Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2024. Vol. 4. No. 1; e-ISSN: 2808-4519

Design of a Safe Security System Based on Internet of Things Using Face and Fingerprint Detection

Nadila Pitaloka[1]*, A M H Pardede[2], Husnul Khair[3]

[1, 2, 3] *STMIK Kaputama*

nadilapitaloka02@gmail.com[1*], akimmhp@live.com[2], husnul.khair@gmail.com [3]

Abstract

Traditional safe security systems usually use manual keys and a combination of numbers or passwords to open the safe. This system has several disadvantages such as being easy to break into, cumbersome, and the owner easily loses the key, even forgets the password needed to open the safe, which causes the safe to be unable to open. This research develops an Internet of Things (IoT)-based safe security system that uses two security options to open the safe, namely face detection and fingerprint authentication to increase security against unauthorized access with a prototype method. The system uses the ESP32-CAM to capture facial images and send them to the Telegram app for manual verification by the owner, while the fingerprint sensor ensures only registered users can open the safe. Arduino Uno serves as the main microcontroller to manage the integration between components such as ESP32-CAM, fingerprint sensor, relay, solenoid lock, LCD, and buzzer. The test results show that this system is effective in providing security to the safe through notifications, although it still relies on manual verification of faces via Telegram and requires a stable internet connection, and fingerprints that have been registered are successfully implemented. Further development is recommended to automate face recognition and improve the overall performance of the system.

Keywords: Safe Security, Face Detection, Fingerprint Authentication

1. Introduction

Security is a top priority when it comes to storing valuables. A safe is a box usually made of iron that is used to store valuable personal items to prevent them from being stolen. Apart from preventing theft, safes are also used to prevent damage in the event of a fire at home or in a bank. Safes are one of the solutions to ensure such security. However, with the advancement of technology, the security of traditional safes no longer seems to be effective. Traditional safes that use manual keys or passwords have several disadvantages, such as being easy to break into, losing keys, and forgetting passwords. To overcome these weaknesses, this research focuses on developing an IoT-based safe security system that uses facial recognition controlled through a smartphone and uses a fingerprint sensor. This system allows the safe owner to receive notifications directly through the Telegram application on the smartphone, which makes it easy to monitor the activities that occur in the safe. By utilizing Internet of Things technology, this system is expected to provide higher security, better convenience, and more comprehensive protection compared to the previous system that only used fingerprint sensors and buzzers, thus ensuring the safety of valuables from various threats.

2. Literature Review

2.1. Design and Build

Design is a process of determining what is to be achieved using various techniques and includes the description of the architecture and details of the components and limitations that will be faced during the process. Creating a new system or replacing or improving an existing system as a whole is called system development or building. In short, design is the drawing, planning, and sketching or arrangement of several different parts into a unified, functioning whole. Therefore, design is the process of transforming the results of analysis into a software package and then creating a new system or improving an old system to maximize the functions of the new system [1].

2.2. Security

Security is an attempt to prevent disruptive crimes. Protection, integrity, authenticity, and access rights are components of ideal security. Many types of information must be protected from illegal access or misuse, including physical security, which focuses on strategies to secure an organization's employees or members, physical property, and workplace from various trusts, including natural disasters, fire, and unauthorized entry.

2.3. Brankas

A safe is a box usually made of iron that is used as a place to store valuable personal items to prevent theft, which is locked with a digital or combination lock. In addition to preventing theft, safes are also used to prevent damage in the event of a fire at home or in a bank. Valuable items that are usually stored in safes include money, jewelry, family documents, keys and more. Safes usually have two types of security: digital or analog/mechanical. There are also safes that use dual authentication, which means they use both mechanical and combination locks. This type of security has some drawbacks. One of the problems is that keys can be duplicated, unlocking takes a long time, combination numbers can be forgotten, and password combinations can be used by others. Safes come in a variety of sizes, from small, portable ones to those that are usually wall-mounted and large, room-shaped safes.

2.4. Internet Of Things (IoT)

Internet Of Things (IoT) is a concept in which Internet connectivity is extended to physical devices equipped with sensors, software, and other technologies that enable them to collect and exchange data over the Internet used in everyday life. An important aspect is the ability of IoT to communicate and relate to each other without requiring constant human intervention. Today, more people know about Internet Of Things technology through products related to the idea of a “smart home”, such as home security systems that use internet-connected cameras [2].

2.5. Face Detection

Biometric systems are evolving rapidly. Facial recognition systems utilize a person's facial features to identify and authenticate individuals. Face recognition is a technology that uses computer control to identify faces through cameras. Face recognition systems can recognize faces in real-time from photos and videos. Face recognition is highly accurate. The mechanism of face identification is similar to human vision. Face detection tools match the shape, texture, and other elements that characterize a person. The visualization created by the computer consists of pixels or picture elements. Brightness, contrast, contour, color, shape, and texture are some of the components that affect the visual appearance. The process of facial recognition is already much more secure than conventional security methods. Although it is not as advanced as iris and retina recognition, the problem is that iris and retina recognition technologies are much more expensive. Other than that, they are available at a much cheaper price [3].

2.6. Microcontroller

Microcontrollers are small electronic circuit controllers that have a CPU, memory, timers, serial and parallel communication channels, and many ports that allow them to control the circuit's working process. When compared to personal computers, microcontrollers have a lower data processing speed. The operating speed of a PC usually ranges from 1-16 MHz, while the speed of a microcontroller reaches the order of GHz. In addition, the RAM and ROM capacity of personal computers is lower, with RAM and ROM capacity only ranging on the order of bytes/Kbyte [4].

2.7. Arduino Uno

Arduino UNO is an Atmega328-based microcontroller board that has 14 digital I/O, 16 MHz ceramic resonator, 6 analog inputs, voltage connector, ICSP header, and reset button. Compared to other microcontroller boards that require an external programmer, the Arduino microcontroller has a bootloader, which makes the process of downloading programs to the flash-on-chip memory easier. The Arduino Uno, which is capable of supporting microcontrollers, can be connected to a computer via a USB cable, and to start it, it can be powered by a battery or by an AC-to-DC adapter [5].

2.8. ESP32-CAM

For IoT (Internet Of Things) projects that require camera features, the ESP32-CAM is a microcontroller with additional features such as bluetooth, wifi, camera, and micro SD slot. Unlike the ESP32-Wroom module, the ESP32- CAM module has fewer I/O pins, so we have to use USB TTL or utilize the computer's USB port to program it. The ESP32-CAM module comes with two sides. The front has the OV2640 camera module which is a small-sized camera that can function independently, a microSD, and a flash as an additional light for the camera if needed. 21 The back has an internal antenna, external connectors, male pins for I/O, and the ESP32S as its brain. The specifications of the ESP32-CAM are as follows [6].

- Low-power dual-core 32-bit CPU for application processors Main frequency up to 240MHz, computing power up to 600 DMIPS
- Built-in 520 KB SRAM, external 4M PSRAM
- Supports interfaces such as UART/SPI/I2C/PWM/ADC/DAC
- Support OV2640 and OV7670 cameras, built-in flash
- Support image WiFi upload
- Support TF card
- Support multiple sleep modes
- Embedded Lwip and FreeRTOS
- Support STA/AP/STA+AP working mode

2.9. Fingerprint Sensor

Fingerprint sensor is an electronic device that reads the owner's fingerprint by applying a scanning sensor for identity verification purposes. The fingerprint itself is a stroke located on the palm of the fingertip. Fingerprint sensors are commonly used in various electronic devices

that require a high level of security and can only be accessed by the owner himself, such as Smartphones, home/room entrances, and employee attendance management tools [7]**.**

2.10.Selenoid Door Lock

An electronic device with an electromagnetic working principle is the selenoid door lock. The solenoid functions as an actuator, and is usually used to lock automatic doors. When voltage occurs, the solenoid will move or operate. The working principle of the door lock solenoid is usually 12 volts, but there are also 6 volts and 24 volts. Under normal conditions, the solenoid is in the locked or extended lever position, and if any voltage is applied, the lever will open or retract.

2.11.Jumper Cable

By using jumper cables, electrical components on the breadboard can be connected without soldering. Jumper cables are commonly used on breadboards or other prototyping tools to make circuits easier to build. The main function of jumper cables is as an electrical conductor to connect electrical circuits. Each end is usually equipped with pins or connections called “male connectors” and “female connectors”. Jumper cables come in three categories, namely male to female, male to male, and female to female.

2.12.Reley

Relay is an electrically operated switch and is an electromechanical component consisting of two main parts, namely: electromagnet (coil) and mechanical components (switch / set of switch contacts). By using electromagnetic principles, relays can move the switch contacts so that they can deliver higher voltage electricity with low electric current.

2.13.LCD (Liquid Cristal Display)

A type of display media that uses liquid crystals as the main displayer is called an LCD (Liquid Crystal Display). LCDs have been used in various industries, such as electronic devices like televisions, calculators, and computer screens. In the application post, a dot matrix LCD with 2 x 16 characters is used. This LCD functions as a viewer that shows the working status of the device.

2.14.Breadboard

Breadboard or commonly called a project board is the basis for building an electronic circuit and prototyping an electronic circuit without the need for soldering. By using a breadboard, the electronic components used will not be damaged and can be reused to make other circuits. Electronic test circuit made with breadboard. Most electronic components in an electronic circuit can be interconnected by inserting leads or terminals into holes and if required, connecting them via wires. If you look closely, you can see that the holes in the top and bottom rows are connected horizontally and bifurcated in the center, while the holes in the middle row are connected 186 vertically.

2.15.Buzzer

A buzzer is a component that converts electric current into sound. The working principle of a buzzer is almost the same as a speaker. The buzzer consists of a diaphragm that has a coil. When the coil is electrified so that it becomes an electromagnet, the coil will be pulled in or out, depending on the polarity of the magnet. Each vibration of the diaphragm makes the air vibrate so that it will produce sound. The buzzer has two pins. One pin serves as a positive voltage input of +5VDC, and the other serves as a negative or ground input.

2.16.Arduino IDE

The Integrated Development Environment (IDE) is a computer program specifically designed to help create programs for the Arduino board. The Arduino IDE is a very advanced Java program. The Arduino IDE consists of three components including, Program Editor: a window that allows the owner to write and edit programs in Processing language. A module known as Compiler serves to convert the program code created in Processing language into binary code. Microcontrollers will not be able to understand Processing language, so a compiler is necessary for this situation. Uploader: a module that can be used to load binary code from a computer into the Arduino board's memory [8].

2.17.Smartphone

A smartphone is a mobile phone with features and functions similar to a computer. It has a microprocessor, memory, display, and modem. A Smartphone is a multimedia phone that combines the features of a PC and a phone into an elegant device. There is no factory standard that defines what a Smartphone is. For some, a Smartphone is a phone operated by an entire operating system software, which allows application developers to communicate in a conventional way. Smartphones have features such as text messaging, camera, music player, video, games, email, search engine, personal information manager, internet phone service, GPS, and can even function as a credit card. To others, a Smartphone is just a phone with advanced features such as email, internet, and the ability to read e-books or a keyboard, whether plugged in or not. In other words, a Smartphone is a computer with the size of a small phone [9].

2.18.Telegram

Telegram is a free, non-profit social messaging application used to send messages and exchange photos, videos, stickers, audio, and other file types, and can also exchange large documents. This cloud-based multiplatform application can be used on a variety of mobile devices and computers, including Android, iOS, Windows, and Linux. Telegram has the ability to share files up to 1.5 GB in size per file. The Bot

feature is an account that is run by the Telegram app. Bots feature artificial intelligence. Bots can do anything on the internet, such as playing games and broadcasting [3].

2.19.C Language Programming

The C language uses the concept of sequence (the program is executed in order from top to bottom), so when writing other functions below the main function, it is necessary to write a prototype section, which is intended to tell the compiler the list of functions to be used in the program. However, the prototype section above is no longer necessary if the other functions are written above or before the main function. In addition, we will be familiar with header files in the C language, which are usually written with the extension h(*.h), which are help files used to store a list of functions to be used in the program. For those who have learned Pascal language, header files are similar to units. A typical header file in C++ for an input or output process is <stdio.h> [8].

3. Analysis and Design

3.1. Research Methods

To design and build a safe security system based on Internet Of Things (IoT) and biometrics, this research uses a prototype approach. The software development method known as the prototype approach centers on developing a system that describes the final results of the research conducted and determines how the system design should be better. This approach allows the functionality and effectiveness of the design to be tested and evaluated first. In this way, improvements can be made before the system is fully implemented, thus ensuring that the end result better meets the needs and expectations of the owner.

3.2. Data Collection Methods

In the project Designing an Internet Of Things-Based Safe Security System Using Face and Fingerprint Detection, the preparation process is carried out as follows:

1. Literature Study Researchers review references obtained from a number of scientific works such as previous thesis journals and books related to research topics.
2. Literature Study Literature study is the collection of data and information obtained by researchers by reading reference books, e-books, websites, and documents. The documents in question include the results of previous research written into books, journals, and articles related to the object of research.
3. Consultation Researchers consulted with the supervisor to solve the problems that occurred during the process of making the hardware research under study.
4. Tool Testing Researchers conduct tool testing to experiment and test tool modules and how these modules are connected to the system control program to function simultaneously and obtain test results that match the research results.

3.3. System Requirements Analysis

Analysis of the system requirements needed in designing an Internet Of Things-Based Safe Security System Using Face and Fingerprint Detection includes two main components, namely hardware and software.

1. The hardware that will be used in this research is as follows:
    a. Arduino Uno R3
    b. ESP32-Cam
    c. Fingerprint Sensor
    d. Selenoid Door Lock
    e. Jumper Cable
    f. Adapter
    g. Relay
    h. 16x2 LCD with I2C
    i. Battery 12v
    j. Breadboard
    k. Buzzer
    l. Smartphone
    m. Plywood 40
    n. Glue and Insulation
2. The software to be used in this research is as follows:
    a. Arduino IDE
    b. Telegram
    c. Fritzing

3.4. Block Diagram

The block diagram of this system can be seen in Figure. The main component used in this system is Arduino Uno as a microcontroller that manages all the components contained in this study. The way the tool works can be seen where the Arduino Uno is powered by electricity with the connecting media using an adapter. ESP32-Cam acts as the main input to take pictures of the owner's face and send them to the microcontroller. ESP32-Cam must be connected to WiFi first before sending data. Once connected, the owner can use the Telegram

application on the Smartphone to receive notifications about the status of the safe door and verify the face image taken by the ESP32-Cam. Fingerprint also acts as an input to send fingerprint data to Arduino Uno. After that, Arduino Uno receives input from ESP32-Cam and fingerprint to manage the owner's face data and fingerprint data, then matches it with the data stored in the system to authenticate. Telegram is used to send notifications and images of the face scan results to the owner, allowing manual verification. The 16x2 LCD screen that has been equipped with I2C functions as an output of Arduino Uno processing results to display information or system status, such as authentication success or failure. Meanwhile, the relay acts as an output that is controlled by Arduino Uno to activate or deactivate the door lock solenoid. Then, the Buzzer is also used as a microcontroller processing output to provide a sound signal indicating that authentication has succeeded or failed.

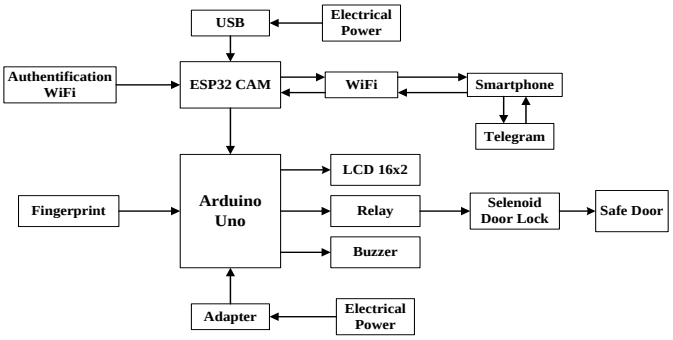


Fig. 1: System Block Diagram

3.5. Overall Tool Set

A fairly complex circuit is shown in Figure which connects various electronic devices with Arduino UNO as the main controller. For power in this circuit using a Charger Adapter and USB Cable as an intermediary. This circuit has a purpose for each component, namely:

1. Fingerprint and Camera Based Access Control: ESP32-CAM can be used to take pictures or videos for surveillance or verification and use a fingerprint sensor to confirm the owner's identity.
2. Visual and Audio Indication: Fingerprint verification results, system status, and other information are displayed on the I2C LCD. A buzzer provides audible notification when important events occur, such as verification success or failure. Jumper cables and breadboard serve as a connecting tool from one device to another without soldering media.
3. Selenoid Control: Depending on the result of face and fingerprint verification, the relay will control the selenoid to open or close the safe door.

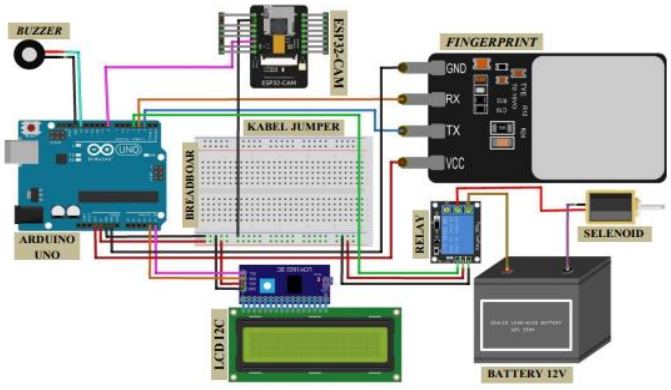


Fig. 2: Overall Tool Set

3.6. Design of an Internet of Things-Based Safe Security System Using Face and Fingerprint Detection

The picture shows the Internet of Things Based Safe Security System Design Using Face And Fingerprint Detection. This safe has a height of 31 cm, a length of 32 cm, and a width of 35 cm. The ESP32-CAM module is connected to the ESP32-CAM-MB, which facilitates code uploading via a USB connection directly to a computer, allowing the ESP32-CAM to be deprogrammed easily without the need for additional devices. Once programmed, the ESP32-CAM can capture images and send them via Wi-Fi network to other devices, such as a connected smartphone with the Telegram app. Arduino Uno acts as the main control in this system, receiving inputs from the fingerprint sensor and signals from the ESP32-CAM. The Arduino then manages outputs such as the 16x2 LCD to display status, controls relays to operate the door lock solenoid, and activates the buzzer as an audio signal based on specified conditions. This combination of devices allows the IoT-based safe security system to perform face and fingerprint authentication, send notifications, and control access effectively.

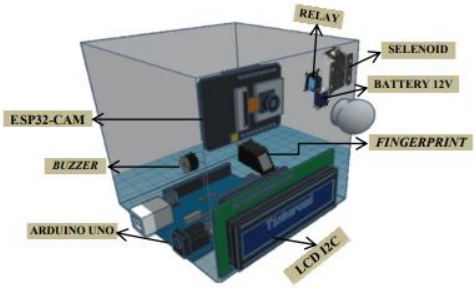
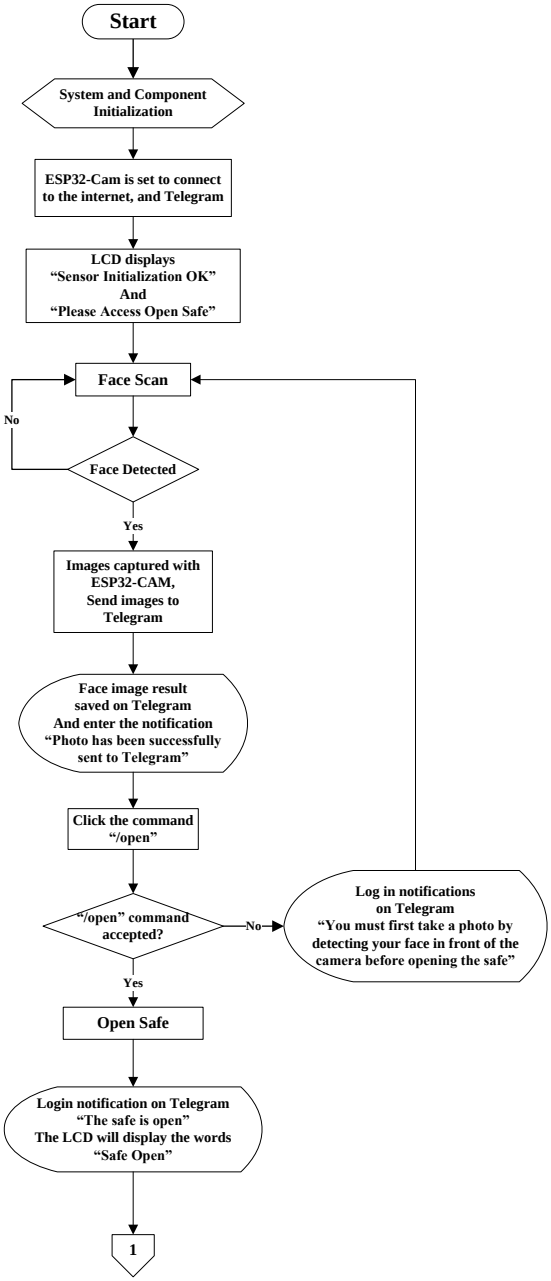


Fig. 3: Barber Design

3.7. Circuit Flowchart

The design of the device begins with the creation of a Flowchart (flow chart) to facilitate the planning and creation of programs on the microcontroller. Making Flowchart in this study aims to make it easier to understand the work process of the tool. In this study, Flowchart includes the control system of the face and fingerprint detection device that functions to automatically unlock the safe. The Flowchart of the Tool Work System can be seen in the picture below:



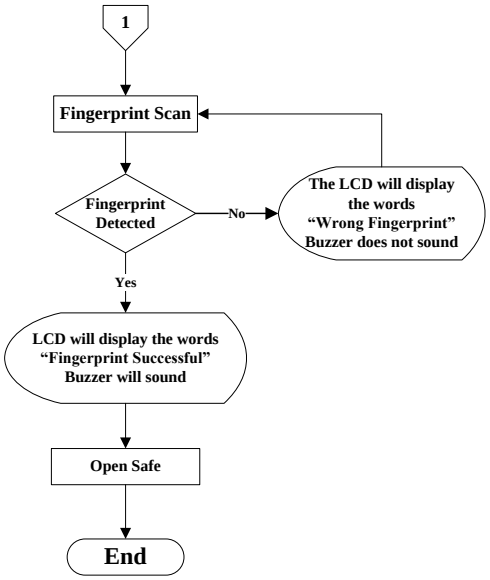


Fig. 4: Flwochart of Tool Working System

4. Discussion And Implementation

4.1. Discussion

This chapter will explain and display the results of testing the design of the tool made. Testing is done by designing and programming tools using the Arduino IDE application to regulate the operation of connected electronic components. By using this system, the owner can access the safe safely and receive instant notifications via the Telegram application.

4.2. Software Testing

To ensure that the ESP32-CAM and Arduino Uno microcontroller circuits work properly, testing will be done by programming and inputting data from the computer into the ESP32-CAM and Arduino Uno microcontroller circuits.

1. The first step to start testing is to open the Arduino IDE software. After the Arduino IDE application is opened, it will see the main interface as shown in Figure 5 below. Make sure that the Arduino IDE is configured correctly for ESP32-CAM and Arduino Uno. After that, make sure to select the right board and serial port for each microcontroller. Then, it can proceed to programming and installing commands.

Fig. 5: Arduino IDE Software Display

2. Next, the program written must match the functions and needs of the safe security system being created before it can program the ESP32-CAM microcontroller. Make sure the application allows image capture, WiFi connection settings, and integration with Telegram for sending notifications and receiving commands. Figure 6 below shows an example of the program used.

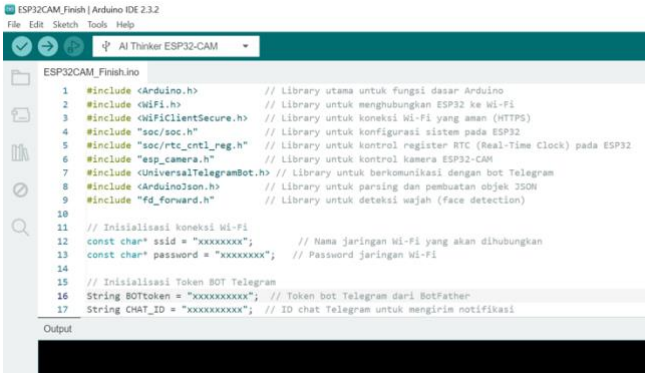


Fig. 6: ESP32-CAM Program View

3. In the next step, the program must be uploaded to the ESP32-CAM microcontroller by selecting the Upload menu in the Arduino IDE. Before starting the upload process, make sure the connection between the computer and ESP32-CAM through the ESP32-CAM-MB programmer is well connected. After selecting the Upload menu, wait until the upload process runs smoothly and reaches 100%, and the program is ready to run on ESP32-CAM. The display of the upload process that has been completed can be seen in Figure 7 below.

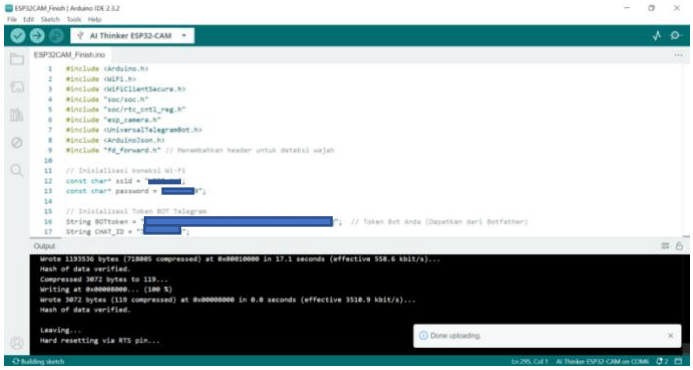


Fig. 7: Upload Process Completed Display

4. To program the Arduino Uno, type a program that matches the functions and needs of the safe security system being developed. To show the authentication results, the program should include the fingerprint sensor settings, relay settings to operate the door lock solenoid, and buzzer activation. Figure 8 below shows the program that can be used for Arduino Uno.

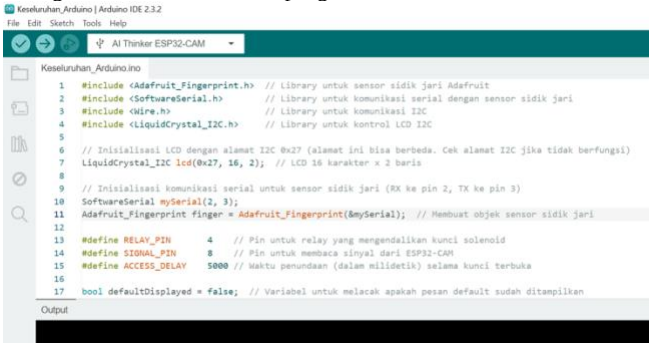


Fig. 8: Arduino Uno Program View

5. Next, it must ensure that the program in the Arduino IDE has been uploaded successfully to the ESP32-CAM. Once done, the ESP32-CAM will be connected to the WiFi network and can communicate with the pre-configured Telegram bot. By using the Telegram application on a smartphone, it can access this Telegram bot and use commands such as "/flash" to turn on the ESP32-CAM LED and the "/open" command to open the safe after the face image is sent. Figure 9 below shows the Telegram interaction view.

Fig. 9: Telegram Interaction View

4.3. Hardware Testing

After all the circuits that have been designed are completed on the "Internet of Things-Based Safe Security System Design Using Face and Fingerprint Detection" tool, the next step is to unite all the components and circuits of the tool with each other. This includes the integration of ESP32-CAM, fingerprint sensor, Arduino Uno, relays, solenoid door locks, and other components that have been adapted to the system design. The face recognition system is ready to be used to find out the expected results of this research after the hardware is assembled and the microcontroller is uploaded with the appropriate program. At this stage, all hardware components, including ESP32-CAM, Arduino Uno, fingerprint sensor, door lock solenoid, relay, LCD, and buzzer, will work together with the implemented program. The system will detect fingerprints and faces, and send notifications via Telegram. Figure 10 below shows a complete picture of the hardware circuit.

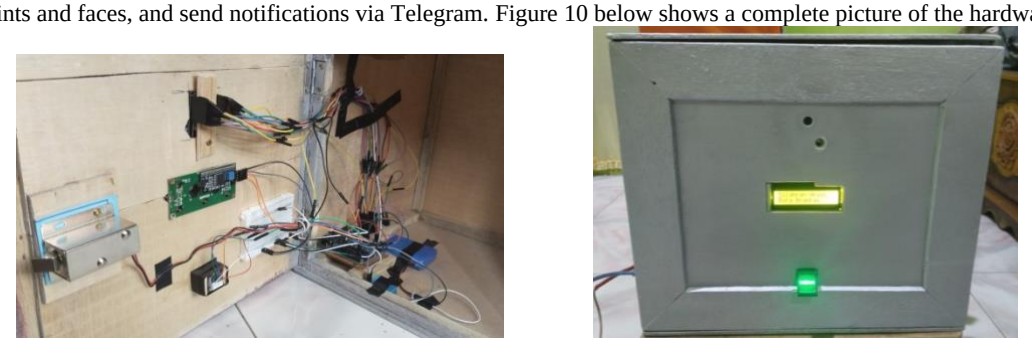


Fig. 10: Hardware Set

4.4. Testing Results of Face Detection or Recognition on Telegram Bots

The ESP32-CAM was used to test the IoT-based safe security system, which captures facial images for verification. When the owner is in front of the camera, the ESP32-CAM captures an image of the face in front of him. This image is then automatically sent to a Telegram bot for the owner to manually verify. If the captured face photo matches the authorized owner, the owner can proceed to the next step by using the "/open" command to open the safe. Figure 11 below shows the results of the face image and the "/open" command on the Telegram Bot.

Fig. 11: Result of Face Image and "/open" Command on Telegram Bot

4.5. Fingerprint Sensor Testing Results

The IoT-based safe security system uses a fingerprint sensor as the main authentication method. The owner must scan their fingerprint on the fingerprint sensor connected to the Arduino Uno when they want to open the safe. The sensor reads the scanned fingerprint and sends the data to the Arduino Uno to ensure that the fingerprint stored in the system is the correct one. The LCD will display the result of the fingerprint verification process. If the scanned fingerprint matches the stored data, the LCD will display the message "Fingerprint Successful" and the relay will be activated to open the safe lock solenoid. In addition, the buzzer will sound to indicate that the authentication has been successful. If the scanned fingerprint does not match the existing data, the message "Incorrect Fingerprint" will be displayed on the LCD. In this case, the safe remains locked and the buzzer will not sound. This display tracks the status of the fingerprint authentication and ensures that only the authorized owner can view the contents of the safe. Figure 12 below shows the results of Successful Fingerprints and False Fingerprints

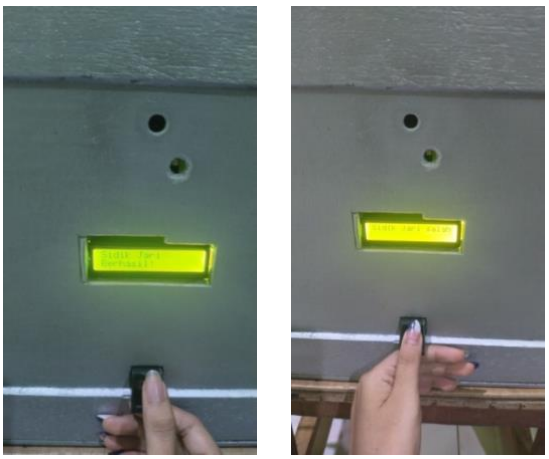


Fig. 12: Successful Fingerprint and Incorrect Fingerprint Results

5. Conclusion

Based on the results of research and testing that has been carried out on an Internet of Things (IoT)-based safe security system using face and fingerprint detection, it can be concluded that:

1. Security System Effectiveness: The safe security system using ESP32-CAM for face detection and fingerprint sensor successfully enhances security by providing two layers of authentication. The ESP32-CAM allows the system to take a face image and send it to Telegram for manual verification by the owner, while the fingerprint sensor ensures only the registered owner can open the safe.
2. Notification via Telegram: The Telegram app works effectively to provide immediate notifications about the status of the safe, such as when the safe is opened or if there is a forced opening attempt. In addition, the system allows the owner to control access to the safe through Telegram commands.
3. Well-running Component Integration: With the Arduino Uno as the main control, the integration between the ESP32-CAM, fingerprint sensor, relay, lock door solenoid, LCD, and buzzer went as planned. Each component works well according to the programming, and the system responds to commands appropriately.
4. System Restrictions: Although the system can send face images for manual verification to Telegram, facial recognition technology has not been fully implemented in automation. This limits the system's ability to perform face authentication without direct owner interaction via Telegram.

References

[1] Rahmat Gunawan, Arif Maulana Yusuf, and Lysa Nopitasari, "Rancang Bangun Sistem Presensi Mahasiswa Dengan Menggunakan Qr Code Berbasis Android," *Elkom J. Elektron. dan Komput.*, vol. 14, no. 1, pp. 47–58, 2021, doi: 10.51903/elkom.v14i1.369.

[2] R. T. Budiyanti, *Buku Ajar Internet of Things*. 2021.

[3] M. B. Sopandi Bara and Dewi Hendrawati, "Rancangan Smart Door Lock Berbasis IoT dengan Verifikasi Wajah," *SEMNASTERA (Seminar Nas. Teknol. dan Ris. Ter.*, pp. 451–457, 2023.

[4] Mambang, *BUKU AJAR TEKNOLOGI KOMUNIKASI INTERNET (Internet of Things)*, no. April. 2021. [Online]. Available: https://www.researchgate.net/publication/360289401

[5] Y. Irawan, R. Wahyuni, D. Rahmawati, and H. T. Saputra, "Sistem Keamanan Smart Brankas Menggunakan Fingerprint Android," *J. Jar. Sist. Inf. Robot.*, vol. 6, no. 1, pp. 14–19, 2022, [Online]. Available: http://ojsamik.amikmitragama.ac.id

[6] D. Didit Wahyu, S. Aryuanto, and S. I Komang, "Rancang Bangun Lengan Robot Pemilah Barang Berdasarkan Berat dengan Pemanfaatan Internet Of Things (IoT) Sebagai Kontrol Dan Monitoring Jarak Jauh," *Semin. Has. Elektro S1 ITN Malang*, vol. 21, no. 1, pp. 1–2, 2020.

[7] O. R. Arsyad and K. P. Kartika, "Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 5, no. 1, pp. 1–6, 2021, doi: 10.36040/jati.v5i1.3285.

[8] I. Syukhron, "Penggunaan Aplikasi Blynk untuk Sistem Monitoring dan Kontrol Jarak Jauh pada Sistem Kompos Pintar berbasis IoT," *Electrician*, vol. 15, no. 1, pp. 1–11, 2021, doi: 10.23960/elc.v15n1.2158.

[9] F. Chaining and C. Factor, "Sistem_Pakar_Menggunakan_Forward_Chainin," vol. 8, no. 2, 2020.