Journal of Industrial Automation and Electrical Engineering
Vol. 02, No. 01, June 2025, pp. 201~209
ISSN: 3089-1159

Layered security system on safe using RFID, finger print, camera and keypad based on Internet of Things

Muhammad Rehan Aulia Yazid[1], Irma Husnaini [1]
[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia

Article Info

Article history:

Received November 12, 2025
Revised January 25, 2025
Accepted May 20, 2025

Keywords:

Layered Security
RFID
Fingerprint Sensor
ESP32 Cam
Password
Internet of Things

ABSTRACT

The development of technology along with the development of the era touches all aspects of life including the security system. The existence of security systems that are developing with the aim of security can be maintained better, such as in the storage of valuables carried out in safes. Layered security is carried out through four stages, the stages are RFID using a recognized card, fingerprint sensors using fingerprints of people who are allowed to access the safe, facial recognition with ESP32 Cam, and passwords via keypad. The security system must be carried out sequentially and correctly. If an error occurs in passing the security system up to three times, it must be repeated from the beginning again. Using the ESP32 Microcontroller with resources from the power supply, this tool can work well to maintain the security of the safe in layers and will automatically open the safe door so that security can be passed correctly.

Corresponding Author:

Muhammad Rehan Aulia Yazid
Department of Electrical Engineering, Faculty of Engineering, Universitas Negeri Padang
Kampus UNP Pusat, Jl. Prof. Hamka, Air Tawar, Padang 25131, Indonesia
Email: rehanauliaa11@gmail.com

1. INTRODUCTION

The rapid development of technology is reflected in the variety of electronic equipment used by humans. The development of technology certainly gives rise to new ideas and innovations, one of which is in the security system, such as the security of valuable storage places, namely safes [1]. Previous research on security systems but in rooms using 2 layers of security, namely RFID (Radio Frequency Identification) and Keypad [2]. Further research has succeeded in creating a layered security system that can monitor door status and user data via the web and database [3]-[5].

Then research in 2021, namely research on the design of a door security system using face detection. This study uses ESP32-Cam and an internet of things-based keypad [6]. Furthermore, research in 2023 on the Layered Security System on Doors using RFID, Finger Print and Keypad with Voice Output based on the Internet Of Things ESP32. It can be concluded that this study has made progress, namely layered security and the internet of things in its system [7]-[10].

Security like previous studies, namely using RFID (Radio Frequency Identification), a technology that uses radio waves to automatically identify an object in many cases, namely in the form of reading chips such as those in cards or other items. It has the advantage that it can only be read or read and written, does not require direct contact and functions in various environmental conditions [11]. Then in security, ESP32-Cam is used which can detect faces through its camera. In the context of developing technology, the ESP32 Cam has a feature that allows it to connect to the internet so that it can be based on the Internet of Things [12]. Security is also carried out using a fingerprint sensor that can recognize unique human fingerprints for each person. A fingerprint sensor is a tool that can record and then store the reading results for future identification [13]. The use of fingerprint sensors is generally on electronic devices such as smartphones, doors, attendance devices and various electronic equipment that require high levels of security [14]-[16]. The security used next is using a password that is input via the keypad. The keypad used is a 4x4 matrix with 8

pins for 16 buttons has a simple shape and saves ports for the microcontroller [10]. The microcontroller used is ESP32 which has been equipped with features to connect to wifi so that it can access the internet and has 18 pins. Based on several previous research descriptions with the aim of development and better, research was conducted on the layered security system on the safe using RFID, fingerprint, ESP32 Cam Camera and keypad based on the ESP32 internet of things. This research consists of ESP32 components as a microcontroller, RFID sensor, fingerprint sensor, ESP32 cam camera and keypad which will be multiple security and will produce sound from the speaker when the door security password is correct and the door opens using the Selenoid door lock when successfully passing the security system.

2. METHOD

This research was conducted in several manufacturing processes. Starting from hardware manufacturing to programming on the Microcontroller used, namely ESP32. The tools and materials used in the research are generally designed like the block diagram in Figure 1 below.

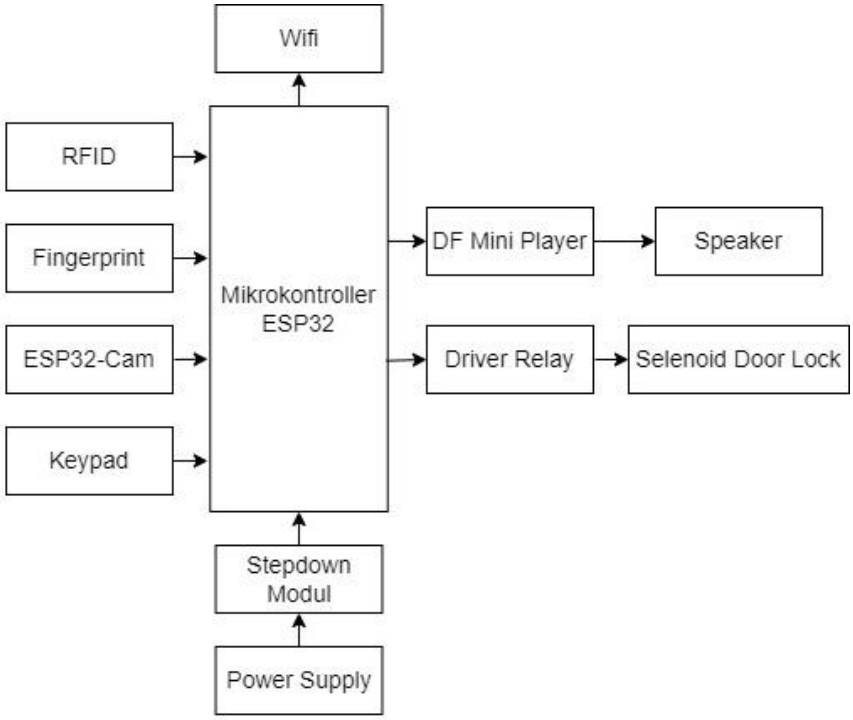

Figure 1. Block diagram of overall system design

The system block diagram in Figure 1 illustrates the system structure consisting of several components with different functions. The microcontroller used, namely ESP32, gets its voltage source from a power supply that has been reduced in voltage through a step down. The input of this system is a sensor and security system tools in the form of RFID, fingerprint sensor, ESP32-Cam, and Keypad. And the output as an output is a DF mini player which is forwarded to the speaker and relay driver which will regulate the solenoid door lock as a lock for the safe door. This tool has a working principle of implementing all sensor functions consisting of an RFID module which is used as security to protect the safe by implementing the function of a card, then there is a fingerprint sensor on the second safe security system with fingerprint detection. Continued with the ESP32-Cam which also adds a security function using facial recognition on the safe, then the last security is the keypad which requires a password to be able to open a safe containing valuables or objects and has a high value. When there is a failure in carrying out the steps in opening the safe, the user has 3 chances of error before having to repeat the steps from the beginning. Then after all the input from security is correct, there will be an output in the form of an active speaker that emits a google voice that speaks and informs that the safe has been successfully opened and ends with the opening of the solenoid door lock through the conditions activated via the relay driver. All of these working principles are also explained in the following flowchart.

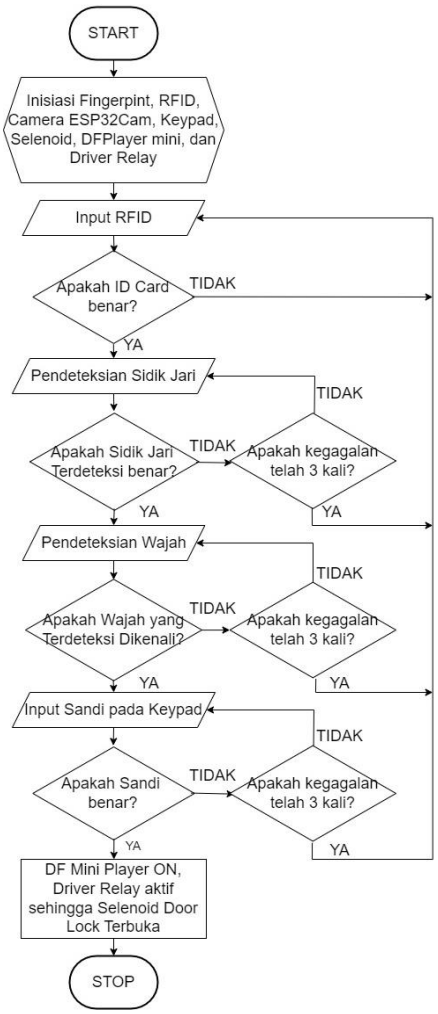

Figure 2. System flowchart

Figure 2 provides a detailed explanation of the system workflow with a flowchart as a visual representation. The initial step is system initiation, namely all components are activated and prepared so that they are able to run system operations.

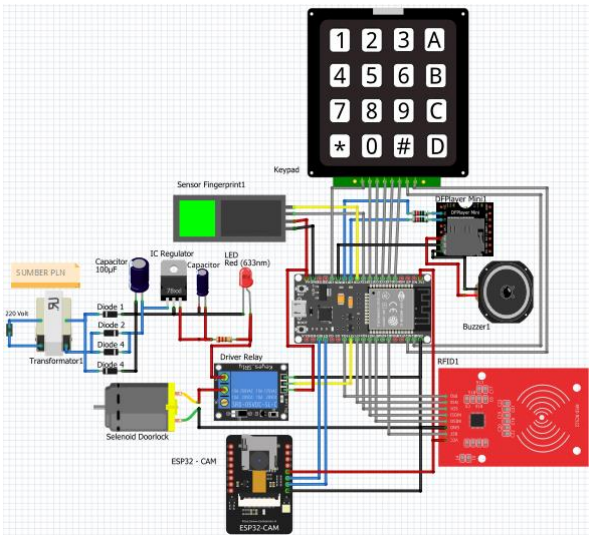

Figure 3. Circuit Schematic

Figure 3 shows a circuit schematic with a breakdown of the relationships between components used in the system. This schematic is designed in accordance with the description in the block diagram which also reflects the relationship between components. As for the mechanical design of the hardware tool, it can be seen in Figure 4 below. Figure 4 shows the layout of the components used in this study, this design functions to determine the manufacture of hardware.

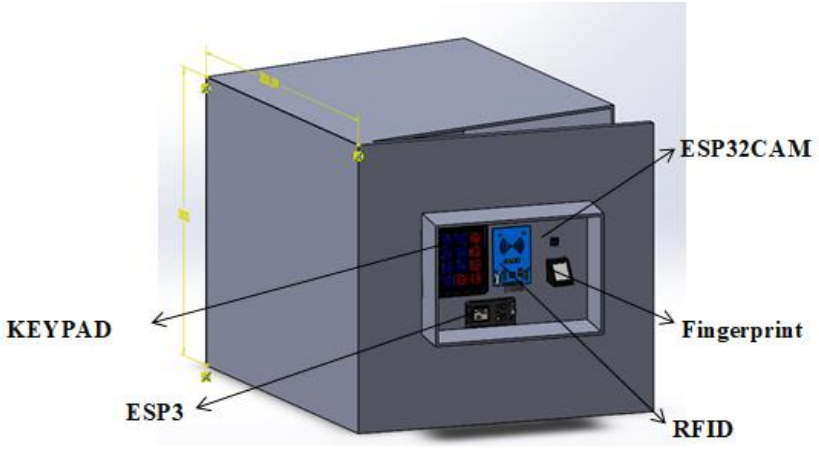

Figure 4. Mechanical design

3. RESULTS AND DISCUSSION

In The results of this research start from the hardware that was created, the hardware results can be seen in Figure 5 below.

Figure 5. Hardware Results

Testing is carried out starting with testing the components used such as power supply and solenoid. Testing on the power supply is done by measuring using a multimeter on the input, namely AC voltage and on the output, namely DC voltage. Can be seen in Figure 6 below.

(a) (b)

Figure 6: Figure (a) AC Input Voltage Measurement on Power Supply, Figure (b) DC Output Voltage Measurement on Power Supply

Figure 6 shows the results of measuring the AC voltage (Alternative Current) or can be called alternating voltage which is the input of the power supply which is 234 VAC while the output voltage of the power supply in the form of DC voltage (Direct Current) is 11.99 VDC. It can be concluded that the input voltage of the power supply is a voltage of 220 VAC but in the measurement obtained a measurement of 234 VAC, this can be caused by the PLN voltage in the voltage checking condition then the measurement of the DC voltage output of the power supply which produces an output voltage of 12 VDC. Furthermore, testing on the solenoid driver aims to see the work of the solenoid in maintaining the security of the safe door, carried out by measuring the voltage at the input and output to determine the driver voltage when working. The results are obtained as in Table 1 below.

Table 1. Solenoid Driver Measurement Results

Measuring point	Measurement
Input Voltage	11.95 VDC
Output Voltage	11.57 VDC

It can be seen in table 1 that the difference in reading between input and output does not change that much and the solenoid can be controlled and works well after being recognized through the driver. Until the final conclusion, the input voltage of the solenoid is 11.95 VDC and the output voltage is 11.57 VDC, and the solenoid can work well as a safe door lock. Furthermore, testing was carried out on the components that were programmed, namely on the safe-layered security components, namely RFID, ESP32-Cam, fingerprint sensor, and keypad. Testing was carried out to find out how the program that had been created was running and whether it worked according to the initial design.

Testing began on RFID (Radio Frequency Identification) which can read cards that have chips. This is done by trying to read the card and the reading results are viewed via the serial monitor on the Arduino IDE. The RFID reader can read a value on a card that has RFID (Radio Frequency Identification) in the form of a card inside and get a value, namely a UID Tag code to be accessed on the RFID (Radio Frequency Identification) reader. The test was successful with the display in Figure 7 below.

```
UID tag : 79 97 7F 53
Message : Akses Anda Diterima
Kiped Benar terkirim
Sandi Benar terkirim
003 Benar terkirim
```

Figure 7. RFID Serial Monitor View

The serial monitor displays the UID of the card attached to the RFID, which is in the form of letters and numbers whose data has previously been stored in the program so that it can be read. In this test, the card UID is 79 97 7F 53. Furthermore, testing on the Finger Print sensor is carried out the same as in the RFID test, namely viewed through the serial monitor in the Arduino IDE application as in Figure 8 below.

```
2
Send any character to search for a print...
Waiting for valid finger
.

Send any character to search for a print...
Waiting for valid finger
Image taken
Image converted
Remove finger

Found a print match!
Found ID #6 with confidence of 105
OK REHAN
Kiped Benar terkirim
Sandi Benar terkirim
003 Benar terkirim
```

Figure 8. Serial Monitor Finger Print Display

The description of the serial monitor display results in Figure 8 is as follows: the fingerprint is ready to read, then the tool will take the fingerprint in the form of an image and convert it into data. The read fingerprint will be tried to be matched with the existing data and the final result is a fingerprint that matches the user's fingerprint. As in the test results in Figure 8, the fingerprint used matches ID #3 on the system. The test was continued with the ESP32 Cam test, carried out by trying to access facial recognition on a recognized face with an unrecognized face. Can be seen in Figure 9 below.

(a) (b)

Figure 9: Figure (a) Testing on familiar faces, Figure (b) Testing on unfamiliar faces

Testing is done on recognized facial data, then testing is done on unrecognized facial data so that it can be known for sure that the ESP32 Cam can work well. Then the test results are also seen from the serial monitor on the Arduino IDE.

```
WiFi connected
Starting web server on port: '80'
Starting stream server on port: '81'Camera Ready! Use
http://172.20.10.4 to connect
No Match Found
No Match Found
No Match Found
No Match Found
Enrolling Face ID: 0
Enrolling Face ID: 0 sample 1
Enrolling Face ID: 0 sample 2
Enrolling Face ID: 0 sample 3
Enrolling Face ID: 0 sample 4
Enrolling Face ID: 0 sample 5
Enrolled Face ID: 1
Match Face ID: 0
Match Face ID: 0
Match Face ID: 0
```

Figure 10. ESP32 Cam Facial Recognition Serial Monitor Display

In Figure 10, it can be seen that initially the ESP32 Cam did not detect any users, then there was a user whose face was recognized as Face ID 1 after matching with 5 samples and declared as a user. Meanwhile, if the prospective user's face is not recognized, it will not be detected and declared as an intruder. The final test was carried out on the Keypad, in the same way as the previous security layer, namely viewed via the serial monitor. The following is a display of the Keypad serial monitor.

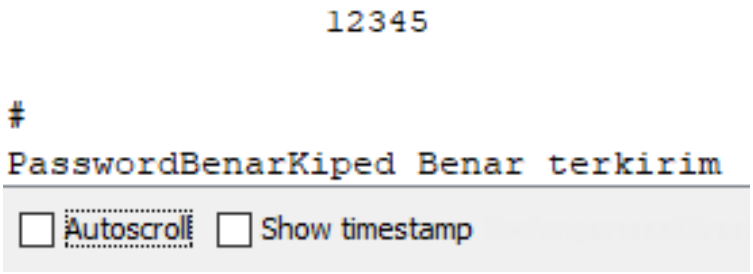

Figure 11. Serial Monitor Keypad Display

In Figure 11, the password input, namely the password "12345" is the correct password with the output from the serial monitor display when the keypad inputs the correct password or password, there will be output text on the serial monitor. From the results of the tests that have been carried out, it can be stated that the components can work properly.

Furthermore, testing is carried out as a whole in sequence from the layers of security that have been created. Having a security sequence from RFID with a card, fingerprint reading via a fingerprint sensor, then face recognition with ESP32 Cam, and ending with inputting a password via the keypad. The results of the overall system test can be seen in Table 2.

Table 2. Overall System Test Results

Condition	Input				
	Card	Finger Print	User Face	Password	Information
Card Recognized	✓	-	-	-	Continue to Finger Print
Card Not Recognized	✓	-	-	-	Repeat card usage
Fingerprint Recognized	-	✓	-	-	Proceed to Face ID
Fingerprint Unrecognized	-	✓			Repeat the fingerprint reading, if the error occurs 3 times, repeat the use of the card.
Face Recognized	-	-	✓	-	Continue to Password
Face Unrecognized	-	-	✓	-	Detected as Intruder, if the error has been repeated 3 times from card usage
Password Correct	-	-	-	✓	The Safe Door Will Open
Password Incorrect	-	-	-	✓	Repeat entering the password, if the error occurs 3 times, repeat using the card

From Table 2 the test results can be concluded that the input must be started with RFID first then continued with fingerprint then facial recognition and ended with password input via keypad, without making a mistake 3 times then DFPlayer mini will be active by providing output on the speaker in the form of google voice. Then the door will open automatically.

4. CONCLUSION

Based on the data and results of the tests that have been carried out, it can be concluded that the tool can function well based on the desired design. The components of the tool such as the power supply and solenoid can work well. Then the components designed as a security layer, namely FID, fingerprint sensor, ESP32 Cam, and Keypad have been tested individually and then tested sequentially according to the research design and also work very well. Testing of the safe security layer is carried out using cards, fingerprints, faces, and passwords that have been programmed and the data stored in advance so that it can be recognized. The tool as a whole can work well to maintain the security of valuables stored in the safe.

REFERENCES

[1] M. Nagabushanam, S. Jeevanandham, S. Ramalingam, K. Baskaran and A. Maheshwari, "AI based E-ATM Security and Surveillance System using BLYNK-loT Server," *2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4)*, Bangalore, India, 2022, pp. 1-5, doi: 10.1109/C2I456876.2022.10051613.

[2] K. S. Keerthi, A. A. Yadwad, K. S. Kumar, Amandeep and A. M, "Independent, Integrated, Reconfigurable IOT based Home Security System," *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2022, pp. 27-34, doi: 10.1109/ICSSIT53264.2022.9716511.

[3] N. Litayem and A. Al-Sa'di, "Exploring the Programming Model, Security Vulnerabilities, and Usability of ESP8266 and ESP32 Platforms for IoT Development," *2023 IEEE 3rd International Conference on Computer Systems (ICCS)*, Qingdao, China, 2023, pp. 150-157, doi: 10.1109/ICCS59700.2023.10335558.

[4] S. V, S. R, A. B, V. S. V and P. Vigneswari, "IoT based Healthcare Monitoring and Tracking System for Soldiers using ESP32," *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2022, pp. 377-381, doi: 10.1109/ICCMC53470.2022.9754076.

[5] 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.

[6] A. B. Sinabang, M. Martias, and H. Adianto, "Alat Pengaman Brankas Berbasis Fingerprint Menggunakan Nodemcu Esp8266 Notifikasi Telegram," *Insantek*, vol. 4, no. 1, pp. 18–24, 2023, doi: 10.31294/insantek.v4i1.2121.

[7] M. Chamdun, A. F. Rochim, and E. D. Widianto, "Sistem Keamanan Berlapis pada Ruangan Menggunakan RFID (Radio Frequency Identification) dan Keypad untuk Membuka Pintu Secara Otomatis," *J. Teknol. dan Sist. Komput.*, vol. 2, no. 3, 2014, doi: 10.14710/jtsiskom.2.3.2014.187-194.

[8] 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.

[9] M. AlSelek, J. M. Alcaraz-Calero and Q. Wang, "Dynamic AI-IoT: Enabling Updatable AI Models in Ultralow-Power 5G IoT Devices," in *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14192-14205, 15 April15, 2024, doi: 10.1109/JIOT.2023.3340858.

[10] N. K. Daulay and M. N. Alamsyah, "Monitoring Sistem Keamanan Pintu Menggunakan RFID Dan Fingerprint Berbasis Web Dan Database," *Jusikom J. Sist. Komput. Musirawas*, vol. 4, no. 02, 2019, doi: 10.32767/jusikom.v4i2.632.

[11] R. Muwardi and R. R. Adisaputro, “Design Sistem Keamanan Pintu Menggunakan Face Detection,” *J. Teknol. Elektro*, vol. 12, no. 3, 2021, doi: 10.22441/jte.2021.v12i3.004.
[12] R. L. Singgeta, P. D. K. Manembu, and M. D. Rembet, “(Ryan L. Singgeta, dan Pinrolinvic Manembu)Paper Sistem pengamanan pintu rumah,” *Semin. Nas. Ris. dan Teknol. Terap. 2018*, vol. 2018, no. Ritektra, pp. 88–97, 2018.
[13] H. A. Kusuma, S. B. Wijaya, and D. Nusyirwan, “Sistem Keamanan Rumah Berbasis Esp32-Cam Dan Telegram Sebagai Notifikasi,” *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 8, no. 1, p. 30, 2023, doi: 10.32897/infotronik.2023.8.1.2291.
[14] R. Diharja, S. Pakpahan, S. Wiji Lestari, and P. Studi Teknik Elektro, “Penerapan Sensor Sidik Jari pada Rancangan Prototipe Smart Home untuk Akses Pencahayaan dan Pintu Application of Fingerprint Sensor in Prototype Design of Smart Home for Lighting and Door Access,” *Telka*, vol. 8, no. 1, pp. 82–94, 2022.
[15] O. R. Arsyad and K. P. Kartika, “Rancangan Bangun Alat Pengaman Brankas Menggunakan Sensor Sidir Jari Berbasis Arduino,” *JATI (Jurnal Mhs. Tek. Inform.*, vol. 5, no. 1, 2021, doi: 10.36040/jati.v5i1.3285.
[16] M. Chandra, M. Sandeep, P. P. Kumar Reddy, R. S. Kumar Reddy, P. C. Sowrya and A. Kumar, "Door Lock System Using HumanFaces With ESP32-CAM," *2023 Fourth International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, Bengaluru, India, 2023, pp. 1-5, doi: 10.1109/ICSTCEE60504.2023.10584952.