ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Design and Development of a Smart Auto Intruder Alarm System with GSM Network

M.Ehikhamenle[1], B.O. Omijeh[1]

Department of Electronic and Computer Engineering, University of Port Harcourt, Choba, Rivers State, Nigeria[1']

ABSTRACT : This project is based on the design and construction of an intruder detecting and alerting system. This was achieved using an AT89C52 microcontroller for the control of the other component, a SIM900-GSM module that communicates between the home owner phone and the PIR sensor (motion sensor). The interfacing between the GSM module and the microcontroller was achieved using an IC called MAX232 (this IC converts TTL voltage level (+5V) to RS232 voltage level (plus minus 7.5V) vice versa) and the microcontroller was programmed using assembly language. At the end of this project we were able to design and construct a device that is not only cheap but efficient. We overcome the problem of false alarm by using a PIR sensor (passive infrared: this sensor only respond to infrared emitted from the human body and animals) and after testing, the microcontroller responded to the information sent by the PIR sensor and in the occurrence of intrusion send an alert message to the home owner as well sounding an alarm to alert the neighbours using a buzzer.

KEYWORDS; Intruder Detecting, G S M Module, P.I.R. Sensor

I. INTRODUCTION

Security is a prime concern in our day-to-day life. Everyone wants to be as much secure as possible. In recent times the world has experienced an exponential increase in the rate of crime. Criminals break into houses on a daily basis around the world carting with huge amount of money and precious items. Sensitive and confidential documents, materials and equipment by corporation are constantly declared missing from where they are kept. So there is a need to provide a device that can detect unauthorized persons in an environment.

In a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An Intruder Detection System (IDS) is a collection of the tools, methods, and resources to help identify, assess, and report intrusions.

Intrusion detection is typically one part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure (Ngad, 2008). In (Zhang et el, 2003), intrusion is defined as: “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource” and intrusion prevention techniques (such as encryption, authentication, access control, secure routing, etc.) are presented as the first line of defense against intrusions.

However, as in any kind of security system, intrusions cannot be totally prevented. The intrusion and compromise of a node leads to confidential information such as security keys being revealed to the intruders. This results in the failure of the preventive security mechanism. Therefore, IDSs are designed to reveal intrusions, before they can disclose the secured system resources. IDSs are always considered as a second wall of defense from the security point of view. IDSs are cyberspace equivalent of the burglar alarms that are being used in physical security systems today (Patcha and Park, 2007). As mentioned in (Zhang et el, 2003), the expected operational requirement of IDSs is given as: “low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected”.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

II. RELATED WORKS

Considering the current global security environment, the importance of good physical security is difficult to ignore. Physical security services are becoming a private rather than public service i.e. individuals and organizations tend to hire private security firms and install security equipment and use the police as the back. According to the Bureau of Labor Statistics (2004), private security officers outnumber police officers by more than 2 to 1 in the United States of America.

Recent reports suggest that this trend holds true for both daily security operations responding to terrorism, natural disasters. Physical security has seen less attention and it is primarily an applied field, it has no dedicated line of research. Instead, it is scattered through fields like engineering, computer science, chemistry and physics as well as social sciences such as criminology, sociology and psychology. The different types of existing security systems will be analyzed below.

- **Electrical Locks**

Electric locks come in many forms. The most basic is a Magnetic Lock (commonly called a mag lock). A large electro-magnet is mounted on the door frame and a corresponding armature is mounted on the door. When the magnet is powered and the door is closed, the armature is held fast to the magnet. Mag locks are simple to install and are very attack resistant. But mag locks are also problematic. Improperly installed or maintained mag locks have fallen on people. Also there is no mechanical free egress. In other words, one must unlock the mag lock to both enter and leave.

This has caused fire marshals to impose strict codes on the use of mag locks and the access control practice in general. Other problems include a lag time in releasing as the collapsing magnetic field is not instantaneous. This lag time can cause a user to walk into the door. Finally, mag locks by design fail unlocked, that is if power is removed they unlock. This could be a problem where security is a prime concern.

- **Electric Strikes** replace a standard strike mounted on the door frame and receive the latch and latch bolt. Electric strikes can be simple to install when they are designed for drop-in replacement of a standard strike. But some electric strikes require that the door frame be heavily modified. Electric strikes allow mechanical free egress: As a user leaves, he operates the lockset in the door, not the electric strike in the door frame. Electric strikes can also be either fail unlocked, as a mag lock, or the more secure fail locked. Electric strikes are easier to attack than a mag lock. It is simple to lever the door open at the strike. Often the there is an increased gap between the strike and the door latch. Latch guards are often used to cover this gap
- **Electric Mortise** and **Cylindrical Locks** are drop in replacements for the door mounted mechanical locks. A hole must be drilled in the door for electric power wires. Also a power transfer hinge is used to get the power from the door frame to the door. Electric mortise and cylindrical locks allow mechanical free egress. Electric mortise and cylindrical locks can be either fail unlocked or fail locked.
- **Electrified Exit Hardware**, sometimes called panic hardware or crash bars, are used in fire exit applications. The idea is that one simply pushes against the bar to open it, making it the easiest of mechanically free exit methods. Electrified exit hardware can be either fail unlocked or fail locked. A drawback of electrified exit hardware is their complexity which requires skill to install and maintenance to assure proper function.
- **Motor Operated Locks** are used throughout Europe. A European motor operated lock has two modes, day mode where only the latch is electrically operated, and night mode where the more secure deadbolt is electrically operated (www.wikipedia.com).

USER AUTHENTICATION SYSTEMS

When implemented with a digital access system, one of the following access systems or digital authentications systems can be with an electric lock. These however are only a few of the numerous authentication devices available.

- **Numerical Codes, Passwords and Passphrases:** Perhaps the most prevalent form of electronic lock is that using a numerical code for authentication; the correct code must be entered in order for the lock to deactivate. Such locks typically provide a keypad, and some feature an audible response to each press. Combination lengths are usually between 4 and 6 digits long. A variation on this design involves the user entering the correct password or passphrase. A major hindrance however is the fact that users are capable of forgetting their codes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Forgetfulness is especially common in older people and this system will not be convenient for them. These codes are, in some cases, easy to crack.

- **Security Tokens:** Another means of authenticating users is to require them to scan or "swipe" a security token such as a smart card or similar, or inter act a token with the lock. For example, some locks can access stored credentials on a personal digital assistant using infrared data transfer methods. However, just as in the case of an ATM card, the magnetic tape tends to wear off with time either resulting to time wasting in accessing a room or the inability of the user to access the room at all.
- **Biometrics:** As biometrics become more and more prominent as a recognized means of positive identification, their use in security systems increases. Some new electronic locks take advantage of technologies such as fingerprint scanning, retinal scanning and iris scanning, and voiceprint identification to authenticate users. This is a very secure way of identifying a person's identity but it is limited by the occurrence of an accident or disfiguration to the part of the body used for identification.

III. MATERIALS AND METHODS

The block diagram below shows the sections and the signal flow. The circuit diagram shows the different component required for the system to function properly.

The Circuit Analysis

The motion based security system is made up of the following stages;

i. Power Supply Unit
ii. Input stage: the input stage comprises of;
   - Motion sensor
iii. Control stage
   - Microcontroller
iv. Output stage
   - Buzzer
   - LCD Screen
   - Bulb
   - G S M module

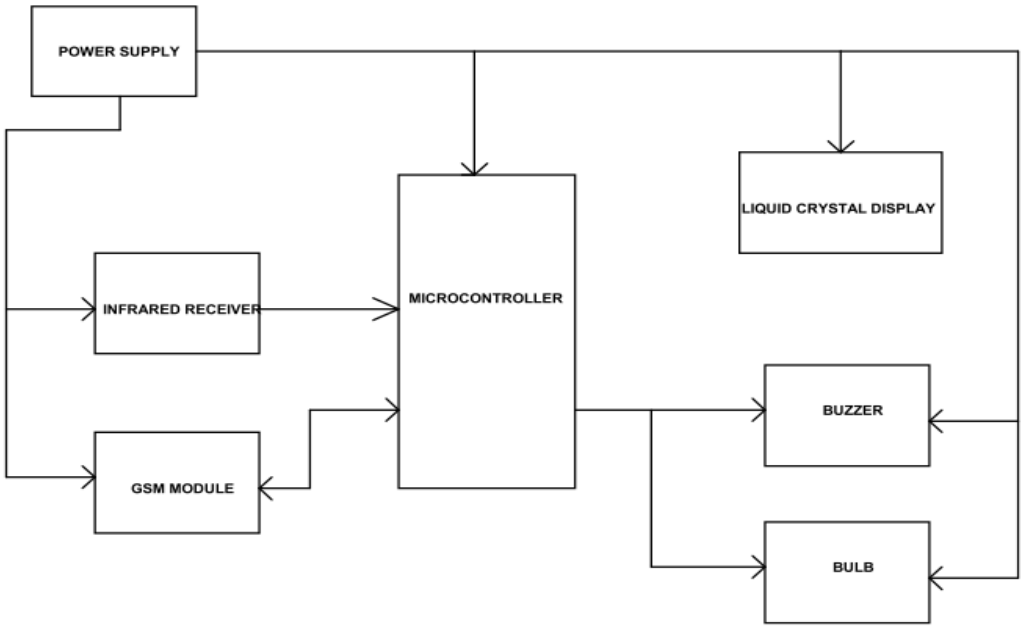

Fig 3.1 The Block Diagram of the System

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A. POWER SUPPLY UNIT

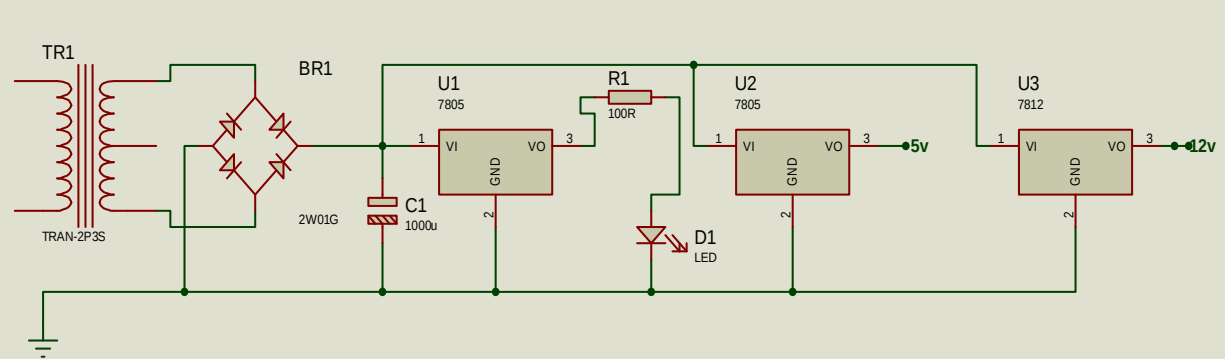

Figure 3.2: Diagram of Power Supply Unit

The power supply serves as the main supply of electrical power to the system. The supply voltage is 220Vac that is step down by a 220Vac/12Vac, 500mA transformer. The 12V AC voltage is then rectified by a bridge rectifier to have a DC output. After the rectification process the remaining AC ripples are filtered off by a bypass capacitor. The output from the bypass capacitor is unregulated thereby causing a drastic voltage drop when a load is connected. To solve this problem an integrated IC chip voltage regulator is used to get fixed output.

i. Analysis of Power Supply

A 240/24V center tapped step – down transformer was used, to feed 24V to the circuit.

Secondary voltage of transformer = $24V\ (Vrms)$

the peak secondary voltage, $V_{peak} = \sqrt{2} \times Vrms$ …… 3.1

$= \sqrt{2} \times 24 = 33.9V$

The bridge rectifier diode will rectify the 24V from the secondary of the step down transformer.

The full-wave bridge rectifier 5W001 was used because it have a peak inverse voltage of 50V and can pass a peak current of 2A which is suitable for our circuit design.

$V_{L(peak)} = V_{(\max)} - 2V_{d(on)}$ … … … … … … … … … … 3.2

Where $V_{L(peak)}$ is the peak to peak voltage of the load

$V_{(max)}$ is the maximum voltage of the alternating current

$V_{d(on)}$ is the voltage drop across the bridge rectifier diode

$[33.9 - 2(0.7)] = 32.5V$

The PIV rating of the diode to be used should be at least

$PIV = V_{(max)} - V_{D(on)}$ … … … … … … … … … … 3.3

$= 33.9 - 0.7$

$= 33.2V$

Therefore the 50v PIV is far greater than this value 33.2v, thus making it suitable for this design.

For a suitable filter capacitor value to be employed the following calculations was considered

$$Vr = Io/2fc$$

Where $Vr = ripple\ voltage = 1.0V$

$$f = frequency = 50Hz$$

$$Io = regulator\ output\ current = 250mA$$

Therefore, $C = \frac{Io}{2fVr} = \frac{250mA}{2x50x1.0}$

$= 2500 \times 10^{-6}$ farad

$= 2500\mu f$.

Since 2500µf is not a standard value, 2200µf was used.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

ii. Voltage regulator
Three voltage regulators were used, two 7805 and 7812 both of them gives 5v and 12v respectively.

iii. Light emitting diode (Indicator)
A light emitting diode is connected in the circuit this will notify that there is power in the circuit. A resistor is connected in series with the light emitting diodes. The resistor limit the amount of current entering the light emitting diode. The value of the resistor is gotten from the calculation below.

$V = V_d + IR$

$V = Supply\ voltage$

$V_d = Operating\ voltage\ of\ light\ emitting\ diode\ (LEDS)$

$I = Allowable\ current\ through\ the\ LEDS\ \ (20mA)$

$R = Limiting\ current\ \text{Re}sistor$

$V = 5v$

$V_d = 2v$

$I = 30mA$

$$\therefore R = \frac{V - V_d}{I} = \frac{5 - 2}{30mA} = \frac{3}{30\ x\ 10^{-3}} = \frac{3\ x\ 1000}{30}$$

$R = 100\Omega$

B. INPUT UNIT
The input unit is made up of the motion sensor that senses if there is a movement in the restricted area the block diagram is shown below.

.

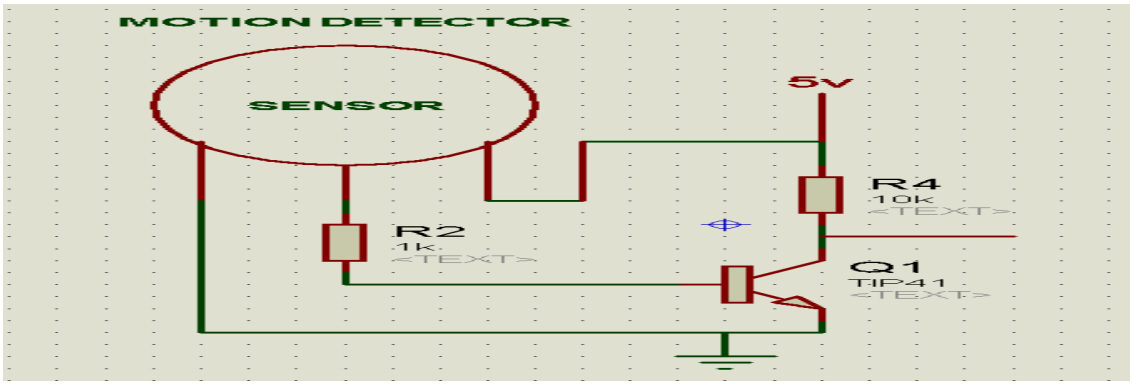

Fig 3.3 circuit diagram of the motion sensor

The motion sensor is used to detect the movement of a human body. It gives a low voltage when there is no motion, when there is motion it sends a 5volt, this will trigger the transistor. The transistor will send the zero voltage to the microcontroller. The transistor used in this circuit is used as a logic inverter. The voltage applied at the base is inverted at the collector terminal. When there is no intruder the motion sensor produces a low at its output terminal, the base of the transistor is connected to the output terminal of the motion sensor. The low signal switches off the transistor thereby preventing current from flowing via the resistor to the emitter. This is an open circuit condition, the voltage that will be gotten at the collector emitter junction is the maximum voltage applied at the collector terminal (5volt). This voltage is sent to the microcontroller.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

When the sensor senses motion it outputs a 5v for one second then goes back to zero, to search if there is any movement again. When the output is five volts the transistor is switched on making the collector voltage to have a zero voltage. The zero voltage notifies the microcontroller that an intruder has been detected. The motion sensor has a range of 6m

D. CONTROL UNIT

The control unit is the microcontroller (AT89c52). It is used to processes the security detecting system. The motion sensor is connected to the pin 1 of the microcontroller via the transistor logic inverter. When the microcontroller receives a low voltage from the input of the motion sensor it turns on the light, bulb, sends message to three individual and displays intruder detected on the liquid crystal display. The diagram of the control circuit is shown below

From figure 3.5, p1.0 is connected to the motion sensor via the logic inverter; p2 is connected to the liquid crystal display. Where p2.0, p2.1, p2.2 and p2.3 is connected to the data pins of the liquid crystal display and p2.5 and p2.7 is connected to the register select and enable of the liquid crystal display. P3.0 and P3.1 are the serial terminals of the microcontroller; it is connected to the GSM module via max232. The max232 is used to convert the voltage from the GSM to TTL voltage as well as converting TTL voltages to the acceptable voltage of the GSM module.

The buzzer is connected to port 3.5 via a transistor when an intruder is detected; the microcontroller sends a 5volt to the base of the transistor. This switches the transistor and the buzzer is turn on.

The light bulb is connected to relay which is connected to p3.6 of the microcontroller via the transistor, this illuminate the area of intrusion.

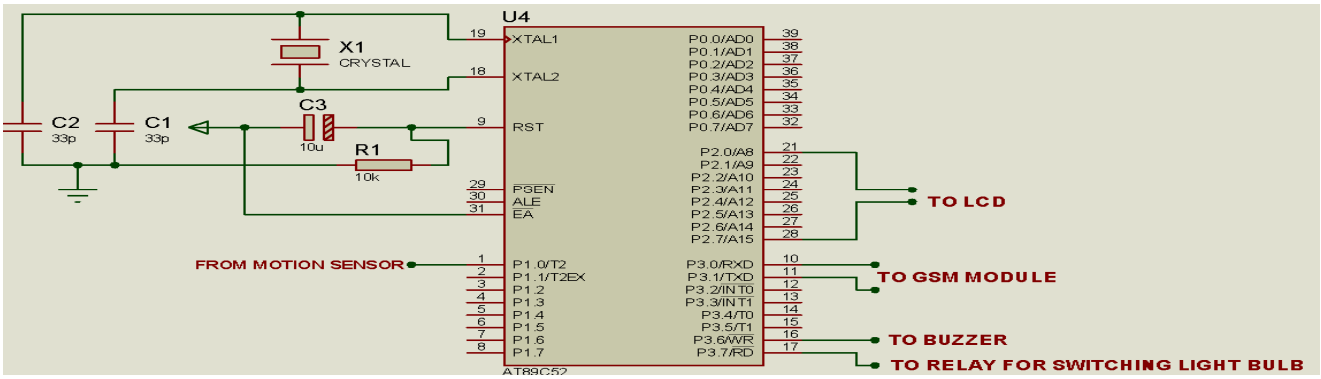

Fig 3.4 control unit

E. OUTPUT UNIT

The output unit consists of;

i. LCD Screen
ii. Buzzer
iii. Lamp

i. LCD Screen

The LCD screen is used to display that an intruder has been detected; this is possible due to its data terminals and command register that the microcontroller is connected to. The buzzer sounds an alarm when an intruder is detected either from the infrared sensing system or the ultrasonic module.

ii. *Buzzer*

The buzzer sounds an alarm when an intruder is detected from the motion detecting system.

iii. Lamp

The lamp is connected to the microcontroller via a relay and transistor. When an intruder is detected the microcontroller switches on the bulb through the transistor and relay.

iv. *GSM* module

The GSM module is used to sends message to three individual using AT commands. This is done by the microcontroller when an intruder is detected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

F. CONSTRUCTION OF CIRCUIT AND ASSEMBLY OF COMPONENTS

After designing the circuit in a software environment Proteus Version 7.8 and simulating it. The values of each component were obtained and ordered from the marketers and when they arrived construction began.

The construction started with mounting of components on the Vero board; each component was tested before mounting and then soldered to the Vero board.

The power supply unit was built first and the voltages from the voltage regulator were tested before going into the next stage. The control unit was soldered and tested. The output unit was soldered last and tested. Each stage is connected (joined) by a connecting wire or placed in the same row for continuity and tested before packaged with a plastic adaptable box. After packaging (casing) the prototype was tested and checked for any fault arising because of vibration and shaking owing to packaging.

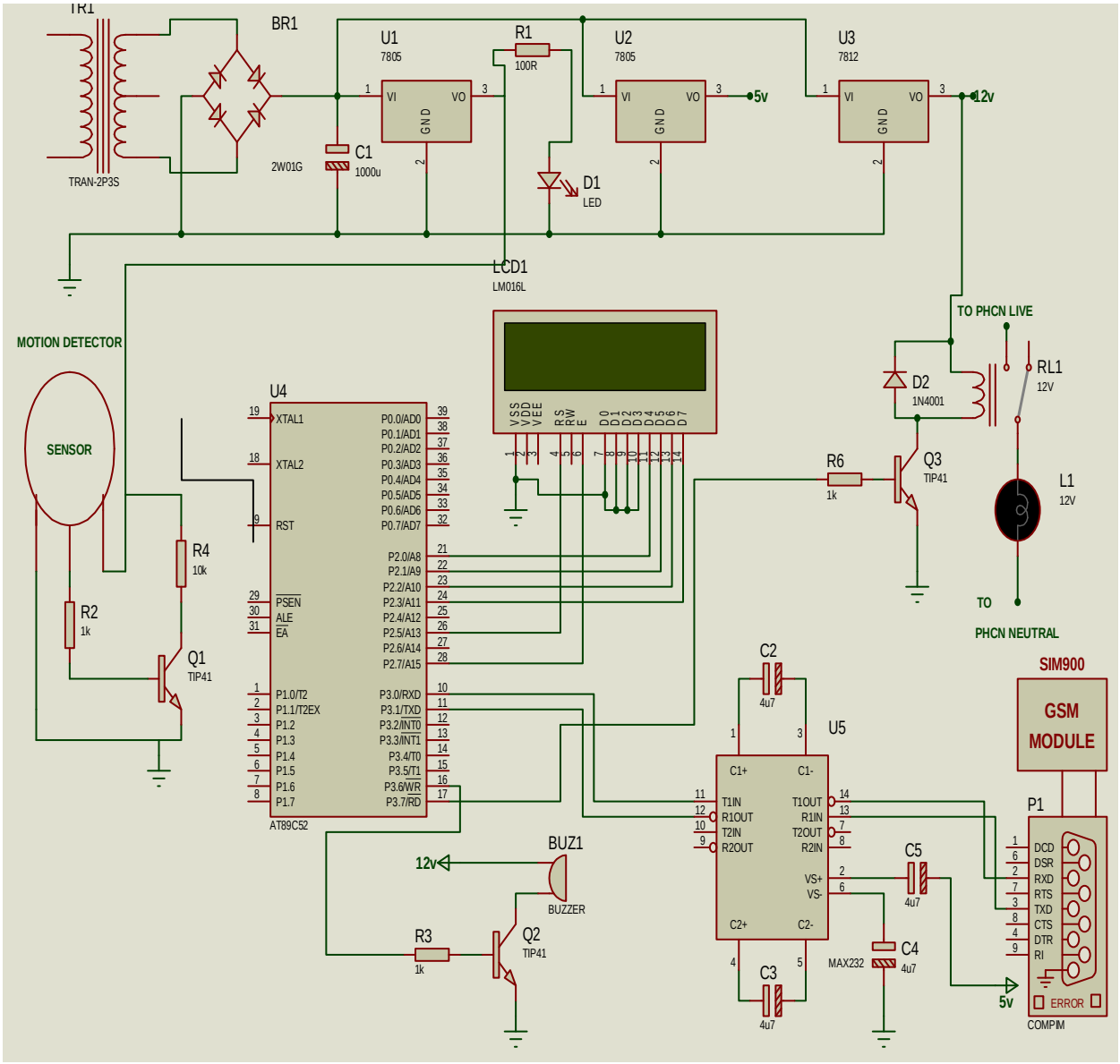

Figure 3.5: Circuit Diagram of the Motion Based Security System

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

IV. RESULTS AND DISCURTIONS

Before using any component it is advisable to test them before soldering and also to test each stage of the project during construction. This approach provides us with an easy way to trace fault and easily correct them. The power supply unit was checked for proper voltage level from its output pins with a multi-meter. The motion sensor and GSM module were also tested, as well as the entire circuitry. The software programmed was simulated and checked in the assembler (M.I.D.E studio), the hex file was generated with no error recorded before it was burned into the microcontroller chip using a TOPWIN programmer.

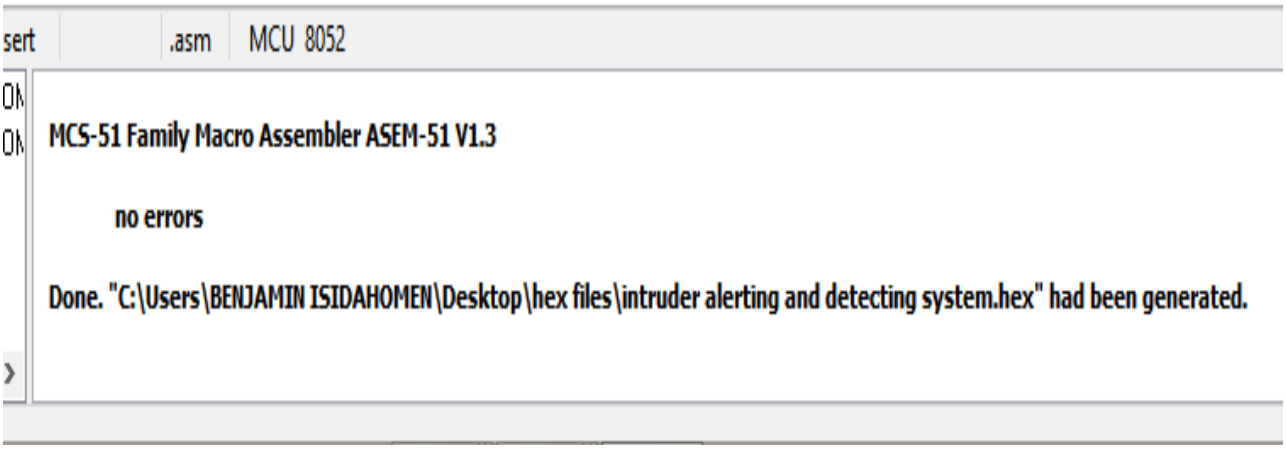

Fig 4.1 testing of source code using M.I.D.E studio

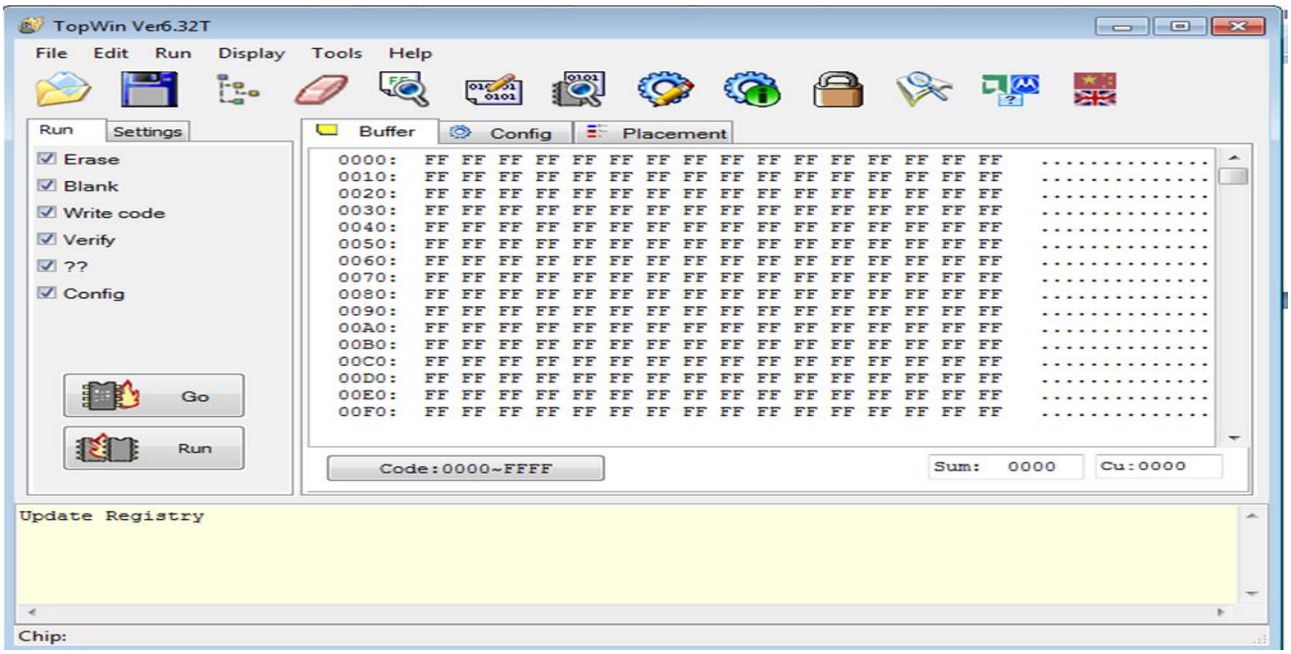

Fig 4.2 burning of program into chip using topwin

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A. POWER SUPPLY UNIT

Table below shows the power supply test using DC Multimeter.

Table 4.1 value of voltages from the power supply stage

Voltage regulator	Voltage (dc)
7812	11.87
7805	5.01
7805	4.98

The motion sensor

The motion sensor was tested by placing the sensor, and sensing for the change of the output voltage. When the sensor senses motion the output is high and when no motion is sense the output is low.

Table 4.2 results from the output of the motion sensor

Motion Sensor	Motion Sense	Voltage (dc)
	No	0
	Yes	5

Table 4.3 Results achieved after the completion of the project

Process	component	Action
Power is turn ON in the circuit	Power indicator led, program indicator led	Both LEDs turn ON
Motion is not sense	No human detected	Buzzer turn off
Motion is sense	Human detected	Buzzer turns on for 5 minute goes off. Bulb turns on. SMS is sent to three persons.

V. CONCLUSION

The aim of the project is to develop a system that can be able to detect when an intruder enters an area, the system should alert the public by sounding an alarm, illuminating the area, as well as sending text messages to three different numbers.

The circuit is an innovative device that is active in detecting an intruder. The device can be used at homes, schools, churches, etc. it will promote security of lives and property in this country if adopted.

In Nigeria where home burglary and robbery is in the increase this circuit will reduce the rate of armed robbery in an area, and it is in line with the government vision 2020.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

REFERENCES

1. Microsoft Encarta Encyclopedia (Student Edition), 2008Bitzer, E. and Hoffman, A. Research Paper: Psychology inthe Study of Physical Security, 2007
2. Bunn, M. & Wier, A. (2004). Securing the bomb: An agenda for Action. Cambridge, MA: Harvard University, Belfer Center for Science and International Affairs
3. Higgins, M. (2005, September 10). Katrina-hit states turn to security firms, The Washington Times.
4. Virasami, B. (2005, April 28). City to Train Private Security Guards. Newsday, p. A17
5. Hassan, M.F. (2008, October 14), Intelligent Intrusion Detection System, Blog. Microchip Technology, PIC16F87x Data Sheet, 2001.
6. http://en.wikipedia.org/wiki/intrusion_detection_systems (Retrieved Date: 6th November, 2008)
7. www.medscape.com/viewaricle/456786 (Retrieved Date: 12th September, 2008)
8. U.S. Department of Labor: Bureau of Labor Statistics (2005) May 2004 National Occupational Employment and Wage Estimates: Protective Service Occupations
9. http://stats.bls.gov/current/oes_33pr.htm (Retrieved Date: April 13, 2005)
10. www.electronics-lab.com/projectsensors/026/ (Retrieved Date: 15th February, 2009)
11. Harris, Tom (March, 2008), "*How Burglar Alarms Work"*, HowStuffWorks.com, Retrieved April 10, 2007,
12. wikipedia (May, 2008), "*Closed-circuit television*", Retrieved May 16, 2008, from
13. http://en.wikipedia.org/wiki/surveillance_cameras wikipedia (May, 2008), "*Security*", Retrieved May 16, 2008,from http://en.wikipedia.org/wiki/security

BIOGRAPHY

Ehikhamenle M. graduated with BEng (Second class upper honors)Electrical/Electronics Engineering from Ambrose Alli University Ekpoma in 2007.He obtained his Master degree in Electrical/Electronics Engineering fromUniversity of Benin (UNIBEN), specializing in Electronics and Telecommunications in 2010. He was Head of Department Essential services, Works and Services Directorate Ambrose Alli University Ekpoma in 2012/2013. He is presently a lecturer in Electronic and Computer Engineering Department University of Port-Harcourt (UNIPORT).He has taught courses in electronics, computer,and telecommunications Engineering. His research interest include: Electronic, telecommunication, power electronic CAD, ICT and Control Systems.