Journal of Industrial Automation and Electrical Engineering
Vol. 02, No. 02, December 2025, pp. 244~254
ISSN: 3089-1159

Microcontroller based server room security system with dual authentication and Telegram as access data

Ibra Medifa[1], Dwiprima Elvanny Myori[1]
[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia

Article Info

Article history:

Received August 12, 2025
Revised September 23, 2025
Accepted October 25, 2025

Keywords:

Security System
Server Room
Dual Authentication
Telegram
Internet of Things

ABSTRACT

Server space security is a critical aspect that requires a robust protection system. Traditional single-authentication security systems have weaknesses against access theft and lack real-time monitoring features. This research aims to design an ESP32-based server room security system with dual authentication using RFID and PIN, as well as monitoring via Telegram. The system integrates ESP32 as the main microcontroller, RFID MFRC522, TFT LCD touchscreen, ESP32-CAM, solenoid lock door, buzzer, and push button with Telegram API for real-time notifications. The research methodology includes hardware design and software development using the Arduino IDE. The test results showed that the system successfully implemented dual authentication with a 100% success rate for valid access, was able to deny access with an incorrect PIN or unregistered card and successfully sent notifications and images to Telegram in real-time. The system provides significant improvements to server space security through multi-layered authentication, remote monitoring, and comprehensive access documentation.

Corresponding Author:

Dwiprima Elvanny Myori
Department of Electrical Engineering, Faculty of Engineering, Universitas Negeri Padang
Kampus UNP Pusat, Jl. Prof. Hamka, Air Tawar, Padang 25131, Indonesia
Email: elvannymyori@gmail.com

1. INTRODUCTION

Server space is a vital center for companies and institutions that function to store and manage all data and network systems. Given the importance of these functions, the security of the server space is a top priority to prevent unauthorized access, operational interruptions, data theft, or sabotage. However, the reality is that there are still many security systems that rely on only one authentication method such as a physical key or PIN. This one-factor security system has quite serious drawbacks because if the key is lost or the PIN is known to an irresponsible party, then the server space can be easily accessed unlawfully [1]. The weakness of traditional security systems lies not only in limited authentication, but also in the lack of a direct monitoring system. This causes supervisors to have difficulty in supervising access and maintenance activities carried out in the server room. In addition, the absence of a well-documented access log logging system makes it difficult to track the activity of entering and exiting the server room, so that in the event of a security incident, it will be difficult to conduct an accurate investigation [2].

The development of Internet of Things (IoT) technology has opened up great opportunities to develop more sophisticated and effective security systems. Dual authentication systems that combine two verification methods such as RFID cards and PIN have been proven to provide a much higher level of security than single-factor systems [3]. This concept works on the principle that even if one of the security methods is successfully breached, access still cannot be done without verification from the second method. The implementation of this layered security system is critical given the increasing threats to the company's information technology infrastructure. Several previous studies have shown the great potential of the application of IoT technology in server room security systems. Elahi designed an ESP32-based security system that integrates with Telegram

bots to provide automatic notifications when suspicious activity is detected [4]. Rodrigues developed an authentication system using a combination of RFID and PIN with Telegram integration that allowed supervisors to conduct surveillance more effectively [5]. Meanwhile, Veerasamy leveraged the ESP32Cam to capture images of users accessing certain areas and send such visual evidence via Telegram [6]. These studies show that the integration of various IoT technologies can create a comprehensive and easy-to-monitor security system.

Another study conducted by Josephinshermila et al. proposed a security system with ESP32 and an RFID sensor capable of recording all access activities to the cloud database automatically [7]. Darnila and Ziad developed an ESP32-based system and Telegram bot that allows administrators to remotely control and monitor access in real-time [8]. Yusuf et al. designed a two-factor authentication system based on RFID and PIN with a Telegram alert system to improve access security [9]. Khamaysah et al. developed a security system that combines RFID and fingerprints with the ability to record activities and send data to servers and Telegram [10]. Despite the research that has been done, there are still gaps in integrating all ESP32, RFID, PIN, and auto-logging components into Telegram in one optimal system.

Based on the analysis of previous studies, this study aims to design and develop a server room security system that integrates RFID-based and PIN-based dual authentication with a monitoring system via Telegram. The developed system will use ESP32 as the main microcontroller, RC522 RFID module for card authentication, TFT keypad as PIN input interface, ESP32Cam for visual user documentation, and buzzer as access notification alarm. The software will be developed using an Arduino IDE with Telegram API integration to send notifications and access logs to supervisors in real-time. With this system, it is hoped that a more robust server room security solution can be created, easy to monitor, and has complete access documentation for security audit and investigation purposes.

2. METHOD

This research adopts a systematic approach in the design and implementation of server room security systems. The methods used include designing hardware and software, as well as testing the system to verify its functionality. The main components used include the ESP32 microcontroller as the main controller, the RC522 RFID module for card authentication, the TFT LCD as the PIN input interface, the ESP32-CAM for the image capture, and the buzzer as the audio indicator. The software was developed using the Arduino IDE to integrate all modules and sensors, as well as utilizing the Telegram API for notifications and access log logging.

Authentication is the process of verifying the identity of a user or device trying to access a particular system or resource to ensure that only authorized individuals can access the server space, thus protecting sensitive data and infrastructure from unauthorized access. Authentication can be implemented using a one-factor method that typically relies on a single verification method such as a password or RFID card, but this method is vulnerable to theft or misuse [11]. Multi-factor authentication (MFA), specifically dual authentication that combines RFID and PIN as proposed in this system, can enhance security by requiring two or more verification information, thereby significantly reducing the risk of unauthorized access. In this system, dual authentication combines RFID-based identification as "something you own" with a PIN entered through the TFT LCD touchscreen as "something you know", in accordance with the principle of two-factor authentication (2FA) [9]. Integration with Telegram for real-time access logging and notifications as well as visual evidence via ESP32-CAM further enhances system security by providing comprehensive monitoring and documentation that can be used for security audits [12].

The design of this server room security system uses a centralized architecture with the ESP32 microcontroller as the main controller that integrates various input and output components to create a comprehensive dual authentication system. The system consists of several main components that work in a coordinated manner: ESP32 Camera which functions to take user images in real-time for visual documentation and monitoring, TFT LCD as user interface (HMI) for PIN input and display system status [13]-[15], MFRC522 RFID module that reads the user's identification card as the first authentication method, push button that allows users to exit the server room without re-authentication, solenoid lock door as a physical access control mechanism that locks and opens doors based on verification results, a buzzer that provides audio feedback for every access activity whether successful or fail, and Telegram integration that serves as a remote monitoring platform to send notifications, access logs, and user images to supervisors. All of these components are controlled by ESP32 which processes data from input sensors, verifies dual authentication through RFID and PIN, activates outputs in the form of solenoids and buzzers, and sends monitoring data to Telegram, creating an integrated security system with real-time monitoring capabilities and complete access documentation for security audit and investigation purposes.

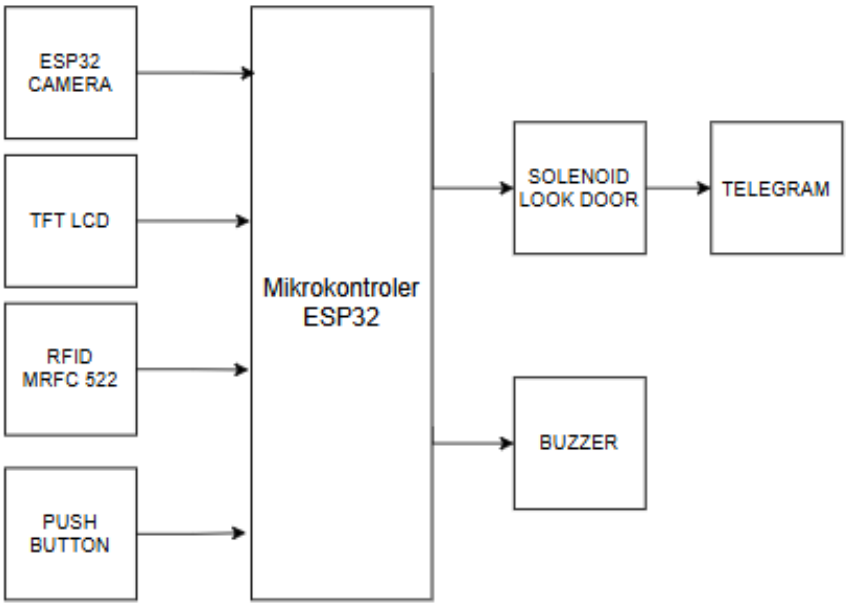


Figure 1. Block Diagram

This server room security system suite scheme uses ESP32 as the primary microcontroller that controls the entire process of dual authentication and surveillance through the interconnection of components integrated in a single circuit. The authentication process begins when the user enters the PIN via the TFT LCD connected to the ESP32, followed by the reading of the RFID card using the MFRC522 module that is also connected to the ESP32 via SPI communication, and if both verifications are successful, the ESP32 will activate the ESP32 Camera to capture the user's image as visual evidence which is then sent to Telegram via a WiFi connection. This system uses a dual power supply with a 5V 2A power supply to supply energy to the ESP32, RFID, TFT LCD, ESP32 Camera, buzzer, and push button, while the solenoid lock door requires a separate 12V power supply to be able to operate optimally in controlling the physical access of the server room door. The buzzer connected to the GPIO ESP32 provides audio feedback for every successful or unsuccessful access activity, while the push button installed on the inside of the server room allows users to exit without going through the re-authentication process by activating the solenoid lock door directly. If the verification fails, the system will deny access, activate a buzzer as a warning, and send notifications to administrators via Telegram, thus creating a layered security system with real-time monitoring that can be monitored remotely.

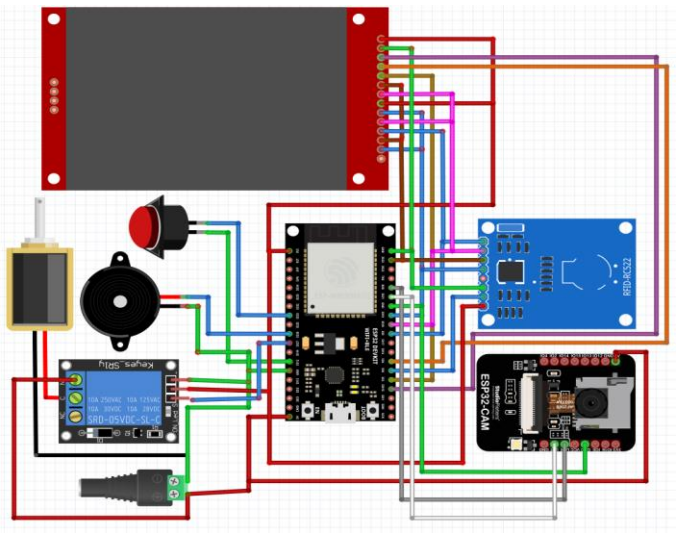


Figure 2. Network schema

System flowchart design depicts the logical flow of the program and the decision-making process in the security system. This flowchart starts with system initialization and connections to Wi-Fi and Telegram. Then, the system will continue to monitor the RFID card readings. If an RFID card is detected, the system will check its validity. If valid, the user is asked to enter a PIN. The PIN will be verified, and if correct, access is granted, an image is taken, and a notification of success is sent to Telegram. If the PIN is incorrect, access is denied and a failure notification is sent. Similarly, if the RFID card is invalid, direct access is denied and a failure notification is sent. The flowchart also includes a flow for access using a push button from within, which will open the door and send a manual access notification to Telegram. This flowchart design ensures that each access scenario is handled accurately and that the system operates logically.

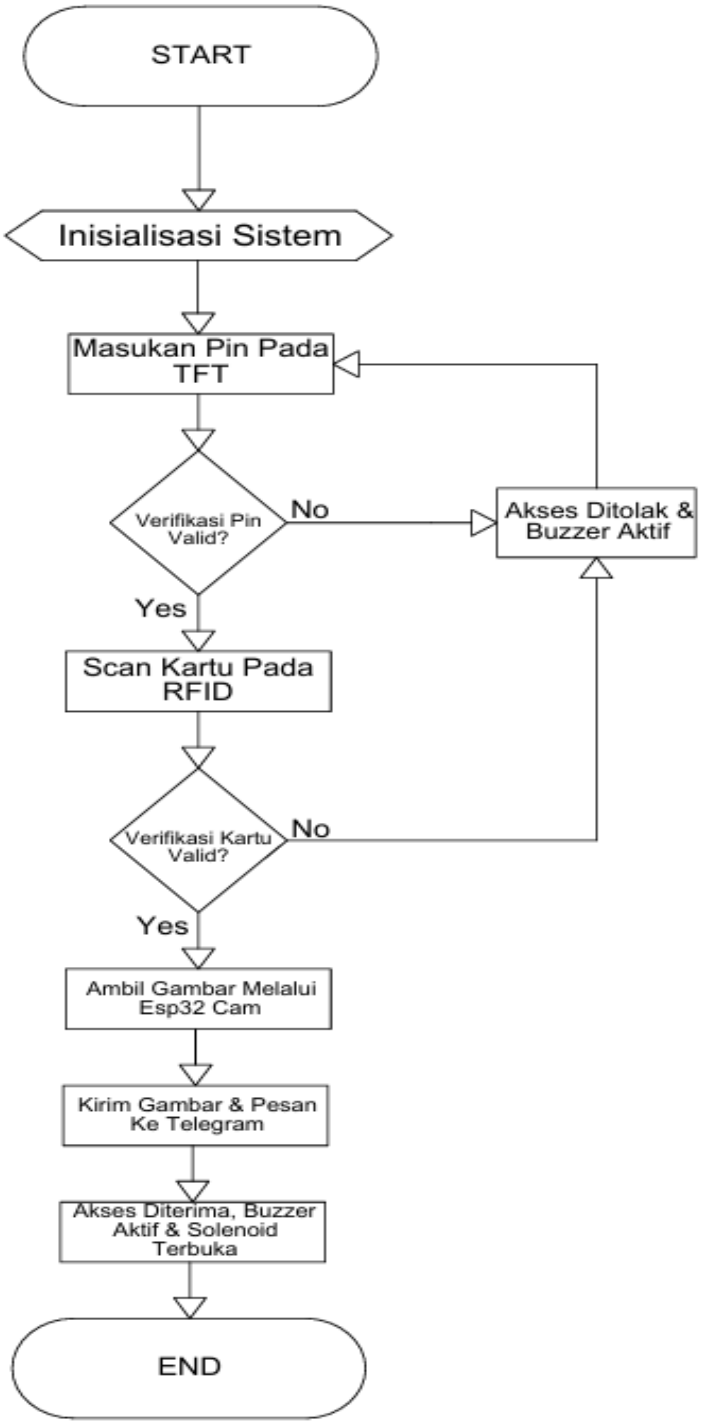


Figure 3. Flowchart

Flowcharts are also used to represent the conceptual structure of complex software systems, serving as design documents used by systems analysts to communicate, negotiate and represent the complexity of a process. The working principle of the system begins when the user brings the RFID card closer to the RFID module MFRC522. The ESP32 microcontroller will read the unique ID of the card. If the card ID is registered in the system database, the user will be asked to enter the PIN via the TFT LCD Touchscreen interface. The ESP32 will then verify the PIN entered. If the PIN entered is correct and matches the stored data, the system will provide access by opening the solenoid lock door. At the same time, the ESP32-CAM will take a picture of the user and a buzzer will sound as an indication of successful access. Notifications in the form of text and images will be sent automatically to the configured Telegram account, recording access details such as username, RFID ID, date, and time. Conversely, if the RFID card is not registered or the PIN entered is incorrect, the system will deny access, the solenoid lock door will remain locked, the buzzer will give an indication of failure, and a notification of denial of access and the reason will be sent to Telegram.

Hardware design involves the selection and integration of the electronic components that make up the security system. The ESP32 was chosen as the premier microcontroller due to its Wi-Fi capabilities and adequate performance to manage a wide range of sensors and actuators. The RFID module MFRC522 used to read RFID cards, while the TFT LCD Touchscreen serves as a user interface for entering the PIN and displaying information. The ESP32-CAM is integrated to take images as visual evidence whenever there is an access attempt. Solenoid lock door is used as an actuator to control the door lock mechanism. Push buttons are provided as a manual access option from within, and a buzzer as an audio indicator. The power supply ensures that all components get stable power. All of these components are assembled and connected according to a schematic that has been designed to ensure optimal functionality.

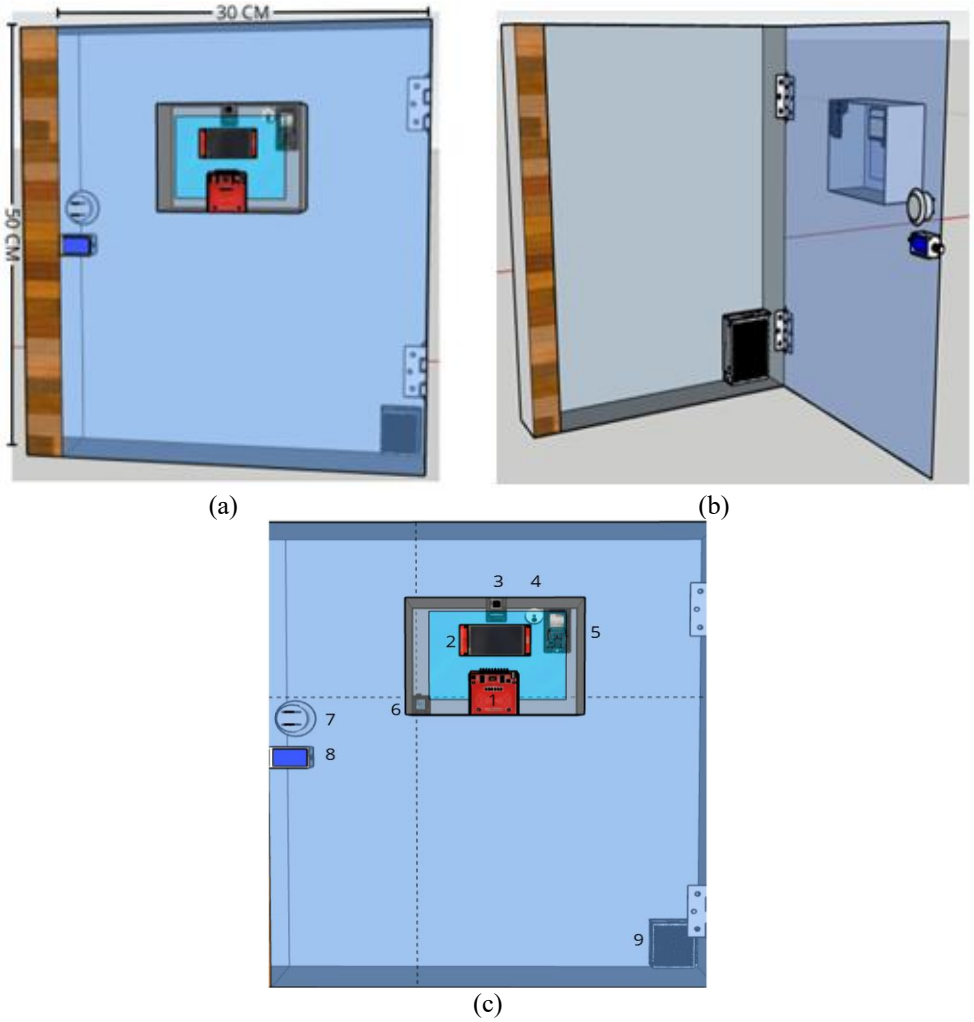
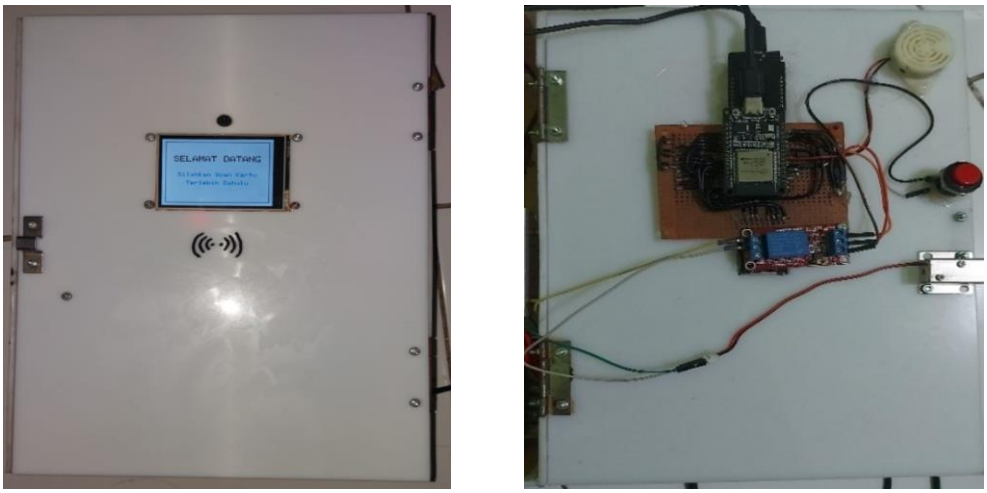


Figure 4. Mechanical design. a) Front View Overall Tool Design, b) Tool Design Seen from the Inside, c) Component Design

3. RESULTS AND DISCUSSION

The physical design of the server room security system has been successfully realized with an optimal component layout, where the system design includes the placement of sensors, actuators, and user interfaces in the context of the actual server room. In the design seen from the outside, there are several main components, namely the ESP32 camera for taking user pictures, TFT LCD 2.8 touchscreen as a PIN input interface, RFID MFRC522 Mini for identification card reading, and door handles integrated with security systems. Meanwhile, in the design seen from inside the server room, there are main control components in the form of ESP32 as a microcontroller, a 1-channel relay module to control the solenoid, a buzzer as an audio indicator, a push button for easy exit, and a 12V solenoid as a door locking mechanism that can be controlled electronically.



(a) (b)

Figure 5. Hardware manufacturing results

Testing of the system's communication with the Telegram platform showed satisfactory results, where the system successfully sent screenshots and notification messages via the ESP32 camera to the Telegram bot with consistent success rates. This test aims to verify the ESP32 camera's function in capturing and sending images to Telegram, as well as testing the validity of the Bot Token and Telegram chat ID used in the system. The test results showed that the Telegram API integration worked well, allowing administrators to receive real-time notifications along with visual evidence whenever there was access activity in the server room.

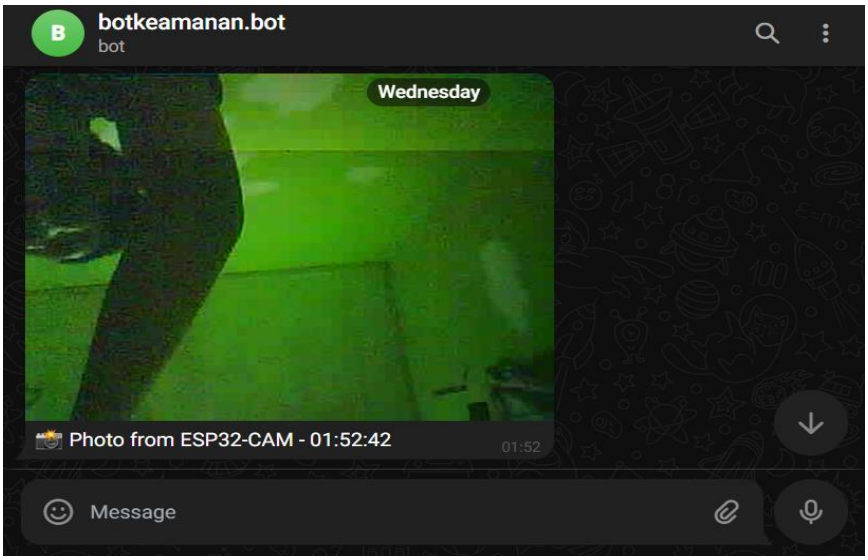


Figure 6. Testing Security Systems with Telegram

During the testing phase of the automatic access log, a technical problem was found with the ESP32 camera where the camera experienced a decrease in image quality and eventually became unable to function at all. Further analysis showed that a malfunction occurred in the ESP32 camera connector, which resulted in the system not being able to capture images clearly. This condition demonstrates the importance of hardware maintenance and the need to replace the ESP32 camera module in the event of a fault in the connector, as forced use can result in permanent damage to the shooting system.

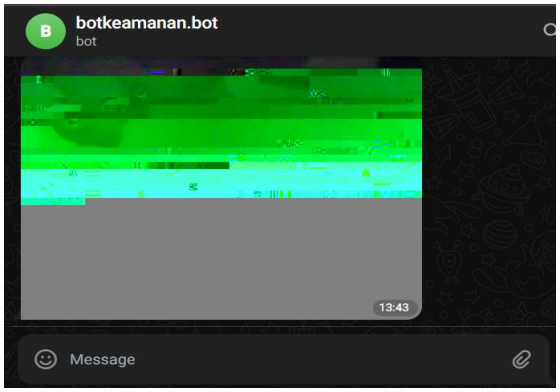


Figure 7. Damage to the Camera Connector

Testing of the system using five different RFID cards that have been registered in the system's database showed consistent results and in accordance with the design. Each test begins with the user bringing a valid RFID card closer, followed by entering the correct PIN via the TFT LCD interface. The test results showed that the system automatically opened the solenoid lock door, provided audio confirmation via the buzzer, and activated the ESP32-CAM to take user images. All of these activities are then recorded and sent as "ACCESS ACCEPTED!" notifications along with user details, dates, access times, and visual images to the Telegram app, allowing for real-time monitoring by administrators.

Figure 8. Experimental results by using valid card, a) First card, b) second card, c) third card, d) fourth card

Testing a dual authentication scenario with a valid RFID card condition but the incorrect PIN indicates the effectiveness of the system in implementing multi-layered security. The system successfully denied access by keeping the solenoid lock door in a locked state, providing an indication of failure through a buzzer, and sending a "ACCESS DENIED! Valid RFID but Invalid PIN" to Telegram. This notification comes with the user's identity details and an incorrect PIN, indicating that both authentication factors must be met correctly to obtain sign-in, thus proving the reliability of the implemented two-factor authentication mechanism.

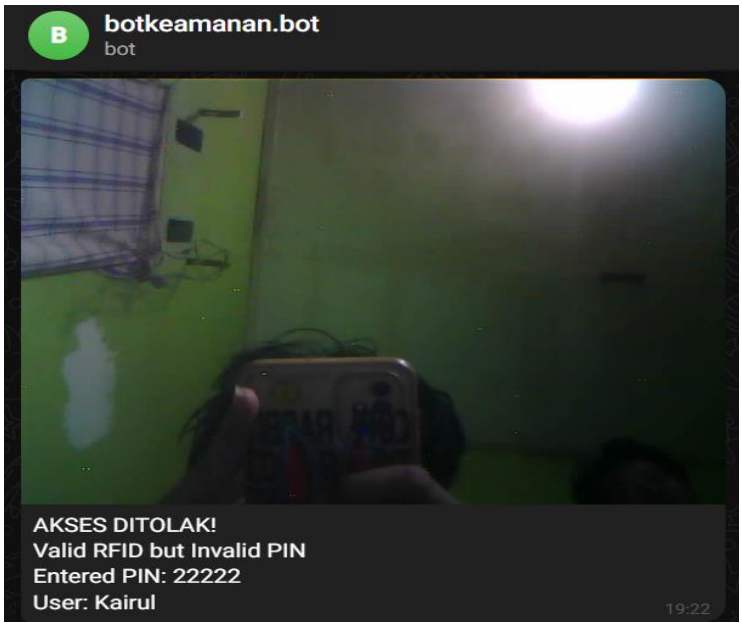


Figure 9. True card and false pin testing

Testing using RFID cards that are not registered in the system's database demonstrates the system's ability to prevent unauthorized access. The system effectively denies access by keeping the solenoid lock door locked, providing failure feedback through the buzzer, and sending a "ACCESS DENIED! Invalid RFID Card" to Telegram. This notification includes details of invalid RFID cards, confirming the system's ability to filter access based on RFID card validity and registration, thus providing effective protection against unauthorized access attempts.

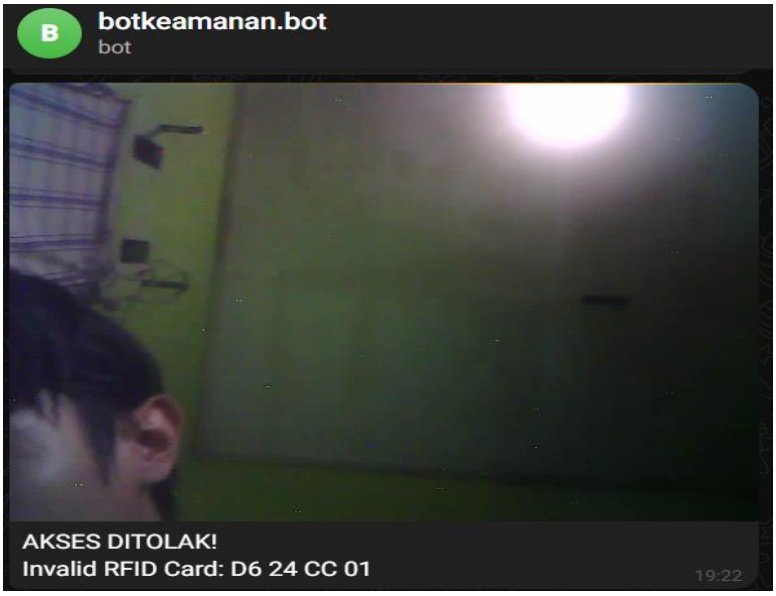


Figure 10. Experimental result with Unregistered RFID Cards

Testing of the push button placed on the inside of the server room showed functionality that made it easy for users to exit the room without going through the re-authentication process. When the push button is pressed, the system automatically activates the solenoid *lock door* to open the door and send a notification to Telegram as documentation of the activity out of the room, complete with information on the date and time of use of the push button. This feature provides operational convenience for users who are in the server room while still maintaining the security aspect through activity logging.

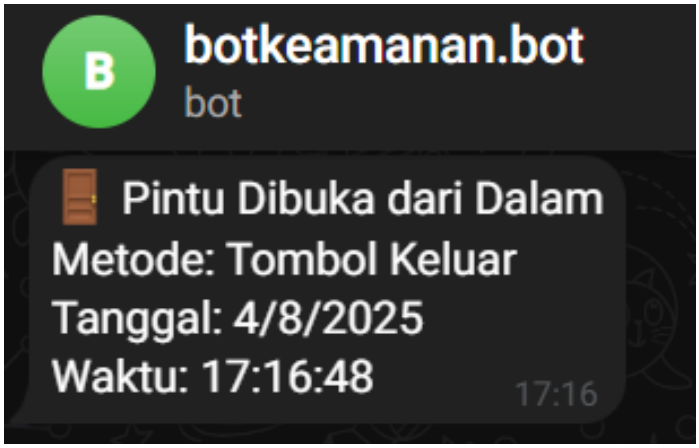


Figure 11. Testing the Push Button Function

Table 1. Security System Testing

Yes	Types of Testing	Card Scan Distance (cm)	Delay Card Scan to PIN (sec)	Delay PIN to Telegram Delivery (seconds)	Delay Between Trials (seconds)	Ket
1	Accepted Access Log Testing (1)	0 cm	0	10.9 seconds	55.1 seconds	Succeed
2	Accepted Access Log Testing (1)	1 cm	0	10.2 seconds	40.2 seconds	Succeed
3	Accepted Access Log Testing (1)	2 cm	0	10.5 seconds	50.5 seconds	Succeed
4	Accepted Access Log Testing (1)	3 cm	0	10.3 seconds	48.3 seconds	Succeed
5	Accepted Access Log Testing (2)	0 cm	0	10 seconds	52.3 seconds	Succeed
6	Accepted Access Log Testing (2)	1 cm	0	11.3 seconds	49.4 seconds	Succeed
7	Accepted Access Log Testing (2)	2 cm	0	10.4 seconds	46.4 seconds	Succeed
8	Accepted Access Log Testing (2)	3 cm	0	10.7 seconds	51.3 seconds	Succeed
9	Log Accepted Testing (3)	0 cm	0	10.1 seconds	50.7 seconds	Succeed
10	Log Accepted Testing (3)	1 cm	0	10 seconds	47.3 seconds	Succeed
11	Log Accepted Testing (3)	2 cm	0	10.8 seconds	56 seconds	Succeed
12	Log Accepted Testing (3)	3 cm	0	10.9 seconds	49.1 seconds	Succeed
13	Accepted Access Log Testing (4)	0 cm	0	10.5 seconds	44 seconds	Succeed
14	Access Log Testing Accepted 4)	1 cm	-	-	-	Fail
15	Accepted Access Log Testing (4)	2 cm	-	-	-	Fail
16	Accepted Access Log Testing (4)	3 cm	-	-	-	Fail
17	Testing Log Access Accepted (5)	0 cm	0	10.3 seconds	53.3 seconds	Succeed
18	Testing Log Access Accepted (5)	1 cm	-	-	-	Fail
19	Testing Log Access Accepted (5)	2 cm	-	-	-	Fail
20	Testing Log Access Accepted (5)	3 cm	-	-	-	Fail
21	Access Log Denied (Incorrect PIN) (1)	1 cm	0	10.7 seconds	50.2 seconds	Succeed
22	Access Log Denied (Incorrect PIN) (2)	0 cm	0	10.4 seconds	55.1 seconds	Succeed
23	Access Log Denied (Incorrect PIN) (3)	0 cm	0	10.8 seconds	43.7 seconds	Succeed
24	Access Log Denied (Incorrect PIN) (4)	0 cm	0	10 seconds	45 seconds	Succeed
25	Access Log Denied (Incorrect PIN) (5)	0 cm	0	10.6 seconds	49.1 seconds	Succeed
26	Denial Access Log Testing (RFID Invalid)	0 cm	-	10.3 seconds	58.7 seconds	Succeed
27	Denial Access Log Testing (RFID Invalid)	1 cm	-	10 seconds	40.6 seconds	Succeed
28	Denial Access Log Testing (RFID Invalid)	2 cm	-	10.5 seconds	50.8 seconds	Succeed
29	Denial Access Log Testing (RFID Invalid)	3 cm	-	-	-	Fail
30	Push Button Exit Testing	-	-	-	6.2 seconds	Succeed
31	Push Button Exit Testing	-	-	-	5.2 seconds	Succeed
32	Push Button Exit Testing	-	-	-	9.4 seconds	Succeed
33	Push Button Exit Testing	-	-	-	3.8 seconds	Succeed
34	Push Button Exit Testing	-	-	-	6.3 seconds	Succeed

This research successfully developed an ESP32 microcontroller-based server room security system with the implementation of dual authentication using RFID and PIN as well as real-time monitoring integration via Telegram. The design results show that the system consists of user interface components in the outdoor part including ESP32 camera for visual documentation, TFT LCD 2.8 Touchscreen as a PIN input interface, RFID MFRC522 Mini as an identification card reader, and integrated door handles. Meanwhile, in the interior there is an ESP32 as the main processing unit, a 1-channel relay module for solenoid lock control, a buzzer as an audio indicator, a push button for exit access, and a 12V solenoid as an automatic locking mechanism. System testing is carried out through multiple scenarios to verify functionality under real operational conditions. The first test validated the ability to send images and messages to Telegram, which successfully integrated the ESP32 camera with the Telegram platform for real-time notifications. However, during the testing process, an error was found in the ESP32 camera connector that was damaged due to mechanical stress, so it was necessary to replace the entire module to maintain optimal connection quality.

Access log testing shows consistent results across a variety of scenarios. Under the condition of access received with 5 different RFID cards, the system successfully verifies double authentication and provides a corresponding response with an average Telegram sending delay of 10-11 seconds. The system is effective at a scan distance of up to 3 cm for most cards, but some types of cards such as ID cards show different sensitivities with optimal success at a distance of 0 cm. Testing of access denied with incorrect PIN and invalid RFID cards demonstrates the system's ability to deny unauthorized access with clear and informative notifications via Telegram. Push button testing for outbound access shows a quick response with a delay of 3.8-9.4 seconds without the need for a re-authentication process. Analysis of the test results shows that the system has met all the designed functionality objectives. Dual authentication is proven to significantly improve security with accurate verification for both factors. Access control via solenoid lock operates optimally with the right response based on the verification results. Real-time logging and notifications via Telegram work efficiently even with delays that can be further optimized. The system shows an informative response to an invalid access condition with sufficient detail for audit and investigation purposes. The integration of all hardware and software components results in a stable and principle-compliant security solution designed for the protection of the server space.

4. CONCLUSION

Based on the results of the implementation and testing of a microcontroller-based server room security system with dual authentication and Telegram as a monitoring platform, it can be concluded that The ESP32-based server room security system with dual authentication (RFID and PIN) is successfully designed using ESP32, RFID RC522, TFT LCD Touchscreen, ESP32Cam, solenoid lock door, buzzer, and push button, ensuring secure two-layer verification to prevent unauthorized access. The implementation of the system by sending data via Telegram was successfully carried out using the Arduino IDE and Telegram API, sending real-time notifications in the form of access status, identity, time, and user images with an average delay of 10 seconds. The system is capable of recording automatic access logs and sending text notifications and images to Telegram, with details of the username, time and visual evidence, supporting surveillance and auditing with an effective scan distance of up to 3 cm for most RFID cards.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Boston, MA: Pearson, 2017.
[2] R. Hidayat and S. Putri, "The Use of Mini MFRC522 RFID for Server Room Security Systems," *Journal of Authentication Technology*, vol. 7, no. 1, pp. 12-20, 2020.
[3] R. Zakaria, C. Dewi, and F. Ranuharja, “Doorbell monitoring system using ESP32-CAM based on Internet of Things (IoT),” *Journal of Industrial Automation and Electrical Engineering.*, vol. 01, no. 01, pp. 222–228, 2024.
[4] G. Bakirtzis, B. J. Simon, C. H. Fleming and C. R. Elks, "Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis," *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Berlin, Germany, 2018, pp. 1-8, doi: 10.1109/VIZSEC.2018.8709187.
[5] G. Bakirtzis, B. J. Simon, C. H. Fleming and C. R. Elks, "Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis," *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Berlin, Germany, 2018, pp. 1-8, doi: 10.1109/VIZSEC.2018.8709187.
[6] D. K. P. Gudavalli, K. Gottapu and V. V. S. N. Yirrinki, "A Prototype of an Intelligent Door Lock Device with Hybrid Security Integration," *2025 Fourth International Conference on Power, Control and Computing Technologies (ICPC2T)*, Raipur, India, 2025, pp. 1-6, doi: 10.1109/ICPC2T63847.2025.10958595.
[7] S. Shetty, S. Shetty, V. Vishwakarma and S. Patil, "Review Paper on Door Lock Security Systems," *2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW)*, Mumbai, India, 2020, pp. 1-4, doi: 10.1109/ICCDW45521.2020.9318636.
[8] S. Sobale, K. Patel, A. Patel, S. Nikam, S. Pathrabe and S. Patil, "OTP Based Door Lock System with Mobile Application using Arduino UNO and ESP8266 Wi-Fi module," *2022 Sardar Patel International Conference on Industry 4.0 - Nascent Technologies and Sustainability for 'Make in India' Initiative*, Mumbai, India, 2022, pp. 1-4, doi: 10.1109/SPICON56577.2022.10180607.

[9] D. Vaishali, A. B. V S, S. J. A R, K. S. Krishna and M. M, "Face Recognition based Door Lock System," *2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, 2024, pp. 1655-1658, doi: 10.1109/ICACRS62842.2024.10841543.

[10] A. F. Ikhfa and M. Yuhendri, "Monitoring Pemakaian Energi Listrik Berbasis Internet of Things," *JTEIN J. Tek. Elektro Indones.*, vol. 3, no. 1, pp. 257–266, 2022.

[11] B. M. Kaumudhi, K. Sita Kumari, A. D. Sai and T. Tejaswini, "Smart Door Lock System using Facial Recognition with Home Automation," *2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India, 2024, pp. 24-29, doi: 10.1109/ICDICI62993.2024.10810778.

[12] M. Shen, "Smart Door Lock System Design Based on UWB Technology," *2024 4th International Conference on Electronic Information Engineering and Computer Science (EIECS)*, Yanji, China, 2024, pp. 485-488, doi: 10.1109/EIECS63941.2024.10800017.

[13] U. Nadiya, M. I. Rizqyawan and O. Mahnedra, "Blockchain-based Secure Data Storage for Door Lock System," *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, Indonesia, 2019, pp. 140-144, doi: 10.1109/ICITISEE48480.2019.9003904.

[14] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," *2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, Miri Sarawak, Malaysia, 2022, pp. 453-457, doi: 10.1109/GECOST55694.2022.10010367.

[15] K. Mahardi, J. W. Simatupang and E. Rismauli, "Security Home Door Automation Using Multi Sensors," *Journal of Electrical and Electronics Engineering*, vol. III, no. 1, p. 88, 2019..