



Design and Construction of Secure Gate Access Control and Monitoring System Using RFID and Fingerprint Technologies

¹Ajayi, O., ²Yahaya, S. M., ¹Abubakar, U.
Department of Computer Engineering,
Ahmadu Bello University, Kaduna.
Department of Electrical and Electronics Engineering
Federal Polytechnic Bida, Niger.

ABSTRACT

The demand for security systems has greatly increased in recent years due to improved technology and the sophistication of criminally minded people. Security systems used for granting access have also evolved through the years in terms of technology and complexity. Biometric technology has been used to authenticate and grant access to people just like the case when using wireless technology like Radio Frequency Identification (RFID) technology. This project work was able to combine both RFID and fingerprint scanning to authenticate users and grant access to them through the gates. The system has a pedestrian gate and a vehicular entrance/exit gate. A known pedestrian activates the system via a button and then scans his/her finger. The system will check for a match and if found, the system allows the user to select the gate that will automatically open and close once the pedestrian enters. For vehicles, the RFID tags were installed in the vehicles. Once a tag is within range, the system checks the ID of the tag and if a match is found, the main gate will open to allow access else access will not be granted. Finally, any unknown user will activate the system but someone in the building will be able to see the unknown user via the video feed which allows the capture of images in VGA format (640x480) and after which he/she will press an appropriate button to open either gate if need be. The system uses cheap but reliable modules and components to ensure quality at a low cost and minimize production time.

ARTICLE INFO

Article History

Received: January, 2022

Received in revised form: January, 2022

Accepted: March, 2022

Published online: June, 2022

KEYWORDS

Biometric, fingerprint scanner, Arduino software, Radio Frequency Identification

INTRODUCTION

Security may be considered as care that is taken against theft, espionage or a person on a thing that secures on guarantees. Security of lives and properties is a very important issue in a country like Nigeria. The Security of properties and lives of citizens is one of the basic provisions of a nation's constitution which must be well protected at all times (Fagbohun & Fagbohun., 2018). Home security is becoming necessary in recent times as the possibilities of intrusion are increasing day by day, and kidnappings with ransom demands are also waxing stronger. Over the years, attempts were made to provide security for all inhabitants. Up-to-date complete security is not discovered (Khan *et al.*, 2019). Lock and key systems were the first steps toward security. It was a single key for a single lock security protocol (Meissner & Gillert, 2017). At that time,

this system was considered to provide the utmost security. For not too long, this system failed because there are now multiple keys unlocking a single lock. Hence, this system is now obsolete.

There came the electronic lock which works using an electronic currency which is usually connected to an access control system in addition to the pin and tumbler used in standard locks. An electronic lock mechanism uses a card key upon which digital codes are imprinted (Ho *et al.*, 2017). This electronic lock connects the bolt or cylinder to a motor within the door using a part called an actuator. An electromechanical locking system includes one or more moveable locking elements and one or more actuators configured to move each of the one or more moveable locking elements between positions (Fowler., 2019). The keycard lock operates with a flat card of similar



dimensions to a credit card. In other to unlock the gate or door. One needs to successfully match the signature within the keycard. The next level of security uses a password as an authenticating tool. The system stores the password of authenticated users for validation. This system offers considerable security to the users as it acts as a secret for authorized users. However, this system has the disadvantage in that a password can be gotten by an unauthorized user by continuously trying all the possible combinations. This system was also one among the hundreds of attempts made for providing security (Khan *et al.*, 2019).

There came the use of the Radio-frequency identification (RFID) card for authentication. The use of RFID was the next level of technological development for providing security for homes and offices. The system enriched the level of security granting access to only the users whose RFID code matches the authorized code. However, this system has the disadvantage of card replication and anyone who has this card can have access to the door. Authentication by the use of a fingerprint sensor was next as we all know the skin on our palms and soles exhibits the flow pattern of ridges called friction ridges. This pattern of friction ridges on each finger is unique and unchangeable. (Khan *et al.*, 2019). For these reasons, the fingerprint is a unique means of identification for everyone. The fingerprint scanner scans the fingerprints of users for verification with the enrolled fingerprint. The door opens if the prints match. However, there are few cases when the user's fingerprint will not be captured or verified as a result of changes in lifestyle like hard manual labour using the hand.

LITERATURE REVIEW

Shankar *et al.*, (2015) presented a security access unit based on the biometric fingerprint to provide security to establishments, institutions, organizations, etc. The research project employed Embedded Systems and Biometrics techniques. The fingerprint scanner scans the fingers of users and grants access to users if and only if the prints match already-enrolled prints. An AT80C51 microcontroller was used to control system processes. The system provides merits in that it is easy to use and requires no special training, additional software or hardware equipment. Each fingerprint is unique for every person with high

accuracy in terms of security. However, an alarm should be introduced so that unauthorized individuals try gaining entry, and an alarm will be activated, thus allowing administrators to take action to prevent future occurrences. Sughanthy (2016) pointed out that RFID eases the tracking, arrangement and location of books and other materials in libraries, all functions done in perfect real-time thus saving time and energy.

The system eases the efficiency of book distribution and management, automates check-in as well as check-out processes, and substantially reduces tracking of inventory from minutes, if not hours or days to seconds. Simultaneous reading of multiple books having installed tags was made possible no distant period while issuing, receiving, transporting, and sorting of shelved library materials are other processes achieved with little effort. The research also pointed out that RFID makes daily scanning of staff and students' items at the reception very easy and convenient during check in and check out. However, the system has some limitations which include the acquisition of numerous RFID devices (tags) since each library material and user must be uniquely identified. Staff training and retraining are essential and cannot be over-emphasized.

The proposed system was designed and successfully deployed in a library and it worked satisfactorily. However, the research suggested the addition of web-based technology which will provide an added merit of ease and speed when searching the books present in the library using computers or mobile devices. Htwe and Htun (2015) designed a system that will authenticate persons before granting access to a building. The security access point was implemented using passive RFID. The system provides authentication and validation functions as users permit to unlock the door in real-time. Merits of passive RFID include less cost, less weight and operation without a power source compared to the active RFID tags. The equipment used is a fingerprint reader, a microcontroller and an RFID reader. The system reads the ID number of any passive tag(s) within range and performs a matching function while the fingerprint device scans any print on the scanner and sends the image with already-enrolled data, and checks for any match. If a match is found for both processes, the controller drives motors controlling the doors



until sensors installed at the doors' edges are activated, which in turn stops the driving motors. This system provided more security procedures than previous systems however, security can be improved further to a desirable level but with additional cost in terms of coding and hardware.

Komol *et al.*, (2018) combined Radio Frequency Identification (RFID) and biometric fingerprint techniques to develop an Automatic Security System to validate entrance into secured locations. A servo mechanism was employed to open the door bar when authentication was successful and access was achieved. In this research, the fingerprint sensor will not activate unless the RFID tagging is passed. The design of the system was done using an internal circuit which includes an RFID reader unit, fingerprint sensor, servo motor Arduino Uno, power supply, and a breadboard. All these components are connected and the power supply was provided through jumper wires. Arduino is powered by a 5v supply. Servo motor powered externally. Security was maintained with the sequential operation of RFID and fingerprint sensor and without the missing one, access was denied. This security system is flexible, cheaper, less time-consuming and also needs not commit any code or password access. However, this is a no-bust security system with automatic sensing and operating action to access or decline.

Nandyal *et al.*, (2017) used a fingerprint sensor, an RFID peruse, GSM module alongside Arduino mega and its product are the components used to design this system that can keep proper and accurate records of attendance of students in a school. The GSM frame is used here to send their nearness to their folks through SMS. Methods to active this will utilize an RFID peruse, unique fingerprint sensor, and GSM inside a school premises to give speedy insinuation to guardians about the non-attendance of some students. The success of this project was that it was possible to easily maintain student and staff records and parents can track their child/children's presence and absence daily by the use of a GSM module. However, a delay in sending an SMS due to a poor network will lead to misinformation.

Mahzan *et al.*, (2019) proposed a system that will solve the problem of multi-entering with one card or unauthorized use of cards as a result of using only RFID. Biometric authentication in the form of fingerprint and

facial recognition has been enhanced tremendously but not to its maximum. System components are Arduino Uno microcontroller, max 232 converters, fingerprint sensor and RFID reader. In the prototype, the inbuilt webcam was used. When a user requests access, he must swipe his tag and if recognized, the web camera captures his face and converts it to video frames. The frames are then processed for facial detection. Once a facial match is detected, the user scans his finger which is then authenticated. If authentication succeeds and a match is found, the user then gains access otherwise denied.

This system is a tri-layer full-proof security system. This system also has an alarm which is triggered if any of the parameters fail the matching test, highlighting the presence of an intruder. This system offers some advantages which include; the prevention of entry by different people using a single access card, with Fingerprint authentication acting as a layer 2 security check thus ensuring attendance records reflect true attendance of the period under investigation. This system ensures sensitive institutions and establishments are devoid of a security breach to a significant extent due to the multiple checks. However, the system has the disadvantage of a long series of verification since a user must pass through the verification chain each time, he uses the system.

Pal *et al.*, (2016) presented a design of an RFID-based biometric electronic voting machine. The fingerprint scanner was used for authentication. An Arduino Mega 2560 microcontroller board was used to store the details of voters which were retrieved from the initial voter's database. A liquid crystal display (16X2) for displaying instructions and voter information and an interfacing unit RS232 that allows communication between the microcontroller and the fingerprint module. A buzzer for alarming the boot officer of any irregularities if detected. The design is powered by a 6volts battery. When a voter comes to cast his vote, the unique RFID tag was first verified to check if it matches. If yes, the voter proceeds to thumbprint. If the fingerprint is captured

successfully, the voter casts his vote. The e-voting system was able to improve the speed of voting and provides better security for the voting processes. However, this type of E-voting didn't record success in remote villages and pooling units.

Sonar, (2016) designed a system that monitors in and out movement of students in the hostel. To achieve this, they used an ARM 11 Microcontroller, fingerprint scanner, camera, GSM module, RFID reader and passive RFID tag. The system automatically monitors all tags entering and exiting students' hostels and then informs parents of any student exiting the hostel via text message. During registration of the students, their fingerprints are captured, passport photos taken and a unique identification number is given to each. A student going out of the hostel must pass the first, second and third levels of authentication before access is granted. A record of the exit/entering of each student is saved and an SMS is sent to the parents. At a distance of about 20 meters, the tag is identified, face scanned and fingerprint taken before the gate can be opened for the student. The condition of one to occur depends on the previous one before it. The system after successful implantation provided security for the students, especially the assurance parents get about the safety of their children since they cannot be physically present there.

METHODOLOGY

The following methodology was adopted for the achievement of the project.

1. To design a secure access control system based on RFID technology, the following procedures were carried out:

- a) The system was powered by a 9V battery via the Vin pin of the Arduino Mega computer-on-chip. Two voltages levels; 3.3V and 5V were obtained through 3.3V and 5V pins of the device to power the peripheral devices. The circuit is shown in Figure 1.

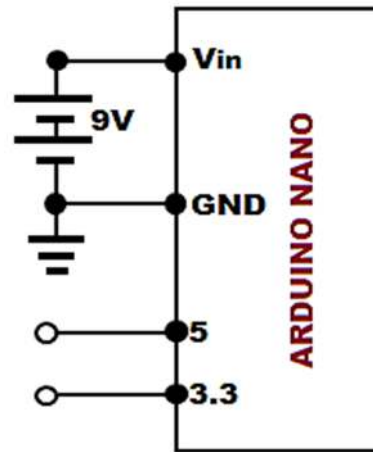


Figure 1: System Power Supply Circuit

- b) The RFID receiver was connected to the controller through pins 50, 51, 53 and 5 and used SPI protocol. The circuit is shown in Figure 2.

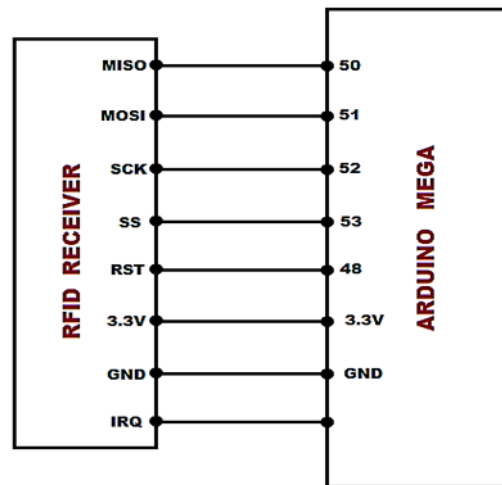


Figure 2: RFID Interface Circuit

- c) The servomotor which controls the gate movement will receive control signals through pins 40 and 41 for the vehicle gate and the small gate. The circuit is shown in Figure 3.

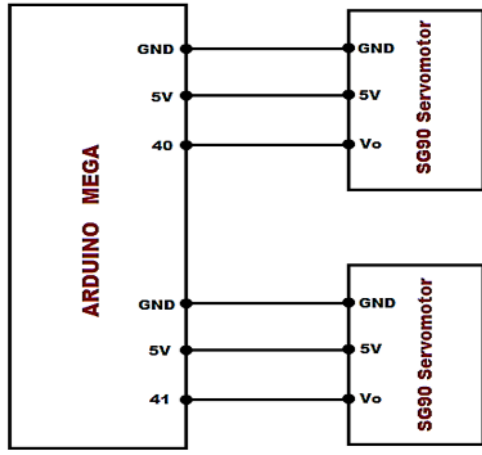


Figure 3: Servomotor Interfacing Circuit

2. Biometric technology using fingerprint was incorporated. The following procedure were carried out:
 a) The Arduino Mega is the controller at the center of connection. The fingerprint scanner uses serial communication protocol and was connected to the controller's pins as shown in Table 1.

Table 1: Arduino Mega to R307 Fingerprint Scanner Connection

Arduino Mega	R307 Fingerprint Scanner
GND	GND
5V	VCC
19 (RX1)	OUT
18 (TX1)	IN

The circuit diagram is shown in Figure 4

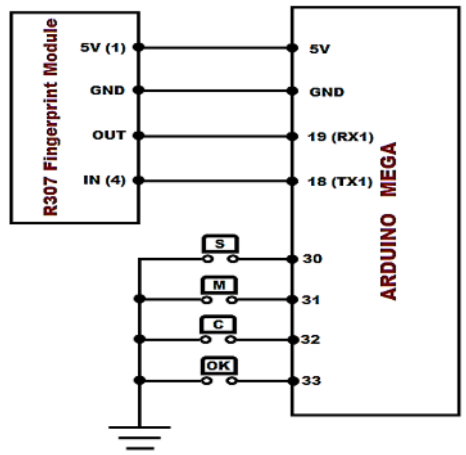


Figure 4: Fingerprint Interfacing Circuit

The program running the hardware of the system was written using Arduino programming language in Arduino IDE version 1.8.10. Arduino and partner, Adafruit provide libraries that were downloaded and added to ease the bulk of programming. The flowchart in Figure 4 is an illustration of how the code was implemented.

3. Incorporating video streaming to the system, the following procedure were carried out.

The OV7670 camera module which uses 3V and controlled using Serial Camera Control Bus (SCCB) was connected to the microcontroller as shown in the Figure 5.

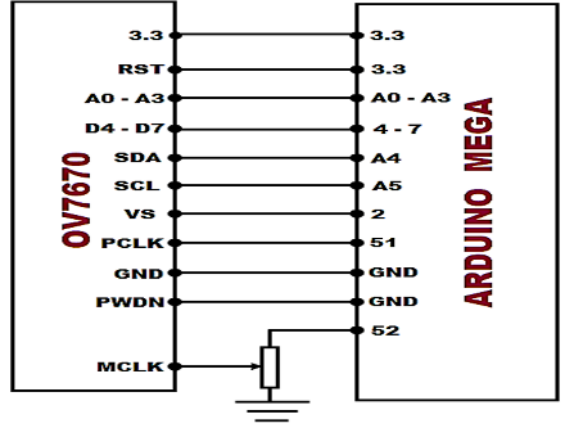


Figure 5: OV7670 Camera Module Circuit

The flowchart of the system is shown in Figure 6 below

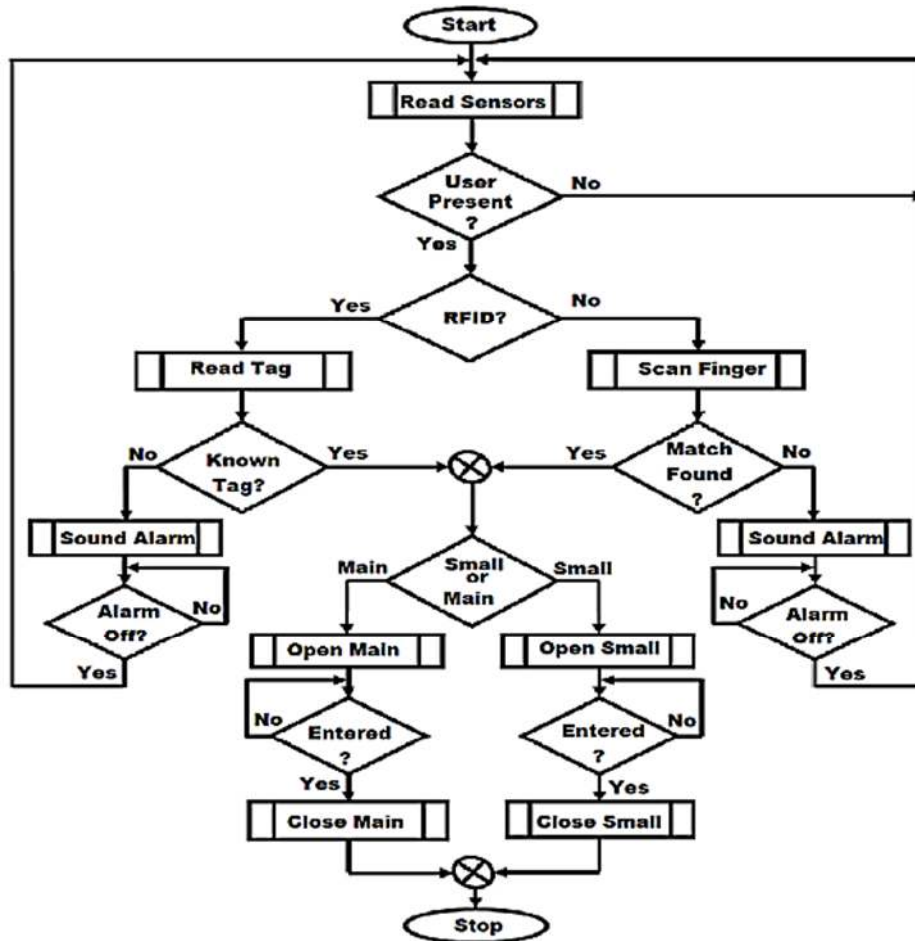


Figure 6: System Flowchart

RESULTS AND DISCUSSION

The results discussed are given in this subsection.

Design of Secure Access Control based on RFID Technology.

The results obtained involves RFID tag identification, RFID tag matching and control of gates. Initially, two RFID tags were identified and added to the code to grant access if any identified tag matched any of the two, else access is denied. Table 2 illustrates the results obtained.



Table 2: RFID Identification and Access Status

Tag Identified	Tag Matching	Selected Gate	Displayed Comment Before Entrance	Gate Status Before Entrance	Gate Status After Entrance	Displayed Comment After Entrance
1746930	Fail	None	Access Denied for tag 1746930 Unknown tag!!! Welcome, Paschal!!! To open press S for the small gate or M for the main gate.	All Closed	All Closed	No comment displayed
Paschal (459330)	Success	Small	Welcome, Blaise!!! To open press S for the small gate or M for the main gate.	Open	Closed	The small gate is closed
Blaise (1309730)	Success	Main	Welcome, Blaise!!! To open press S for the small gate or M for the main gate.	Open	Closed	The main gate is closed
1690170	Fail	None	Access Denied for tag 1690170. Unknown tag!!! Welcome, Blaise!!! To open press S for the small gate or M for the main gate.	All Closed	All Closed	No comment displayed
Blaise (1309730)	Success	Small	Welcome, Paschal!!! To open press S for the small gate or M for the main gate.	Open	Closed	The small gate is closed
Paschal (459330)	Success	Main	Welcome, Paschal!!! To open press S for the small gate or M for the main gate.	Open	Closed	The main gate is closed



The results obtained show that if any tag is within range, the system reads the tag ID, displays it and execute a matching test. If the tag number passes the test, the name assigned tag number is welcomed and permission is granted to open either gate. If the tag number fails the “match” test, access is denied and the system proceeds to continue checking for any print or tag.

a. Incorporation of Biometric technology using fingerprints. The results obtained

in this section are in two parts: fingerprint enrolment and fingerprint matching and control of gates.

b. Results for Fingerprint Enrolment

Five fingers were enrolled and saved on the R307 fingerprint scanner’s EPROM. The fingers are my left thumb, left forefinger, right forefinger, right middle finger and right ring finger saved in locations 2, 16, 49, 13 and 128 respectively. Table 3 shows the fingerprint enrolment.

Table 3: Fingerprint Enrolment

Finger	Stored Location/ID	Status
Left Thumb	2	Success
Left little	16	Success
Right index finger	49	Success
Right middle	13	Success
Right ring	128	Success

CONCLUSION

A secure gate access control and monitoring system using RFID technology and fingerprint technologies was successfully designed and implemented. The system offers an appreciable level of security for homes. On entering, a user is required to scan his finger/RFID tag for authentication and validation. If a tag is known or fingerprint matches, a door is selected and access granted else doors remain closed. Image array operating at up to 25 to 30 frames per second (fps) in VGA. This was achieved after all the components and elements used were well integrated and working together. Though several attempts are made daily to secure lives and properties, there is still a need to improve the security system.

REFERENCES

Fagbohun, O. O., & Fagbohun, O. M. (2018). Design of a Central Wireless Security System Using Atmega328, ZigBee and Arduino. 1-14.

Fowler, J. M. (2019). Electromechanical lock security system: Google Patents.

Ho, H., Saeedi, E., & Ehyae, D. (2017). Increased security electronic lock: Google Patents.

Htwe, K. M., & Htun, Z. M. M. (2015). Design and implementation of bank locker security system based on fingerprint sensing circuit and RFID reader. 4(7), 6-10

Khan, A. A., Bisen, S. T., Thakre, S. J., Naseer, M., & Mam, M. (2019). Finger Print Based Door Locking System. 4.

Komol, M., Podder, A., Ali, N., & Ansary, S. (2018). 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), 15-22.

Mahzan, N. N., Shafie, R., Faiz, M., Ilman Fikry Mohd, Zahari, M., Fadzliil Amin, . . . Systems, E. (2019). Design of Arduino Based Home Security using GSM. 1(2).

Meissner, P., & Gillert, J. (2017). Lock-key system: Google Patents.

Nandyal, S. K., Gadghey, B., & Pujari, V. (2017). RFID and Fingerprint Based Smart Attendance System.pdf. *International Journal for Research in Applied Science & Engineering*.

Pal, N. S., Singh, A., Malik, D., Kumar, P., Singh, H., & Studies, M. (2016). RFID BASED BIOMETRIC ELECTRONIC VOTING MACHINE. 2(12), 452-458.

Corresponding author: Ajayi, O. ✉ agoreofe@abu.edu.ng ✉ Department of Computer Engineering, Ahmadu Bello University, Zaria. © 2022. Faculty of Technology Education. ATBU Bauchi. All rights reserved



- Shankar, A. A., Sastry, P., Ram, A. V.,
Vamsidhar, A. J., & Science, C.
(2015). Finger Print Based Door
Locking System. 4(3), 10810-
10814.
- Sonar, S. (2016). Hostel In Out
Management and Monitoring
System Using RFID, Face, Thumb
Recognition. 5(4).
- Suganthy. (2016). RFID LIBRARY
MANAGEMENT
SYSTEM. *International Journal of
Research -
GRANTHAALAYAH*, 4(5SE), 87-
91.
<https://doi.org/10.29121/granthaalayah.v4.i5SE.2016.2729>.