Vol 8. No. 1 Issue 2 – May, 2015

African Journal of Computing & ICT

www.ajocict.net

Two-Level Verification Access Control System

K.A. Amusa, A. Adewusi, O.O. Nuga, A.J. Olanipekun, [4]Nuga O. O. & [5]Akinduko O. A.
Electrical and Electronic Engineering Department
College of Engineering
Federal University of Agriculture
P.M.B 2240, Abeokuta, Ogun state
amusaakinwale@gmail.com , walecdma@yahoo.com, nugabusola@yahoo.co.uk, akindukooa@gmail.com

ABSTRACT

This paper presented a two-level verification access control system. Conventional locks had not been able to provide a satisfactory solution to the safety of properties and valuable belongings such as jewelleries and print documents, hence, the need for a more secured and better access control system to such custody. The proposed two-level verification access control system was designed to ensure improve access control method where it was deployed. Atmega328p microcontroller occupied the central part of the developed two-level access control system. Radio Frequency Identification (RFID) card reader and fingerprint reader provided the required windows for the two-level verifications. The actual lock mechanism was provided by a solenoid, an electromechanical device, whose operation was dependent on issued command from the Atmega328p in response to inputs from both RFID reader and fingerprint reader. Only users having an authentic RFID tag and registered fingerprints would be granted access. A user attempted entry, by presenting both an authentic RFID tag and fingerprint to the system. A granted access would unlock the solenoid lock. The system had a processing time of less than 2 seconds and maximum average false rejection rate of 0.2%.

Keywords: RFID, fingerprint reader, access control, verification system

African Journal of Computing & ICT Reference Format:
K.A. Amusa, A. Adewusi, O.O. Nuga, A.J. Olanipekun & O.A. Adewale (2015): Pyro-Electric Infrared Sensor-Based Intrusion Detection and Reporting System. Afr J. of Comp & ICTs. Vol 8, No. 1, Issue 1. Pp 175-180

1. INTRODUCTION

This incidence of burglary has become a common phenomenon in our society. Advancement in science and technology has resulted in an increase in the rate and sophistication of crime. This has necessitated the need to provide adequate security of lives and properties. Common method of securing a place of interest is via the use of mechanical locks of different kinds and configurations. Even with the use of mechanical locks, the crime rate is still on the increase due to the fact that these locks are easily compromised [1]. Consequently, there is a need for other types of locks especially electronic ones [2].

Electronic access control system is application of electronic means to check unauthorized entry or access into a restricted domain; this could be a cash box, a safe, bank vaults or homes. Such domain are kept secured and restricted, in order to avoid theft, infringement on the privacy of the owners, or unauthorized access whatsoever. In order to guarantee security, different measures have been put in place to check this demand. Traditionally, verified users have gained access to their property or service via dozens knowledge based security techniques [3]. Knowledge security measures are those means of restricting access to a sensitive domain, using electronic devices that will grant a user access to a domain, only if authorized materials or facts are tendered by the user. Example of such measure includes passwords and Personal Identification Number (PIN), tags and smart cards. However, this knowledge based security schemes and associated hardware is characterized by major drawbacks such as loss of tags or cards and the passcode can be easily forgotten. A number of uni-modal electronic lock systems are already in the circulation, common ones include card sensor locks, which make use of cards as keys. Examples of uni-modal electronic lock system include RFID-based lock system where electromagnetic fields are used to identify objects in a contactless way [4], [5] and electronic combination locks which works via use of code, when the correct code is input by means of an external device the lock is opened, such that only authorized users that know the code can open the lock and gain access to the restricted area. Biometric electronic locks are recent and are still developing.

It is an electronic lock system which utilizes quantifiable data (or metrics) related to human characteristics and traits in the operation of the lock system. Such human features include fingerprint pattern, face recognition, palm print, iris recognition, typing rhythm, gait, voice etc. [6], [7]. Each of the above highlighted electronic methods of access control and lock systems are often deployed singly in practice to provide uni-modal system of access control.

Multimodal access control systems use multiple approaches to overcome limitations of uni-modal systems. For instance, a major drawback of RFID-based lock system is cloning (mirroring or duplication) of tags through which a user gains access to a restricted area. The need to ensure improved security and better access control mechanism necessitated the development of the two-level verification vault access control system using RFID and fingerprint technologies.

2. PROBLEM STATEMENT

The working population of a nation constitutes the youths (within the ages of 18 - 49 in Nigeria). In a country like Nigeria, where high unemployment rate is the talk of the town, youths have to find ways to make ends meet, some embrace entrepreneurship, by learning a trade. However substantial number of them take to criminal engagements such as theft and burglary, these ones are the cause of increase in the nation's crime rate. Conventional locks had not been able to provide a satisfactory solution to the safety of properties and valuable belongings such as jewelleries and print documents, hence, the need for a more secured and better access control system to custody where these items are kept. It is to this effect that an alternative, reliable, secured and efficient two-level verification access control system utilizing RFID and fingerprint technologies is proposed to provide the needed control measure.

3. METHODOLOGY

To actualize the development of the two-level verification access control system, the following materials were used: resistors, capacitors, a crystal oscillator, NPN transistors, an RFID module, a fingerprint scanner, a solenoid lock, a voltage regulator, 220V/12V transformer, a bridge rectifier, Atmega 328/p microcontroller and Light Emitting Diodes (LEDs).

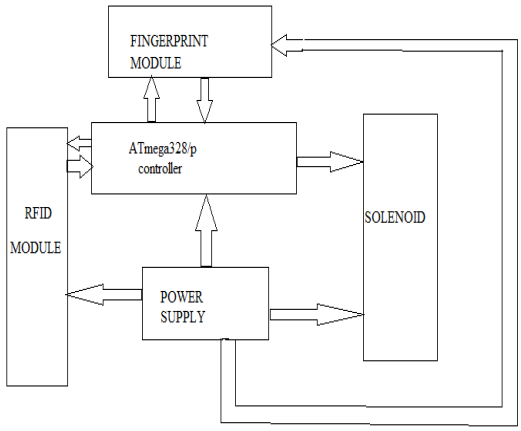


Fig. 1: Block diagram of two-level verification vault access control system

The developed access control system, applies an existing technology in the use of fingerprint and RFID systems for securing restricted areas. A pair of RFID transmitter – receiver acts as sensor in conjunction with a fingerprint identification module.

The RFID system verifies the identity of the user and thereafter grants the user privilege to proceed to use the fingerprint identification module for verification and authentication. Then, a decision is made whether to grant access or not through the operation of the solenoid mechanism. On the successful verification of both the RFID and fingerprint systems, the micro-controller is activated to turn on the solenoid lock. The block diagram of the developed electronic lock system is as shown in Figure 1. Five building blocks are involved in the realisation of the access control system. Design considerations for components making up each of the building blocks are discussed in what follows.

3.1 Hardware Components

The RFID module: In a normal RFID communication, the RFID module is fixed and the user positions the card near the module whenever there is a need to start the interaction. To achieve this, a PN532 breakout is used. The RFID system used contains a PN532 chip of NXP Semiconductors for contactless communication. Together with its PCB-antenna, it forms an NFC reader that conforms with ISO 14443 standard. To increase the communication range of the PN532 breakout board, the antenna had to be matched to the PN532 chip. The PN532 chip generates signal at a frequency of 13.56MHz and the antenna is matched to the chip when the impedance is 50Ω.

Fingerprint Identification module: The identification module that was used is ZFM-20 series fingerprint identification module. The module itself does all of the heavy lifting behind reading and identifying the fingerprints. It has an on-board optical sensor and 32-bit CPU, which makes it compatible with a programmable processor. It can store up to 256 different fingerprints and the database of prints can even be downloaded from the unit and distributed to other modules. This is an advantage in areas where multiple users are required.

Microcontroller: The microcontroller employed in this work is ATmega328p. It has 14 digital input/output pins, 16 MHz crystal oscillator, a USB connection and a reset button among others. Atmega-328/p has a maximum input of 5V DC with a maximum output current of 40mA. Crystal oscillator terminals are connected to pin 9 and pin 10 of the microcontroller to drive the device from an external clock source. Two capacitors C_1 and C_2 form the load capacitance for the crystal and for the smoothening of the clock pulses. This frequency is required to keep track of time, to provide a stable clock signal for the circuit and to stabilize frequencies for the RFID Module. The frequency of the crystal is 16 MHz; this implies that the time taken for the microcontroller to execute an instruction is $62nS$. The values of smoothening and load capacitances are obtained as follows;

Assuming C_1=C_2, then,

$$C_L = \frac{C_1}{2} + C_s \qquad (1)$$

where

C_L, C_s are respectively the optimum load capacitance for a given crystal (which is specified by the crystal manufacturer as 16.5pF) and the stray capacitance on the printed circuit board (whose value can be assumed to be 5.5pF for design purposes). Using these information in equation (1)

$$16.5*10^{-12} = \frac{C_1}{2} + \left(5.5*10^{-12}\right)$$

$C_1 = C_2$ is determined to be 22pF.

Solenoid Lock: Solenoids have found useful applications in areas where there is need to induce linear motion for pushing, pulling or controlling switches and levers. It works on electromagnetic induction principle and can be controlled from electric input from electronic circuits. Specifications of Solenoid used in this design are listed below:

a) The solenoid is to be powered with 9-12 DC volts, but lower voltage results in weaker/slower operation, it draws 500 mA current at 9V when activated.
b) It has a throw of about 6mm and dimensions: 23.57mm / 0.92" x 67.47mm / 2.65" x 27.59mm / 11.08" which is compatible with the conventional door lock sockets, hence can be used to substitute such locks without much stress.
c) The wire lead is long enough to connect to the processor board from the door socket and is terminated with a 4-pin connector, the wire length: 222.25mm / 8.75".
d) It is usually set in a locked position in order to check the possibility of absent mindedness.
e) The holding period for activation is 10 seconds.

The maximum pin current of an Atmega328/p is 40mA, at 5V, this is not sufficient to drive a solenoid. Consequently, a driver circuit is required. The driver circuit implemented consists of a power transistor (TIP102) and a diode (IN4001) to raise the current to 500mA from 40mA at the microcontroller pin. The circuit diagram of the driver circuit is shown in Fig. 2.

The value of the series resistance R_1 to TP102 is obtained as follows:

$$V_{in} - i_b R_1 \le V_{BE}$$
$$R_1 \ge \frac{V_{in} - V_{BE}}{i_b} \qquad (2)$$

From datasheet, $V_{BE} = 2.8V$ and $i_b = 3mA$, $V_{in} = 5V$, then

$$R_1 \ge \frac{5 - 2.8}{3\times10^{-3}} = 0.73k\Omega$$

The value $R_1 = 1k\Omega$ is chosen. With a 12V DC at the solenoid port and $V_{CE} = 2V$ for TP102,

$$V_{sol} = V - V_{CE} \qquad (3)$$
$$= 12 - 2 = 10V$$

where V_{sol} is the voltage across the solenoid.

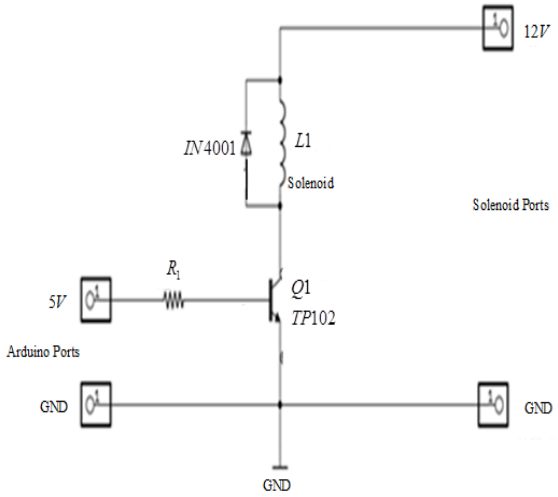


Fig. 2: A circuit diagram of the solenoid driver

From the above analysis, 10V is within the permissible range of the voltage that can drive the solenoid, however the 500mA current is provided by the power supply, TIP102 has the capacity to allow a maximum collector current of 8A,and is therefore suitable for this application. The IN4001 diode is used to ensure forward bias voltage across the solenoid.

Alarm unit: This is provided to sound an alert when an incorrect fingerprint is tried on the system. This alarm system is implemented between the RFID and fingerprint verification stages. This is done to ensure that a stage has already been passed, in the case of a burglar attempting to by-pass the system, it will be evident that the burglar already has access to a valid card, and is trying his fingerprint on the system, the alarm will therefore notify the house owner or the administrator depending on the context of usage. Fig. 3 explains the design considerations of the alarm unit.

Using information obtained from the datasheet of transistor 2N2222, the base current $i_b = 1.5mA$, $V_{BE} = 2V$ and $V_{CE} >$ 2V, the value of limiting resistor R_1 is chosen to be 2.2kΩ. Usually the buzzer operates within a 9V to 12V DC supply, which is guaranteed bearing the size of collector-emitter drop.

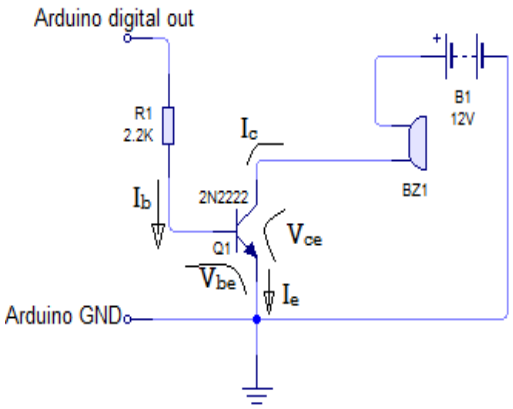


Fig. 3: A circuit diagram of the buzzer driver

3.2 Software Interface

The main purpose of this component is to provide an interface between the fingerprint module, RFID module and the microcontroller unit. In addition, it is required in order to improve the security of the whole system as the condition for granting user access is defined and separated at this stage. The developed software interface is loaded on ATmega328 processor, which is attached to the solenoid lock, fingerprint scanner and RFID reader. For the solenoid, no software is required. The software design of the RFID has just authentication stage while that of fingerprint scanner is divided into two segments: the enrolment and the authentication stages. C++ computer programming language on Microsoft Visual studio is used to write the driver and the header files for the sensors interface between the microcontroller and the output section of the hardware components for proper communication.

RFID authentication mode: This is the mode in which the user's card gets authenticated. This will come up at the point of access to the restricted area. It involves granting the user's card access to use the fingerprint scanner if valid. *Fingerprint software process:* This is the enrolment stage where the authorized users, including the administrator are registered to create database of fingerprints. It involves the capturing of the fingerprint of the users and assignment of identification number to the users. This is then saved and stored in the memory for accessibility when there is a need for authentication. The authentication stage is one in which the users get authenticated after the registration. This comes up at the point of accessing the restricted area. It involves granting the user's fingerprint access if registered and appears in the database or rejecting if the user's fingerprint does not appear in the database.

The flowchart describing the entire procedure is shown in Fig. 4.

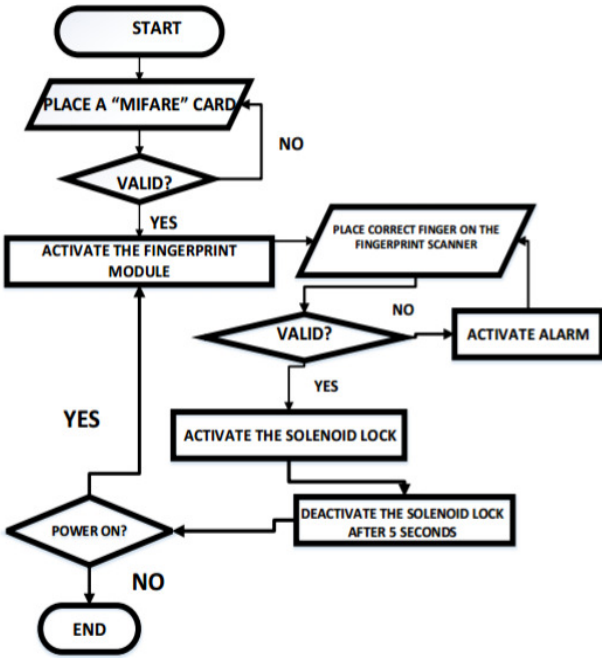


Fig. 4: Flow chart depicting the procedure of operation of the developed two-level access control system

3.3 Implementation

The entire construction procedures centred on running of Atmega328p in a standalone mode without Arduino board. This improves the aesthetic features of the work after packaging, for this reason a compact standalone version of the Arduino board was implemented and was used to interface the fingerprint identification module and the RFID module with the solenoid lock. Each of the hardware components and modules described earlier were assembled then assembled.

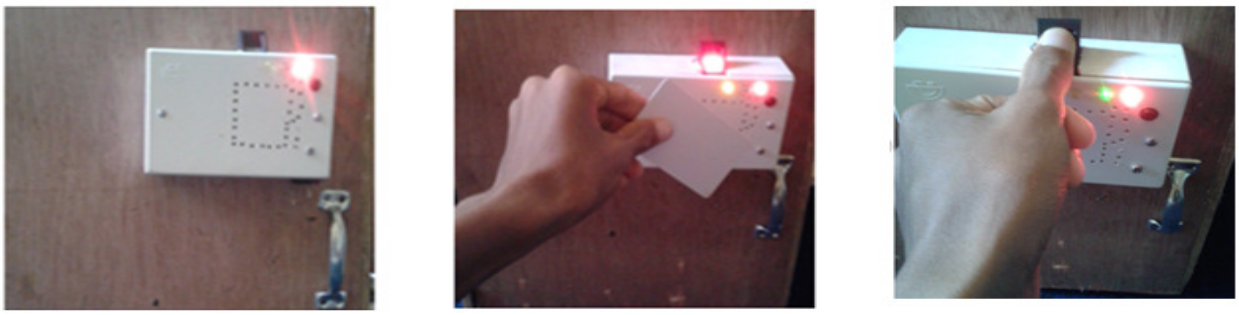
4. PERFORMANCE TESTS

The two-level access control system employs fingerprint and RFID as sensors to control the state of a solenoid lock. After the construction, tests were carried out from the input stage to the final output stage. Each of the modules that make up the developed system was tested after the construction and was found to be working as expected before they were assembled. The entire system was then tested; the response time of the system was measured. Under certain test conditions the variation of the system access denial rate (defined to be the false rejection rate of the fingerprint identification module) with various patterns of fingerprints was determined. The test was conducted on 21 individuals with various fingerprint pattern and finger characteristics. Each individual attempted to access the system 30 times, the results obtained is presented in Table 1.

The test results show that the processing time is generally small irrespective of the finger conditions. In terms of false rejection rate, smooth surface finger has the least average figure of 0.03% while both dry rough-finger and small- sized finger have the highest average with a value of 0.17%. The processing time of fingerprint scanner is generally than 1.5 second. Rough surface finger has average scanner processing time of 1.35 second and the smooth surface finger has the least processing time of 1.17 second. The overall processing time of the developed system is less than 2 seconds with smooth surface finger having the least 1.30 second and rough surface finger taking 1.48 second as average total processing time. With these results, it is evident that, irrespective of the finger conditions, the average processing time required by the developed electronic lock system is less than time required in the operation of mechanical lock system. This is in addition to improve security measure that comes with the two-level verifications involved.

Table 1: Result of tests on the developed vault access control System

Test finger conditions	Fingerprint Pattern	False Rejection Rate (%)	Fingerprint Processing Time (Sec)	RFID Processing Time (Sec)	Total processing time (Sec)
Smooth surface finger	Whorl	0.03	1.17	0.13	1.30
	Loop	0.03	1.18	0.13	1.31
	Arch	0.03	1.17	0.13	1.30
Rough surface finger	Whorl	0.16	1.31	0.13	1.44
	Loop	0.16	1.43	0.13	1.56
	Arch	0.17	1.30	0.13	1.46
Sweaty smooth finger	Whorl	0.40	1.30	0.13	1.46
	Loop	0.40	1.32	0.13	1.45
	Arch	0.43	1.35	0.13	1.48
Dry rough finger	Whorl	0.17	1.29	0.13	1.42
	Loop	0.16	1.19	0.13	1.32
	Arch	0.17	1.22	0.13	1.35
Small sized finger	Whorl	0.17	1.33	0.13	1.46
	Loop	0.17	1.31	0.13	1.44
	Arch	0.16	1.35	0.13	1.48
Medium sized finger	Whorl	0.10	1.30	0.13	1.46
	Loop	0.10	1.32	0.13	1.45
	Arch	0.07	1.30	0.13	1.43
Large sized finger	Whorl	0.20	1.31	0.13	1.44
	Loop	0.23	1.35	0.13	1.48
	Arch	0.17	1.33	0.13	1.46



(a) (*b*) (*c*)

Fig. 5: Plates showing the prototype of the developed access control system during testing (a) power on (b) RFID card verification (c) fingerprint verification

5. CONCLUSION

A robust two-level access control system that is based on RFID and fingerprint technologies has been developed to control the state of a solenoid lock. This can be deployed to provide adequate restriction of unauthorized access to sensitive domains. The results obtained show that the developed system has potential for large scale implementation. In addition to this, the developed system has been shown to overcome some of the challenges posed by uni-modal access control system.

6. FUTURE WORK

This work has been implemented and installed on a locker; however, the application of this development is not limited to lockers as the design has been made to be flexible. It can as well be deployed for building doors, Safes, Vaults and other applications that make use of doors to restrict unauthorized access to a particular place of interest. The possibility of power outage has been factored in during the design, consequently, the system work with either AC or DC power supply.

It is recommended that the system is switched OFF, until its use is required so as to extend the lifespan of the device. In addition, the microcontroller can be programmed to reset automatically after elapse of pre-set time expected for a user to complete the two -level of authentications.

Lastly, the developed access control system can be improved upon by making provision for transaction logging of users over a specify period of time.

REFERENCES

[1] Zungeru, A.M., Kolo, J.G. and Olumide, I. (2012). A simple and reliable touch sensitive security system, International Journal of Network Security & Its Applications (IJNSA), 4(5):149-16

[2] Koenig, J.A., & Taylor, L. 1998. Perimeter Security Sensor Technology Handbook. Electronic Security Systems Engineering Division, North Charleston, U.S.A, 67- 86.

[3] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S. (1999). Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC.

[4] Finkenzeller, K. 2003. RFID-Handbook, Second Edition, Wiley & Sons, Ltd

[5] Simson, G., Henry, H. (2005), Understanding RFID Technology, Garfinkel Book, 15

[6] Ashbourn, J. (2004). Practical Biometrics: From Aspiration to Implementation, pp. 27-28.

[7] Zhaoxia, Z. and Fulong, C. (2011). Fingerprint Recognition-Based Access Controlling System for Automobiles, IEEE 4th International Congress on Image and Signal Processing, 7(11), 4244-9306.