locker to open automatically. The locker's condition is then observed to determine its status as "Open" or "Not Open." These findings confirm that the actuator control system functions properly in accordance with the established design.

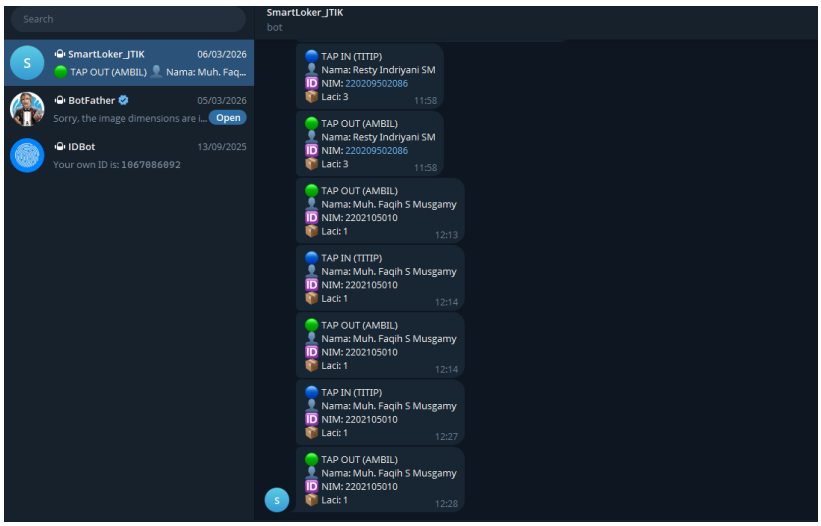

Figure 12. The System Successfully Sent a Notification to Telegram

Figure 12 shows that the system successfully sent a notification to Telegram. The Telegram bot interface displays that the notification was sent automatically. The information sent includes the KTM UID, username, and timestamp, indicating that the system is capable of providing real-time alerts to administrators. When a registered KTM is detected, the system successfully verifies it with the status "Recognized." Conversely, if an unregistered KTM is detected, the system provides two responses simultaneously: it sends a warning notification containing the user's UID and additional text that will be customized later.

Several additional test scenarios were implemented to simulate real-world conditions, as shown in Table 13 below.

Table 13. Additional Test Scenarios

No.	Testing Aspect	Test Condition	Number of Trials	Test Result
1	Wi-Fi Connection Loss	Turning off the Wi-Fi router/modem or reducing the power supply so that data cannot be transmitted/synchronized.	3	The device could not be used and was unable to execute commands for detecting and unlocking the locker because the system could not send requests to the database.
2	Database Response Delay	Sending multiple requests to the database simultaneously.	5	The device continued to operate normally because the system was configured to allow only one database request per trial.
3	Power Failure and Recovery	Disconnecting the device's power supply while the application is active and then restoring power.	2	The system automatically rebooted if the Wi-Fi connection remained active. The device returned to standby mode; however, a locker-opening failure could occur if the power interruption happened during the authentication process.
4	Damaged Card Condition	Using a defective or physically damaged card.	3	The RFID reader was still able to read the card ID correctly as long as the embedded chip remained intact.

The tests in Table 13 were conducted to determine the extent to which the system can withstand or respond to conditions outside ideal circumstances. The results show that although the system is stable under controlled conditions, there are operational vulnerabilities related to external factors. A loss of Wi-Fi connection causes a complete failure in database verification because the prototype depends on online requests before access can be granted. This internet dependency is therefore a core operational limitation for campus deployment, particularly in parking areas where network coverage may fluctuate. An offline fallback using internal memory (EEPROM/SPIFFS) could preserve basic access when connectivity is unavailable. The power-on/off scenario also reveals a risk of transaction-state loss if power is interrupted during authentication. Because the fail-secure lock becomes inaccessible without power, a state-saving recovery mechanism and a backup battery or mini UPS are recommended so that the system can complete critical operations and restore the last valid state after power returns.

System Accuracy Measurement Test Results

This test aims to measure the system's accuracy in detecting registered KTMs, matching registered UIDs with the database, and the accuracy of real-time notification delivery via the Telegram bot. Under limited testing conditions, the system demonstrated excellent performance

Table 14 presents the results of 40 trials for KTM detection, 40 trials for registered and unregistered UID matching, and 40 trials for real-time notification delivery. A 100% success rate was observed for all three parameters under the controlled testing conditions. These findings characterize functional accuracy within the tested scenarios and do not represent the full range of field conditions. In a real-world environment, electromagnetic interference, fluctuating network quality, changes in database-server load, weather exposure, and component degradation may affect long-term performance.

Table 14. System Measurement Test Results

No.	Testing Category	Number of Trials	Correct	Incorrect	Accuracy (%)
1	Student ID Card UID Detection	40	40	0	100%
2	UID Matching Accuracy with Database	40	40	0	100%
3	Real-Time Notification Delivery	40	40	0	100%

KTM UID Detection Testing

This test aims to measure the system's ability to read or detect the UID of each KTM to be used.

Table 15. KTM UID Detection Test Results

No.	User ID	Number of Trials	Detected	Not Detected	Result
1	MFZ	4	✓	-	Successful
2	AAT	4	✓	-	Successful
3	AAM	4	✓	-	Successful
4	AUZ	4	✓	-	Successful
5	STK	4	✓	-	Successful
6	NAI	4	✓	-	Successful
7	AUR	4	✓	-	Successful
8	RDM	4	✓	-	Successful
9	AAC	4	✓	-	Successful
10	IND	4	✓	-	Successful

Based on Table 15, out of a total of 40 experiments conducted on 10 different users, the system demonstrated accurate performance by successfully reading the UID on each user's KTM.

$$Accuracy = \frac{40}{40} \times 100\% = 100\%$$

The test results show that, out of 40 trials by 10 different users, all were successful. The experiment showed that, based on the calculations using the formula above, the KTM detection accuracy test yielded a result of 100%. Based on this, the KTM detection accuracy test was deemed successful.

UID Detection and Matching Testing Against the Database

This test aims to measure the system's ability to consistently identify KTMs whose data is stored (Recognized) or not stored (Not Recognized) in the database.

Table 16. Results of UID Detection and Matching Tests Against the Database

No.	Participant Code	Number of Trials	Recognized	Not Recognized	Result
1	MFZ	4	✓	–	Successful
2	AAT	4	✓	–	Successful
3	AAM	4	✓	–	Successful
4	AUZ	4	✓	–	Successful

No.	Participant Code	Number of Trials	Recognized	Not Recognized	Result
5	STK	4	✓	–	Successful
6	NAI	4	✓	–	Successful
7	AUR	4	✓	–	Successful
8	RDM	4	–	✓	Successful
9	AAC	4	–	✓	Successful
10	IND	4	–	✓	Successful

The results shown in Table 16 indicate that, out of a total of 40 trials conducted on 10 different users, the system demonstrated accurate performance. In 28 trials where the KTM status was "Recognized" (registered), the system successfully identified all cases correctly. Meanwhile, in the 12 trials with a KTM status of "Unrecognized" (unregistered), the system was also able to classify them correctly. The results were calculated using the same formula Equation (2) .

Data analysis indicates that out of 40 trials involving 10 different users, all were successful. The results show that the UID detection and database matching tests achieved a 100% success rate. Therefore, the accuracy testing and UID database matching tests are deemed successful. These results demonstrate the system's ability to distinguish between registered and unregistered cards in a limited test scenario.

Real-time Notification Delivery Testing

This test was conducted to evaluate the system's accuracy in sending alert notifications via text message through a Telegram bot after detecting both registered and unregistered KTM UIDs.

Table 17 shows the system's performance in sending real-time notifications from both registered and unregistered KTMs until the notifications are received by the administrator. These results indicate that the system is quite reliable in providing early warnings. The calculations were performed using the same formula Equation (2).

Table 17. Real-Time Notification Delivery Test Results

No.	Participant Code	Number of Trials	Test Result
1	MFZ	4	Successful
2	AAT	4	Successful
3	MAA	4	Successful
4	AAZ	4	Successful
5	STK	4	Successful
6	NAI	4	Successful
7	AUR	4	Successful
8	RDM	4	Successful
9	AAC	4	Successful
10	IND	4	Successful

The experimental findings show that all notifications were delivered in the 40 tested trials. This result demonstrates functional delivery success under the tested network conditions, not a

guarantee of uninterrupted real-time performance. The mean Telegram delivery time was 3.25 seconds, and delivery performance remained dependent on Telegram server conditions and Wi-Fi stability.

Performance Efficiency Test Results

These tests evaluated the prototype's response speed and technical performance under the defined operational conditions. The analysis considered the mean response time together with the standard deviation, minimum, and maximum values calculated from the ten participant-level averages reported for each timing parameter.

Table 18. Performance Efficiency Test Results

No.	Test Parameter	Response Time	Unit
1	Student ID Card (KTM) Detection Time	1.85	seconds
2	LCD Notification Delivery Time	3.55	seconds
3	Telegram Notification Delivery Time	3.25	seconds
4	Student ID Card (KTM) Detection Distance	1	centimeter

Based on the ten participant-level average values reported in Tables 19-21, KTM detection had a mean of 1.85 seconds (SD = 0.34; range = 1.25-2.25 seconds), LCD notification response had a mean of 3.55 seconds (SD = 0.44; range = 3.00-4.00 seconds), and Telegram notification delivery had a mean of 3.25 seconds (SD = 0.29; range = 3.00-3.75 seconds). These variability measures describe variation among the participant-level averages available in the manuscript; trial-level timing distributions were not retained. The measurements characterize prototype performance under the tested conditions and should not be generalized to all real-world environmental and network conditions.

KTM Detection Time Test

This test aims to measure the time it takes for the system to read or detect the UID of each KTM to be used

Table 19 reports a mean KTM detection time of 1.85 seconds across the ten participant-level averages, with a standard deviation of 0.34 seconds, a minimum of 1.25 seconds, and a maximum of 2.25 seconds. The mean was calculated using Equation (3).

Table 19. KTM Detection Time Test Results

No.	Participant Code	Number of Tests	Average Time (s)
1	MFZ	4	2.25
2	AAT	4	2.00
3	MAA	4	2.00
4	AAZ	4	2.25
5	STK	4	1.50
6	NAI	4	1.75
7	AUR	4	2.00
8	RDM	4	2.00
9	AAC	4	1.50
10	IND	4	1.25

No.	Participant Code	Number of Tests	Average Time (s)
	Mean / total trials	40	1.85

All 40 detection trials were completed successfully; however, the observed range shows that the response time was not identical across participants. The reported variability is based on the ten participant-level averages because individual trial-level times were not retained.

LCD Notification Delivery Time Test

This test aims to measure the system's ability to send notifications to the LCD after a user taps their card in or out.

Table 20 reports a mean LCD response time of 3.55 seconds across the ten participant-level averages, with a standard deviation of 0.44 seconds, a minimum of 3.00 seconds, and a maximum of 4.00 seconds. The calculation used Equation (3), and all 40 trials were completed successfully.

Table 20. LCD Notification Delivery Time Test Results

No.	Participant Code	Number of Trials	Average Time (s)
1	MFZ	4	4.00
2	AAT	4	4.00
3	MAA	4	3.75
4	AAZ	4	3.75
5	STK	4	3.00
6	NAI	4	3.00
7	AUR	4	3.75
8	RDM	4	4.00
9	AAC	4	3.25
10	IND	4	3.00
	Mean / total trials	40	3.55

The mean LCD response remained below the predefined five-second prototype criterion. Nevertheless, the observed range indicates measurable response-time variation. A possible bottleneck occurs when the microcontroller writes characters to the LCD while transmitting data to the server; code optimization or a higher I2C communication speed may further reduce the response time.

Telegram Notification Delivery Time Test

This test aims to measure the system's ability to send notifications to the Telegram bot after a user taps their card in or out.

Table 21 reports a mean Telegram notification delivery time of 3.25 seconds across the ten participant-level averages, with a standard deviation of 0.29 seconds, a minimum of 3.00 seconds, and a maximum of 3.75 seconds. All 40 trials were completed successfully, and the mean remained below the predefined five-second prototype criterion. The observed variation should be interpreted in relation to Wi-Fi quality and Telegram server conditions.

Table 21. Telegram Notification Delivery Test Results

No.	Participant Code	Number of Trials	Average Time (s)
1	MFZ	4	3.75
2	AAT	4	3.25
3	MAA	4	3.75
4	AAZ	4	3.25
5	STK	4	3.00
6	NAI	4	3.00
7	AUR	4	3.25
8	RDM	4	3.00
9	AAC	4	3.25
10	IND	4	3.00
	Mean / total trials	40	3.25

KTM Detection Range Testing

This test aims to measure the system's ability to read the UID of each KTM based on the distance used.

Table 22. KTM Detection Test Results

No	Name	Number of Tests	Average Distance (cm)
1	MFZ	4	1
2	AAT	4	1
3	MAA	4	1
4	AAZ	4	1
5	STK	4	1
6	NAI	4	1
7	AUR	4	1
8	RDM	4	1
9	AAC	4	1
10	IND	4	1
	Total	40	1

The research findings shown in Table 22 indicate that the average KTM detection distance was 1 cm across 40 trials, with all trials successfully detecting the card. The 1 cm reading range is acceptable for the intended locker workflow because access is designed as a deliberate tap-in/tap-out action, so close placement reduces unintended reads from nearby cards. However, this short range also introduces a usability trade-off: users must position the KTM consistently near the RFID-RC522 reader, and misalignment may increase failed-read attempts. The limited range is influenced by the RC522 antenna characteristics and the physical obstruction created by the locker-box material. Physical card damage may also reduce electromagnetic coupling, although the tested cards remained readable while their embedded chips were intact.

Reliability Test Results

This test was conducted to evaluate the system's reliability in consistently and continuously performing its primary functions under various operational conditions. The evaluation focused not only on the system's operational success but also on its ability to maintain stable performance without experiencing disruptions or failures during use.

Table 23. Reliability Test Results

No	Test Type	Number of Trials	Results		Accuracy (%)
			Success	Failures	
1	KTM UID Detection	40	40	0	100%
2	Notification Delivery	40	40	0	100%
3	Continuous Operation (12 hours)	5	5	0	100%

The aspects tested in Table 23 include KTM UID detection, notification delivery, and continuous operation over a defined period. Repeated testing was used to characterize reliability within the specified prototype scenarios. These results do not represent complete ISO/IEC 25010 reliability conformance or long-term field reliability under changing environmental, network, and hardware-aging conditions.

KTM UID Detection Testing

This test aims to measure the system's ability to read or detect the UID of each KTM that will be used repeatedly.

Table 24. KTM Detection Test Results

User code	Trials	Successes	Failures	Accuracy (%)
MFZ	4	4	-	100%
AAT	4	4	-	100%
MAA	4	4	-	100%
AAZ	4	4	-	100%
STK	4	4	-	100%
NAI	4	4	-	100%
AUR	4	4	-	100%
RDM	4	4	-	100%
AAC	4	4	-	100%
IND	4	4	-	100%

The analysis indicates that, based on the data shown in Table 24, out of a total of 40 experiments conducted on 10 different users, the system demonstrated accurate performance by successfully reading the UID on each user's KTM. The results show that repeated KTM detection tests yielded a 100% accuracy rate. Based on this, the reliability testing indicates that the system is highly reliable under the limited test conditions.

Notification Delivery Testing

This test aims to measure the system's ability to send notifications both via the LCD and in real-time through Telegram.

Table 25. Notification Delivery Testing

User code	Trials	Successes	Failures	Accuracy (%)
MFZ	4	4	-	100%
AAT	4	4	-	100%
MAA	4	4	-	100%
AAZ	4	4	-	100%
STK	4	4	-	100%
NAI	4	4	-	100%
AUR	4	4	-	100%
RDM	4	4	-	100%
AAC	4	4	-	100%
IND	4	4	-	100%

All 40 notification trials involving ten users successfully delivered the expected LCD and Telegram notifications (Table 25). The 100% success rate met the study's highly reliable category under the tested conditions; it does not establish long-term field reliability.

Continuous Operation Testing (12 Hours)

This test examined continuous operation during the specified 12-hour test periods.

Table 26. Continuous Operation Test Results

Day	Trials	Successes	Failures	Accuracy (%)
1	1	✓	-	100%
2	1	✓	-	100%
3	1	✓	-	100%
4	1	✓	-	100%
5	1	✓	-	100%

Based on Table 26, all five continuous-operation experiments conducted over five days functioned as expected. The resulting success rate was 100%; therefore, the system was classified as highly reliable under the tested conditions.

Usability Test Results (User Questionnaire)

This usability evaluation was conducted to describe preliminary user perceptions and ease of interaction with the smart locker prototype. The content-validated study-specific instrument consisted of 10 statements administered to 24 student respondents using a five-point Likert scale. The responses in Table 27 are raw scores retained in their original coding direction.

Table 27. Usability Test Results

No	Code	Statement No.										Total
		1	2	3	4	5	6	7	8	9	10	-
1	ASF	5	4	5	4	4	4	4	4	4	4	42
2	NHT	4	4	4	4	5	4	4	4	4	4	41
3	LTS	4	4	5	4	4	5	4	5	3	3	41
4	ITA	5	5	5	5	5	5	5	5	5	5	50

No	Code	Statement No.										Total
		1	2	3	4	5	6	7	8	9	10	-
5	AKM	5	5	4	5	5	5	5	5	4	5	48
6	UGS	5	5	5	5	5	5	5	5	5	5	50
7	POJ	5	5	5	5	5	4	5	4	5	5	48
8	NAI	5	5	5	5	5	4	4	5	5	4	47
9	MFF	5	4	4	5	5	4	4	5	5	4	45
10	AAT	4	5	5	5	5	4	5	5	4	3	45
11	MAA	4	4	4	5	5	4	5	4	4	3	42
12	AAZ	5	4	4	5	5	4	5	5	4	3	44
13	STK	5	5	4	4	5	4	3	5	5	5	45
14	AUR	5	4	5	5	5	4	5	5	4	3	45
15	HDY	5	4	4	5	5	5	4	5	5	4	46
16	DSM	5	4	4	5	5	3	5	5	4	4	44
17	MLH	5	5	4	4	5	4	4	5	5	4	45
18	MFQ	4	4	4	5	4	5	4	5	5	5	45
19	RIS	4	5	5	4	5	4	4	5	4	3	43
20	ZAR	5	4	4	5	5	4	5	4	4	3	43
21	NSE	5	4	5	5	4	5	4	5	5	5	47
22	HZH	5	4	4	5	5	4	4	4	5	5	45
23	MAT	5	5	4	5	5	5	5	4	5	3	46
24	STA	5	5	5	4	5	5	4	4	3	3	43
Total		114	107	107	113	116	104	106	112	106	95	1,080

Note: Table 27 presents raw Likert responses in their original scoring direction. The negatively worded items were not transformed, and the respondent totals are shown only for transparency; they are not interpreted as a standardized overall usability or feasibility score.

$$x = \frac{\sum x}{n}$$

The sum of the 24 raw respondent totals in Table 27 is 1,080. Dividing this value by 24 produces a mean raw respondent total of 45.00 out of 50, as shown in Equation (5).

$$x = \frac{1{,}080}{24} = 45.00$$

The mean raw total of 45.00 is not classified as "Highly Feasible" because the questionnaire contains mixed-polarity statements retained in their original scoring direction and was developed specifically for this study. Accordingly, the questionnaire findings are reported as preliminary descriptive user perceptions. The high raw scores observed across both positively and negatively worded items also require cautious interpretation and may reflect response-direction effects that should be addressed in future instrument refinement.

Security Testing Results

This test aims to assess the system's security level in protecting access and preventing unauthorized actions. The evaluation focuses on the system's ability to distinguish between registered and unregistered users, manage potential abuses such as duplicate access (spam scans), and maintain a locked state during manual intrusion attempts.

Table 28 summarizes the tested access-control and physical-misuse scenarios: 10 registered-card tests, 10 unregistered-card tests, 10 repeated-scan tests, and five limited manual opening attempts. Within these specific scenarios, the system correctly distinguished registered and unregistered access and remained locked during the limited manual attempts. These observations do not establish comprehensive cyber or physical security.

Table 28. Security Test Results

No.	Test scenario	Expected result	Successes	Failures
1	Registered KTMs accessed	Locker opens successfully	10	0
2	Access to unregistered KTMs	Lock remains locked	10	0
3	Repeated scans	Each UID can only perform Tap-in and Tap-out alternately.	10	0
4	Manual opening attempts	The system remains locked	5	0

However, these security tests were limited to basic access-control and physical-misuse scenarios: registered access, unregistered access, repeated scans, and simple manual bypass attempts. The prototype was not evaluated against advanced threats such as RFID cloning, UID spoofing, replay attacks, database or Google Apps Script endpoint manipulation, Telegram bot-token exposure, or attacks on communication encryption. Therefore, the reported security results demonstrate resistance only under the tested scenarios and should not be interpreted as proof of comprehensive system security. Future work should evaluate these attack vectors and incorporate stronger credential protection, secure endpoint controls, encrypted communication, and circuit-level protection.

Testing of Registered KTMs

This test was conducted to ensure that the system is capable of granting valid access to users registered in the database. Each registered KTM was tested by scanning it with the RFID module.

Table 29. Results of Registered KTM Access Testing

Trial	Finding	Successful	Failed
1	Locker opened successfully	Yes	-
2	Locker opened successfully	Yes	-
3	Locker opened successfully	Yes	-
4	Locker opened successfully	Yes	-
5	Locker opened successfully	Yes	-
6	Locker opened successfully	Yes	-
7	Locker opened successfully	Yes	-
8	Locker opened successfully	Yes	-
9	Locker opened successfully	Yes	-
10	Locker opened successfully	Yes	-

The results in Table 29 show that all 10 registered-card tests opened the locker as expected. This demonstrates that the RFID UID-based authentication and database-verification workflow functioned successfully for the registered cards used in the controlled trials. The result should be interpreted within the tested scenarios and does not establish resistance to untested credential attacks or broader deployment reliability.

Testing for Unauthorized KTM Access

This test aims to evaluate the system's ability to deny access to unregistered users. Several KTMs not found in the database were used as test inputs.

Table 30. Results of the Unregistered KTM Access Test

Trial	Finding	Successful	Failed
1	Locker remained locked	Yes	-
2	Locker remained locked	Yes	-
3	Locker remained locked	Yes	-
4	Locker remained locked	Yes	-
5	Locker remained locked	Yes	-
6	Locker remained locked	Yes	-
7	Locker remained locked	Yes	-
8	Locker remained locked	Yes	-
9	Locker remained locked	Yes	-
10	Locker remained locked	Yes	-

The results in Table 30 show that all tested unregistered KTMs were consistently denied access and the locker remained locked. This indicates that the UID-based validation mechanism successfully prevented unauthorized access under the specific unregistered-card scenarios tested, with no false acceptance observed in these trials. These results should not be generalized to untested attacks such as RFID cloning, UID spoofing, replay attacks, or backend compromise.

Dual-Access Testing

Dual-access testing was conducted to identify potential system misuse, particularly in situations involving repeated or non-sequential card scans. In this scenario, the same UID was used to scan the card multiple times without following the proper usage procedure (tap-in and tap-out).

Table 31. Results of Dual-Access Testing

Trial	Finding	Successful	Failed
1	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
2	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
3	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
4	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
5	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
6	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
7	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
8	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
9	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-
10	Each UID can only perform Tap-in and Tap-out alternately.	Yes	-

The results in Table 31 show that the system enforced the predefined alternating tap-in and tap-out workflow in all 10 repeated-scan tests. This demonstrates that the programmed logical control operated as intended under the tested abnormal-use scenario, but it does not represent protection against advanced replay, cloning, or backend attacks.

Manual Testing (Physical Forced Entry)

This test examined whether the locker remained closed during five limited manual opening attempts performed without a KTM. The test was non-instrumented: applied force, tools, duration, and access points were not standardized or quantitatively measured. It therefore represents only a basic operational check rather than a formal physical-security or forced-entry test.

Table 32. Manual Testing Results

Trial	Finding	Successful	Failed
1	The system remains locked	Yes	-
2	System remains locked	Yes	-
3	System remains locked	Yes	-
4	System remains locked	Yes	-
5	System remains locked	Yes	-

In the five limited manual attempts reported in Table 32, the locker remained closed and did not respond electronically. This finding demonstrates resistance only to the specific non-instrumented attempts conducted. It should not be interpreted as evidence of adequate or comprehensive physical security, because force, tools, duration, structural resistance, and standardized acceptance criteria were not evaluated.

Discussion

To highlight the contribution and novelty of this research, a comparative analysis was conducted of several previous studies on similar topics in the development of smart locker systems based on identification and access control technologies. Abdahu et al. (2024) developed a Smart Helmet Cabinet using mobile QR Code authentication, with ESP32-CAM employed to scan user credentials and ESP32 NodeMCU used to control the locker access mechanism. Their system demonstrated that digital authentication could be effectively applied to identify users and manage access to secure helmet storage. However, the system relied on QR Code-based authentication and did not utilize existing institutional identity cards as access credentials. In contrast, the system developed in this study uses RFID-enabled Student Identity Cards (KTM) integrated with ESP32, allowing students to access the locker using their existing campus identification cards while also supporting cloud-based data logging and real-time Telegram notifications.

Rozy and Fahruzi (2022) utilized the PN532 RFID/NFC module for card authentication and reported that reading performance was influenced by distance and obstacles. In the present prototype, the RC522 module successfully read the tested cards at an intentional tap distance of approximately 1 cm under controlled conditions. The system also integrated cloud logging and notification functions; however, the short reading range and dependence on network connectivity remain practical limitations.

Amin et al. (2022) developed an Android application-based notification system using NodeMCU, whereas the present prototype used Telegram as an existing cross-platform notification medium. Nugraha et al. (2024) implemented a Bluetooth Low Energy (BLE)-based keyless system using ESP32 and reported sensitivity to physical obstacles and environmental conditions. The present study used RFID-enabled KTM authentication and achieved successful access-control operation in the defined trials. These comparisons indicate differences in implementation approach, but they do not establish that RFID is universally more stable or secure than BLE or other authentication technologies.

Based on these comparisons, the contribution of this study is a prototype-level integrated access-control and monitoring pipeline rather than a technically novel component or evidence of deployment readiness. The system combines ESP32, RFID-enabled KTM authentication, cloud-based records, and real-time notifications. Under controlled testing conditions, functional suitability and repeated-operation testing each achieved 100% success. The participant-level timing summaries

were 1.85 seconds for KTM detection (SD = 0.34; range = 1.25-2.25), 3.55 seconds for LCD response (SD = 0.44; range = 3.00-4.00), and 3.25 seconds for Telegram notification delivery (SD = 0.29; range = 3.00-3.75).

The evaluation was informed by selected ISO/IEC 25010 quality characteristics rather than conducted as a complete conformity assessment. Smart-campus literature identifies IoT, cloud computing, and RFID as enabling technologies for connected campus services. Within the limitations of a single-locker prototype, controlled tests, internet dependency, and preliminary user-perception data, the present integration may be viewed as a small-scale access-control and monitoring component with potential relevance to future smart-campus development.

CONCLUSION

This study developed an ESP32-based smart helmet locker using RFID-enabled student identity cards (KTM), Google Sheets and Google Apps Script logging, and Telegram notifications. Functional and repeated-operation tests each achieved 100% success under the controlled test conditions. Mean card-detection, LCD-response, and Telegram-notification times were 1.85, 3.55, and 3.25 seconds, respectively. The results demonstrate prototype-level access control and monitoring, rather than a measured reduction in helmet theft.

The evaluation was limited to a single prototype, selected quality characteristics, and a small user sample. The mixed-polarity questionnaire responses were retained in their original direction, so the raw mean total of 45.00 out of 50 is not a validated overall usability score. Future work should refine the instrument, test offline recovery and stronger authentication, assess multiple lockers under varied network and environmental conditions, and measure field security outcomes before deployment claims are made.

ACKNOWLEDGMENT

The authors would like to express their sincere appreciation to the Department of Informatics and Computer Engineering, Faculty of Engineering, Universitas Negeri Makassar, for providing academic support and facilities throughout this research. The authors are also grateful to the supervisors and validators for their valuable guidance, suggestions, and constructive feedback during the development and evaluation of the proposed system. In addition, the authors would like to thank all respondents who participated in the usability testing and system evaluation process. Their contributions and participation played an important role in the successful completion of this study.

AUTHOR CONTRIBUTION STATEMENT

MFR: Conceptualization, Methodology, Software, Investigation, Formal Analysis, Writing - Original Draft. HA: Methodology, Supervision, Writing - Review & Editing. SGZ: Methodology, Supervision, Writing - Review & Editing. JMP: Validation, Supervision, Writing - Review & Editing. SA: Methodology, Validation, Formal Analysis, Writing - Review & Editing. All authors read and approved the final version of the manuscript.

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known financial, professional, or personal conflicts of interest that could have influenced the work reported in this manuscript.

AI DISCLOSURE STATEMENT

During the preparation of this manuscript, the authors utilized ChatGPT, an artificial intelligence tool developed by OpenAI, to assist with language enhancement, grammar correction, and improvement of the overall readability of the manuscript. All outputs generated with the assistance of this tool were carefully reviewed, revised, and verified by the authors to ensure the accuracy, originality, and integrity of the scientific content. The authors assume full responsibility for all statements, interpretations, and conclusions presented in this manuscript.

REFERENCES

[1] A. S. Rahmatullah, D. S. Kencono, and E. Harianto, "Membangun budaya tertib lalu lintas di kalangan pelajar: Studi pengabdian di MA Plus Nururrohmah [Building a culture of traffic discipline among students: A community service study at MA Plus Nururrohmah]," *Jurnal Penelitian and Pengabdian Masyarakat*, vol. 3, no. 3, Aug. 2025, doi: 10.61231/jp2m.v3i3.374.

[2] S. S. Bosawer, R. Rahmadian, and Z. D. Rofinda, "Hubungan penggunaan helm dengan derajat cedera kepala akibat kecelakaan lalu lintas pada pengendara sepeda motor di RSUP Dr. M. Djamil Padang tahun 2016-2017 [Association between helmet use and the severity of head injuries resulting from traffic accidents among motorcycle riders at Dr. M. Djamil General Hospital Padang, 2016-2017]," *Jurnal Ilmu Kesehatan Indonesia*, vol. 1, no. 3, pp. 352-357, May 2021, doi: 10.25077/jikesi.v1i3.74.

[3] J. Sudastin and Y. Alwinda, "Studi karakteristik pengendara sepeda motor and penggunaan helm di Kabupaten Kuantan Singingi [A study of motorcycle rider characteristics and helmet use in Kuantan Singingi Regency]," *Journal of Infrastructure and Civil Engineering*, vol. 1, no. 1, pp. 22-34, 2021, doi: 10.35583/jice.v1i01.5.

[4] N. Hifzilia, R. Zalida, F. P. Ali, H. N. Khairiyyah, and Yoserizal, "Analisis kepatuhan mahasiswa terhadap aturan lalu lintas di lingkungan Universitas Andalas: Studi kasus pada pemakaian helm [Analysis of student compliance with traffic regulations at Universitas Andalas: A case study of helmet use]," *Jurnal Kewarganegaraan*, vol. 1, no. 1, Nov. 2024.

[5] L. Liu, H. Liu, D. Long, and X. Huang, "Revealing the differences in bicycle theft and motorcycle theft: Spatial patterns and contributing factors," *Humanities and Social Sciences Communications*, vol. 12, no. 1, Art. no. 174, Feb. 2025, doi: 10.1057/s41599-025-04507-6.

[6] J. S. Yalli, M. H. Hasan, and A. A. Badawi, "Internet of Things (IoT): Origins, embedded technologies, smart applications, and its growth in the last decade," *IEEE Access*, vol. 12, pp. 91357-91382, 2024, doi: 10.1109/ACCESS.2024.3418995.

[7] H. Zhang, R. Zhang, and J. Sun, "Developing real-time IoT-based public safety alert and emergency response systems," *Scientific Reports*, vol. 15, no. 1, Art. no. 29056, Aug. 2025, doi: 10.1038/s41598-025-13465-7.

[8] H. A. Wahid, J. Maulindar, and A. I. Pradana, "Rancang bangun sistem penyiraman tanaman otomatis Aglaonema berbasis IoT menggunakan Blynk and NodeMCU-32 [Design and implementation of an IoT-based automatic watering system for Aglaonema using Blynk and NodeMCU-32]," *Innovative: Journal of Social Science Research*, vol. 3, no. 2, pp. 6265-6276, 2023.

[9] H. Belfqih and A. Abdellaoui, "Decentralized blockchain-based authentication and InterPlanetary File System-based data management protocol for Internet of Things using ASCON," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, Art. no. 16, Apr. 2025, doi: 10.3390/jcp5020016.

[10] A. C. Permana, A. I. Pradana, and D. Hartanti, "Smart loker berbasis IoT dengan autentikasi QR code terintegrasi dengan web [IoT-based smart locker with web-integrated QR-code authentication]," *Jurnal Informatika and Teknik Elektro Terapan*, vol. 13, no. 3, Jul. 2025, doi: 10.23960/jitet.v13i3.6573.

[11] A. Mardhatillah and Dahliyusmanto, "Sistem notifikasi and kontrolling smart home berbasis Internet of Things [Internet of Things-based smart-home notification and control system]," *INOVTEK Polbeng - Seri Informatika*, vol. 9, no. 1, Jun. 2024, doi: 10.35314/isi.v9i1.4043.

[12] M. R. Abdahu, U. Ristian, and H. Hasfani, "Implementasi smart helmet cabinet pada penyimpanan helm berbasis mobile QR code [Implementation of a mobile QR code-based smart helmet cabinet for helmet storage]," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 9, no. 1, pp. 78–85, Jan. 2024, doi: 10.30591/jpit.v9i1.6593.

[13] F. Rozy and I. Fahruzi, "Sistem pengaman loker menggunakan smart card PN532 RFID/NFC [Locker security system using a PN532 RFID/NFC smart card]," *Jurnal Integrasi*, vol. 14, no. 2, pp. 114-121, Oct. 2022, doi: 10.30871/ji.v14i2.4503.

[14] M. Amin, R. Ananda, M. H. Habib, and N. Novita, "Implementasi kartu tanda penduduk sebagai kunci loker helm di Kampus STMIK Royal Kisaran dengan memanfaatkan notifikasi Android [Implementation of the national identity card as a helmet-locker key at STMIK Royal Kisaran using Android notifications]," *Teknisi*, vol. 2, no. 2, p. 75, Aug. 2022, doi: 10.54314/teknisi.v2i2.1108.

[15] K. S. Nugraha, A. O. Putri, and L. P. Pratama, "Rancang bangun smart keyless locker dengan BLE tag and ESP32 pada loker kunci ruangan lab di Laboratorium JakartaGlobal University [Design and implementation of a smart keyless locker using BLE tags and ESP32 for laboratory room-key lockers at JakartaGlobal University]," *Kohesi: Jurnal Multidisiplin Saintek*, vol. 4, no. 6, 2024.

[16] A. Fikri, "Simple IoT-based home security system using ESP32 and Blynk," *Data Science: Journal of Computing and Applied Informatics*, vol. 9, no. 2, Aug. 2025, doi: 10.32734/jocai.v9.i2-22595.

[17] V. Popa, A. I. Petrariu, P. M. Mutescu, A. A. Maftei, and A. Lavric, "Standalone RFID access control system with data-integrity verification capabilities," *Sensors*, vol. 26, no. 9, Art. no. 2892, May 2026, doi: 10.3390/s26092892.

[18] S. R. Mhaskar, "RFID and IoT-based personalized access system," *International Journal of Scientific Research in Engineering and Management*, vol. 9, no. 4, pp. 1-9, Apr. 2025, doi: 10.55041/IJSREM46634.

[19] F. Hidayat and M. Nizar, "Model ADDIE (analysis, design, development, implementation, and evaluation) dalam pembelajaran pendidikan agama Islam [The ADDIE model (analysis, design, development, implementation, and evaluation) in Islamic religious education learning]," *Jurnal Inovasi Pendidikan Agama Islam*, vol. 1, no. 1, pp. 28-38, Dec. 2021, doi: 10.15575/jipai.v1i1.11042.

[20] A. W. Bramantyo, "Perancangan sistem kontrol akses rumah pintar menggunakan RFID dengan mikrokontroler ESP32 [Design of a smart-home access-control system using RFID and an ESP32 microcontroller]," *Jurnal Restikom: Riset Teknik Informatika and Komputer*, vol. 7, no. 3, pp. 374-382, 2025.

[21] O. D. Hussein and A. Muhudin, "Smart logistics: Leveraging RFID and IoT for seamless operations," *SSRG International Journal of Electronics and Communication Engineering*, vol. 11, no. 11, pp. 146-152, Nov. 2024, doi: 10.14445/23488549/IJECE-V11I11P113.

[22] A. Wardana, A. A. Batubara, B. S. Wanandi, C. Muzaddidah, K. Andrea, and M. A. Hafizh, "Rancangan desain prototipe RFID pada presensi mahasiswa menggunakan KTM di Program Studi Sistem Informasi UINSU [Design of an RFID prototype for student attendance using student identity cards in the Information Systems Study Program at UINSU]," *JUKTISI*, vol. 1, no. 3, pp. 199-207, Feb. 2023, doi: 10.62712/juktisi.v1i3.40.

[23] K. Baba, N.-E. Elfaddouli, and N. Cheimanoff, "The role of information and communication technologies in developing a smart campus with its four pillars' architectural sketch," *Education and Information Technologies*, vol. 29, pp. 14815-14833, 2024, doi: 10.1007/s10639-023-12445-6.

[24] M. A. Putriasih, U. K. Usman, and A. Hambali, "RFID access control for underground optical distribution cabinets with real-time monitoring via Google Sheets," *in 2025 12th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2025, pp. 1-7, doi: 10.1109/ICITACEE66165.2025.11233066.

[25] F. M. Sarimole, S. W. Yudha, Sutisna, and R. A. Akmal, "Implementation of an RFID card-based automatic door lock system using NodeMCU with integration of Telegram notifications and IoT services," *International Journal of Applied Mathematics and Computing*, vol. 2, no. 4, pp. 16–23, Oct. 2025, doi: 10.62951/ijamc.v2i4.126.

[26] F. T. Yuniko, W. Anaputri, and T. Hadyanto, "Rancang bangun sistem monitoring jam malam asrama mahasiswa berbasis IoT menggunakan KTM and notifikasi Telegram di Universitas Dharmas Indonesia [Design and implementation of an IoT-based student dormitory curfew monitoring system using student ID cards and Telegram notifications at Universitas Dharmas Indonesia]," *Journal of Vocational Education and Information Technology*, vol. 7, no. 1, pp. 219–226, 2026, doi: 10.56667/jveit.v7i1.2324.