RFID – Enabled Security Access System With Interloper Detection

B.Mahesh[1], Ch.Aryan[2] and D.Pardhasaradhi[3]

[1] Undergraduate Student, Institute of Aeronautical Engineering(Autonomous),JNTUH,

Telangana - 500043

[2] Undergraduate Student, Institute of Aeronautical Engineering(Autonomous),JNTUH,

Telangana - 500043

[3] Undergraduate Student, Institute of Aeronautical Engineering(Autonomous),JNTUH,

Telangana - 500043

Abstract: ***-Investing in a contemporary home security system that enables remote property monitoring is essential to combating the growing rate of domestic theft. A good way to improve security when the house is empty is to swap out standard door locks for solenoid locks, which are more difficult to copy.A three-tiered home security system prototype with fingerprint, RFID, and keypad biometric sensors has been created by researchers. Ten testing sessions were conducted on the prototype to confirm its functioning. Upon successful authentication, a solenoid door lock that is incorporated as part of the locking mechanism is activated by an Arduino Uno microcontroller. The fingerprint sensors proved to be successful in securing access, with an average fingerprint recognition time of 3.7 seconds.***

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

1. INTRODUCTION

For the purpose of limiting unwanted access to digital and physical locations, security solutions are crucial. The most typical security methods include classic door locks and electronic identification systems. Traditional locks are simple devices with a simplistic design that offer fundamental security. Nevertheless, they are susceptible to manipulation, which might enable unauthorized people to get around them and enter restricted regions [1].Users of smart homes can remotely control security features, such as home access, via internet-connected devices . When it comes to house security, systems may be built using various door lock kinds, such mechanical or electronic ones, with the main entry serving as a primary security focal point. The development of IoT technology has increased convenience, but it has also brought about potential security risk.

Every house has an entryway, and locks are usually used to safeguard doors . To increase security, locks that are mechanical or electrical have both been employed. But even with these locks in place, there are still weaknesses that might allow for breaches. To keep control over access, certain keys may need to be deactivated and others may need to be reactivated, depending on the circumstances.

Because of this, it's important to think about other lock types that are more difficult to tamper with, because even if they could be, it would be much harder than with traditional locks. Initially, this study simply employed an RFID card that was tapped onto the RFID reader; later, it also included a fingerprint sensor that was used to scan fingerprints.

The application of RFID technology to access control systems for door security has been studied by several specialists. The authors used an RFID sensor as the only security measure in their study. Between the reader and tagged RFID object is not needed an inherent line of sight [2].The technology of RFID uses radio waves to identify an animate or an inanimate [3]. Previous studies have also proposed a smart door lock system that combines a keypad with RFID. The authors advise including a password-based system so that only the owner knows the password for the automatic door, as a password-free system may appear less safe.

The purpose of this article is to introduce a safe smart door lock that offers improved security, user control, and ease of access. The three layers of sensors in the authors' suggested security system are fingerprint, RFID, and keypad. In addition, the ESP32 CAM module is set up to send an email to the user in case of a mismatch or security violation.

2. Methodology

2.1 System Design

The device has three outputs: an LCD screen, a solenoid door lock, and a buzzer. It also has two inputs and a power supply. A fingerprint and an RFID tag are the two main inputs. The keypad module, fingerprint sensor, and RFID module are the three primary sensors. All sensor data is processed by the Arduino Uno, which is powered by the central power source. The 16x2 LCD information panel, the buzzer for notifications, and the solenoid door lock are among the outputs. The buzzer will sound if it detects an unregistered RFID tag. As shown in Figure 1, the system proceeds to the keypad upon scanning a valid RFID. If the right password is input, the relay is actuated, which opens the solenoid door lock.

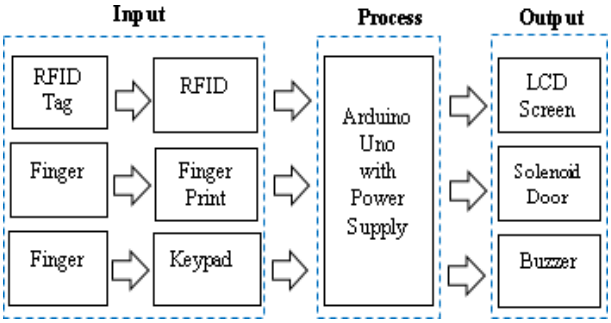


Figure 1. Block diagram of device prototype

Here in this figure, we present the schematic of our device prototype after completion. The three main components include: the RFID chip, a fingerprint scanner, and a podium key that acts as a password gate for the door. The voltage of the fingerprint sensor and RFID module predominately operates at 3.33V. Other equipment such as the keypad module, including the LCD 16X2, I2C, buzzer, input 5V and relay require 5V. The MB102 power supply for all the device prototypes was required in order to keep the device operating under the requisite power levels, even when the output solenoid door lock YaM706-12 supplies 12V and 9V outputs.

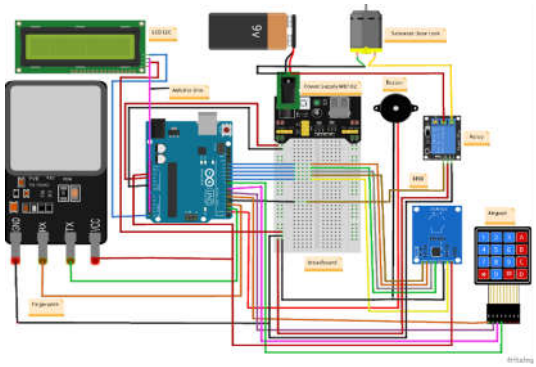


Figure 2. Schematic diagram of prototype

To obtain precise and trustworthy findings, this study makes use of fingerprint sensors, RFID cards, and keypads. If the experiment's results match the original design expectations, the prototype will demonstrate the experiment's efficacy. The performance of each sensor will be evaluated using the data collected from these studies, with an emphasis on figuring out how long the sensors that are integrated into the smart door lock system would typically last for operation.

The flowchart that shows how the system operates is shown in Figure 3. The power supply is used to power the Arduino in the first phase. The user starts by entering passwords from keypads and fingerprint data into the database. When users try to access the door, this saved information will be utilised to authenticate them.

The fingerprint sensor provides the initial identification. The fingerprint is then given an output If it is correct, it will proceed to the RFID reader. The system will go on to keypad input if the fingerprint data is valid. To strengthen the security mechanism, users can use the keypad to generate a password that consists of the letters ABCD and the numerals 1 through 9. The relay functions as a digital switch, and it will activate to deliver electricity to the solenoid to unlock the door if the three sensors yield correct data.

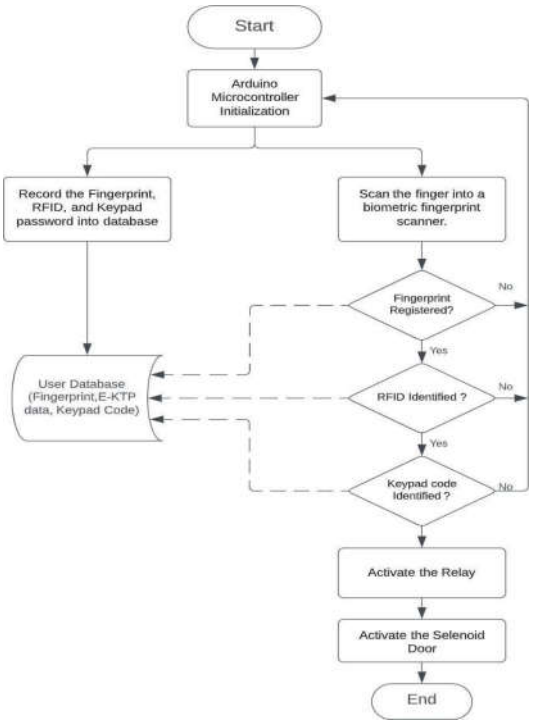


Figure 3. Flowchart Of The Prototype

2.2 ARDUINO MEGA 2560

The Figure 4 shows Arduino Mega 2560 is a microcontroller board based on the ATmega2560 microcontroller. The Mega 2560 is specifically designed for more complex and demanding projects, offering a substantial increase in both memory and input/output capabilities compared to other Arduino boards, such as the Arduino Uno. It features a robust and user-friendly platform for creating interactive objects or environments. The open-source nature of the Arduino platform encourages community collaboration, providing a vast library of code examples, tutorials, and forums for troubleshooting and project inspiration. This combination of versatility, ease of use, and community support makes the Arduino Mega 2560 a powerful tool for prototyping and implementing sophisticated electronic projects. The microcontroller may be powered by a battery or an AC-to-DC adapter, or it can be connected to a computer via a USB connection to begin operation [4].

Figure 4. Arduino Mega 2560

2.3. Fingerprint Sensor

A biometric fingerprint is shown in Figure 5. The information from the fingerprint is used as the benchmark of Identification. Fingerprint processing has two steps: enrollment of fingerprint and matching of the fingerprint (the matching of fingerprints can be either 1:1 or 1: N). In 1:1, compare the fingerprint with particular template assigned in the fingerprint module memory and in 1: N, look through the entire fingerprint module library for the matching finger [5].

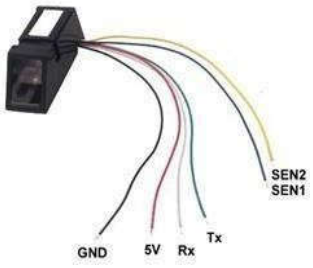
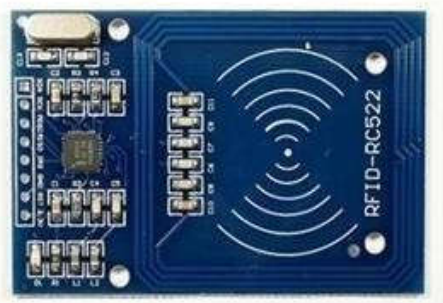


Figure 5. Fingerprint Sensor

2.4. RFID(Radio Frequency Identification)

The 13.56 MHz electromagnetic field produced by the RC522 RFID Reader Module is used to communicate with RFID tags, as seen in Figure 3.6. Radio waves are used by RFID technology to identify items. User ID data may be identified via the RFID RC-522

system, which is based on an Arduino Uno [6].The basic components of an RFID system include RFID tags, RFID readers, and a backend database or system for processing and



storing information.

Figure 6 .RFID RC522

2.5. LCD 16X2

As Shown in Figure 3.7 16x2 LCD display is an alphanumeric display module that features two rows of 16 characters each .The compact size and readability make them ideal for projects that require a simple, yet effective method for displaying data, instructions, or status updates to the user.

Figure 7. LCD16x2

2.6. Keypad

A keypad is an input device that consists of a set of buttons or keys, typically arranged in a grid format. These keys can be used to input numbers, letters, or other symbols into an electronic device, such as a computer, telephone, or security system . To unlock the solenoid door lock, as shown in Figure 8, a password must be entered into the keypad module. The 4x4 keypad matrix is used in this project to collect input data. The eight terminals on the module are used to connect and control its sixteen buttons [7].

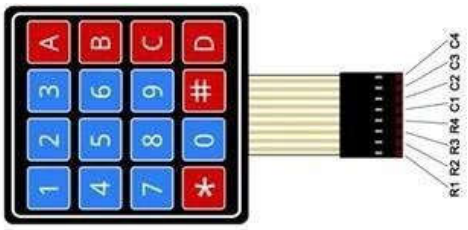


Figure 8. Keypad

2.7. Electromagnetic Door Lock

As shown in Figure 9 electromagnetic door lock, commonly referred to as a maglock, is a locking mechanism that uses an electromagnet to secure a door. When the electromagnet is powered, it creates a magnetic field that strongly attracts and holds the metal plate, effectively locking the door. This system is often used in commercial and high-security applications due to its reliability and strength.

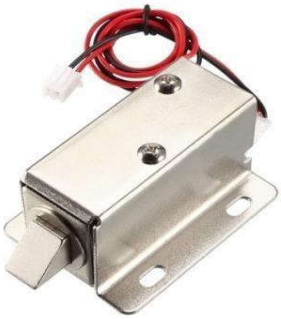


Figure 9 . Electromagnetic Door Lock

2.8. ESP32 CAM

As shown in Figure 10 the ESP32-CAM is a compact development board that integrates the ESP32-S chip with a camera module, making it a powerful tool for IoT (Internet of Things) applications involving image capture and processing. It features a 2MP OV2640 camera, which provides a balance between image quality and performance.

Figure 10. ESP32 CAM

2.9 Buzzer

Buzzers are used for auditory signalling; they can be mechanical, piezoelectric, or electromechanical devices. A lot of designs are similar to the ones in Figure 11. Sound conversion from audio signals is their main job [8]. It is frequently used in timers, alarm clocks, printers, computers, and other electronic equipment that are powered by DC voltage.

Figure 11. Buzzer

2.10. Relay

As shown in Figure 12, a relay is a mechanical switch that is electrically driven. It is composed of two primary components: a mechanical switch and an electromagnet (coil). By switching at low power voltage, it uses electromagnetic principles to regulate high voltage electricity [9].This mechanism allows a small electrical signal to control a much larger load, providing isolation between the control circuit and the load circuit. Relays are essential in various applications, including industrial automation, telecommunications, and automotive systems.

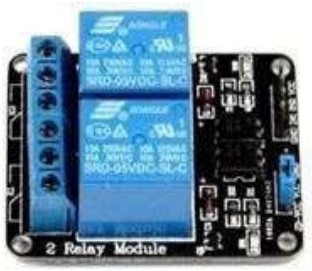


Figure 12. Relay

3. RESULTS AND DISCUSSIONS

With the gadget prototype constructed, Figure 13. The fingerprint sensor, RFID module, and keypad performance are the three main sensors that are used to determine the project's success. The testing procedure is broken down into three phases, each of which corresponds to a major sensor, for the purpose of clarity and easy of comprehension.

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

The fingerprint sensor is the main focus of the first test, as seen in Figure 14. The biometric sensor in this test was configured by the authors using a fingerprint as the input.

Figure 14. A finger was put on a biometric fingerprint scanner for this experiment.

Table1 shows the average access time after 10 successful fingerprint tests. The authors placed one of their fingers into a biometric fingerprint scanner used in the testing. Table 1. The result of the fingerprint sensor, this is output after ten time successful testing with the average time for door access is equal to 3.7 seconds.

Table 1. The Average time results in scanning finger

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

As presented in Table 2, the data show that the correct password was entered ten times, with an average processing time of 3.7 seconds per entry. In this test, the authors entered the password, and upon validation, the relay was triggered. The relay then delivered 12V to the solenoid, automatically opening the door. The door stays open for three seconds before closing again. Afterward, the fingerprint sensor can be used to scan a fingerprint, initiating the entire experiment sequence.

Figure 15. Point of view input password to keypad sensor

As an indication that an effort to unlock the door has been attempted but been failed, the Arduino will turn on the buzzer and provide power to it. If all three main parts are attempted, starting with the fingerprint sensor, this happens. The keypad, RFID module, and fingerprint sensor are the three primary sensors in the prototype; other parts function as supporting components. The primary goal of the initial testingphase is to conduct research with the fingerprint sensor.

Table 2. The Average time results in scanning passwords

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

The statistics, as displayed in Table 2, demonstrate that the right password was input 10 times, with an average processing time of 3.7 seconds for each password entry. The writers input the password during this test, and the relay was turned on if it was accurate. The door then opened automatically as a result of the relay feeding the solenoid with 12V. The door opens and stays open for three seconds before shutting on its own. The entire experiment may then be started by scanning the finger using the fingerprint sensor.

The system sounds a warning when the fingerprint sensor finds a discrepancy between the fingerprint being scanned and the registered fingerprint data. In this instance, the user is informed of the unsuccessful authentication attempt via an LCD display notification that reads, "Not valid fingerprint".

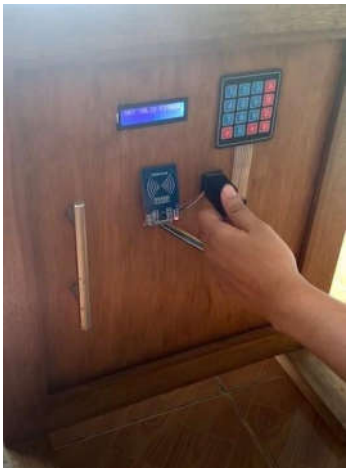


Figure 16. Notification on the LCD for the invalid data

Additionally, the system immediately takes a picture of the unauthorized user as an extra security measure. This feature ensures accountability and improves general security by facilitating identification or additional inquiry in the future. In the event of repeated illegal efforts, the recorded data can be strengthened by storage or usage as a point of reference.

Figure 17. Image captured with camera module

4. Conclusion

We have designed, implemented and successfully tested a three-level security door lock system using RFID module keypad sensor as well as fingerprint detection sensor. As for the fingerprint sensor concerned, it is relatively free from fingerprints when compared and takes about 3.7 seconds to complete a scan. For instance, if the ID card has been registered in the Arduino code, then as soon as it touches against RFID reader door will be unlocked. Door remains locked, No pass keys but buzzer warns when an unregistered card tries to access.

RFID scanned RFID cards in 2.4 seconds on average over 10 trials. Additionally, the keypad sensor meaningfully recognizes password submissions in 3.66 seconds on average

over ten trials (Fig. On average, the 3- level multi sensor prototype can open doors in 9·76 seconds. Finally when all the operations are done, a image will be sent to the user's mobile using ESP32-CAM Module. And also an alert will appear on the LCD screen in case the fingerprint scanner recognizes data which differs from the recorded one.

REFERENCES

[1] *P.Adole1, J.M.Môm, and G. Igwue, "RFID Based Security Access Control System with GSM Technology". American Journal of Engineering Research (AJER). Vol.5, pp-236-242, 2016.Q. Song and M.J. Shepperd, "Missing Data Imputation Techniques," Int. J. Bus. Intell. Data Min., vol. 2, no. 3,* ***(2007)*** *October, pp. 261-291.*

[2] *Y.Huang, "Secure Access Control Scheme of RFID System Application" Fifth International Conference on Information Assurance and Security ,Vol.1,pp- 525-528,2009.A. A. Ahmad and H. Polat, "Prediction of Heart Disease Based on Machine Learning Using Jellyfish Optimization Algorithm," Diagnostics (Basel), vol. 13, no. 14,* ***(2023)*** *July, pp. 2392.*

[3] *A.Ashraf, D.Rasaily , A.Dahal, "Password Protected Lock System Designed using Microcontroller",International Journal of Engineering Trends and Technology (IJETT),Vol 32,no.4,pp-180- 183,February, 2016.*

[4] *M. Lastra J. M. Benítez, P. D. Gutiérrez, and F. Herrera, "A High Performance Fingerprint Matching System for Large Databases Based on GPU," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 62- 71, Jan. 2014.*

[5] *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..Trends and Technology (IJETT),Vol 32,no.4,pp-180- 183,February, 2016.T. Muntinova, "Data Analysis of Heart Attack Risk Factors: Insights from Machine Learning," presented at the VI International Scientific Conference, Toronto, Canada,* ***(2024)*** *February.*

[6] *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..*

[7] *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.*

[8] *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.*

[9] *N.Sadikin, M.Sari and B.Sanjaya, "Smarthome Using Android Smartphone, Arduino uno," in 1st International Conference of SNIKOM, Medan, Indonesia, 2018. International Research Journal of Modernization in Engineering Technology and Science, vol. 3, no. 11, p. 783, 2021.*