Development of a Quadruple Security System Combining Keypad, RFID, Fingerprint, and Bluetooth modules

Gyongbong Ju[a], Cholhyon Sim[a], Choljin Kim[b], Yongmin Kim[a]

[a] Hamhung University of Hydraulics and Power, Ham Hung, DPR of Korea
[b] Pyongyang University of Architecture, Pyongyang, D P R of Korea

- ABSTRACT

Today, the security problem is emerging as a crucial problem for people, and research into solving this problem is now on its way worldwide. Everyone is aware of the urgency and seriousness of the security problem, and at this time, this problem has a giant impact on the overall social life. As science and technology develop, researches for solving security problems are advancing to a new stage, and their reliability is increasing day by day.

In this study, a powerful quadruple security system was designed and realized by combining Keypad, RFID, Fingerprint, and Bluetooth (HC06) modules to thoroughly secure the security of medicines, jewelry, documents, and other valuables and doors.

This system is based on the Arduino Mega 2560 microcontroller and is an intelligent system with a display function, voice function, SMS transmission function by GSM module, and alarm function. The system is an excellent system that can thoroughly guarantee the safety of security with low cost and low power consumption.

-Keywords

Keypad, RFID, Fingerprint, Bluetooth, GSM, microcontroller, security system

1. Introduction

Security issues emerge as essential issues in ensuring the safety of people's lives and valuables. There is no security guarantee since the mechanical lock can be opened by an intruder forcibly. At present, with the development of science and technology, more secure and intelligent security systems are emerging using digital encryption technology, RFID technology, biometrics technology, and wireless communication technology.

Figure 1 shows a block diagram of the microcontroller based digital door lock security system using keypad [1].

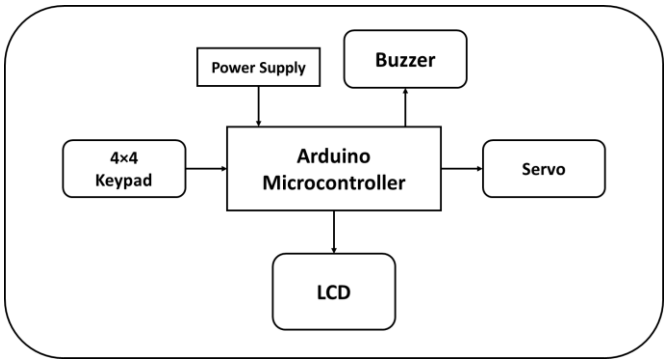


Figure1. Block diagram of the microcontroller based digital door lock security system using keypad

The security system contains a 4X4 keypad input unit for entering the Personal Identification Number (PIN) and a display unit in form of Liquid Crystal Display (LCD) for visual display of information. It also contains a servo motor that serves as a switching for locking and unlocking the door and a programmed microcontroller that processes the input information and take appropriate action. When a user enters a PIN into the security system installed at any entrance, the system captures the PIN and compares it with the stored PINs for a match. If the captured PIN matches with any of the stored PINs, access granted is displayed on the LCD and the door opens; otherwise, access denied is displayed on the LCD and the door remains closed.

This system has a high possibility that an intruder can secretly steal the user's hand movements and unlock the password with a combination of numbers and letters, so security cannot be completely has guaranteed.

The mobile phone-based security system [2] is a system that can install and cancel security using a mobile phone. When the user dials the number of the security system, the system gets opened or closed, with the specific code interpreted. Figure 2 shows the mobile phone-based security system. One flaw of this system is that it is unable to be used when the user's mobile phone is power off or an internet connection failure occurs due to abnormal weather. Another flaw is that it is unable to keep security if the user's phone is in an intruder's hands.

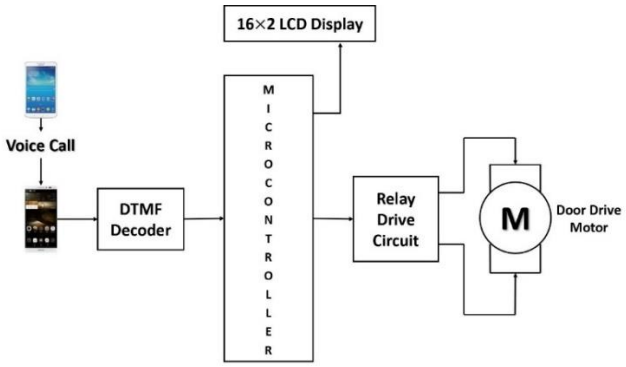


Figure 2. Mobile phone-based security system

RFID-based security systems [3,4] use RFID tags, and the system operates only when the tags registered in the system match with the input tags. The RFID-based security system is unable to be used by the user when he or she loses the RFID tag, and there exists a security risk when the user tag falls into the hands of intruders.

Biometrics-based security systems are playing a decisive role recently in constructing stark security systems in various spaces. Biometric is an automated technique of recognizing a person based on his physical attributes like the face, fingerprint, hand geometry, handwriting, iris, retinal, vein, and voice.

Fingerprint recognition-based security system [5] is a superior security system that identifies users by analyzing the fingerprint image. However, this system requires a high-resolution scanner.

The bank security system [6] built to identify users based on vein detection and iris recognition requires a lot of memory to store data.

The face recognition-based security system [7] introduced a principal-component analysis method to identify users by matching face images captured by a web camera with face images stored in a database. The face recognition-based security system has a problem to improve reliability and robustness.

The GSM-based security system [8-11] uses a GSM module for communication purposes. When an intrusion occurs, it sends an SMS to the user to notify the user of the crisis in time or to remotely control the system according to the user's purpose. However, this system is heavily affected by the Internet.

The Bluetooth-based security system [12] is based on the Arduino platform and locks or unlocks the locking device through communication between the Android smartphone and the Bluetooth module.

Recently, IoT-based security systems [13,14] are also widely introduced, but they are also heavily influenced by the Internet.

Figure 3 shows a block diagram of the locker security system [15] using Keypad and RFID.

This system lifts security only when the user password entered through the Keypad matches the password registered in the system, and the user's RFID number and the system's RFID number match.

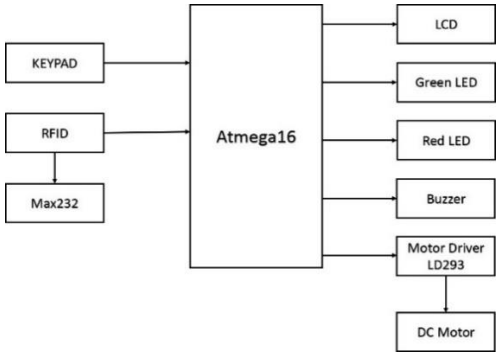


Figure 3. Block diagram of a locker security system using Keypad and RFID

The literature [16] shows the development of a dual security system using RFID and fingerprint.

Here, the system also lifts security only when the user's RFID number matches the RFID number registered in the system, and the user's Fingerprint and the Fingerprint registered in the system match.

Figure 4 shows the workflow diagram of a dual security system using RFID and fingerprint [16].

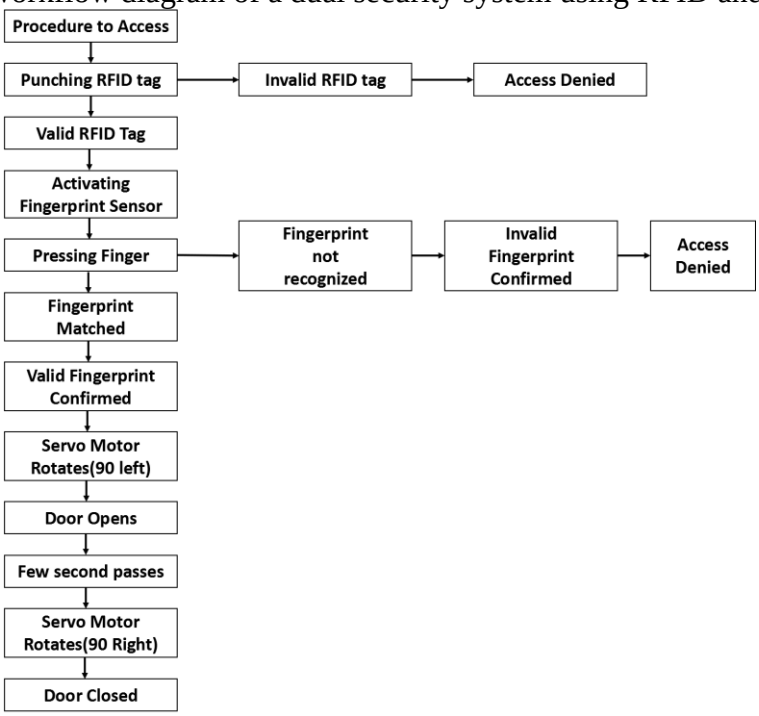


Figure 4. Workflow diagram of dual security system using RFID and fingerprint

Figure 5 shows the configuration diagram of a locker security system using a keypad, fingerprint, and GSM module.[17]

This system identifies the user by password input and fingerprint, and when an intrusion occurs, the GSM module sends SMS to the user.

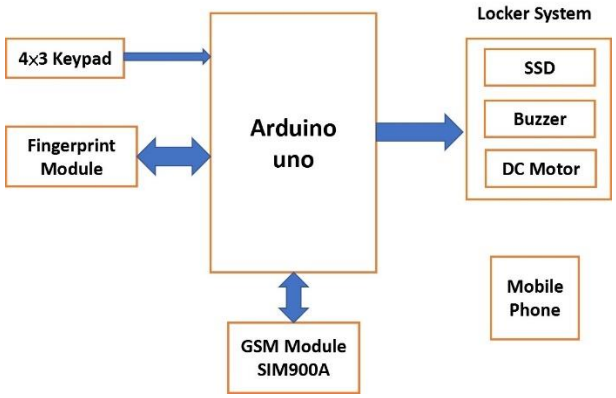


Figure 5. Configuration diagram of locker security system using Keypad, fingerprint and GSM module

As seen above, the result of the comprehensive analysis of the previous studies is as follows:

Each imprisonment module constituting the security system has its advantages and disadvantages, and security is unable to be guaranteed through only one imprisonment module. Therefore, to increase the reliability of the security system, two or more modules must be combined when building the system. Also, the system must be able to cope with unexpected situations.

A quadruple security system was designed and realized by combining the Keypad, RFID, Fingerprint, and Bluetooth (HC06) modules to ensure thorough security. The system consists of a 4×4 Keypad module, RFID module, Fingerprint module, Bluetooth (HC06) module, GSM module, LCD, Mp3 module, Buzzer, Relay, and Solenoid door lock.

If the input password matches with the password registered in the system after the password input started in the 4×4 Keypad module, the system requests RFID card input. If the input card ID also matches with the system-registered card ID, then fingerprint verification is required.

If the input fingerprint matches the fingerprint registered in the system, a password transmission through Bluetooth is requested. If the password sent from the user's mobile phone matches with the Bluetooth password registered in the system, the system finally sends a signal to the relay to operate Solenoid and release the security.

Fixed time is allowed for each step, and the system automatically proceeds to the first step when the allowed time is past.

The LCD informs the status of each step and instructions for subsequent actions in text, and the Mp3 module advises by voice.

Since the GSM module immediately transmits the status of each step of the security system to the user via SMS notification, the user can take countermeasures as soon as an intrusion occurs.

In the event of an unexpected situation, such as password-forgotten, card loss, or internet problem, you can unlock security with more than five fingerprints.

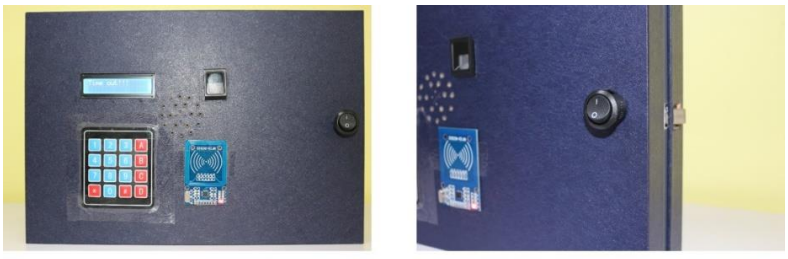
2. System design

The security system proposed was designed to use a keyboard input password, RFID tag, valid fingerprint, and Bluetooth transmission password (including letters, numbers, and special symbols) as access keys. Figure 6 shows the schematic diagram of the system.

As shown in Figure 6, 4 inputs and five outputs are controlled by the Arduino mega 2560.

Figure 6. Configuration diagram of the quadruple security system

Figure 7 shows the external structure of a model device with a quadruple security system implemented.



a b

Figure 7. External structure diagram of a model device with a quadruple security system implemented (a-front view, b-side view)

The device's internal circuit design includes Arduino mega2560 microcontroller, 4×4 Keypad module, RFID module, Fingerprint module, Bluetooth (HC06) module, GSM module, LCD, Mp3 module, Buzzer, Relay, Solenoid, power supply, and breadboard.

All the components connected to the Arduino mega 2560 receive a power supply through the jump wire. Arduino Mega 2560 receives a 5V power supply, and Solenoid, a 12V power supply from an external source. Figure 8 shows the internal schematic of the system.

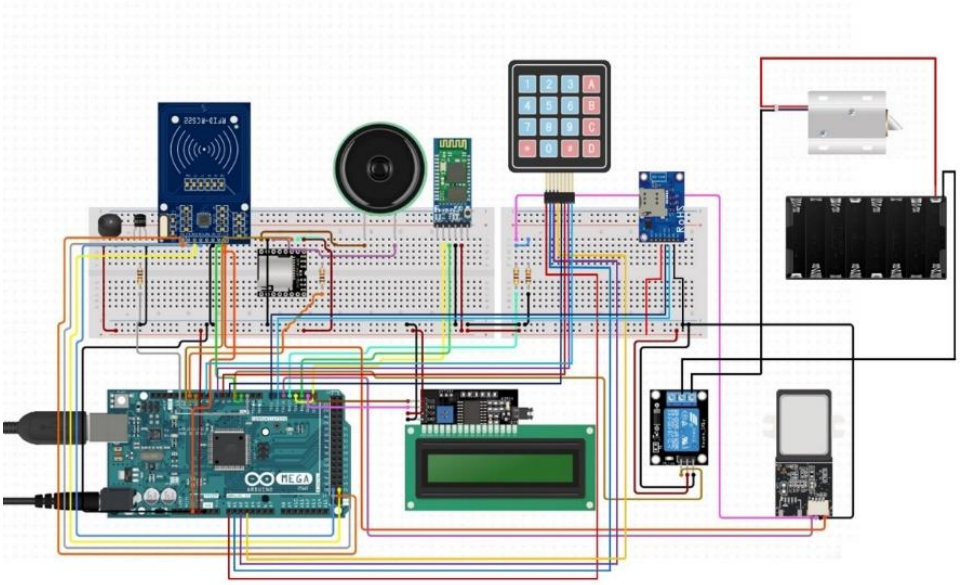


Figure 8. Internal circuit diagram of the quadruple security system

Table 1 shows the internal circuit wiring table.

Table 1. System internal circuit wiring table

Control module		Arduino Mega 2560
4×4 Keypad	R1	A0
	R2	A1
	R3	A2
	R4	A3
	C1	D5
	C2	D6
	C3	D7
	C4	D8
RFID	RST	D3
	SDA	D53
	MISO	D50
	MOSI	D51
	SCK	D52
	3.3v	3.3V
	GND	GND
Fingerprint	RX	D17
	TX	D16
Bluetooth	RX	D19
	TX	D18
GSM	RX	D15
	TX	D14
Mp3	RX	D11
	TX	D10
Relay		D4
Buzzer		D2

3. Components of the system

This system is composed of eleven modules. In other words, the system consists of Arduino mega2560 microcontroller, 4×4 Keypad module, RFID module, Fingerprint module, Bluetooth (HC06) module, GSM module, LCD, Mp3 module, Buzzer, Relay, Solenoid.

3.1 Arduino mega 2560

Arduino is a convenient, flexible, and easy-to-use Open Source Prototype Platform. [18-21] Included in Arduino are hardware (various types of Arduino boards) and software (Arduino IDE).

Arduino is based on the Open Source Single I / O Interface version and has a Processing / Wiring development environment similar to Java and C languages.

It mainly consists of hardware and Arduino IDE. The hardware is the Arduino circuit board used to connect the circuit, and the Arduino IDE is the computer's program development environment.

After programing the IDE and building the program on the Arduino board, the program will perform the task.

Arduino Mega 2560 is a core circuit board with a USB user interface which has 54 numeric inputs and outputs, so it is suitable for designs requiring a lot of IO interface. [22]

This system also requires a lot of IO interface, so Arduino UNO or Arduino nano is unable to be used. Therefore, in this study, selected was the Arduino mega 2560. Figure 9 shows the Arduino mega 2560 module.

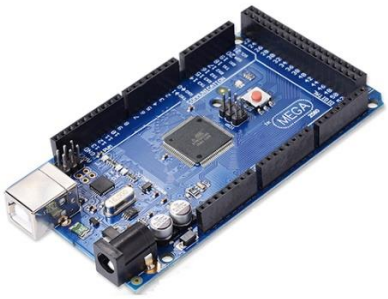


Figure 9. Arduino mega 2560 module

The processor core of the Arduino Mega 2560 is ATmega 2560.

It consists of 54 numeric input/output ports (15 available as PWM outputs), 15 analog inputs, 4 UART interfaces, 16MHz crystal oscillator, USB port, power socket, an ICSP header, and reset button.

Arduino Mega 2560 is also compatible with expansion boards designed for Arduino UNO. After comparing with two previous versions, new features has been expanded on the Arduino Mega2560 as follows:

SDA and SCL are added to AREF to support the I2C interface.

Also, the expansion board is compatible with 5V and 3.3V core boards.

And, improved was the reset circuit design. USB Interface Chip replaced ATmega8U2 with ATmega16U2.

3.2 Keypad

The keypad is connected in the form of a matrix of push-button switches to form a circuit. The most commonly used keypad is a 4×4 keypad.

The 4×4 keypad consists of 4 rows (R1, R2, R3, R4) and four columns (C1, C2, C3, C4), and Figure 10 shows the principle of operation and physical form of the keypad.

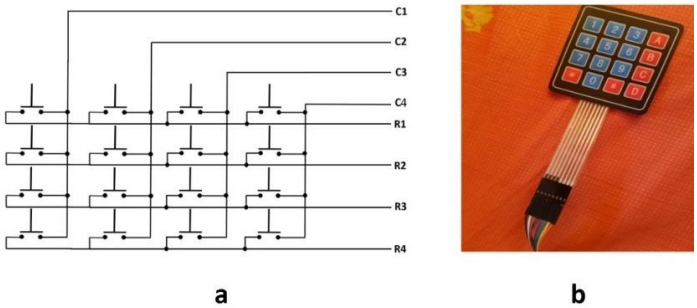


Figure 10. Principle (a) and physical form (b) of 4×4 keypad

Press the switch, and the row and column are connected. Then the port connected to the row becomes input, and the port connected to the column becomes output, and the row number and column number of the pressed switch are acquired.

3.3 RFID

RFID is a technology that uses electromagnetic or electrostatic coupling to the radio frequency portion of the electromagnetic spectrum to identify an object or person. [23, 24]

RFID has the advantage of not requiring direct contact or line of sight scanning. There are three components of RFID: an antenna, a transceiver, and a transponder.

Figure 11 shows the configuration and physical form of RFID.

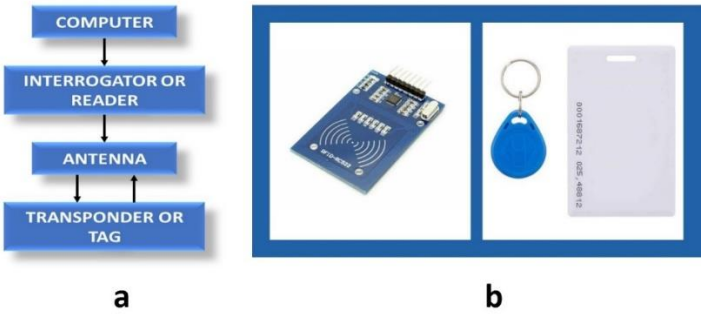


Figure 11. RFID system (a-RFID configuration diagram, b-RFID Reader and tag

The antenna transmits a signal that activates the transponder using radio frequencies. When activated, the data is sent back toward the antenna. The ID written on the tag is called EPC (Electronic Product Code).

3.4 Fingerprint

Fingerprints are one of the various forms of biometrics used to verify identity. [25-27]

Analyzing a fingerprint for matching purposes usually requires comparing several features of a printed pattern. They include the collective feature pattern of the ridges and feature points unique to each pattern.

The study used the FPM10a optical fingerprint module with an excellent fingerprint recognition effect. The FPM10a optical fingerprint module has an optical fingerprint sensing unit and a DSP processor with high performance and high speed. It is also an intelligent module with independent fingerprint registration, fingerprint image processing, fingerprint comparison, fingerprint search, and storage functions. Table 2 shows the characteristic parameters of the FPM10a optical fingerprint module.

Table 2. Characteristic parameters of FPM10a optical fingerprint module

Characteristic parameter	value
Operating voltage	3.8~7.0V
Operating current	< 65mA
Fingerprint image registration time	< 0.5 seconds
storage capacity	1000
Safety Class	5 (max)
Working temperature	-20℃~+60℃
Relative humidity	40%RH~85%RH

Figure 12 shows the FPM10a optical fingerprint module.

Figure 12. FPM10a optical fingerprint module

3.5 Bluetooth module (HC06)

Bluetooth is a wireless technology that supports short-range (generally within 10m) communication of devices. [28, 29]

It allows the wireless exchange of information between various devices such as mobile phones and computers.

This small-scale wireless connection technology is one of the mainstream technologies for wireless personal area network communication because it can implement convenient, fast, flexible, secure, low-cost, low-power data communication and voice communication between devices.

The Bluetooth HC06 is a master-slave Bluetooth serial port module. [30, 31] In short, if one device is connected to another device successfully through Bluetooth, you can ignore the Bluetooth internal communication protocol and use Bluetooth as a serial port directly. Once the connection succeeded, both devices can share the same serial port, as one device can transmit data through the serial port, and the other can receive data through the serial port.

HC06 features include:

- Bluetooth v2.0 + EDR
- 2.4GHz ISM band frequency
- Default baud rate: 9600
- Power supply: 3.6V ~ 6V DC

The HC06 board requires four wires for communication, such as the VCC, GND, RX, and TX pins. There are two additional pins on the board. One is the STATE pin, and the other is the EN pin. The reset pin is for resetting the Bluetooth module by sending a reset signal from the Microcontroller. Figure 13 gives the physical form of the Bluetooth HC06.

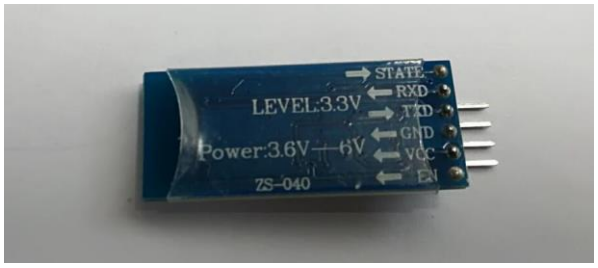


Figure 13. Physical form of Bluetooth HC 06

The HC06 operates in serial communication. The Android app is programmed to send data serially to the Arduino Bluetooth module by entering the transmit password and pressing the send button. The Arduino Bluetooth module receives the data and sends it to the Arduino through the Bluetooth module's TX pin (connected to the Arduino's RX pin). The code uploaded to the Arduino checks and compares the data received. During connection, you can open the serial monitor and view the received data.

3.6 GSM module

In this study, the SIM800L, generally used in GSM modules, was selected to send the security system status instantly to users via SMS.

Mini GSM/GPRS breakout board is based on SIM800L module and supports Quadband GSM/GPRS network, used to transmit GPRS and SMS messages. [32, 33]

Features are as follows.

- Quad band 850/900/1800 / 1900MHz.
- Connects to all GSM networks.
- Voice calls available.
- SMS transmission statement transmission possible.
- GPRS data transmission possible.
- Operating voltage: 3.7 ~ 4.2V
- Peak current: 1A

Figure 14 shows the physical form of the SIM800 GSM module.

Figure 14. Physical form of SIM800 GSM module

3.7 MP3 module

This system uses an MP3 module to inform the user of each situation of the security system by voice. Chosen for this purpose is DFPlayer Mini MP3.

Figure 15 shows the physical form and pin structure of the DFPlayer Mini MP3 module.

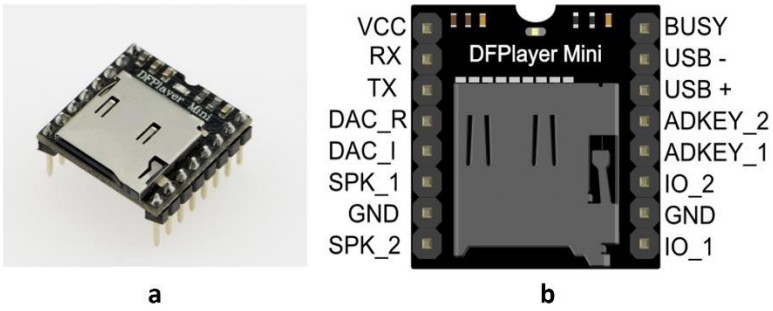


Figure 15. Physical form (a) and pin structure (b) of DFPlayer Mini MP3 module

DFPlayer Mini is a small and low-cost MP3 module that can output to the speaker directly. This module can become a standalone module with a battery, speaker, and pushbutton attached to it, or used in combination with Arduino or any other devices with RX/TX function.

It supports general audio formats such as MP3, WAV, and WMA, and also supports TF cards with FAT16 and FAT32 file systems.

In this study, VCC, RX, TX, SPK_1, GND, and SPK_2 terminals are necessary for usage. Connect 5V of Arduino to VCC pin and 1KΩ resistor to RX and TX, respectively, and connect to pin10 and pin 11 of Arduino. Connect the speaker's + terminal to SPK_1 and the speaker's-terminal to SPK_2.

3.8 LCD

The LCD is used as a display device to inform the status of the security system in text.

This system uses Grove-16 x 2 LCD, an I2C LCD that is easy to use in Arduino.

Grove-16x2 LCD consists of 16 rows and two columns and can display 32 characters all together, including letters, numbers, and special symbols on the screen.

Grove-16x2 LCD only needs two signal pins (data pin SDA and CLOCK pin SCL) and two power pins (VCC, GND).

Figure 16 shows the physical form of the Grove-16x2 LCD.

Figure 16. Physical form of Grove-16x2 LCD

3.9 Solenoid door lock

In this study, selected as the locking device of the security system was a solenoid door lock. Instead of a solenoid door lock, you can choose a lock that uses a motor.

Figure 19 shows the physical shape of the solenoid door lock. This device must guarantee DC12V externally. Figure 17 shows the physical form of the solenoid door lock and how it works. Solenoids are electromagnetic devices that can convert electrical energy into kinetic energy. Inside the solenoid is a wire wound around an iron core. When an electric current passes through these wires, a magnetic field is generated, creating energy that can push the iron core away.

The kinetic energy produced by a solenoid is usually through pushing and pulling motion.

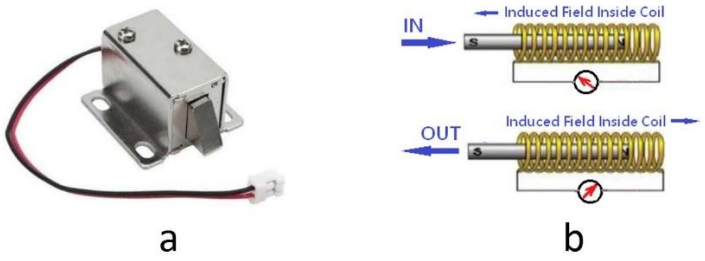


Figure 17. Physical form (a) and operation principle of the solenoid door lock (b)

3.10 Relay

Relay is for operating a 12V Solenoid door lock device with a 5V signal.

When the quadruple security is released, D4 from Arduino mega 2560 sends a signal to the IN pin of the Relay. At this time, 12V power is supplied to the solenoid to release the locking device.

Fig. 18 shows the control process of the locking device by relay.

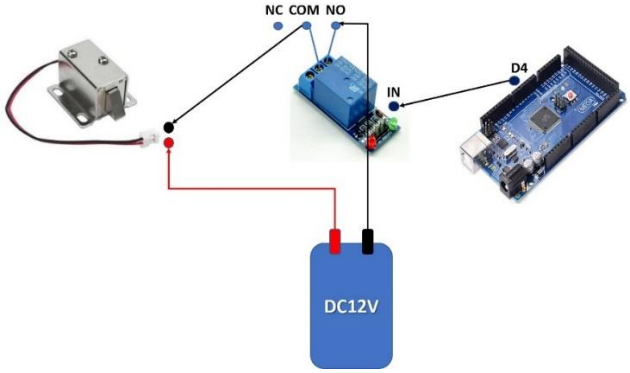


Figure 18. The control process of locking device by relay

3.11 Buzzer

The buzzer is equipment installed to generate an alarm sound in case respondents failed to respond accurately to the request of the system. Figure 19 gives the physical shape of the buzzer.

When an intrusion occurs, D2 of Arduino mega 2560 transmits a single to the “+” pin of the buzzer to generate alarm sounds. The “-” pin of the buzzer connects to the GND.

Figure 19. The physical form of buzzer

4. System workflow

This security system is an intelligent system with four input functions and five output functions.

4.1 Numerical password input through 4×4 keypad

The first step of this security system is the step of entering a numeric password through a 4×4 keypad. The system has built-in predefined passwords (for example, 1234).

When the user enters the password and presses the "#" button, the program compares the password entered by the user with the password built into the system proceeds programmatically.

If the passwords match, the system proceeds to the next step. If the passwords do not match, the user has to start over. To change the password, you must enter the password you want to change and press the “*” button in the state that all security is off. Fig. 20 shows the password input process through the 4×4 keypad.

Figure 20. Password input process through 4×4 Keypad

Table 3 shows the output result for the password input process through the 4×4 Keypad.

Table 3. The output result of the password input process through 4×4 Keypad

Output module	Password match	Password mismatch
LCD	Password OK! Insert Card!	Password failure!
MP3	Password input was successful. Enter your card.	Password input was not successful.
GSM(SMS)	The numeric password has been canceled.	Someone is trying to decrypt the number.
Buzzer	Alarm off	Alarm on
Relay	off	off

4.2 ID identification through RFID

If the password input through the 4×4 keypad is successful, the system proceeds to the ID identification step through RFID. Figure 21 shows the ID identification process through RFID.

Figure 21. ID identification process through RFID

The ID identification code is usually an eight-digit hexadecimal number (for example, bf5fa03d), and the user's ID is already in the system through Arduino programming. When a user attaches an RFID tag to an RFID reader, it compares the user's ID with the ID built into the system. If the IDs match, the system moves to the next step, the fingerprint recognition step, and if they don't, the system forcibly goes back to the first step, the password input step. It also sets a timeout of 10 seconds that forcibly returns to the first step unless it recognized the correct tag within 10 seconds.

Table 4 shows the output result of the ID identification process through RFID.

Table 4. The output result of the ID identification process through RFID

Output module	RFID match	RFID mismatch	Time out
LCD	RFID OK! Insert Finger!	RFID fails!	Time out!
MP3	Card input was successful. Please enter your fingerprint.	Card input was not successful.	The time has expired.
GSM(SMS)	RFID has been released.	Someone is trying to disable RFID.	Timeout at the RFID stage!
Buzzer	Alarm off	Alarm on	Alarm on
Relay	off	off	off

4.3 Fingerprint recognition through the fingerprint module

If ID identification through RFID is successful, it moves to the next step, the fingerprint recognition step. Fig. 22 shows the fingerprint recognition process through the fingerprint module.

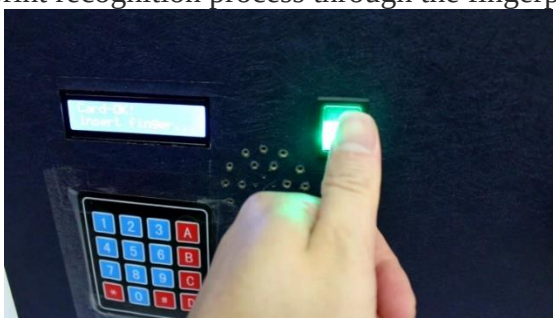


Figure 22. Fingerprint recognition process through the fingerprint module

The fingerprint module analyzes the fingerprint image to generate an ID. When the generated ID and the fingerprint ID embedded in the system match through programming, it moves to the next step.

When multiple people manage the system, the system allocates a registration number along with an ID to registered members. Only when the RFID registration number and the fingerprint registration number match, the system regard the fingerprint recognition as a success and proceed to the next step. In other words, it is impossible to steal another person's RFID or fingerprint among registered members. If the fingerprint recognition time exceeds the set time, the system forcibly turns the process back to the first step. Table 5 shows the output result of the ID identification process through fingerprint.

Table 5. The output result of the ID identification process through fingerprint

Output module	Fingerprint match	Fingerprint mismatch	Time out
LCD	Fingerprint OK! Send your BT key!	Fingerprint failure!	Time out!
MP3	Fingerprint input was successful. Send the Bluetooth Password.	Fingerprint input was not successful.	The time has expired.
GSM (SMS)	Fingerprint recognition was successful.	Someone is trying to unlock your fingerprint.	Timeout in the fingerprint recognition stage!
Buzzer	Alarm off	Alarm on	Alarm on
Relay	off	off	off

4.4 Final confirmation via Bluetooth

After entering a numeric password through a keypad, identification through RFID, and fingerprint recognition through a fingerprint, it finally enters the user authentication through Bluetooth. Today,

intelligent mobile phones are becoming an integral part of people's business and life, and their range of usage is expanding day by day.

In this study, we finally identified the user and unlocked the security system through Bluetooth communication between the user's intelligent mobile phone and the security system.

The user's intelligent mobile phone must have an Android app installed to realize Bluetooth communication with the security system. To this end, in this study, an Android app for Bluetooth communication with the security system was created using MIT App Inventor (http://appinventor.mit.edu).

The MIT App Inventor has the advantage of perfectly-building intelligent mobile phone applications in a free online environment. Figure 23 shows the process of sending a password to a security system through a Bluetooth app installed on an intelligent phone.

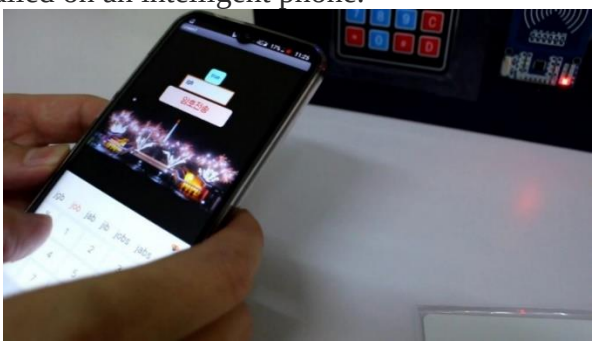


Figure 23. Password transmission process through Bluetooth

First, launch the Android app to connect Bluetooth to the security system. When Bluetooth is connected, the Bluetooth setting button changes to "True." Then enter the password in the text box and click the "Send Password" button to send the password to the system. Passwords can contain letters, numbers, and special symbols. When the system receives the password, it compares the built-in password with the transmitted password and, if they match, sends signals to Relay to activate the solenoid and finally unlock the quadruple security system. If the passwords do not match, the system will halt. Table 6 shows the output result of the password transmission process through Bluetooth.

Table 6. Password transmission process through Bluetooth

Output module	Bluetooth Password match	Bluetooth Password mismatch	Time out
LCD	All are OK! Open the door!	Unknown Password!	Time out!
MP3	All certifications have been passed.	You have failed authentication.	The time has expired.
GSM(SMS)	The quadruple security system has been released.	Authentication through Bluetooth has failed.	Timeout at the Bluetooth authentication stage!
Buzzer	Alarm off	Alarm on	Alarm on
Relay	on	off	off

Figure 24 shows the process of solenoid operation when a signal is applied to the relay.

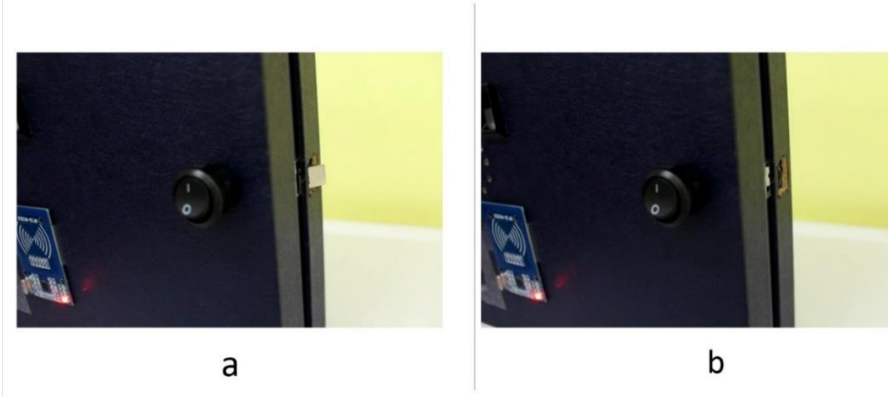


Figure 24. The process of solenoid operation when a signal is applied to the relay

Figure 24(a) shows the state before the release of the quadruple security system, and Figure 24(b) shows the situation after the release of the quadruple security system.

4.5 Workflow diagram of the quadruple security system

Figure 25 shows the flow chart for creating a quadruple security system program.

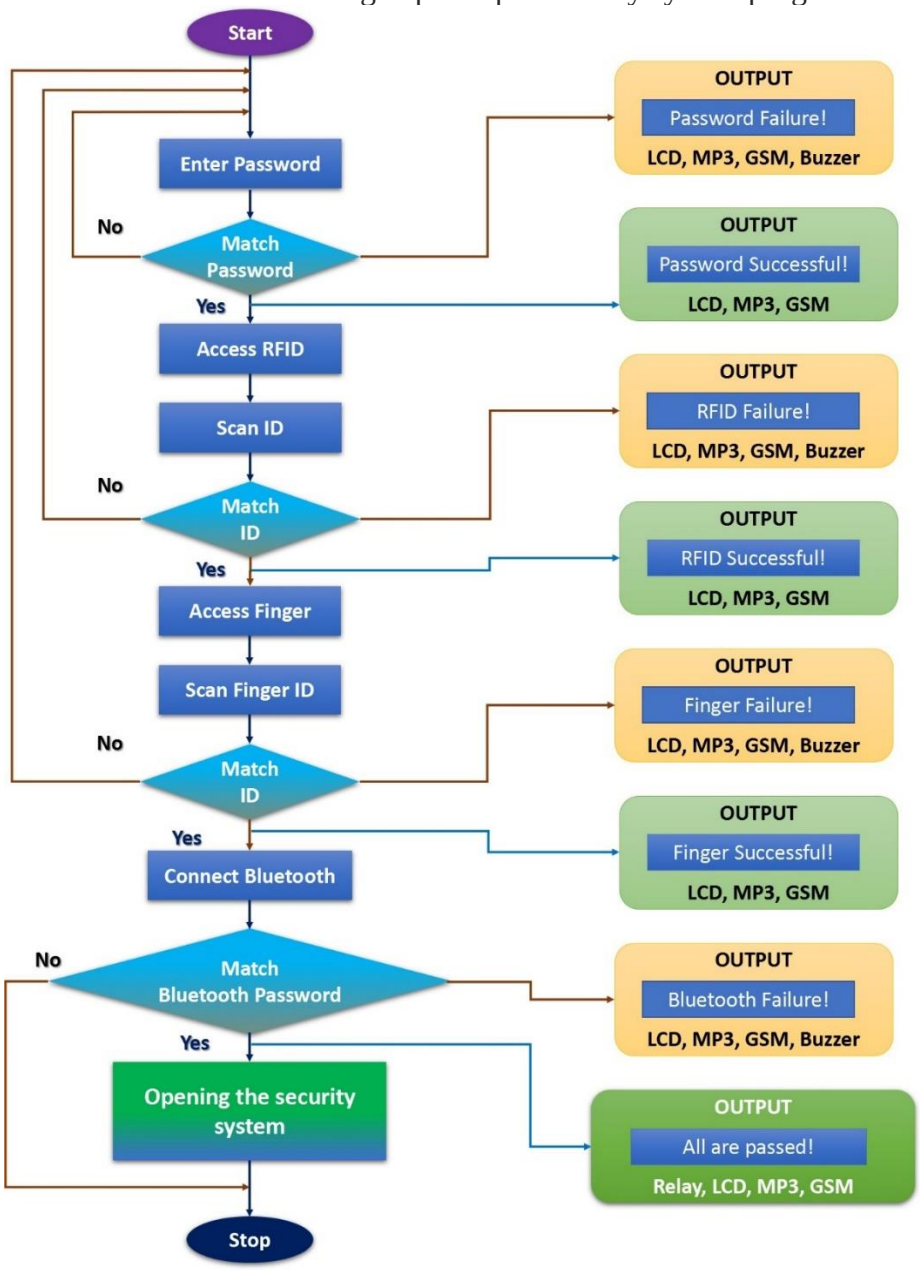


Figure 25. Workflow diagram of the quadruple security system

Used for writing the program for the quadruple security system was C language in the Arduino IDE environment.

5. System performance evaluation

Table 7 shows the results of five evaluation tests of the performance of the system.

Table 7.4 Performance Evaluation of Security System

No	Keypad	RFID	Fingerprint	Bluetooth	Solenoid door lock
1	Failure				Close
2	Success	Failure			Close
3	Success	Success	Failure		Close
4	Success	Success	Success	Failure	Close
5	Success	Success	Success	Success	Open

As can be seen from the table, the security barrier is removed only after passing through four security barriers. In other words, the security never gets removed by anyone except the user with actual authority. The reliability of the quadruple security system is 100%, and it is very convenient to use with the help of a screen and voice. Besides, through SMS notification, though far away from the security system, the user can check the status of the security system and taken measures. In case of forgetting the password, losing the RFID card, or unavailable telephone service, the system requires more than five fingerprint inputs and releases the security if the fingerprints match.

The sensitivity degree of every module is very high, and it takes about 10 seconds for a user with actual authority to unlock the system.

6. Conclusion

In this study, a quadruple security system came into reality through Keypad, RFID, Fingerprint, and Bluetooth. With four security barriers set, the security is guaranteed thoroughly. It is also a low cost, low power consumption, and highly-intelligent system.

The system can be applied anywhere needed for a security guarantee, and the degree of security can be adjusted if necessary. Also, it is possible to add an iris recognition function and face recognition function at the request of the user.

Reference

[1]. Orji EZ, Nduanya UI, Oleka CV. Microcontroller Based Digital Door Lock Security System Using Keypad. International Journal of Latest Technology in Engineering, Management & Applied Science. 2019;8(1):92-7.

[2]. Jadhav, Ashish, Mahesh Kumbhar, and Mahesh Walunjkar, Feasibility study of implementation of cell phone controlled, password protected door locking system, International Journal of Innovative Research in Computer and Communication Engineering 1.6 (2013).

[3]. Verma, Gyanendra K., and Pawan Tripathi, A digital security system with door lock system using RFID technology, International Journal of Computer Applications 5.11 (2010): 6-8.

[4]. Ravi, K. Srinivasa, et al, RFID based security system, International Journal of Innovative Technology and Exploring Engineering 2.5 (2013): 132-134.

[5]. Nafi, Kawser Wazed, Tonny Shekha Kar, and Sayed Anisul Hoque, An advanced door lock security system using palmtop recognition system, International Journal of Computer Applications 56.17 (2012).

[6]. Ramesh, S., Soundarya Hariharan, and Shruti Arora, Monitoring and Controlling of Bank Security System, International Journal of Advanced Research in Computer Science and Software Engineering 2.10 (2012): 401-405.

[7]. Yugashini, I., S. Vidhyasri, and K. Gayathri Devi, Design and implementation of automated door accessing system with face recognition, International Journal of Science and Modern Engineering (IJISME) 1.12 (2013).

[8]. Khan, Sadeque Reza, et al., Design and implementation of low-cost home security system using GSM network, International Journal of Scientific & Engineering Research 3.3 (2012): 1.

[9]. Ogri, Ushie James, Donatus Enang Bassey Okwong, and Akaiso Etim, Design and construction of door locking security system using GSM, International Journal of Engineering and Computer Science 2.7 (2013): 2235-2257.

[10]. Bangali, Jayashri, and Arvind Shaligram, Design and Implementation of Security Systems for Smart Home based on GSM technology, International Journal of Smart Home 7.6 (2013): 201-208.

[11]. Khalid, Marwa, and Sadia Majeed, A Smart Visitors' Notification System with Automatic Secure Door Lock using Mobile Communication Technology, IJCSNS 16.4 (2016): 97.

[12]. Kamelia, Lia, et al., Door-automation system using Bluetooth-based android for mobile phone, ARPN Journal of Engineering and Applied Sciences 9.10 (2014): 1759-1762.

[13]. Ha, Ilkyu, Security and usability improvement on a digital door lock system based on internet of things, International journal of security and its applications 9.8 (2015): 45-54.

[14]. Basha, S. Nazeem, S. A. K. Jilani, and Mr S. Arun, An intelligent door system using Raspberry Pi and Amazon web services IOT, International Journal of Engineering Trends and Technology (IJETT) 33.2 (2016): 84-89.

[15]. Mohammed, Salma, and Abdul Hakim Alkeelani, Locker Security System Using Keypad and RFID, 2019 International Conference of Computer Science and Renewable Energies (ICCSRE). IEEE, 2019.

[16]. Komol, Md Mostafizur Rahman, et al., RFID and Finger Print Based Dual Security System: A robust secured control to access through door lock operation, American Journal of Embedded Systems and Applications 6.1 (2018): 15-22.

[17]. Murthy, B. Rama, et al., Development of GSM Based Advanced Alert Home Locker Safety Security System Using Arduino UNO, International Journal of Scientific Research in Science and Technology (IJSRST) 4.2 (2018): 1154-1160.

[18].Badamasi, Yusuf Abdullahi, The working principle of an Arduino, 2014 11th international conference on electronics, computer and computation (ICECCO). IEEE, 2014.

[19]. Severance, Charles, Massimo banzi: Building Arduino, Computer 47.1 (2014): 11-12.

[20]. Louis, Leo, Working principle of Arduino and using it, International Journal of Control, Automation, Communication and Systems (IJCACS) 1.2 (2016): 21-29.

[21]. Adriansyah, Andi, and Akhmad Wahyu Dani, Design of small smart home system based on Arduino, 2014 Electrical Power, Electronics, Communicatons, Control and Informatics Seminar (EECCIS). IEEE, 2014.

[22]. Kusriyanto, Medilla, and Bambang Dwi Putra, Smart home using local area network (LAN) based arduino mega 2560, 2016 2nd International Conference on Wireless and Telematics (ICWT). IEEE, 2016.

[23]. Finkenzeller, Klaus, RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. John wiley & sons, 2010.

[24]. Blumberg Jr, David, RFID system, U.S. Patent No. 8,610,577. 17 Dec. 2013.

[25]. Maltoni, Davide, et al., Handbook of fingerprint recognition, Springer Science & Business Media, 2009.

[26]. Ratha, Nalini, and Ruud Bolle, eds., Automatic fingerprint recognition systems, Springer Science & Business Media, 2003.

[27]. Bjorn, Vance C., and Serge J. Belongie, Fingerprint recognition system, U.S. Patent No. 6,741,729. 25 May 2004.

[28]. Shepherd, Robert, Bluetooth wireless technology in the home, Electronics & Communication Engineering Journal 13.5 (2001): 195-203.

[29]. Singh, Pratibha, Dipesh Sharma, and Sonu Agrawal, A modern study of bluetooth wireless technology, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT) 1.3 (2011).

[30]. Asadullah, Muhammad, and Khalil Ullah, Smart home automation system using Bluetooth technology, 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT). IEEE, 2017.

[31]. Juned, Mohammed, and Srija Unnikrishnan, Bluetooth Based Remote Monitoring & Control System, Journal of Basic and Applied Engineering Research 1.8 (2014): 108-111.

[32]. Engineers, Last Minute, Send Receive SMS & Call with SIM800L GSM Module & Arduino, (2018).

[33]. Iyer, Saikumar, et al., IoT based Intruder Detection System Using GSM, Available at SSRN 3572326 (2020).