ELKHA : Jurnal Teknik Elektro, Vol. 14, No.2, October 2022, pp. 125 - 131
ISSN: 1858-1463 (print), 2580-6807 (online)

Multi-Security System Based on RFID Fingerprint and Keypad to Access the Door

Ramses Wanto Tambunan [1)], Abdul Aziz Ar-Rafif [2)], and Mia Galina [3*)]

[1,2,3)] Department of Electrical Engineering, President University, Indonesia
Corresponding Email: [*)] miagalina@president.ac.id

***Abstract* – It is necessary to prepare for the increasing crime rate of household theft with a modern home security system that allows customers to monitor home security remotely. This can be accomplished by replacing the standard lock with a solenoid door lock, which is more difficult to duplicate and reduces the likelihood of theft when the house is unoccupied. Researchers developed a three-tiered home security system prototype that includes fingerprint, RFID, and keypad biometric sensors. The device's finished prototype was tested ten times after it was designed. The Arduino Uno microcontroller, which also serves as the door-locking mechanism, turns on the door-lock solenoid. When authentication is successful, someone will be granted access to the door. The results show that, first, the fingerprint sensors' usefulness is demonstrated by their capacity to read fingerprints in an average of 3.7 seconds. Second, the RFID sensor detects the E-KTP, and the RFID scans the card in an average of 2.4 seconds. Lastly, the password needed to unlock the door is stored in the keypad. After ten repetitions, the experiment input yields an average time of 3.66 seconds. Opening a door with a 3-level multi-sensor typically takes 9.8 seconds. In this study, the installation of each sensor is notified via a GSM SIM800L module, allowing customers to monitor security remotely.**

Keywords: Arduino, Fingerprint, Home security, Keypad, RFID

I. INTRODUCTION

A smart home is a convenient home setting in which appliances and devices can be controlled remotely using a mobile device or another network device from anywhere with an internet connection. The temperature, lighting, home theater, door locks, televisions, thermostats, home monitors, cameras, lights, and even appliances like a refrigerator can all be controlled by a single home automation system. The desire for security has become one of the primary motivations for individuals to build their homes. Every house has at least one main hallway [1] . Users can remotely manage home security access thanks to the internet-connected devices in smart homes [2]. In terms of home security, it is possible to construct a security system by designing various door locks, such as mechanical or electric ones. The main entry is a crucial security focus in terms of system security. It has been demonstrated that the best safety and well-being come from having safety measures to control entry into homes.

Every house has a doorway, and every door has a lock [3]. Various mechanical and electrical doorway lock types have been employed to ensure security. Even after employing such a lock, deception persists due to its limitations. On a case-by-case basis, some keys can be disabled, and others can be reinstated. As a result, it is essential to keep an eye out for different lock types that cannot be quickly destroyed because even if they can be broken into, it will not be as easy as doing so with other sorts of locks. This research initially just utilized the RFID card that snaps onto the RFID reader before attempting to employ a Fingerprint sensor to scan a finger.

Numerous professionals have employed RFID technology to discuss access control systems for door security. In the research [4], the Authors utilized just one form of protection—an RFID sensor. The security system with one keypad sensor serving protection is described in the paper [5]. While the security system in [6] uses only Bluetooth, reference [7] describes the security with two sensors utilizing RFID and fingerprint. The smart door lock security system with RFID and Keypad is described in research [8]. Because the security system feels less secure when no password is entered, the writers propose a security system with a password. Furthermore, the owner only knows the password for the automatic door.

This paper aims to introduce a protected smart entryway lock that is intended to offer high security, simple access, and control. The authors' proposed security system includes three levels of sensors: fingerprint, RFID, and keypad. RFID labels and Global System for Mobile (GSM) modules are used in the proposed framework to create a secure yet simple framework. It will most likely replace the current door lock system. The GSM SIM800L module will notify the user's cellphone number of a mismatch or violation [9].

II. METHODOLOGY

A. System Design

In addition to a power source and two inputs, the device has three outputs: an LCD screen, a solenoid door, and a buzzer (an RFID tag and fingers). The RFID module, a fingerprint sensor, and a keypad module are the three important sensors. With a power supply in the middle, the Arduino Uno processes all of the sensors. There is also an output solenoid door, a 16x2 LCD screen for display, and a buzzer for notification. The buzzer will sound If the RFID is identified as unregistered there. If the RFID is correct, it will pass through to the Keypad module, and if the password entered is correct, the Relay will turn on, and the solenoid will open the door, as shown in Figure 1.

Manuscript received 2022-09-02; revised 2022-10-11; accepted 2022-10-12

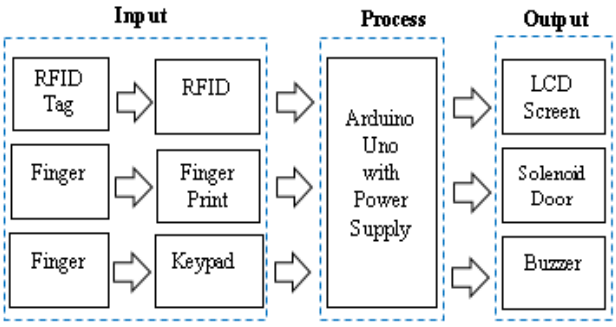

Figure 1. Block diagram of device prototype

Figure 2 shows a schematic representation of our completed device prototype. The key components are a fingerprint sensor, an RFID chip, and a keypad (polyphonic tone) for entering the password to unlock the door. The RFID module and fingerprint sensor have a 3.33 V primary voltage. In contrast, the keypad module, LCD 16X2, I2C, Buzzer, input 5V, and Relay all require 5 V. While the solenoid door lock requires input voltages of 12 V and 9V, all device prototypes must use the MB102 power supply to keep the voltage constant and stable.

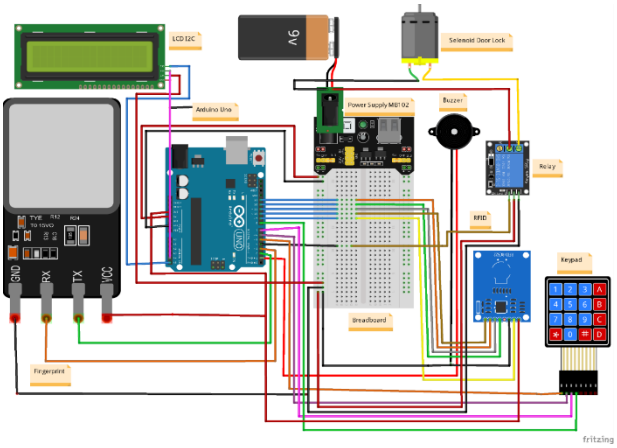

Figure 2. Schematic diagram of prototype

This study employs keypads, RFID cards, and fingerprint sensors to obtain precise and acceptable results. The data obtained by observing and analyzing will be visible through the prototype developed in this study if this experiment is effective and produces correct results if it follows the initial design. Data from experiments will be collected and analyzed in order to determine the average lifespan of each sensor installed in the smart door lock.

Figure 3 shows the work's flowchart. In the first step, Arduino uses the power supply as an input. The user will initially add the database for the fingerprint, e-KTP data, and keypad password. When users access the door, this database will be used as part of the authentication process. The user inserted his or her finger into a biometric fingerprint scanner.

The fingerprint sensor provides the initial identification. The fingerprint is then given an output voltage by Arduino, which determines whether the fingerprint is accurate. If it is correct, it will proceed to the RFID reader. The RFID reader module will scan an e-KTP with a chip inside by moving the e-KTP closer to the RFID for reading. If the data is correct, it will proceed to keypad input. A keypad sensor enables the authors to create a password using the letters ABCD and the numerals 1 through 9 and then use it to maximize the security system. A relay functions as a digital switch. If the three primary sensors' results are successful and correct, the Relay will send a voltage to the Solenoid, which will open the door.

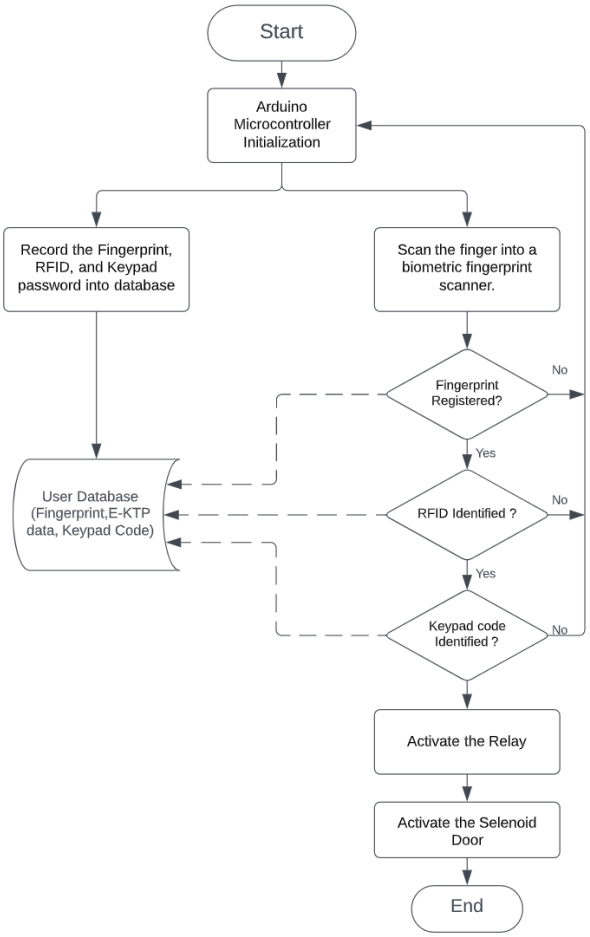

Figure 3. Flowchart of the prototype

B. Radio Frequency Identification (RFID)

As shown in Figure 4, the RC522 RFID Reader Module generates a 13.56 MHz electromagnetic field that is used to communicate with the RFID tag. RFID technology uses radio waves to identify an object. The Arduino Uno-controlled RFID RC-522 system [10] can identify user ID data. The reader is linked to the microcontroller via a 4 pin Serial Peripheral Interface (SPI) with a data rate of up to 10 Mbps. The module's operational voltage range is 2.5 V to 3.3 V. Passive RFID tags do not have a power source. They collect energy to power the chip in the tag and use inductive coupling (LF & HF tags) or propagation coupling (UHF tags) with the reader antenna to reflect the signal to the reader. The RFID sensor network inherits several traits.

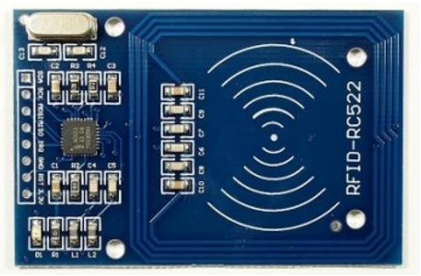

Figure 4. RFID RC522 [4]

C. *Keypad*

As shown in Figure 5, the keypad module requires an input password to access the solenoid door lock. The Arduino Uno microcontroller supplies a voltage of 3.33 volts to this component. The project receives input data from the 4x4 matrix of this component. The 16 buttons on the module control the component's eight terminals [5].

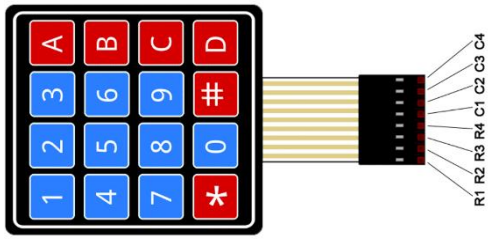

Figure 5. Keypad Module [11]

D. *Arduino Uno*

Figure 6 shows an Arduino Uno microcontroller board module with special details used in this prototype. The ATmega328P serves as its foundation. The Arduino ATmega328P features a 16 MHz ceramic resonator (CSTCE16M0V53-R0), six analog inputs, 14 digital I/O pins, six of which can be used as PWM outputs, a USB connection, a power jack, an ICSP header, and a reset button. To begin using this microcontroller, simply connect it to a computer via a USB cable or power it with an AC-to-DC adapter or battery [12].

Figure 6. Arduino Uno Module [12]

E. *Fingerprint AS608*

A biometric fingerprint is shown in Figure 7. Every human fingerprint produced by the fingerprint scanner will have ridges and troughs. This allows the sensor to be large and to be produced on a wide scale. It operates at 3.3 volts and based on the specification, it can store fingerprints with a maximum of 127 distinct values as stated in the work [7]. In this study, we used three sensors to add more innovation to previous research and make it more secure. In the future, it may be possible to use more fingerprints if the user requires more than one fingerprint to open the door.

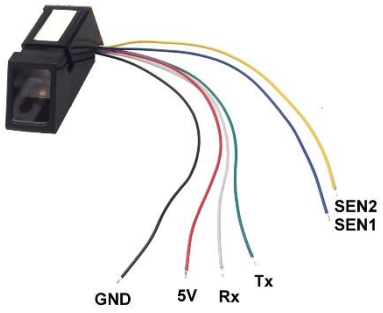

Figure 7. Fingerprint Sensor [13]

F. *Relay*

A relay is a mechanical switch that uses electricity. It is made up of two primary components: an electromagnet (coil) and a mechanical switch, as described in Fig. 8. Relay conducts high voltage electricity using the electromagnetic principle to switch at low power voltage [14].

Figure 8. Relay [5]

G. *GSM SIM 800L*

GSM stands for Global System for Mobile Wireless Communication. Users can make and receive calls, send and receive SMS, and make and receive SMS via a GSM connection. In this work, the author uses the SIM800L micro or small dial mobile module [15]. The GSM Sim800L's key selling point is its affordable, tiny footprint and sleek design, as described in Figure 9.

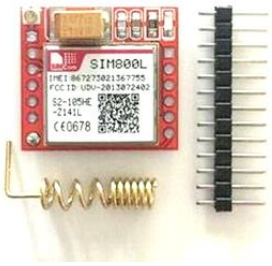

Figure 9. GSM SIM 800L

This component has connectivity class 1 (1W) on DCS 1800 and PCS 1900GPRS, while in class 4 (2W) on GSM 850 and EGSM 900. It also has a quad-band network of 850/900/1800/1900 MHz, GPRS Class 12, Data Rate 85.6 Kbps, Serial Interface, and Voltage 3.4 - 4.3V.

H. LCD 16X2

A Character LCD is an ideal LCD for showing text or characters, as shown in Figure 10. The LED-backlit display shows 32 ASCII characters in two lines, each with 16 characters, as described in Fig.10.

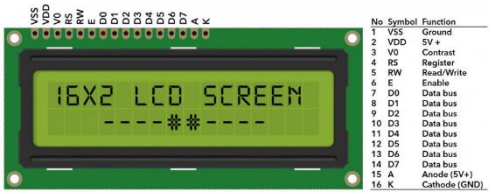

Figure 10. LCD screen with 16X2 [16]

I. Buzzer

Buzzers are a type of audio signalling device that can be electromechanical, piezoelectric, mechanical, or appear as buzzers with physical appearances similar to those shown in Figure 11. The transformation of audio impulses into sound is its main purpose [13]. It is often powered by DC voltage and utilized in timers, alarm clocks, printers, computers, and other electronic devices.

Figure 11. Buzzer [17]

J. e-KTP

The only form of identification for each resident is their National Identity Number embedded in an e-KTP card, as shown in Figure 12. The electronic KTP is a nation's original population document, which includes an RFID chip that allows it to function as one of the sensors as a security or control system based on the national population database which is valid for their entire life.

Figure 12. e-KTP identity card

III. RESULTS AND DISCUSSION

Figure 13 represents the completed device prototype. The success of this project's outcomes will be determined by three primary sensors: fingerprint, RFID, and keypad. The testing will be divided into three parts to make them accessible for readers to understand.

Figure 13. Complete device prototype of 3-level security system (front-view)

The first test is taken from the fingerprint sensor, as shown in Figure 14. The authors used a finger as input for the biometric fingerprint sensor.

Figure 14. Point of view scan the fingerprint sensor

In this test, the authors put a finger into a biometric fingerprint scanner. Table 2 shows the results of the fingerprint sensor, which is the output of ten successful fingerprint testing with the average time for door access being 3.7 seconds.

Table 2. The Average time results in scanning finger

Experiment	Time (s)
1	3.6
2	3.8
3	3.5
4	3.7
5	3.9
6	3.8
7	3.7
8	3.6
9	3.9
10	3.5
Average	3.7

The second test is the RFID function reader. An RFID (Radio Frequency Identification) sensor doubles as a card reader and a chip transmitter. In this work, the Author uses an e-KTP with a chip inside. This allows the e-KTP to be scanned by the RFID reader module by moving the e-KTP closer to the RFID for reading, as shown in Figure 15. The RFID reader module scans the second results using e-KTP. For reading, the e-KTP is brought close to the RFID.

Figure 15. Point of view scan the RFID card with e-KTP

The findings from the RFID scanner are shown in Table 3, and it takes an average of roughly 2.4 seconds to process one e-KTP reading.

Table 3. The average time results to scan e-KTP

Experiment	ID Card	Time (s)
1	04 7B 12 6A 43 5A 80	2.0
2	02 AC 95 11 40 4D F0	2.2
3	04 25 FA C8 78	2.5
4	B0 03 DE ED 28	2.1
5	02 C4 B9 D0 22	2.2
6	D9 24 22 F1	2.6
7	04 25 5CFA 81 5B	2.4
8	02 AC9511 40 4D F0	2.9
9	02 B6 DC 11 10 D0	2.4
10	CF B7 F5 DC	2.7
Average		**2.4**

Lastly, the third test is a keypad function test. A keypad sensor helps the authors to utilize the letters ABCD and the numerals 1 through 9 to create a password and use it to maximize the security system. Moreover, there are extra parts, such as a buzzer and relay. Relay performs the role of a digital switch. If the results of the three primary sensors are successful and correct, the relay will trigger the voltage to the Solenoid, which functions to open the door. By processing the entered password, the Keypad sensor provides the third result, as shown in Figure 16.

Figure 16. Point of view input password to keypad sensor

The Arduino will activate and supply electricity to the buzzer as a signal that someone is attempting to unlock the door but is unsuccessful if they try the three primary components, starting with the first, which is the fingerprint. This prototype consists of three primary sensors: the keypad, RFID, and fingerprint. Others function as auxiliary elements. To make the results easy to grasp for readers, they will be split into three sections. The first testing comes from research using fingerprint sensors.

Table 4. The average time results in scanning passwords

Experiment	Time (s)
1	3.6
2	3.8
3	3.5
4	3.7
5	3.9
6	3.5
7	3.7
8	3.8
9	3.5
10	3.6
Average	**3.66**

As shown in Table 4, the data indicate that the correct password was entered ten times and that it took an average of 3.7 seconds to scan the password. In this test, the authors enter the password; if it is accurate, the Relay is activated. After that, the relay sends a 12V to the solenoid, and the door automatically opens. The door may open and operate for three seconds before closing immediately. The finger can then be scanned using the fingerprint sensor to start the overall experiment.

Furthermore, if the fingerprint sensor data entered differs from the data that has been registered, a notification with the message "Not valid fingerprint" will appear on the LCD display as shown in Figure 17.

Figure 17. Notification on the LCD for the invalid data

IV. CONCLUSION

A 3-level security door lock system with a fingerprint sensor, RFID module, and keypad sensor has been successfully designed, implemented, and tested. This fingerprint sensor can read fingerprints with, on average, 3.7 seconds to complete a fingerprint scan task and protect against fingerprint similarities. When the ID card with the RFID chip approaches the RFID reader, the door will open if the ID card has been entered into the Arduino code. Furthermore, if the ID card is not inserted, the door remains locked, entry is prohibited, and a buzzer sound is generated. The average time for RFID to read an RFID card with ten trials is 2.4 seconds. Furthermore, the keypad sensor works correctly after ten trials of entering a password with an average time of 3.66 seconds. Overall this 3-level multi-sensor prototype is able to open the doors in 9.78 seconds on average. After completing all the procedures, a notification will be sent to the mobile phone user via the GSM SIM800L module. A notification will flash on the LCD display if the fingerprint sensor data entered differs from the data that has been recorded.

REFERENCES

[1] A.T.Mahesa, H.Rahmawan, A. Rinharsah and S.Ariffin, "Sistem Keamanan Brankas Berbasis Kartu e-KTP," *Jurnal Teknologi & Manajemen Informatika*, vol. 5, no. 1, p. 4, 2019.

[2] K.Mahardi, J.W.Simatupang and E.Rismauli, "Security Home Door Automation Using Multi Sensors," *Journal of Electrical and Electronics Engineering*, vol. 3, no. 1, p. 88, 2019.

[3] E.D.Widianto, A.Masruhan and A.B.Prasetijo, "College Room Door Control using RFID and Arduino Integrated with Presence Web Application," *Jurnal Telekomunikasi, Elektronika, Komputasi, dan Kontrol (TELKA)*, vol. 7, no. 2, p. 79, 2021.

[4] M.Andriansyah, M.Subali, I.Purwanto and A.Irianto, "e-KTP as the Basis of Home Security System using arduino UNO," in *4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, 2017.

[5] A.Vadakkan, A.Babu.V.K and C.Pappachan, "DOOR LOCKING USING KEYPAD AND ARDUINO," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 3, no. 11, p. 783, 2021.

[6] H.Amiliansyah, M.Galina and J.W.Simatupang, "ACCESS CONTROL AND SECURITY SYSTEM VIA BLUETOOTH APPLICATION ON ANDROID SMARTPHONE," *Jurnal Teknik Elektro, Teknologi Informasi dan Komputer (ELTIKOM)*, vol. 6, no. 1, p. 101, 2022.

[7] M. M. R. Komol, A. K. Podder, M. N. Ali and S. Ansary, "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*, vol. 6, no. 1, p. 16, 2018.

[8] S.A.Prity, J.Afrose and Md.M.Hasan, "RFID Based Smart Door Lock Security System," *American Journal of Sciences and Engineering Research*, vol. 4, no. 3, p. 163, 2021.

[9] M.I.Saputra, S.R.Sulistyanti, S.Purwiyanti and U.Mardika, "Design of Prototype Measuring Motor Vehicles Velocity Using Hall Effect Sensor Series A-1302 based On Arduino Mega2560," in *2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE)*, Lombok, Indonesia, 2020.

[10] R.Rizaluddin, R.Yuliani and E.A.Nugroho, "Identifikasi Alat-alat kerja Berbasis Pasif RFID RC-522," *Jurnal Elektra*, vol. 3, no. 2, p. 1, 2018.

[11] K.Pattabiraman, "Circuit Basics," 2018. [Online]. Available: https://www.circuitbasics.com/how-to-set-up-a-keypad-on-an-arduino/. [Accessed Mei 2022].

[12] V.Chikhale, R.Gharat, S.Gogate and R.Amireddy, "Voice Controlled Robotic System using Arduino Microcontroler," *International Journal of New Technology and Research (IJNTR)*, vol. 3, no. 4, p. 93, 2017.

[13] Y.M.Win, O.Nyein and S.Aung, "Wireless Student Attendance System using Fingerprint Sensor," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 3, no. 4, p. 1665, 2019.

[14] N.Sadikin, M.Sari and B.Sanjaya, "Smarthome Using Android Smartphone, Arduino uno," in *1st International Conference of SNIKOM*, Medan, Indonesia, 2018.

[15] P.Kanani and M.Padole, "Real-time Location Tracker for Critical Health Patient using Arduino, GPS Neo6m and GSM Sim800L in Health Care," in *4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2020.

[16] "hackaday.io," [Online]. Available: https://hackaday.io/project/170249-i2c-lcd16x2-arduino. [Accessed Mei 2022].

[17] M.B.Parsusah, A.Sambas and I.Haerudin, "Design of Arduino-Based Metal Detector Robot," *Solid State Technology*, vol. 63, no. 6, pp. 12401-12411, 2021.