



DESIGN AND IMPLEMENTATION OF AN INTEGRATED ELECTRONIC SECURITY SYSTEM

*Abubakar, I. N.¹; Yusuf, H. M.²; Ambafi, J. G.³; & Ajagun, A. S.⁴

^{1,2,3,4} Department of Electrical and Electronics Engineering Federal University of Technology, Minna

*Corresponding author email: is.abubakar@futminna.edu.ng

ABSTRACT

Insecurity can lead to loss of lives and properties in our society. Consequently, the microcontroller deployment to improve security and control took centre stage when threats to engineering equipment such as machines, telecommunication devices, electronic devices and ammunition warehouses became imminent. This paper deals with design analysis and implementation of an integrated electronic security system to aid in securing infrastructures. The objectives are: to optimise a security lock with minimal cost when compared with mechanical locks, design and implement a locking mechanism which gives genuine users the privilege to have access to their premises and also provides an avenue for password changing whenever an admin password is provided using a microcontroller (ATMEGA 16). In achieving these objectives, the design was categorised into the software and the hardware section. Atmel Studio 5 and Proteus ISIS software were used for coding (C-Language) and simulation for the software section whereas; the hardware section comprises of a keypad, relay, buzzer and the microcontroller. The control unit either activate the pin in which the relay is connected to grant access to the user or activates the pin to which the buzzer is connected when the wrong password is used. The system is designed to activate the relay when the correct password is inserted; however, it activates the buzzer when the wrong pin is inserted depicting that it is an intruder. For flexibility, an admin password is provided which grants the owner access to an interface to change password whenever the need arises. The results presented show that the system responded as designed.

Keywords: ATMEGA 16, Buzzer, Keypad, Liquid Crystal Display, Relay.

1 INTRODUCTION

Due to the need to improve the security of life and properties in our habitations (Sadeque and Farzana et al., 2015), choice of security systems are made in a peculiar manner minding who access a given location and distinctive personal trait of the user (Abel, 2017). As we all know security is one of the primary concern of the present day (Diptanil, 2015) and the first thing that should be desired when you look at your family and home should be safety (Sudhir et al., 2016). It also serves the function of decoding or detecting intrusion. From time past until present traditional techniques of alarm based security have gained much popularity (Raqibull et al., 2015), security locks usually includes mechanical engineering components made up of forged metal, i.e. simple lock and bolt (Mehek et al., 2015), the door chain, pin tumbler lock, the jam lock and padlock. Other recently innovated security devices are gadgets such as laser beam detectors (Liu Ying-nan et al., 2017), motion or presence detectors (Jer-vui et al., 2013), metal detectors and magnetic card readers. Most recent of these gadgets are an offshoot of biometric engineering. They include voice recognition systems, fingerprint readers, retina eye scanners etc. The principal objective

of security devices is to prevent an intruder from gaining access to a designated location. Most of these devices can be compromised which at the end of the day gives an unauthorised persons access to where they are barred. The simple jam lock and padlock can be forced open or their keys easily duplicated by illegal persons. In biometric devices, physical changes of the individual concerned can fail in authenticating user's identity for granting access. Hence they cannot provide the maximum security that is needed.

Furthermore, these devices are costly; its use is restricted to only a few individuals or organisations that can pay the price. Systems such as motion detectors; light detectors among others are vulnerable to be triggered by wrong signals such as sound impulses, whenever its sensitivity increased. There suitable for most outdoor security protection is limited because they do not possess high discriminative capability during operation and are relatively expensive. Therefore It is imperative to provide a locking mechanism which is efficient and reliable; with high discriminative capacity, non-reliance on the physical quality of the individual concerned, which when forced open triggers an alarm and they are less expensive than their counterparts. The facts presented have led to the design and

implementation of an electronic security system. It comprises using correct personal identification numbers to activate the locking device and conditioning the access created on the formation of the security device thereby granting access to the user with the right password access. The electronic security system finds application in homes, banks, in the field of military use, i.e. ammunition warehouse, Academic libraries (Odaro, 2011), households (Prity, *et al.*, 2016) industries, (Nandeesh, *et al.*, 2014) ministries, and government offices etc.

2 METHODOLOGY

The electronic security system is a user-defined password system that allows only authorised access to users. This section of the paper contains the processes involved to get the system working. This section mainly deals with the designed aspect of the hardware and the analysis of individual part that made up the device. Figure 1 shows a block representation of the electronic security system.

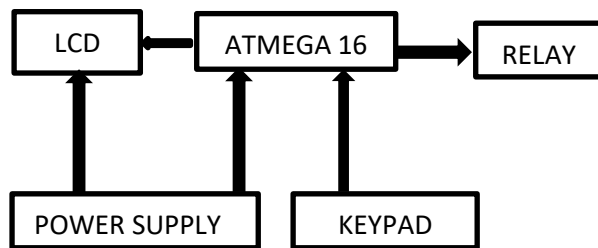


Figure 1: Block Diagram of the Electronic Security System

2.1 POWER SUPPLY SECTION

The AC source was stepped down from 220Vac to 15Vac using a transformer. The low AC voltage was then rectified to DC and then filtered by a capacitor to clear ripples. The dc was further regulated to 5Vdc using a regulator (LM7805) and 12Vdc using another regulator (LM7812) to power the microcontroller and relay respectively (Abubakar *et al.*, 2017).

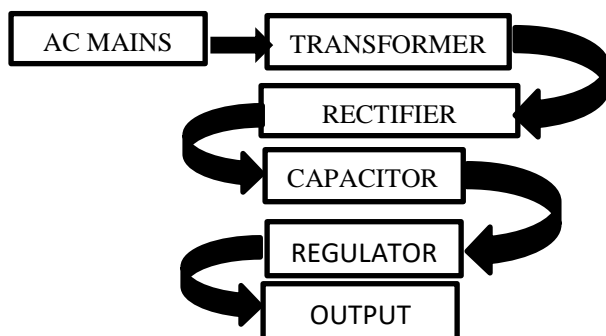


Figure 2: Block diagram of the power supply

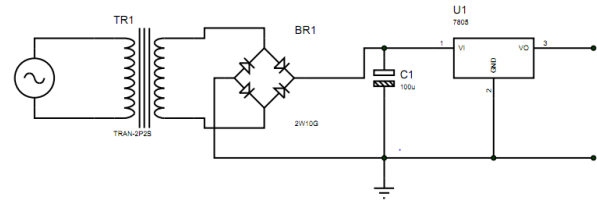


Figure 3: The circuit diagram of the power supply

2.2 THE CONTROL SECTION

The control section uses a microcontroller ATMEGA 16 which is equipped with inbuilt memory (both ROM and RAM) that allow both temporary and permanent storage of codes. The EEPROM of the controller was used to store the password. The controller was programmed to communicate with the LCD, buzzer and relay connected to the load which is responsible for the switching.

2.3. LCD SECTION

This section was achieved by the use of a liquid crystal display (LCD). Instructions from the datasheet are employed in interfacing the LCD with the controller. The different control signals that could initialise the system were specified. All these instructions were adhered to for success in the prototype made. The symbolic representation of the device is shown in Figure4.

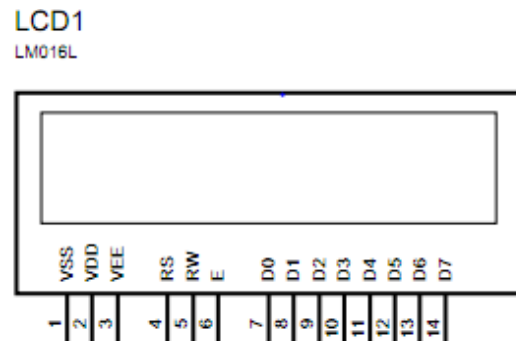


Figure 4: Symbolic Representation of an LCD

2.4 RELAY SECTION.

The unit function is switching between the user's load when the correct password is used and vice versa. The diagram in Figure4 is the relay circuit.

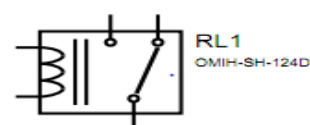


Figure 5: Relay Circuit

2.5 KEYPAD SECTION.

The design uses a 4 by 4 matrix keypad which allows for alphanumeric entries. It consumes no power. It has 8 pins, one for each of the four rows and four columns of buttons. The connections of the 8 pins keypad were to the 8 pins of the microcontroller's port B. The pins representing the four columns are also connected to ground each through a 10kohm resistor. A digital multimeter was used to test for continuity in determining which pin is connected to each row and each column. When the switch is pushed on, a connection is established between the input pin for the row and the input pin for the column in which the switch is located. Suppose the input pin for the second column is grounded and a voltage is supplied at the input pin for the first row. If no button is pressed, no current will flow, through any row input pin. If however button 0 is pressed, a connection is made between the two input pins and current flows through them thus representing continuity indicated on the multi-meter. Current will not flow between these two pins when any other switch is pressed.

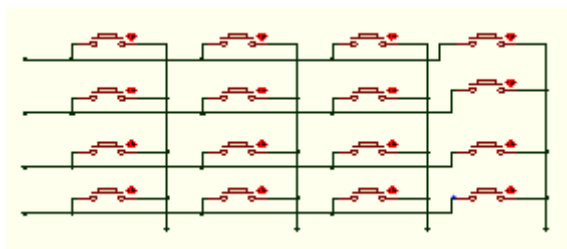


Figure 6: Keypad

2.6. LOAD CONTROL SECTION

In this paper, the load used was a bulb driven by a relay. The relay is an electromechanical device that enables a small signal to be used to control a very high current and voltage. The relay is of two made parts which are: the electrical part and the mechanical part. When a logic high was sent to the transistor, since the relay cannot be driven directly by the microcontroller, the amplification transistor is introduced to boost the current to control the relay more effectively. The resulting magnetic field set up in the relay coil attracts the armature and results to movement of the movable contact to either make or break a connection with a fixed contactor. If the set of contacts were closed when the relay was de-energised, then the movement opens the contacts and breaks the link and vice versa. If the current into the coil is withdrawn, the armature returns forcefully, roughly half the strength of the magnetic force to its stress-free position. Typically, this force is provided by a spring, except in industrial motor starters that commonly use gravity. Most relays are manufactured to operate quickly. In a low voltage application, this is to reduce noise. In a high voltage or high current application, this is to reduce

arcing. When dc energises the coil, a diode is placed across the coil which dissipates the energy from the collapsing magnetic field at deactivation. Also, it generates a voltage spike dangerous to circuit components. Some automotive relays already have a diode in their relay case. Alternatively, the surge may be absorbed by a series connection of a resistor and a capacitor which forms a protection network. If ac is to energise the coil by design, end of the solenoid should be crimped with a small copper ring.

This "shading ring" produces a small out-of-phase current, which raises the minimum pull on the armature during the ac cycle.

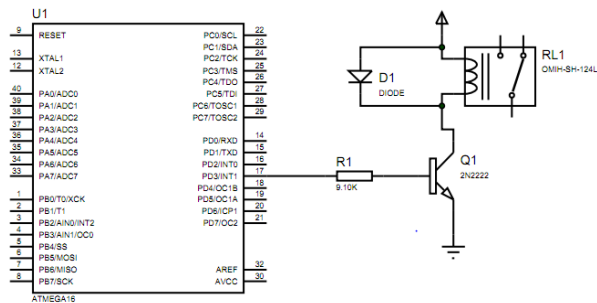


Figure 7: Load Control Section

2.7 OVERALL CIRCUIT DIAGRAM OF THE ELECTRONIC SECURITY SYSTEM

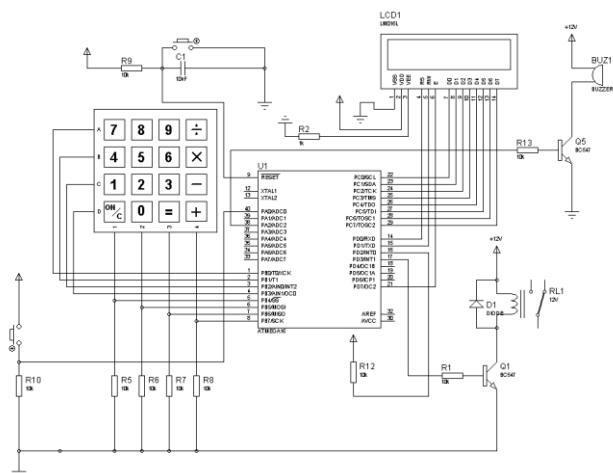


Figure 8: Circuit diagram of the Overall Design

2.8 IMPLEMENTATION OF THE INTEGRATED ELECTRONIC SECURITY SYSTEM

The casing for the electronic security system was locally constructed using plastic in four corners to form a box. The casing built is shown in Plate1.



Plate I: Casing of the electronic security system

3 TESTING AND RESULTS

The testing of components for the prototype system was carried out before the implementation was made.

3.1 POWER SUPPLY TEST

The testing of the system started with the power supply unit. The output of the power supply was first tested using digital multimeter before connecting it to the main circuit. The output was measured to be constant 5V at all the time. The input ac supply fluctuation does not affect the magnitude of the output due to the 7805 voltage regulator that was used. The output waveform was observed under oscilloscope to be a straight line without ripples due to the filtering capacitor used at the output of the supply.

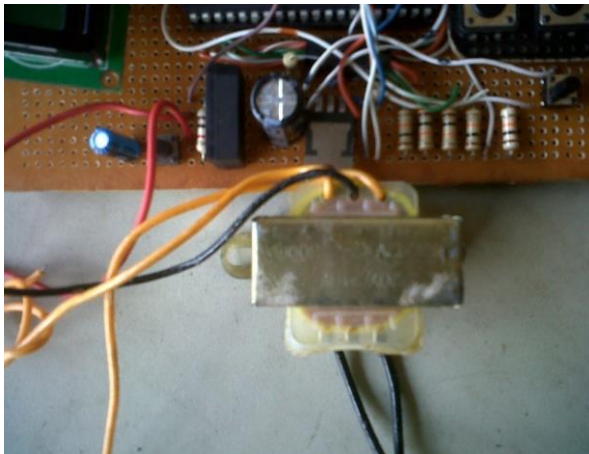


Plate II. Power Supply Test.

3.2 KEYPAD, LCD, RELAY & IC TEST

The keypad was tested by measuring the continuity between one row and its corresponding column, e.g. row1 and column1. When any button is press, the corresponding row and column will be short-circuited of which it enables the signal from the row to be passed directly to the column. The keypad was constructed using 16 pieces of a soft-touch button. This button creates a path for the current to flow whenever it is press and has immediate de-bounce back effect whenever it is

released. The keypad host numbers from 0 to 9 and proceeded with the alphabet from **a** to **f** which was written using AVR studio4 software in C language was debugged so many times to make it an error-free program. Afterwards, it was burned into the memory of the Atmega16 microcontroller. The microcontroller was tested by interfacing it with keypad, LCD and the relay. The LCD (liquid crystal display) provides the visual display of all the operation carried out with the system. The LCD was tested by powering the circuit, it backlight LED comes ON immediately and the character written to the memory of the IC displayed showing that both the program and the LCD are OK. The relay was tested separately by connecting it across a 12V battery and its energies. It means that if the relay should receive a signal from the microcontroller, it will activate any device connected across the **common** and **normally open**.



Plate III. Keypad Test.

Table 1: Power supply test

Point of taking readings	Multimeter reading
Output terminals of the transformer	11.5Vac
The output of rectified DC	12.07
The voltage across the capacitor	12.05
The output of the voltage regulator	4.95

Table 2: KEYPAD/LCD TEST

Test	Result
2222 entered (correct password by default)	LCD shows "ACCESS GIVEN"
2848 (Admin password)	LCD shows "ENTER OLD PASSWORD"

3.3 DISCUSSION OF RESULT

Reliability and efficiency of the system were achieved through the authentication of a password before access can be granted to any user. The password entered was compared with the one stored in the EEPROM of the microcontroller before granting or denying access to the user when there is a match or mismatch respectively. This makes the system attain optimisation. The use of Atmega 16 microcontroller is advantageous to the system in the sense that it is compact as it is having internal storage of 512 Bytes thereby eliminating the need of an external memory which would have contributed to system bulkiness. The LCD used in the design enhances users interaction with the system by displaying appropriate commands on its screen. The idea makes the system more user-friendly and less tedious to operate. The model also offers an extra level of flexibility by making it possible for the user of the system to change the system password at will at an infinite number of times sequel to the entering of the admin password. This feature could come in quite handy in situations where the user suspects the system's password may have been compromised. The user may then change the password to a unique password known to him alone. Figure 8 shows the action on the LCD as simulated using Proteus ISIS.

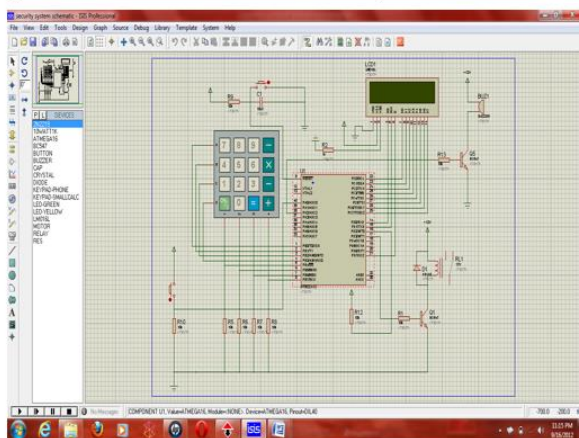


Figure 9: Circuit Diagram Simulation

4 CONCLUSION

In this paper, the Integrated Electronic Security System was designed and implemented, considering the additional feature of the ATMEGA 16 microcontroller, i.e. electrically erasable programmable read-only memory (EEPROM), password manipulation and storing was executed. The relay was activated when the correct password was inserted and access was given to the user. However, a case of wrong password access was denied by the user and the alarm was triggered by signifying an intruder. The electronic security system finds application in homes, banks, in military

ammunition warehouses, industries, ministries, and government offices etc.

REFERENCES

- Abel, A. Z. (2017). An Approach to Smart Home Security System using Android. *Electrical Engineering: An International Journal (EEIJ)*, 4, 2-3.
- Abubakar, I. N., Jacob, T., & Mustapha, B. (2017). Enhancement of Electrical Energy Transaction Through the Development of a Prepaid Energy Meter using GSM Technology. *International Journal of Research Studies in Electrical and Electronics Engineering (IJRSEEE)*, 3(4), 10-18. DOI:- <http://dx.doi.org/10.20431/2454-9436.0304003>.
- Diptanil, C. (2015). GSM Based Home Security System. *International Journal of Engineering and Technical Research (IJETR)*, 3(2), 38-40.
- Jer-vui, L., Yea-dat, C., & Chin-Tin, C. (2013). A Multilevel Security System. *International Journal of Smart Home*, 7(2), 49-60.
- Liu, Y., Yi, S., & TaoGui, X. (2017). Laser Alarm System based on GSM Module Family. *International Journal of Smart Home*, 11(5), 41-50. DOI: <http://dx.doi.org/10.14257/ijsh/2017.11.5.04>.
- Mehek, P., Chimnani, A., Vishal, C., & Amit, H. (2015). Home Security System Using Gsm Modem. *International Journal of Engineering Research and Applications*, 5(4), 143-147.
- Nandeesh, G. S., Srinivasalu, B., & Sunil, K. L. (2014). Intelligent Security System for Industries by using GPS and GSM. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 2(1), 119-127.
- Odaro, O. (2011). Electronic Security Systems in Academic Libraries: A Case Study of Three University Libraries in South-West Nigeria. *Chinese Librarianship: an International Electronic Journal*, 32, 1-10
- Prity, K., Kalyani, P., Priyanka, D., & Rupali, D. (2016). Automatic Smart Home Security System. *International Research Journal of Engineering and Technology (IRJET)*, 3(4), 2178-2180.
- Raqibull, H., Mohammad, M., Asaduzzaman, A., & Israt, J. R. (2015). Microcontroller Based Home Security System with GSM Technology. *Open Journal of Safety Science and Technology*, 5, 55-62. DOI: <http://dx.doi.org/10.4236/ojsst.2015.52007>



1st International Civil Engineering Conference (ICEC 2018)
Department of Civil Engineering
Federal University of Technology, Minna, Nigeria



Sadeque, R. K., & Farzana, S. D. (2015). Android Based Security and Home. *International Journal of Ambient Systems and Applications (IJASA)*, 3(1), 15-24.

Sudhir, C., Neha, D., & Arvind, S. (2016). An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. *Wireless Sensor Network*, 8, 61-68. DOI: <http://dx.doi.org/10.4236/wsn.2016.84006>