American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Design and Implementation of a Mobile-Based Home Security System

Eseosa Ehioghae Efe[a]*, Samson Ogunlere[b]

[a,b]*Department of Computer Science, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria*

[a]*Email: eseosaehioghae@gmail.com*

[b]*Email: ogunleres@babcock.edu.ng*

Abstract

The security of homes and properties has always been a crucial concern as the rate of burglary and home breaking has been on the increase all through the years. Although various solutions have been proposed to tackle the problem, burglary and home breaking are still rife everywhere every day. The proposed research is a low-cost, highly configurable, and mobile home security system that secures homes from illegal entities attempting to gain illegal entry into such homes. The system was implemented using Arduino with ATmega2560 microcontroller, which was interfaced with a Passive Infrared (PIR) sensor, a 16x2 Liquid Crystal Display (LCD) screen, a 4x4 matrix keypad, a Global System for Mobile Communication (GSM) module, and a burglar alarm. The physical home security system was simulated using Proteus 8 Professional simulation software, while Arduino Integrated Development Environment (AIDE) and the C programming language were used to program the microcontroller instructions on the Arduino ATmega2560 microcontroller. Furthermore, Android Studio and the Java programming language were used to develop an Android mobile application to control and interact with the physical home security system. The results from the system were depicted in snapshots taken during the implementation and testing of the system. Judging from the research findings, it is imperative to adopt this system as a means of effectively securing homes from illegal intrusion. Further research could be done as an add-on to ensure security from internal threats within homes, such as fire and gas leakages with the addition of more sensors.

Keywords: Android Mobile Application; Arduino Integrated Development Environment (AIDE); ATmega2560; Burglary; Home Security.

---

* Corresponding author.

1. Introduction

The loss of properties in a home could be tragic, most especially when the cause of such loss is as a result of 'unwanted visitors' illegally finding their way into such a home without the homeowner's consent. These 'unwanted visitors' are commonly known as burglars.The security of homes and properties cannot be overemphasized as it is a prime concern in everyday living. People, organizations, companies, and countries spend a lot on one form of security. For example, in the year 2014, Nigeria spent $32 billion on security and defense, yet, Nigeria was not any safer [1]. Despite the massive spending on security, the problem of insecurity in homes still exists, as a 2018 Federal Bureau of Investigation (FBI) crime statistics estimated that a burglary occurs somewhere every 26 seconds in the United States of America [2]. Furthermore, a study conducted by Oguntunde, Ojo, Okagbue, and Oguntunde [3], which analyzed burglary crime rates in Nigeria between 1999 and 2013, revealed burglary as having the second-largest number of total reported crime cases. The advancement of technology and the proliferation of smartphones have provided the basis for developing security systems capable of effectively securing homes. This has further led to the development of different home automation and security systems, utilizing technologies such as Bluetooth [4], Global System for Mobile Communication (GSM) [5], Zigbee [6], and the Internet [8]. These technological solutions give homeowners the ability to secure and monitor their homes from wherever they are. However, most of these systems present one problem or the other, such as poor communication range, interference, and high implementation costs. In this paper, we design and implement a low-cost, highly configurable, mobile home security system that utilizes GSM technology and a mobile application to give homeowners the ability to protect their homes from the intrusion of burglars. This system was implemented using a Passive Infrared (PIR) sensor, a 16x2 Liquid Crystal Display (LCD) screen, a 4x4 matrix keypad, a GSM module, a burglar alarm, and an Arduino ATmega2560 microcontroller. A mobile application was further developed to control and interact with the home security system from wherever the homeowner might be. Furthermore, the circuit design of the physical home security system was simulated using Proteus 8 Professional simulation software, while Arduino Integrated Development Environment (AIDE) and the C programming language were used to program the microcontroller instructions on the Arduino ATmega2560 microcontroller. Android Studio IDE and the Java programming language were used to develop the Android mobile application, which was used to control and interact with the home security system and had a crucial functionality of alerting homeowners of an intrusion, whenever there was one.

2. Related Works

Sriskanthan, Tan, and Karande [4] implemented a home automation system using Bluetooth. Their design incorporated a host controller, which interfaced with some microcontroller-based sensors (such as temperature sensor and fan-controller), via a protocol layered on top of Bluetooth called Home Automation Protocol (HAP), which they proposed, to support the communication between the devices and the host. Their proposed HAP enabled multiple sensors to be connected to the host controller using an Inter-IC (I^2C) Connect bus while minimizing cost. The software program controlling the microcontroller was written in the C programming language. It should be noted, however, that Bluetooth poses a huge constraint on communication range, hence, this system was also prone to this constraint. Sarijari, Rashid, Rahim, and Mahalin [6] implemented a wireless home security and automation system using ZigBee technology with multi-hop communication. A multi-hop

arrangement was used for the communication between sensors like fire alarms and intrusion detection alarms, to allow for a wider range of communication with the main controller, which was a PIC18F452 microcontroller. Whenever there was input from any of the sensors, an SMS was sent to some previously set numbers, to alert them of the current intrusion. The microcontroller for their system was a PIC18F452 microcontroller and it had all the pertinent sensors connected to it, while the software controlling the microcontroller was written in the C programming language. Furthermore, homeowners could communicate with their system by sending an SMS, to either turn on or off the sensors connected to the microcontroller. Islam [7] designed a home security system also based on PIC18F452 microcontroller, which had connected to it, sensors that were used to monitor the doors and windows of a house, to sound an alarm in the case of a break-in and further notify the nearest police station of such a break-in. This system also gave the homeowners the ability to switch between a security status and a free-entry status, where the former turned on the security system by ensuring the doors and windows of homes were actively monitored for break-ins, while the latter turned off the security system, allowing free entry in and out of the home. The software program controlling the microcontroller was written in the C programming language. ElShafee and Hamed [8] designed and implemented a home automation system based on WiFi technology. This system consisted of a web server and the hardware sensors which were connected to the server via a hardware interface module, utilizing WiFi technology as the underlying infrastructure. Furthermore, a software application built with ASP.NET framework 4.0 was deployed on the web server and it was responsible for the setup, configuration, and maintenance of the whole home automation system. This was a robust system as it provided more comprehensive functionalities due to the web server and the web application developed. However, it should be noted that systems based on WiFi or the Internet generally pose a great constraint on power consumption to keep the web servers up and running. This system likewise shared this constraint due to the presence of the web server.

3. Materials and Methods

The methodology of the proposed system is divided into two main sections, namely, hardware implementation and software implementation. The hardware implementation consists of the design and development of the physical home security system, with all the sensors connected to the Arduino ATmega2560 microcontroller to enable communication with the signal input from the sensors. While the software implementation can further be divided into two main sections, namely, microcontroller software implementation, which focused on programming the Arduino ATmega2560 microcontroller and mobile application software implementation which focused on developing a mobile application to interface with the entire home security system.

3.1. Hardware Implementation

Microcontroller and the 16x2 LCD Screen: The GND pin of the LCD module was grounded while the VCC pin was connected to 5v to power the LCD. VEE was connected to a 10K potentiometer, which was used for adjusting the contrast of the display. The RS (Register Select) pin of the LCD module was connected to digital pin 42 of the Arduino. The R/W pin of the LCD module was grounded, in effect, it was in write mode, because we were only interested in writing to the LCD and not reading from it. The enable pin of the LCD was connected to digital pin 43 of the Arduino. In this paper, the LCD module and the Arduino ATmega2560

microcontroller were interfaced in 4-bit mode. This meant that only four of the digital input lines (DB4 to DB7 of the LCD) were used in communication. This was because this connection mode was simpler, required fewer connections, while still giving the ability to utilize the right amount of potential of the LCD module. Also, we were only interested in writing to the LCD and not reading from it. Hence, digital lines DB4, DB5, DB6, and DB7 were respectively connected to digital pins 44, 45, 46, and 47 of the Arduino. It should also be noted that sending data nibble by nibble does not matter because once we have the variables rightly put into the system, we do not have to worry about how the computer (the microcontroller in this case) will represent and process them [9]. Finally, a 560-ohm resistor R1 was used to limit the current passing through the back-light LED. The hardware interfacing between the LCD and the Arduino ATmega2560 microcontroller is shown in Figure 1.

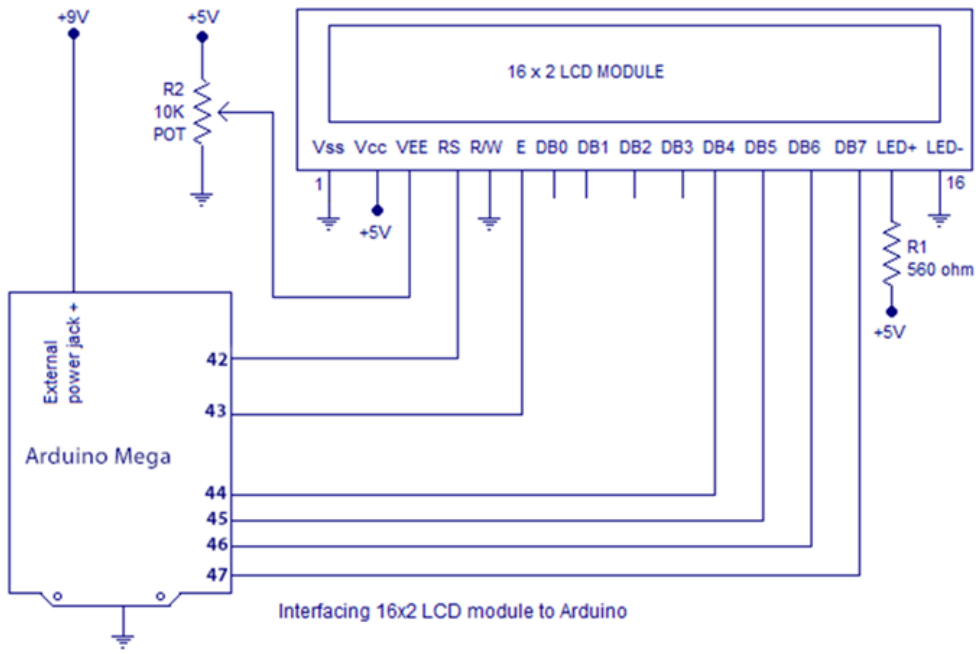

Figure 1: Hardware interfacing between the LCD and the Arduino ATmega2560 microcontroller

Microcontroller and the 4x4 Matrix Keypad Module: Rows R1, R2, R3, and R4 of the keypad module were interfaced with digital pins 22, 23, 24, and 25 pins of the Arduino, respectively. While columns C1, C2, C3, and C4 were respectively interfaced with the digital pins 26, 27, 28, and 29 of the Arduino. Microcontroller and the PIR sensor: The three pins GND, OUTPUT, and VCC of the PIR sensor were connected to GND, digital pin 52 on the Arduino, and +5v, respectively. Pin 53 was used to connect the buzzer (used as a burglar alarm), which was active when a motion was detected by the PIR sensor. Microcontroller and the GSM Module: The serial Tx and Rx pin of the GSM module were connected to two digital pins (pin 6 and 7, respectively) of the Arduino, which was used for the serial communication between the GSM module and the microcontroller. This was made possible with the help of the Arduino SoftwareSerial library, which is an Arduino library that enables serial data communication with the digital pins of Arduino. It was imperative to use this method of communication with the GSM module because, the GSM module uses a serial mode of communication, while the Arduino uses a digital mode of communication, via its digital pins. Hence, the need for a library to aid the communication between the devices. The schematics of the hardware of the entire home security system was designed using

Proteus 8 Professional, an electronic simulation software. The complete schematic diagram is shown in Figure 2.

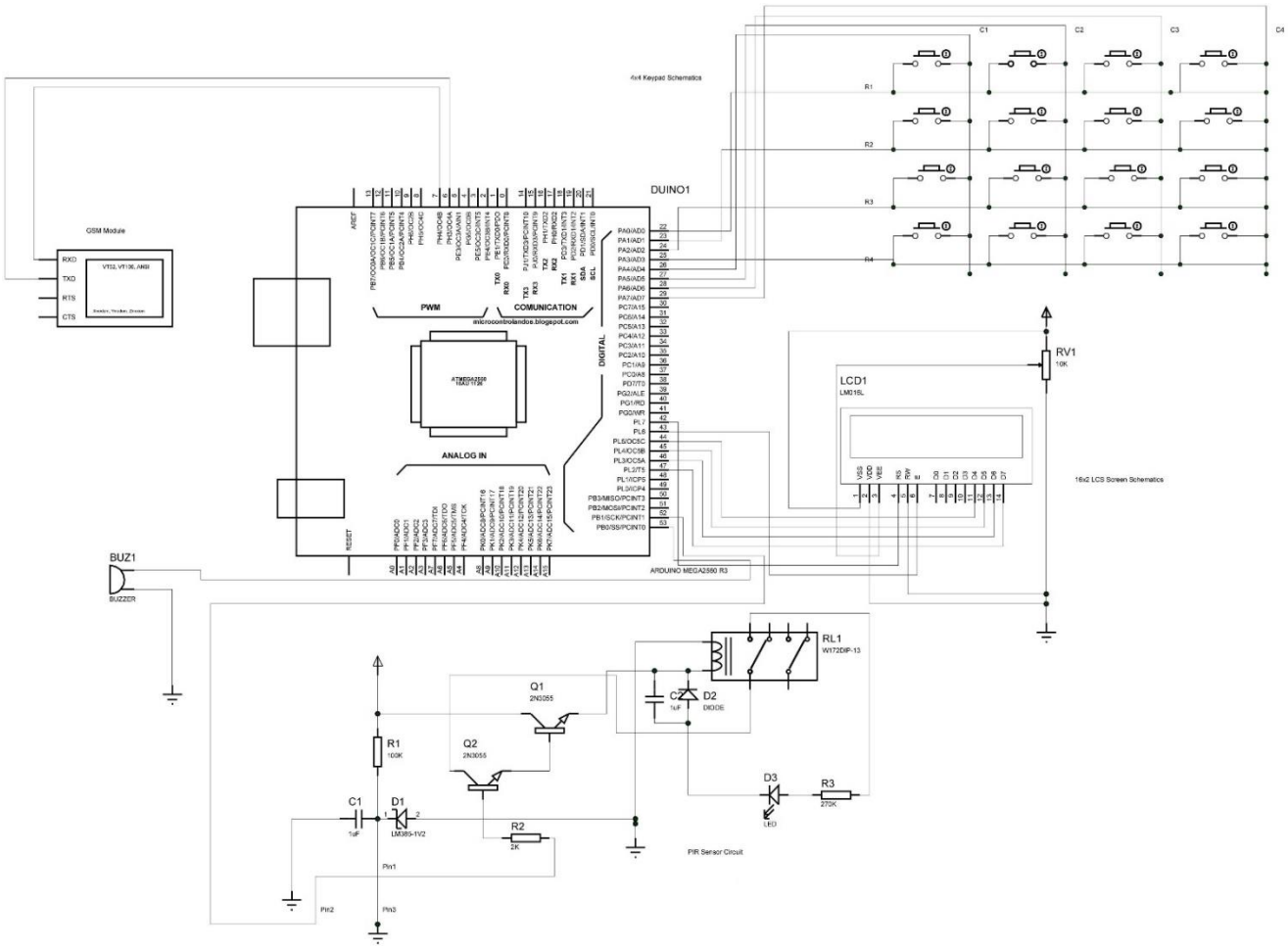

Figure 2: Schematic diagram of the proposed home security system

3.2. Software Implementation

The software implementation of the proposed system can further be divided into two categories, namely, microcontroller software implementation and mobile application software implementation. Microcontroller Software Implementation: The programming of the ATmega2560 microcontroller was done on an Integrated Development Environment (IDE), called Arduino IDE. This provided the requisite tools for writing the microcontroller logic for the Arduino ATmega2560 microcontroller. The C programming language was also used for the programming of the software program which controlled the microcontroller. The code snippet in Figure 3 shows some code logic written on the Arduino IDE for the communication between the microcontroller and the GSM module for sending and receiving SMS.

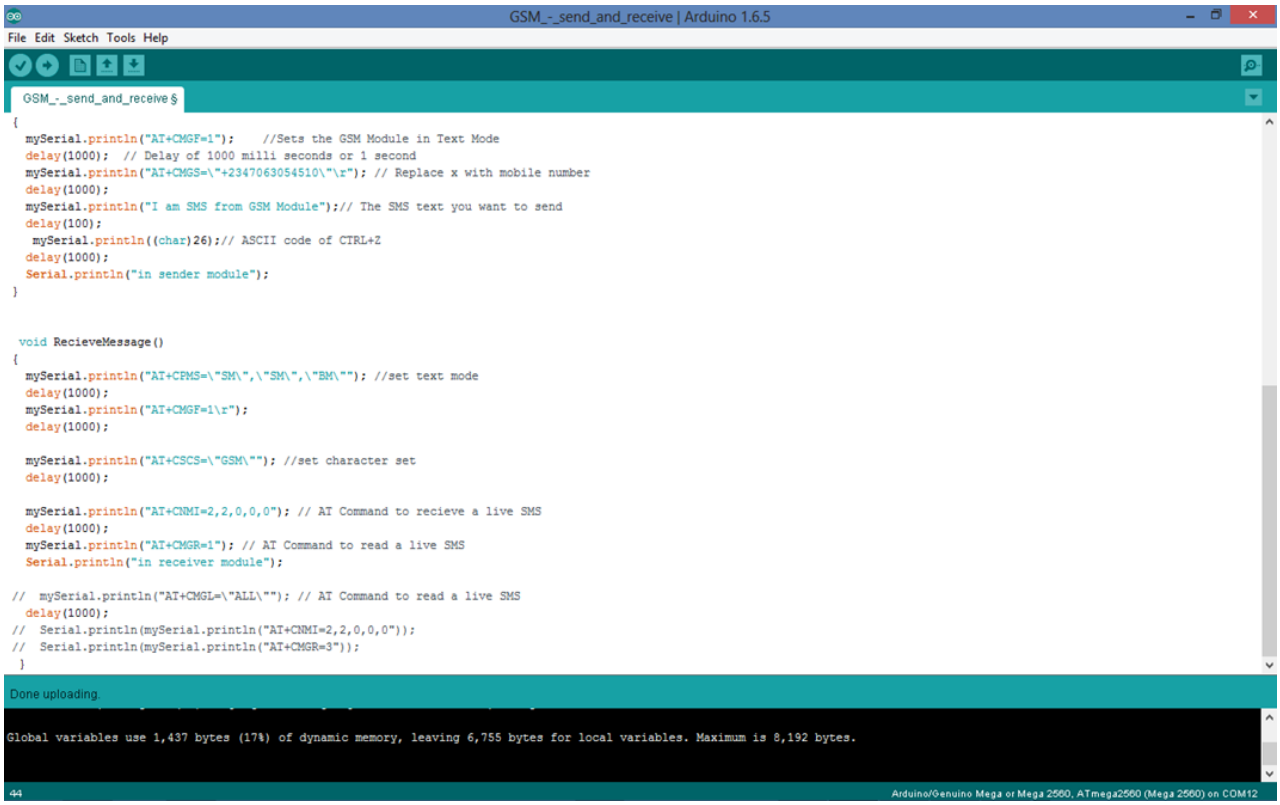

Figure 3: SMS sending and receiving code snippet for the communication between the microcontroller and the GSM module

Mobile Application Software Implementation: The mobile application developed in this paper was an Android application, which was written with Android Studio and the Java programming language. There were two types of the mobile application developed for the system. One was an Administrator application, while the other was a User application. The Administrator application was proposed to be used by the main owner of the home (for example, a father, mother, or guardian of the home). This had all functionality that could be performed by the system. While the User application was proposed to be used by the other occupants of the home (for example, the children or relations living in such homes).

The Administrator application had the following features:

- Receive intrusion alert from the security system.
- Add new users to the security system.
- Remove users from the security system.
- Activate the security system.
- Deactivate the security system.
- Assign permissions to the users.
- Revoke permissions from the users.
- View activity logs in the system.

The User application had the following features:

- Receive intrusion alert from the security system if assigned the permission by the administrator.
- Activate the security system if assigned the permission by the administrator.
- Deactivate the security system if assigned the permission by the administrator.

Three key permissions of Receive Message, Activate System, and Deactivate System were built into the application and could be assigned only by the administrator to the other users. Receive Message gave users the ability to receive an intrusion alert from the home security system, Activate System gave users the ability to turn on the system, Deactivate System gave users the ability to turn off the system. In addition, a database, SQLite, was used alongside the Android application, to store pertinent information required for the operationalization of the system (such as the users' details added by the administrator via the administrator app). The code snippet in Figure 4 shows some code logic written on the Android Studio IDE for receiving SMS from the GSM module.

```
package com.example.s0a.sms;

import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.telephony.SmsMessage;
import android.util.Log;
import android.widget.Toast;

/**
 * Created by £S£0$A on 24/12/2015.
 */
public class SMSReceiver extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent) {
        //---get the SMS message passed in---
        Bundle bundle = intent.getExtras();
        SmsMessage[] msgs = null;
        String str = "SMS from ";
        if (bundle != null)
        {
//---retrieve the SMS message received---
            Object[] pdus = (Object[]) bundle.get("pdus");
            msgs = new SmsMessage[pdus.length];
            for (int i=0; i<msgs.length; i++){
                msgs[i] = SmsMessage.createFromPdu((byte[])pdus[i]);
                if (i==0) {
                    //---get the sender address/phone number---
                    str += msgs[i].getOriginatingAddress();
                    str += ": ";
                }
//---get the message body---
                str += msgs[i].getMessageBody().toString();

            }
```

Figure 4: SMS receiving code snippet for the communication between the Android application and the home security system

4. Results and Discussion

The results from the implementation of the hardware security system and the mobile application software are presented here where snapshots are provided to illustrate this process. For the mobile application, the results shown are based on the administrator application, as that had all the functionality of the mobile application.

Figure 5 shows the final outcome of the home security hardware system with all the sensors and hardware components connected to the Arduino ATmega2560 microcontroller.

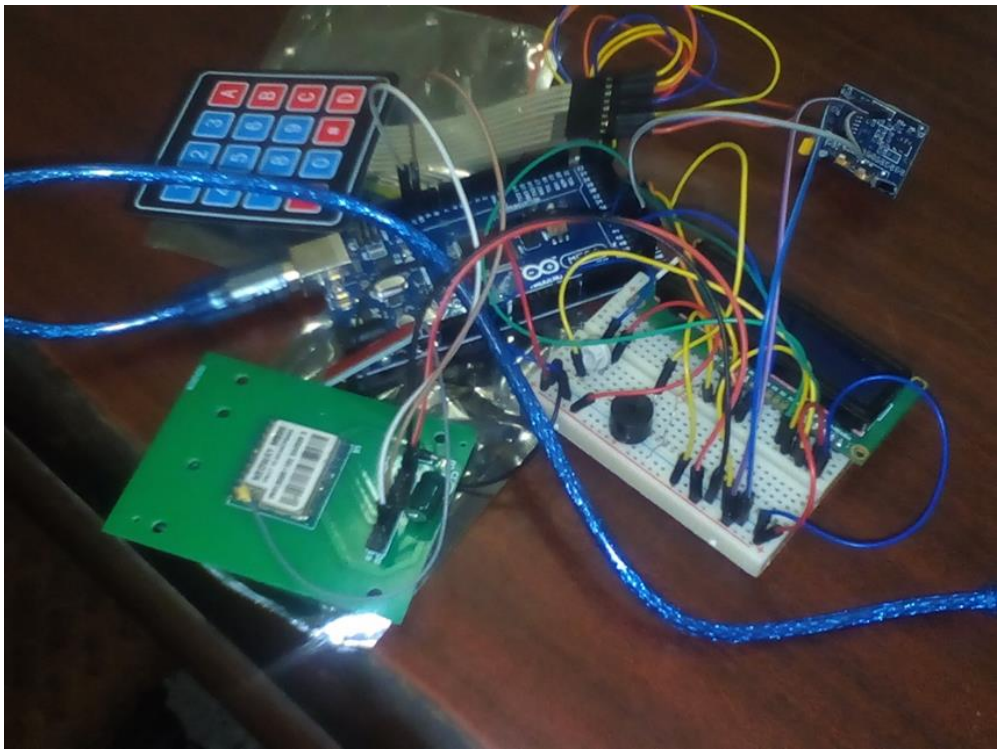

Figure 5: Final outcome of the home security system

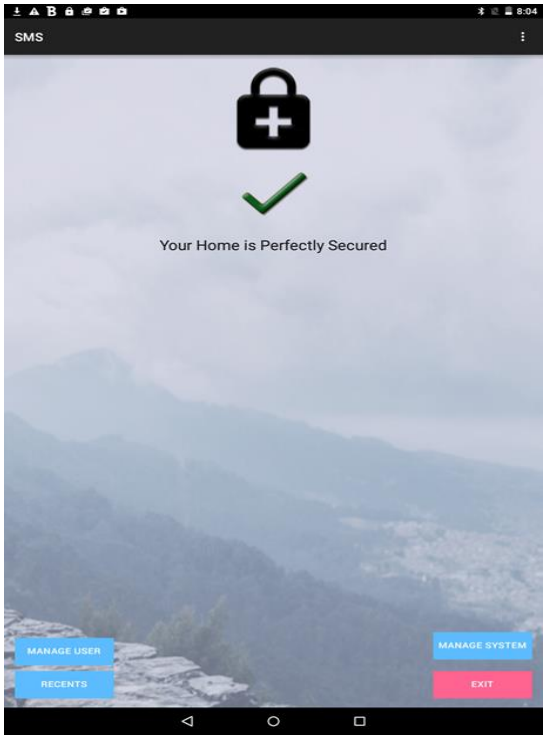

Figure 6: Dashboard of the mobile application

Figure 6 shows the main dashboard of the Android application, with menus for managing users, managing the system, viewing recent activity logs, and exiting the system.

Figure 7 shows the screen for managing users. Three key functionalities of adding users, managing their permissions, and viewing all users could further be performed on this screen. As has been established, three key permissions were built into the system, namely, Receive Message, Activate System, and Deactivate System. These permissions governed what could be done on the security system by the users who were assigned such permissions. Figure 8 further shows the screen for viewing users and their permissions.

Figure 7: Manage users screen of the mobile application

Figure 9 shows the screen for managing the system. This involved turning on or off the security system, depending on whether such a user had been assigned such permissions. This was a crucial aspect of the system as anyone assigned such permissions could turn on, off, or carry out both actions on the system, depending on the assigned permissions.

Figure 8: View users screen of the mobile application

Figure 9: Manage system screen of the mobile application

As has been established, SMS was used as the underlying network infrastructure between the hardware security system and the mobile application software. Whenever there was an intrusion detected by the PIR sensor on the hardware security system, the GSM module sent an SMS to the administrator application and the other users who had the permissions to receive intrusion alerts from the security system. When the mobile application software detected that SMS from the security system, it was able to sound a warning alarm, to immediately alert the homeowner to take action. This was effective in abating any form of burglary that might happen in a home whenever the homeowner was not around. Also, the administrator application and the other users who had the permissions to control the system could turn on or off the entire security system. This was in a bid to give users the ability to fully control the system. The ability to turn off the security system was especially useful to prevent the security system from detecting the homeowner's motion, as a burglary attempt. For example, whenever the homeowner was returning home, he or she could turn off the home security system just before getting home to avoid an intrusion detection by the PIR sensor. These two communication patterns fostered the mobile home security system proposed in this paper.

5. Conclusion

The security of homes is indispensable, as the illegal entry of burglars or other nefarious entities could lead to the undesirable loss of properties. It was established in this paper that the proliferation of smartphones and technological advancement have provided the basis for developing security systems capable of effectively securing homes. Hence, we proposed a low-cost, highly configurable, and mobile home security system to secure homes from the intrusion of burglars and other illegal entities attempting to gain illegal entry. This system ensured that homeowners could effectively secure their homes from their smartphones, via a mobile application developed to interact with the home security system. The hardware of the home security system was built with an Arduino ATmega2560 microcontroller, a PIR sensor to sense an intrusion, a buzzer to sound an alarm when there was an intrusion, an LCD screen, a 4x4 matrix keypad, and a GSM module to send an SMS to the homeowner's phone when there was an intrusion. The software of the home security was built with the Java programming language, for the Android platform. These two aspects of the system worked together in achieving the main objective of this research.

6. Limitation

This research takes the approach of utilizing SMS as the medium of communication between the hardware security system and the mobile application software. This gives a crucial advantage of simplicity and cost minimization with respect to leveraging a more complex and expensive communication medium such as the Internet. However, it poses a downside, as SMS network must be present before the system can be effectively used. It must therefore be taken into cognizance that wherever it will be implemented and used, the underlying network infrastructure required for SMS to work must be present.

7. Recommendations

Building a home security system is a huge and expensive undertaking. The home is a vast and dynamic

environment. In this research paper, a simple mobile home security system was designed and implemented, capable of securing homes from the illegal intrusion of burglars, while ensuring cost minimization. The following recommendations should therefore be taken into consideration:

- This research can firstly be implemented in its current state, after which, more sensors such as fire sensors, gas leakage sensors, and other pertinent sensors, could be added, to ensure a home that is secured from the external threat of illegal intrusion, as well as internal threats of fire, gas leakages and other home-related disasters
- Constant routine maintenance of the hardware components, most especially the PIR sensor, to ensure the accuracy of its sensitivity is recommended.
- Finally, it is recommended that whenever there is an update to the mobile application, the homeowners should install such updates as soon as possible, to ensure the stability and security of the mobile application that controls the entire home security system.

References

[1]. PM News, "Jonathan spent $32bn on security, Nigeria still not safe, says APC," 2014. [Online]. Available: https://www.pmnewsnigeria.com/2014/11/16/jonathan-spent-32bn-on-security-nigeria-still-not-safe-says-apc/. [Accessed 07 August 2020].

[2]. Federal Bureau of Investigation, "FBI - Crime Clock," 2018. [Online]. Available: https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/crime-clock. [Accessed 27 July 2020].

[3]. P. E. Oguntunde, O. O. Ojo, H. I. Okagbue and O. A. Oguntunde, "Analysis of selected crime data in Nigeria," Data in Brief, vol. 19, pp. 1242-1249, 2018.

[4]. N. Sriskanthan, F. Tan and A. Karande, "Bluetooth based home automation system," Microprocessors and Microsystems, vol. 26, no. 6, pp. 281-289, 2002.

[5]. B. Choudhury, T. S. Choudhury, A. Pramanik, W. Arif and J. Mehedi, "Design and implementation of an SMS based home security system," in 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2015.

[6]. M. A. B. Sarijari, R. A. Rashid, M. R. A. Rahim and N. H. Mahalin, "Wireless Home Security and Automation System Utilizing ZigBee based Multi-hop Communication," in 2008 6th National Conference on Telecommunication Technologies and 2008 2nd Malaysia Conference on Photonics, Putrajaya, 2008.

[7]. M. S. Islam, "Home security system based on PIC18F452 microcontroller," in IEEE International Conference on Electro/Information Technology, Milwaukee, 2014.

[8]. A. ElShafee and K. A. Hamed, "Design and Implementation of a WiFi Based Home Automation System," International Journal of Computer and Information Engineering, vol. 6, no. 8, pp. 1074-1080, 2012.

[9]. O. Sam, "Numbering System," in Intel x86 Microprocessor Assembly Language Programming, Lagos, Lagos: Mic 'N' Dell Ventures, 2014, pp. 1-2.