Design and Development of an IoT-Based Room Access Security System with Password Authentication and Real-Time Notification

Ali Ramschie
Department of Electrical Engineering
Manado State Polytechnic

Ronny Katuuk
Department of Computer Engineering
Manado State Polytechnic

Fanny Doringin
Department of Electrical Engineering
Manado State Polytechnic

Sulastri Eksan
Department of Computer Engineering
Manado State Polytechnic

ABSTRACT

Room access security is an essential aspect of safeguarding both physical assets and sensitive data. Although the use of physical keys and access cards is still common, both methods have their weaknesses. Keys can be lost or duplicated, while access cards are at risk of being misused by unauthorized individuals. Such situations may reduce the level of security, especially if not supported by a reliable monitoring system. Therefore, a more modern and secure technology-based solution is needed to ensure room security through the implementation of an IoT-based access control system.

This research designs a room access security system utilizing Internet of Things (IoT) technology, with authentication carried out through password input on a keypad device. If any suspicious access activity occurs, the system will automatically send a notification to the room owner’s smartphone. With this feature, the owner can directly receive information about both authorized and unauthorized access activities.

The method applied in this research is prototyping, with a workflow that includes problem identification, data collection, system design, prototype development, implementation, and system evaluation. The results show that the IoT-based room access security system with password authentication via keypad functions properly. When the detected password input is correct, the door will unlock, and the electrical system in the room will be activated. If the password input is incorrect, the alarm will sound, and the system will send a notification to the owner’s smartphone. Consequently, the room owner can disable the password input function via the keypad and also monitor the room condition through CCTV access.

Keywords

IoT, Room Access Security, Password Authentication, Real-Time Notification, Prototyping Method

1. INTRODUCTION

Room access security is an essential aspect in protecting both physical assets and sensitive data. Conventional methods such as physical keys and access cards are still widely used, but both have inherent weaknesses. Keys can be lost or duplicated, while access cards are vulnerable to misuse by unauthorized individuals [1]. Such conditions may reduce the level of security, especially if not supported by a reliable monitoring system [2]. Therefore, there is a need for a more modern, adaptive, and secure technology-based solution.

The advancement of the Internet of Things (IoT) has created new opportunities for developing intelligent security systems, including room access control. IoT enables the integration of hardware, software, and internet connectivity, allowing systems to provide authentication, monitoring, and real-time notifications [3], [4]. IoT also facilitates room owners to directly receive information on access activities, whether authorized or unauthorized, through smart devices [5].

Several studies have demonstrated that IoT-based implementations in room security systems can improve efficiency and reliability. Akbari et al. proposed a smart door framework using mmWave radar and face recognition, which proved effective in detecting illegal access with high accuracy [6]. Vardakis et al. reviewed smart home security based on IoT and concluded that authentication and real-time monitoring are critical factors in mitigating unauthorized access risks [7]. Other research has also highlighted the need for strong authentication mechanisms, such as passwords, biometrics, and multi-factor authentication [8], [9].

Password-based keypad authentication remains a relevant alternative because it is simple, cost-effective, and easy to implement. However, without integration with alarms and notification systems, this method remains vulnerable to brute force attacks and unauthorized usage [10]. Some studies have enhanced this approach with smartphone-based notifications to improve owner responsiveness to threats [11], [12]. Furthermore, integration with CCTV systems provides an additional layer of real-time visual monitoring [13].

The prototyping methodology is often employed in the development of IoT-based security systems, as it supports rapid design cycles from problem identification, design, implementation, to evaluation [14]. Through this approach, prototypes can be tested directly to assess the reliability of authentication and the effectiveness of notifications [15].

Based on the aforementioned literature, this research designs a room access security system using IoT with password authentication through a keypad. The system is equipped with an alarm and smartphone notifications for unauthorized access attempts. Integration with a CCTV system is also included to enhance the overall room security level.

2. METHODOLOGI

In developing a prototype of an IoT-Based Room Access Security System with Password Authentication and Real-Time Notification, the development process involves several stages, including:

2.1 System Design through Block Diagram and Wiring Representation

The development of an IoT-Based Room Access Security System with Password Authentication and Real-Time Notification, begins with the creation of a block diagram representation. This block diagram illustrates the structural model of the proposed Room Access System, serving as the foundation for subsequent hardware wiring and system implementation, as shown in the Figure 1.

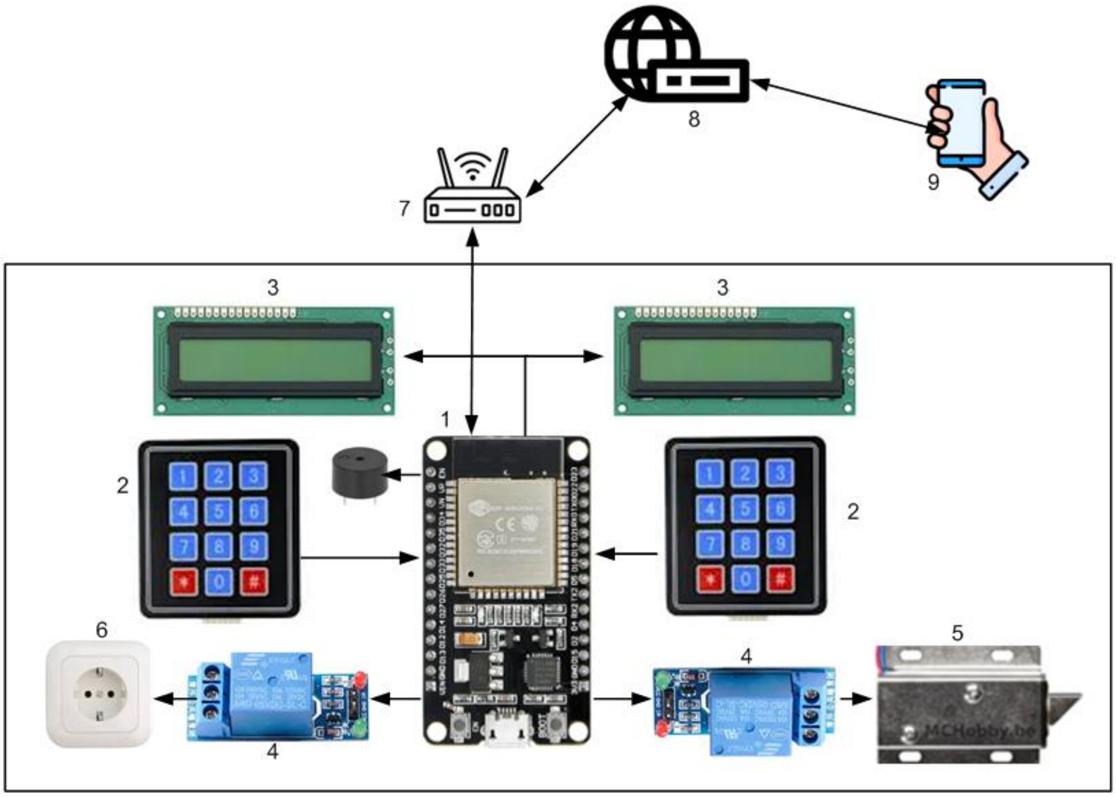


Fig 1: Block Diagram of the Proposed System

Description of the System Block Diagram:

1. **Controller** functions as the central data processing unit for verifying password inputs, granting access to the private room, and controlling the electrical system within the room when access is authorized. Additionally, the controller serves as a communication medium with the web server for monitoring the room access system. If unauthorized access is detected, the controller automatically sends a notification to the room owner through the web server, enabling the owner to disable the access system remotely via a smartphone application integrated with the IoT service provider's platform.
2. **Keypad** functions as the input interface for entering the password, both for accessing the room, locking the door, and when exiting the room.
3. **LCD Display** functions as the information display medium, providing feedback during the password input procedure, indicating whether access is granted or denied, showing occupancy status, and displaying whether the access system is active or locked by the room owner.
4. **Relay Driver** functions as the On/Off switch for the electrical system inside the room, as well as the On/Off controller for the solenoid door lock to open and close the door.
5. **Solenoid door lock** functions as the key mechanism for opening and closing the door.
6. The electrical system inside the room when access is granted.
7. **Access Point (Wi-Fi)** serves as the internet communication medium between the controller and the web server for monitoring and controlling the room access system.
8. **Web Server** serves as the platform for users to remotely monitor and control the security system through a smartphone device.
9. **The user device**, in this case a smartphone, functions as a medium for monitoring and remotely controlling the room access system.

After completing the system block diagram design, the next step is to develop the integrated wiring circuit for the IoT-based room security control and monitoring system. The wiring diagram is presented in the figure 2.

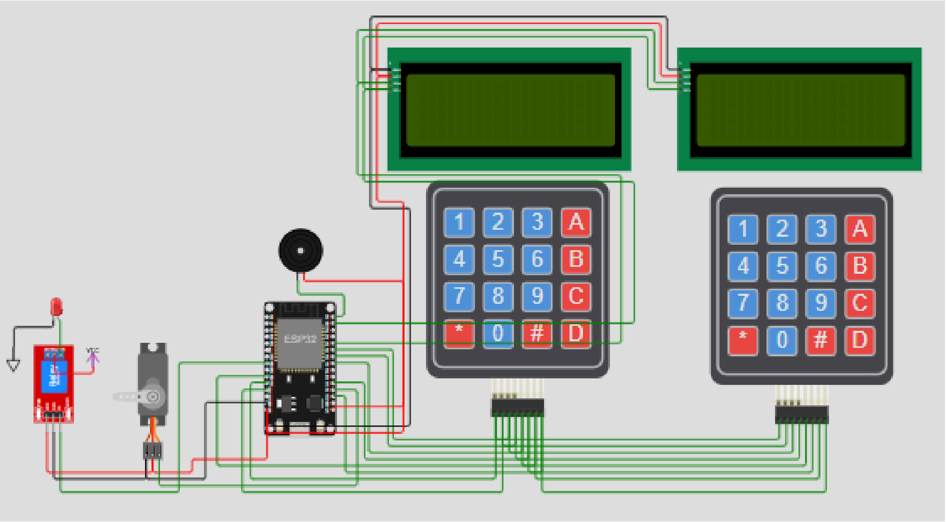


Fig 2: System Wiring

2.2 System Algorithm

The system algorithm is the initial stage in developing the software used to operate the time-based automatic vannamei shrimp feeding system. This algorithm is structured according to the procedural workflow of the system, which is illustrated in the form of a flowchart. The system workflow diagram is shown in Figure 3.

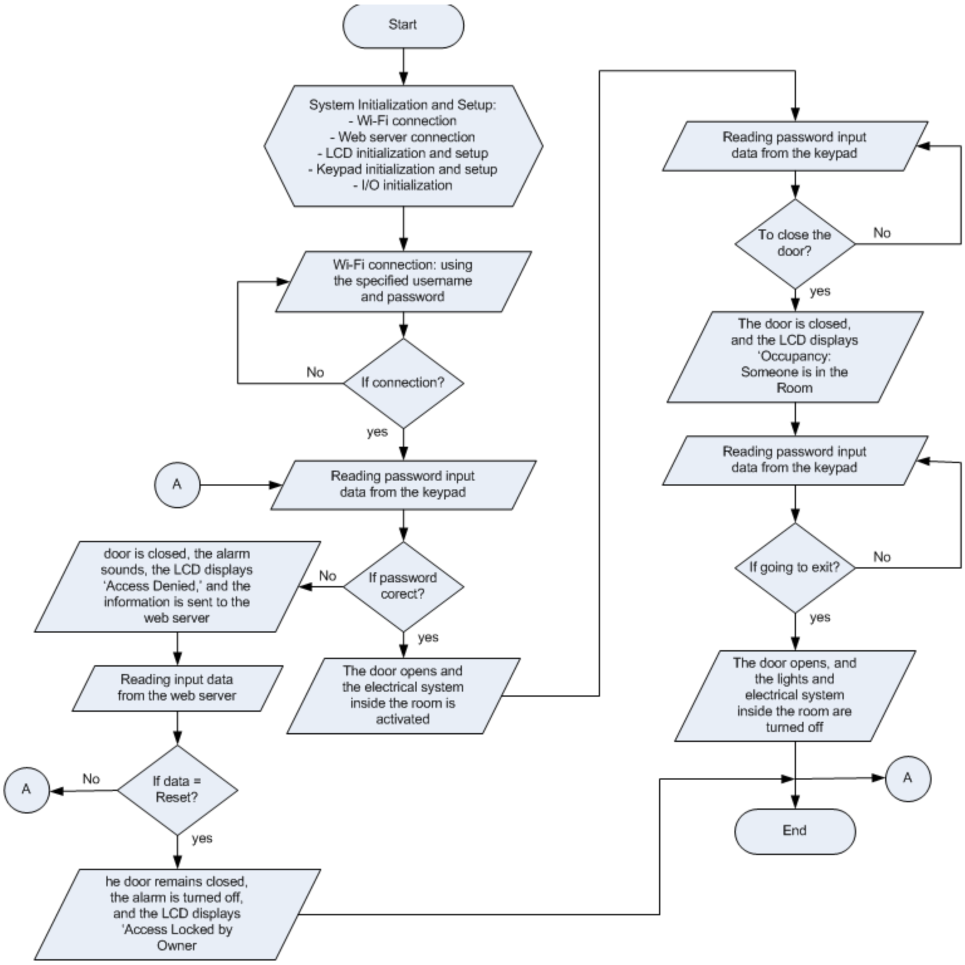

Start
System Initialization and Setup:
- Wi-Fi connection
- Web server connection
- LCD initialization and setup
- Keypad initialization and setup
- I/O initialization
Wi-Fi connection: using the specified username and password
No
If connection?
yes
A
Reading password input data from the keypad
door is closed, the alarm sounds, the LCD displays 'Access Denied,' and the information is sent to the web server
No
If password corect?
yes
Reading input data from the web server
The door opens and the electrical system inside the room is activated
A
No
If data = Reset?
yes
he door remains closed, the alarm is turned off, and the LCD displays 'Access Locked by Owner
Reading password input data from the keypad
To close the door?
No
yes
The door is closed, and the LCD displays 'Occupancy: Someone is in the Room
Reading password input data from the keypad
If going to exit?
No
yes
The door opens, and the lights and electrical system inside the room are turned off
A
End

Fig 4: The Flowchart system

The Flowchart Working Procedure is as follows:

1. **System Initialization and Setup:** When the system is powered on, the first step is system initialization and setup. This includes initializing the necessary libraries and connecting the controller to the web server via the access point (Router) using the access point name, web server address, and token from the web server dashboard. The connection procedure continues until a successful connection is established. Once the connection is successful, the next procedure is executed.

2. **Reading Password Input:** The system reads the password input for room access via the keypad, where the password is set as “1002.” If the entered password is correct, the system unlocks the door by activating the solenoid door lock, which functions as the key mechanism. When the door opens, the room’s electrical system is simultaneously activated, indicated by the lights turning on, and the LCD displays the message: “Door Open, Someone is in the Room.” If the password input is incorrect, the system automatically triggers the alarm and sends a pop-up notification indicating that an unauthorized person attempted to access the room. Based on this notification, the room owner can remotely lock the access system via a smartphone connected to the web server. When the controller detects from the web server that the room access system has been locked, the alarm is automatically deactivated, and the access system becomes unusable.
3. **Closing the Door after Entry:** Once the door has been opened and the person is inside the room, the next procedure is to close the door by pressing the letter “A” on the keypad. When the “A” key is pressed, the door is closed via the solenoid lock, and the LCD displays the message: “Someone is in the Room.” The same information is also sent to the web server.
4. **Exiting the Room:** To exit the room, the procedure is similar to point 2, involving authentication via the web server. After leaving the room and intending to close the door, the user presses the “B” button on the keypad. When this button is pressed, the door automatically closes, and the system returns to the initial procedure of reading password input for access to the private room.

2.3 System Manufacturing

In the development of a room security system prototype based on the Internet of Things (IoT), the process begins with the utilization of input data through keypad operations. The data entered via the keypad is processed by a microcontroller, which functions as the central controller to manage access authorization to the room. The initial stage involves the design and implementation of the hardware, realized through the integration of supporting components with the microcontroller according to the system design specifications.

In addition to hardware development, this stage also includes the design of the software responsible for operating the system based on the established algorithm. The software is subsequently embedded into the microcontroller to enable the autonomous operation of the IoT-based room security system.

Furthermore, the development process incorporates the implementation of a web server using Blynk IoT, which serves as a platform for system monitoring and control. Through this web server, users can remotely monitor room access conditions and manage the security system, thereby enhancing the flexibility and reliability of the developed prototype.

2.3.1 *Hardware Manufacturing*

The hardware design of the IoT-based room security system was developed based on the initial design, which consisted of a block diagram and circuit wiring schematic. The implementation was carried out by integrating all components that support the functionality of the system. The controller serves as the central controller, responsible for processing input data from the keypad as well as transmitting and receiving data to and from the web server via a Wi-Fi connection. Two keypads function as input devices for entering access codes into the system, while two LCD modules are utilized to display relevant information such as code entry instructions, verification status (success or failure), and additional messages.

For the actuation process, a relay is employed to control the solenoid door lock by enabling or disabling it according to the keypad verification results. The solenoid door lock acts as an automatic locking mechanism that unlocks when the entered code is valid. Additionally, a buzzer provides audio feedback, serving either as an alert when an incorrect code is entered or as a notification when access is granted. The prototype system is shown in Figure 5.

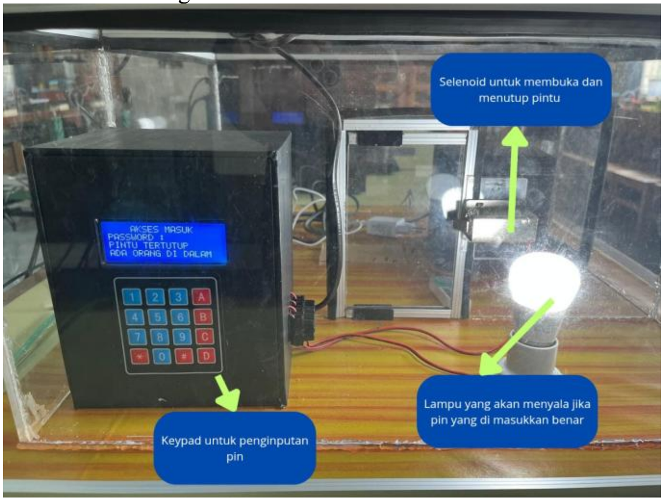

Selenoid untuk membuka dan menutup pintu
AKSES MASUK
PASSWORD :
PINTU TERTUTUP
ADA ORANG DI DALAM
1 2 3 A
4 5 6 B
7 8 9 C
* 0 # D
Lampu yang akan menyala jika pin yang di masukkan benar
Keypad untuk penginputan pin

Fig 5: The Prototype system

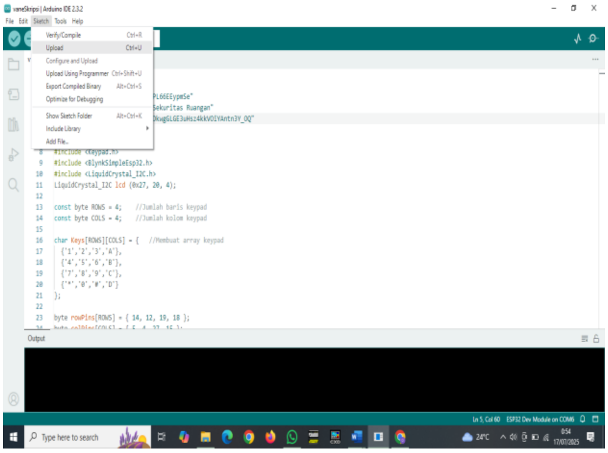
2.3.2 *Software Development For Controller Operations*

The development of the software required for the control and monitoring functions of the IoT-based room security system was carried out based on the system design represented in the form of a flowchart. The flowchart serves as a fundamental guideline for structuring the program logic, ensuring that each operational procedure of the system is represented in a systematic and coherent manner.

The software was developed using the Arduino IDE, selected for its compatibility with various microcontrollers, its user-friendly programming interface, and its extensive library support, which facilitates the integration of components such as the keypad, LCD, relay, and Wi-Fi communication modules. Furthermore, the Arduino IDE provides efficient debugging capabilities, thereby accelerating the testing and refinement process of the implemented program.

The software development stages included library initialization, system parameter configuration, implementation of access authentication algorithms, and the integration of communication between the microcontroller and the web server. These processes were designed to ensure that the software not only controls the hardware according to the established design but also enables reliable system monitoring.

The software design and development process is illustrated in Figure 6, which depicts the flow of program implementation from the initial design phase to the embedding of the software into the microcontroller. Consequently, the developed software functions not only as the central controller of the system but also as a critical interface that ensures real-time interaction between the hardware and the IoT-based server.



```
PL66EEypmSe"
Sekuritas Ruangan"
DkwgGLGE3uHsz4kkVOIYAntn3Y_0Q"

#include <Keypad.h>
#include <BlynkSimpleEsp32.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd (0x27, 20, 4);

const byte ROWS = 4;    //Jumlah baris keypad
const byte COLS = 4;    //Jumlah kolom keypad

char Keys[ROWS][COLS] = {   //Membuat array keypad
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};

byte rowPins[ROWS] = { 14, 12, 19, 18 };
```

Fig 6: Software Development for controller

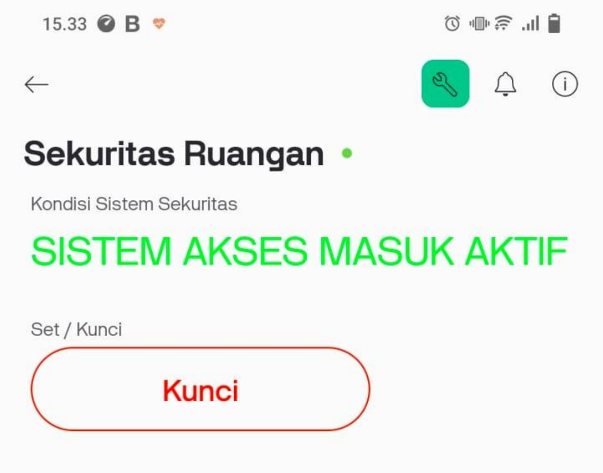
The process of embedding the software into the microcontroller constitutes the final stage of software development, which ensures that the system can be executed directly on the hardware. This stage involves programming the microcontroller with the validated and tested code so that the hardware operates in accordance with the designed system logic. The embedding process is presented in Figure 7, which illustrates the integration of the software into the system.

Fig 7: Process of embedding the software into the microcontroller

2.3.3 Delevlopment For Web Server

To enable users to remotely monitor and control the room access system, a **Blynk IoT–based web interface** integrated through a web server is employed. Blynk IoT was selected due to its flexibility and ease of implementation in Internet of Things applications. Through this interface, users are able to monitor real-time access status, including door conditions (open or closed), authentication results (success or failure), and security alerts in the event of unauthorized access attempts.

In addition to monitoring, the Blynk IoT platform also provides direct control functionalities, allowing users to lock or unlock the door, disable alarms, or reset the system via smartphones or computers connected to the Internet. This integration not only enhances user convenience in interacting with the system but also strengthens the security aspect by providing flexibility for remote access control. Therefore, the utilization of Blynk IoT as a web-based interface plays a vital role in ensuring that the IoT-based room access system is responsive, reliable, and user-friendly. The results of the user interface creation through Blynk IoT are shown in Figure 8.



Sekuritas Ruangan

Kondisi Sistem Sekuritas

SISTEM AKSES MASUK AKTIF

Set / Kunci

Kunci

Fig 8: Web Server Development

3. RESULT AND DISCUSSION

This section presents the results of the implementation and testing of the Internet of Things (IoT)–based room access system that employs a keypad as the authentication device. The primary objective of the testing is to evaluate the system’s ability to recognize predefined passwords, respond appropriately to input conditions, and ensure that the system functions with sufficient accuracy and stability.

In the system design, the ESP32 microcontroller serves as the central control unit responsible for coordinating all operational processes. The ESP32 is connected to several supporting components, including a keypad for entering access codes, a relay module for controlling the electronic door lock, a buzzer that serves as an indicator for errors or access denial, and an LCD display that provides real-time system status information. Additionally, the ESP32 is equipped with Wi-Fi connectivity, enabling seamless integration with the Blynk IoT platform, which allows users to remotely monitor and control the system via a smartphone.

System testing was conducted under two main scenarios, namely local access and remote access, to comprehensively assess the system’s performance under different operational conditions.

3.1 Testing of Room Access via Password Input from the Keypad

The first test was conducted to evaluate the performance of the room access system through authentication using the keypad. In this stage, the user is required to enter a predefined password via the keypad as a prerequisite for access. The system then verifies the input against the stored password in the microcontroller.

If the entered password matches, the system responds by activating the solenoid door lock, which automatically unlocks the door. This process is accompanied by a visual indicator on the LCD display and an audio notification from the buzzer to confirm successful authentication. In addition, the access status is transmitted to the Blynk IoT platform, enabling users to monitor the process in real time via their smartphones.

Conversely, if the entered password is incorrect, the system denies access by triggering an alarm through the buzzer, displaying a failure notification on the LCD screen, and sending an alert message to the Blynk application. This test therefore ensures that the keypad-based authentication mechanism is capable of accurately distinguishing between valid and invalid inputs. Testing of Room Access Using a Valid Password Input show in Figure 9.

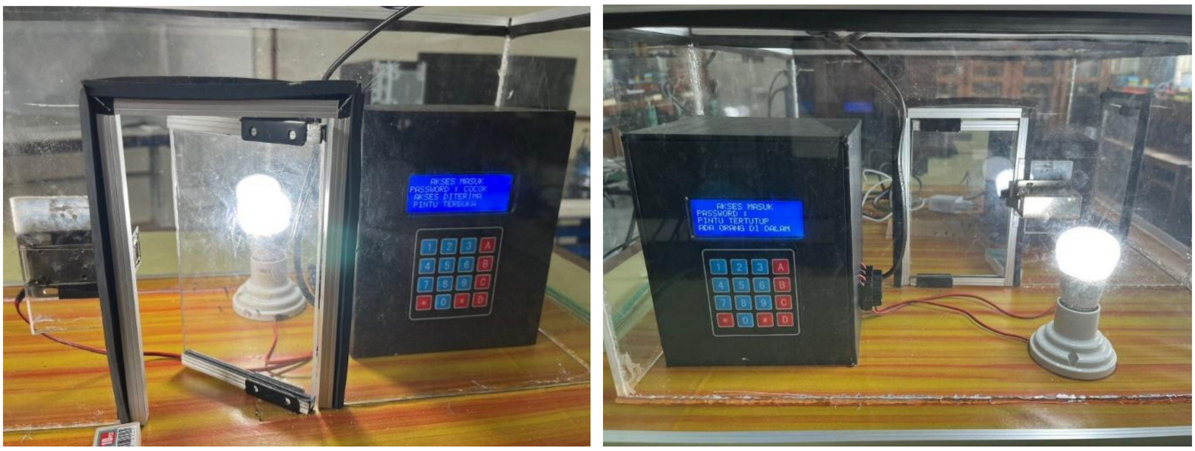


Fig 9: The process when the vannamei shrimp feeding system is activated.

The testing was conducted to evaluate the system's capability in verifying password inputs entered via the keypad as the primary authentication medium. In the first scenario, the user entered the correct password with the numeric configuration *1002*. Once this data was received by the ESP32 microcontroller, the system immediately performed a validation process. The validation result confirmed that the input matched the predefined password. Consequently, the microcontroller activated the relay driver, which unlocked the solenoid door lock, thereby granting access to the room. Simultaneously, the electrical system inside the room was enabled, as indicated by the activation of the lighting system, along with a status message displayed on the LCD screen to notify successful authentication.

Conversely, in the second scenario where the user entered an incorrect password (any input other than *1002*), the system identified it as an unauthorized access attempt. In response, the microcontroller automatically triggered the buzzer as an audible alarm and transmitted a notification to the web server through the Blynk IoT platform. This notification was subsequently forwarded to the room owner's smartphone in the form of a real-time pop-up alert. Such a mechanism enables the room owner to be immediately informed of unauthorized access attempts regardless of their physical location.

The test results for the invalid password case are illustrated in Figure 10, which demonstrates the system's response when detecting an incorrect password input. These findings confirm that the system is capable of effectively distinguishing between authorized and unauthorized access attempts, while providing appropriate responses through both local alerts (alarm and LCD display) and remote alerts (smartphone notifications).

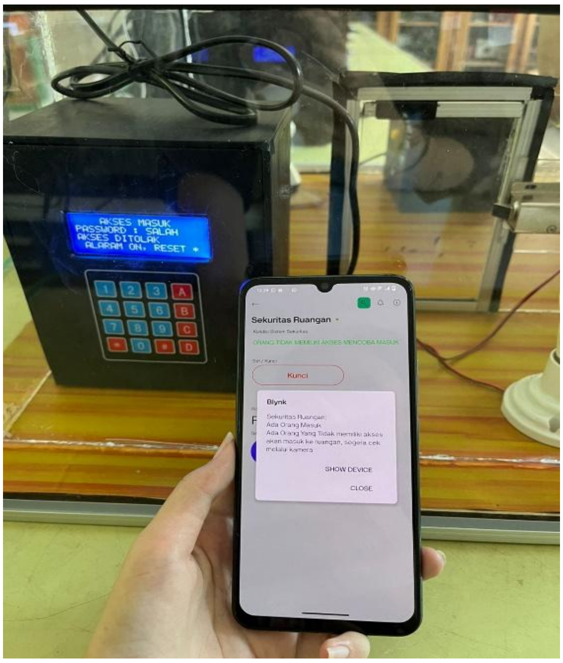


Fig 10: Demonstrates the system's response when detecting an incorrect password input

3.2 Testing Remote Authentication via Blynk IoT

In addition to local password authentication, the system was also evaluated under a remote access scenario to validate its integration with the Blynk IoT platform. This test aimed to examine the capability of the ESP32 microcontroller to establish seamless communication with the web server over Wi-Fi and ensure that access requests transmitted via the Blynk mobile application were executed accurately and in real-time.

During the testing procedure, the room owner initiated an access request through the Blynk IoT interface on a smartphone. Upon receiving this request, the microcontroller validated the command and, if authorized, activated the relay driver to unlock the solenoid door lock. The successful execution of this process was confirmed by both the unlocking of the door and the illumination of the room's electrical system. Concurrently, the LCD module displayed a status update indicating "Room Access Granted," thereby providing direct visual feedback at the local system interface.

Conversely, in scenarios where unauthorized access attempts were simulated, the system successfully detected the invalid request and immediately triggered the alarm mechanism. At the same time, a warning notification was dispatched through the Blynk platform, appearing as a real-time pop-up message on the owner's smartphone. This dual-layered response mechanism—comprising local alerts (buzzer and LCD) and remote notifications—ensures that the owner remains continuously aware of the system status and any security threats, regardless of physical presence.

The experimental results demonstrate that the proposed IoT-based room access system is not only effective in processing local authentication inputs via the keypad but also reliable in facilitating remote access control and monitoring through the Blynk IoT platform. These capabilities collectively enhance the system's flexibility, usability, and resilience in real-world smart security applications.

Figure 11 illustrates the experimental results of the remote access process conducted via the web server.

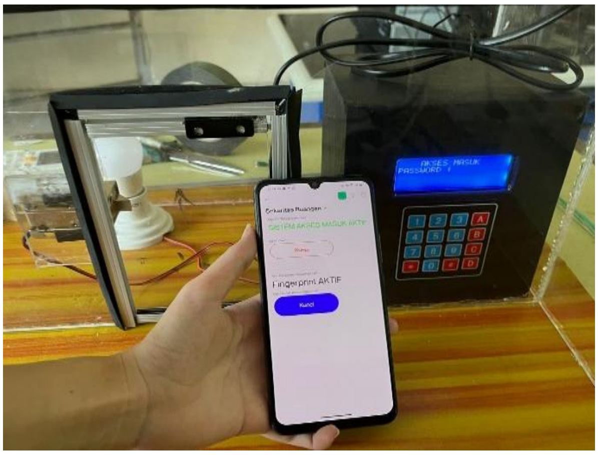


Fig 11: Illustrates the experimental results of the remote access process conducted via the web server.

Based on the experimental results, as illustrated in Figure 11, when the room owner receives a notification on their smartphone indicating an unauthorized attempt to access the room, the user is able to perform direct intervention through the reset button available on the web server application dashboard. Once the reset command is activated, the web server transmits a reset instruction to the microcontroller. The microcontroller then processes this command by executing a series of security actions, which include re-engaging the solenoid door lock, deactivating the alarm, and locking the room access system to prevent further operation. This integrated process ensures that the system promptly neutralizes unauthorized access attempts while maintaining operational stability. For greater clarity, the monitoring and control results via the web server are summarized in Table 1.

Table 1: Monitoring and Control via the Web Server.

System Condition	Keypad Input	Blynk Notification	Hardware Response
Authorized Access	1002 (Valid)	*Access Granted: Door Unlocked*	Solenoid door lock activated (door unlocked); room lighting system turned ON; LCD displays *“Door Unlocked, Room Occupied.”*
Unauthorized Access Attempt	1234 (Invalid)	*Warning: Unauthorized Access Attempt Detected*	Buzzer alarm activated; solenoid door lock remains locked; LCD displays *“Access Denied.”*
Remote Reset Command Executed	N/A	*System Reset Executed via Web Server*	Alarm deactivated; solenoid door lock re-engaged (door locked); system returned to initial state awaiting input.
Remote Access Granted	N/A (via Blynk)	*Access Granted via Remote Control*	Solenoid door lock activated (door unlocked); room lighting system turned ON; LCD displays *“Room Access Granted.”*

In addition to the capability of remotely resetting the room access system, the experimental results also demonstrate that the room owner can directly monitor the room’s condition without being physically present at the location. This functionality is enabled through the integration of a surveillance camera strategically installed near the entrance door. By utilizing this camera, the owner can visually verify the actual situation in real time over the internet, thereby confirming whether an unauthorized access alert represents a genuine security threat or merely an input error.

The remote monitoring feature plays a critical role in enhancing the overall security framework of the system. Beyond textual notifications delivered via the Blynk IoT platform, it provides a complementary layer of visual evidence that strengthens the decision-making process. The combination of alarm mechanisms, real-time notifications, and visual monitoring establishes a multi-layered security approach, thereby improving both the reliability and the sense of safety experienced by the user.

Figure 12 illustrates the visual monitoring process carried out through the camera integrated into the system, serving as an additional tool to verify the actual conditions at the room’s access point.

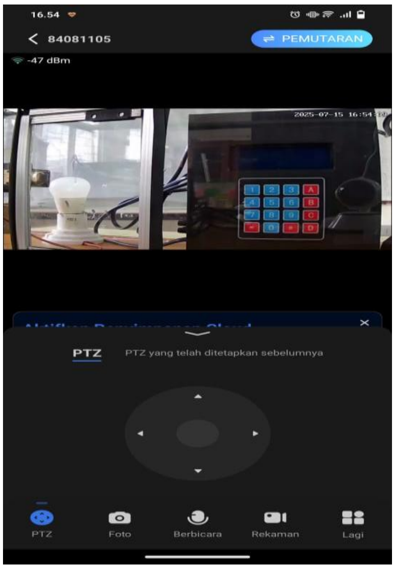


Fig 11: Illustrates the visual monitoring process carried out through the camera integrated into the system

4. CONCLUSIONS

This study successfully designed and implemented an IoT based room access control system that integrates both local and remote authentication mechanisms. The developed system combines hardware components, including an ESP32 microcontroller, keypad, LCD, relay driver, solenoid door lock, buzzer, and surveillance camera with a software framework based on the Blynk IoT platform. The system demonstrated the ability to process local password inputs accurately via the keypad while also enabling reliable remote monitoring and control through a web server interface.

Experimental results confirmed that the system effectively validates correct password inputs, grants access by unlocking the solenoid door lock, and activates the room’s electrical system. Conversely, invalid password attempts were promptly detected, triggering the alarm and generating real-time notifications to the owner's smartphone via the Blynk platform. Furthermore, the integration of a surveillance camera provided an additional layer of security, enabling visual verification of access attempts and reinforcing the system's reliability.

Overall, the integration of keypad-based local authentication, IoT-enabled remote control, real-time notifications, and visual monitoring establishes a robust, multi-layered security approach. These findings demonstrate that the proposed IoT-based room access control system is both functional and reliable for real-world applications, offering enhanced security, flexibility, and usability. Future research may extend this work by incorporating biometric authentication methods, advanced encryption for data transmission, and machine learning algorithms for intrusion detection to further strengthen system performance and resilience.

5. ACKNOWLEDGMENTS

Many thanks to the organizers of the International Journal of Computer Application (IJCA) who have given the author the opportunity to publish this paper, as well as to the Manado State Polytechnic for facilitating the research process.

6. REFERENCES

[1] J. S. Sonamoni, M. S. Islam, and M. M. Rahman, "IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application," *Int. J. Comput. Appl.*, vol. 183, no. 18, pp. 25–30, 2021, doi: 10.5120/ijca2021921534.

[2] Alotaibi, H. Sedky, and A. M. Alshamrani, "A Review of Authentication Techniques for Internet of Things," *Sensors*, vol. 25, no. 7, pp. 3215–3233, 2025, doi: 10.3390/s25073215.

[3] M. Kokila, S. Srivastava, and R. Gupta, "Authentication, Access Control and Scalability Models in IoT Environments: A Review," *Future Generation Computer Systems*, vol. 156, pp. 170–186, 2025, doi: 10.1016/j.future.2025.01.019.

[4] K. Ragothaman et al., "Access Control for IoT: A State-of-the-Art Survey," *ACM Comput. Surv.*, vol. 56, no. 3, pp. 1–37, 2023, doi: 10.1145/3560897.

[5] W. He, X. Liu, and M. Ren, "Rethinking Access Control and Authentication for the Home IoT," in *Proc. 27th USENIX Security Symposium*, 2018, pp. 255–272.

[6] Y. Akbari et al., "A New Framework for Smart Doors Using mmWave Radar and Camera-Based Face Detection and Recognition Techniques," *Sensors*, vol. 24, no. 1, pp. 1–17, 2024, doi: 10.3390/s24010172.

[7] G. Vardakis, P. Liaskos, and I. Tsetsos, "Review of Smart-Home Security Using the Internet of Things," *Electronics*, vol. 13, no. 16, pp. 3343–3357, 2024, doi: 10.3390/electronics13163343.

[8] S. Uppuluri and G. Lakshmeeswari, "Secure User Authentication and Key Agreement Scheme for IoT Device Access Control Based Smart Home Communications," *Wireless Netw.*, vol. 29, no. 3, pp. 1333–1354, 2023, doi: 10.1007/s11276-022-03197-1.

[9] M. A. Khan, H. Abbas, and S. F. Abid, "A Survey of Authentication in Internet-of-Things Enabled Systems," *Sensors*, vol. 22, no. 22, pp. 8793–8812, 2022, doi: 10.3390/s22228793.

[10] M. Choi, K. Lee, and Y. Kim, "Keystroke Dynamics-Based Authentication Using Unique Keypads," *Sensors*, vol. 21, no. 4, pp. 1245–1258, 2021, doi: 10.3390/s21041245.

[11] A. Ramzan, S. Iqbal, and F. Ahmad, "Double-Layered Authentication Door-Lock System Utilizing Multiple Factors," *Sensors*, vol. 25, no. 3, pp. 1153–1166, 2025, doi: 10.3390/s25031153.

[12] Y. Tian, Z. Li, and H. Xu, "Semi-Quantum Secure Protocols for Smart Door Lock Scenarios," *Sensors*, vol. 24, no. 5, pp. 1987–2001, 2024, doi: 10.3390/s24051987.

[13] P. Satanasaowapak, C. Srisomboon, and T. Maneerat, "Residential Access Control System Using QR Code and the IoT," in *Proc. IEEE Int. Conf. on Smart IoT*, 2021, pp. 87–92, doi: 10.1109/SmartIoT52359.2021.00020.

[14] K. Ragothaman et al., "Access Control for IoT-Based Big Data: A State-of-the-Art Discussion," in *Proc. ACM Symp. on Access Control Models and Technologies*, 2024, pp. 115–126, doi: 10.1145/3641234.3641245.

[15] J. Liu, Y. Zhang, and T. Wang, "Blockchain-Based Dynamic Key Authentication Protocol for IoT Access Control," *IEEE Internet Things J.*, vol. 12, no. 4, pp. 3450–3462, 2025, doi: 10.1109/JIOT.2025.3345678.