ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 6, Issue 1, 067-075

An Internet of Things (IoT) Based Neighbourhood Distress Alert System

Wilson Chukwuemeka AHIARA, Chukwugoziem IHEKWEABA

Department of Computer Engineering, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria.
ahiara.wilson@mouau.edu.ng/Ihekweaba.gozie@mouau.edu.ng

Corresponding Author: ahiara.wilson@mouau.edu.ng, +2348039207982

Date Submitted: 16/04/2023
Date Accepted: 25/06/2023
Date Published: 28/06/2023

Abstract. *To acquiesce to the increase in territorial invasion of communities by hoodlums, bandits and kidnappers every day, some communities have resorted to engage the services of security agents or guards to watch over and alert them in the case of any security breach. However, the neighbourhood s found in some locations especially, in the rural areas impact on the cost of employing guards, and the consequent disagreement amongst residents in the neighbourhood security meeting. This paper proposes an Internet of Things (IoT) based system for alerting residents in a neighbourhood as well as reporting the actual location of a particular neighbour in distress. To achieve this, a hardware system based on NodeMCU with built-in Wi-Fi chip for internet routing is designed. Communication is established remotely between the hardware system and the cloud through the server Application Programming Interface (API) that utilizes cloud resources such as Short Message Service (SMS) gateway and Google map API to craft SMS and fetch location coordinate from Google map Uniform Resource Location (URL) respectively. This piece of information is then displayed on the Liquid Crystal Display (LCD) device on users' machine and mobile phones in real time for notification. The test carried out shows that the developed system is reliable and affordable for use in a neighbourhood.*

Keywords: *Alert system, internet of things (IoT), microcontroller, neighbourhood*

1. INTRODUCTION

Security has become a source of worry to any society or country wishing to live in peace and harmony. And so has become everyone's business and *ipso facto* should not be seen as the sole responsibility of the security agents.

In view of this, Rogers in his study, [1] has defined security as the measure taken to protect or prevent people or property from potential harm. Thus, any aberration or negligence to take precautionary measures to tackle the menace of insecurity would spell doom for any country or her citizenry.

Recent happenings have revealed how some vulnerable neighbourhoods have unprecedentedly had criminal elements and brazen hoodlums wilfully invade their territories mostly at night to unleash mayhem. This, in consequence, has left myriad persons brutalized, raped, killed, and rendered homeless. Even the few residents who are yet to be attacked, for fear, have scampered for safety to other neighbourhoods.

Due to these abnormalities, some communities are compelled to either resort to engaging the services of security agents, forming vigilante groups, or engaging untrained local guards with unsophisticated weapons in the neighbourhood to alert people should there be such security breach.

A matching strength to combat and withstand this callous act of these hoodlums would be a collective or collaborative community effort through a notification system that is affordable while keeping residents heads up of burglary. To that effect, [2] employs security cameras to monitor intruders' movements and location around the home, this requires high maintenance capability due to its inherent large storage capacity demands and constant power supply for effective functionality; not many in the neighbourhood can afford this system.

A microcontroller based Global System for Mobile communication (GSM) alert distress system that sends a distress message through a Short Message Service (SMS) to the security officials, as well as registered emergency contacts of the person in danger along with the location of the attack was proposed in **[3]**. This system was implemented using Arduino microcontroller, Global Positioning System (GPS) module, GSM interface and an alert button. A notification is sent on emergency by pressing a button. Modifications can be made to include a hardware or server authentication mechanism to avoid triggering false alarm by careless press on the alert button. Besides, when the system is placed indoors, the GPS module is limited in functionality due to interference from the terrestrial satellite, as well as other communication systems.

The study in [4] proposed a Global System for Mobile communication (GSM) based remote home monitoring model with Passive Infrared (PIR) sensor integration which monitors human presence or motion across the door where it is electrically connected to. On intrusion or security breach, the model alarms the house owner's predefined number through the GSM modem holding the Subscriber Identity Module (SIM). The system is very commendable. However, modification can be made to avoid getting false alarm or notifications as animals or visitors could get in the way of the system to get it triggered.

An Internet of Things (IoT) based smart home security system that makes use of Passive Infrared (PIR) and gas sensors to guard a home against intruder and gas leakage or fire outbreak was proposed in [5]. The authors opined that the system also handles home automation by remotely turning off fan and light bulb through Short Message Service (SMS) sent through the developed application on their phones. This, they achieved using Arduino Uno, ESP8266 WiFi module interface. Although the work appears feasible, there was no experimental analysis or result in display to validate their design.

A security system for smart home that is based on GSM technology was designed in [6]. The paper proposes two approaches for the design: First it deploys the use of web camera to monitor motion across and then alerts owner through a sounding buzzer and a mail. While the second approach uses General Package Radio Service (GPRS) module to alert the owner through an SMS. The central processing device used to interface other sensors is the Atmega644p microcontroller.

A versatile and home security system using a Global System for Mobile communication (GSM) module to send alert message, a Bluetooth activated door code locks through a mobile phone and a keypad for the same door locks was presented in [7]. They integrated a Passive Infrared (PIR) sensor for detecting intruder motion and then a Radiofrequency (RF) transceiver for initiating a buzzer alarm to people outside the home. All or any of these security measures can only be instantiated when consecutive attempts or access is denied. The multilayer security measures adopted in this system makes it robust and good. Unfortunately, it only focuses on the security at home when the user is away from home. Even the use of RF is only effective for short distance (200 meters maximum) within a community.

Thus, these and some other perceived problems ranging from the high cost of engaging the services of trained guards, the nonchalant attitudes or delay of the security agents in responding to crimes, and the contemplation on the number of guards required to man the labyrinth of streets found mostly in the rural and some suburban areas, have often led to an imbroglio in the community making her susceptible to attack. In view of these, this paper proposes an Internet of Things (IoT) based neighbourhood distress alert system for sending multiple alerts: Triggering a buzzer, sending an SMS plus location identification for online access or display on mobile phones, and LCD devices in real time.

2. MATERIALS AND METHODS

2.1 Materials

The materials used in achieving this design are grouped into two broad categories: hardware tools and software development tools. The hardware devices consist of the piezoelectric buzzer, Liquid Crystal Display (LCD), 4X4 keypad, piezoelectric buzzer, pushbutton, Light Emitting Diodes (LED) and NodeMCU Microcontroller as shown in Figure 1. While the software development tools include: Node.js, Hypertext Mark-up Language (HTML), JavaScript, and MongoDB data base.

1) The Hardware Components

The hardware devices integrated to develop the system are discussed as follows:

a) NodeMCU

The NodeMCU is an open source IoT platform that contains Lua firmware which runs on the ESP8266 Wi-Fi System on a Chip (SoC) developed by Espressif Systems and the hardware is based on the ESP-12 module with Transmission Control Protocol/Internet Protocol (TCP/IP). The ESP8266 Integrates 802.11b/g/n Wi-Fi transceiver**,** enabling it to not only connect to a Wi-Fi network but also interact with the Internet, and to as well as set up a network of its own, allowing other devices to connect directly to it. This makes the ESP8266 NodeMCU even more versatile.

b) Liquid Crystal Display (LCD)

The Liquid Crystal Display (LCD) is a programmable output device for displaying alphanumeric text. Hence, it is mostly preferred over multi-segment light emitting diodes and seven segment display. In this work, the 16 x2 display screen size, HD44780 controller LCD is used for displaying the resident’s name, mobile number, and address under distress.

c) Keypad

A 4x4 keypad has been chosen for this design so that users can input their unique passwords into the system before pressing the pushbutton (alert button) to alert residents when under attack. This keypad interface to the microcontroller makes it difficult for unauthorized users or children to slip their fingers on the alert button to send signals or raise alarm without first being validated or authenticated; therefore reducing the chances of raising false alarms.

d) Piezoelectric buzzer

A piezoelectric buzzer is an electronic device that uses the piezoelectric effect for generating sound. The choice of this device is based on its high tone production, low cost and low power consumption.

e) Pushbutton

The pushbuttons (also known as alert button) are typically switches that make and break contacts. Buttons are typically made out of hard material, usually plastic or metal [8]. In this work it serves as the alert button and often triggered by a depression.

f) **Light Emitting Diodes (LED)**

The Light Emitting Diodes are output devices for indicating the status of a circuit. In this design, two LEDs have been used; the first LED indicates the low battery status and the second LED indicates the battery status when fully charged.

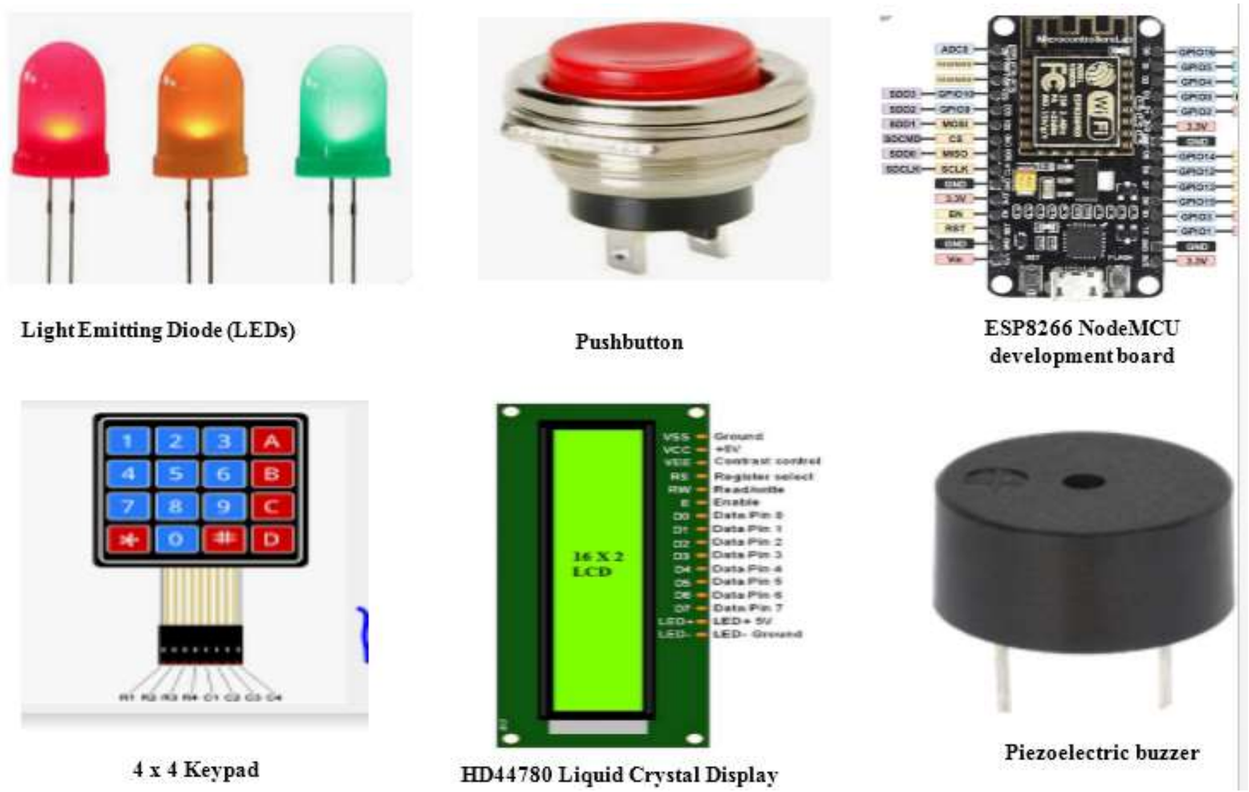

Figure 1: Hardware components

Table 1: Bill of materials (BOM) Cost

COMPONENTS	UNIT QUANTITY	PRICE(₦)
NodeMCU	1	4000
Resistor	6	60
Variable Resistor	2	60
Capacitor	1	200
Transformer	1	300
Rectifying Diodes	4	200
Light Emitting Diodes	2	40
Liquid Crystal Display	1	1000
4 x 4 Keypad	1	1000
Packaging Box(or casing)	1	700
LM338 IC	1	800
Dotted Vero board	1	400
Jumper wire	1 Yard	300
SMS Gateway (Nigeria Bulk SMS API)	100 Text messages	400
Map Service (Google Map API)	100 Maploads or requests	600
Total		**10,060**

2) Software development tools

The software development tools used in this work are discussed as follows:

a) **MongoDB:** is an open source non-relational database management program with support for large data storage.
b) **Hypertext Mark-up Language (HTML):** Since the proposed system consists of a web-based platform for tasks such as data acquisition and registration, the HTML was chosen as a result of the fact that it is a standard mark-up

language for creating web pages and web applications. Web browsers receive HTML documents from a web server or from local storage and render them into multimedia web pages.

c) **Node.js**: It is an open-source, cross-platform JavaScript runtime environment and library for running web applications outside the client's browser [9]. In this work, the Node.js is used for every server side functionality such as sending Short Message Service (SMS), making request to get the location Uniform Resource Location (URL), storing, and retrieving data on and from the database.

d) **JavaScript:** To achieve the client-side execution of tasks in the web application of the remote data processing and retrieval, JavaScript was chosen. It is used alongside with HTML and Cascading Style Sheet (CSS) to control some logical operations on the client side.

3) Cost Implication of System Development

The cost of materials used as at the time of system design and development is depicted in Table 1.

2.2 Proposed Method

The proposed method contains a NodeMCU microcontroller with built-in Esp8266 Wi-Fi router for cloud computing and data processing; a Liquid Crystal Display (LCD) for displaying information of user under attack; a pushbutton which is only triggered after the user inputs their password through a keypad interface to avoid raising false alarm and a piezoelectric buzzer that sounds alarm to notify the user. The block diagram in figure 2 depicts the components interface to the microcontroller.

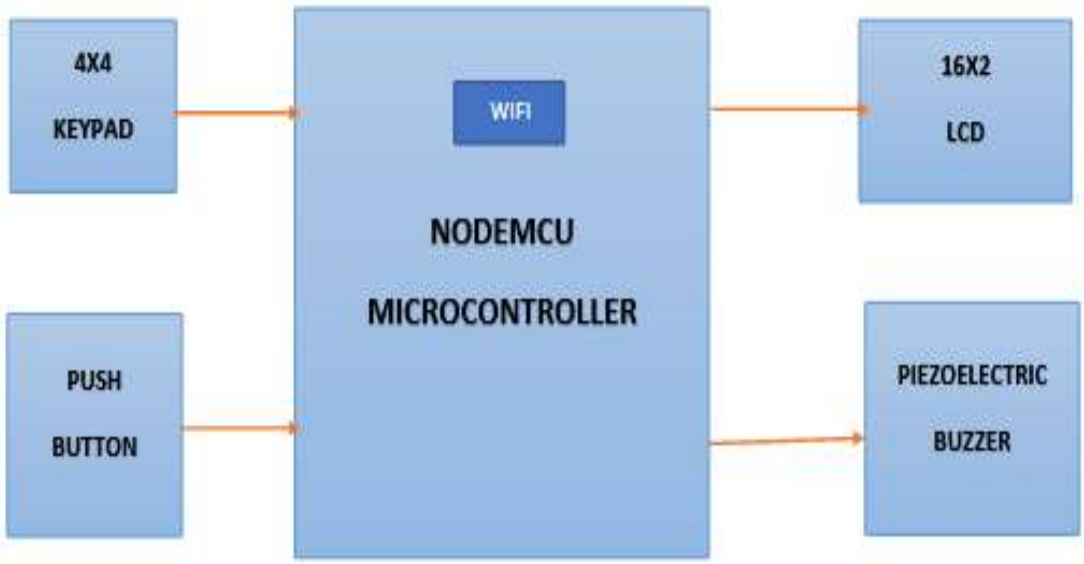

Figure 2: System block diagram

1) System schematic

Figure 3 shows the system circuit schematic containing various hardware components interface with the NodeMCU to form unit integration. It also has a regulated battery-powered supply voltage and a switch for energy conservation.

2) Mode of Operation

To achieve functionality as shown in figure4, both the hardware and software components form a unit integration. First, all the hardware components are initialized; the hardware system is connected to the remote server through the on-board Wi-Fi Esp8266 chip on the NodeMCU microcontroller. As a user under attack presses a button, an alarm is raised after entering their password correctly through the keypad interface on the system. If a user enters a wrong password, he is prompted to try again for a maximum of 3 times, and if the password is still wrong on the third attempt, the system is blocked. The password authentication and validation is done on the remote server Application Programming Interface (API) to identify the machine token. So on pressing the alert button the API makes request to fetch unique user predefined data and Google map generated link stored on the data base record during registration process.

It is only on passing validation that the Google map Uniform Resource Location (URL) link for location address or coordinate is then attached on the crafted Short Message Service (SMS) and sent for display on mobile phones and Liquid Crystal Display (LCD) screens of the users' or residents' machine in the neighbourhood. The display message is also accompanied with a resounding alarm from the piezoelectric buzzer on the machine to get users on the alert.

Also, for the LCD message display capability on the hardware system, the machine is programmed to listen through a loop for record update or changes on the database. The Google map API key was loaded from https://cloud.google.com [10].

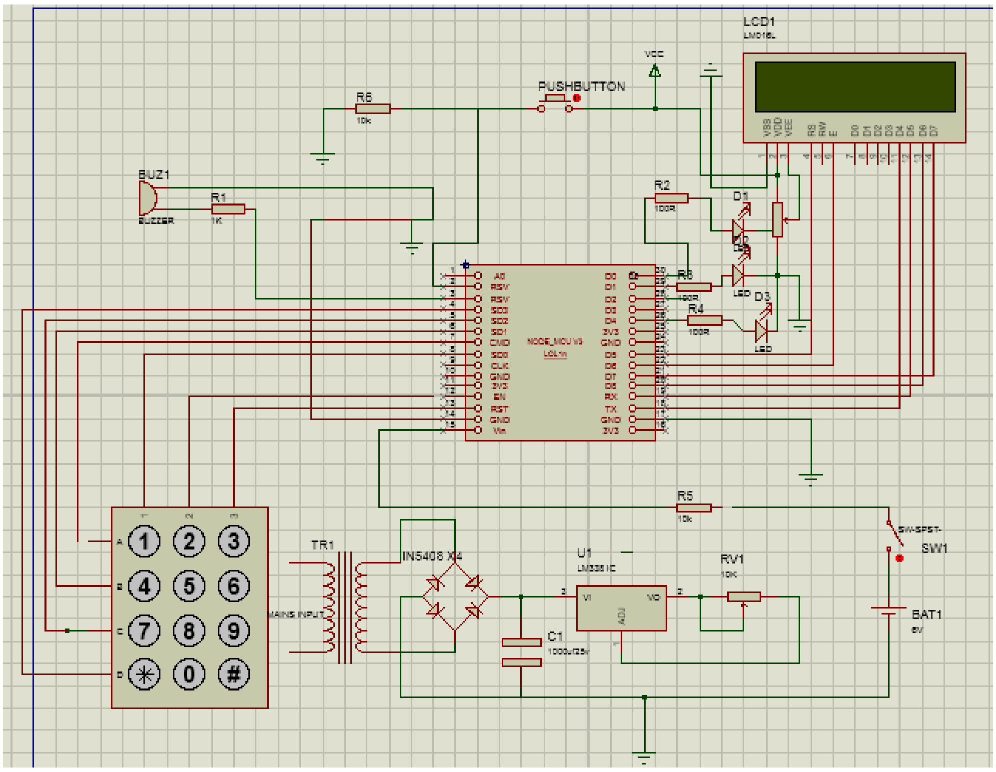

Figure 3: System circuit schematic

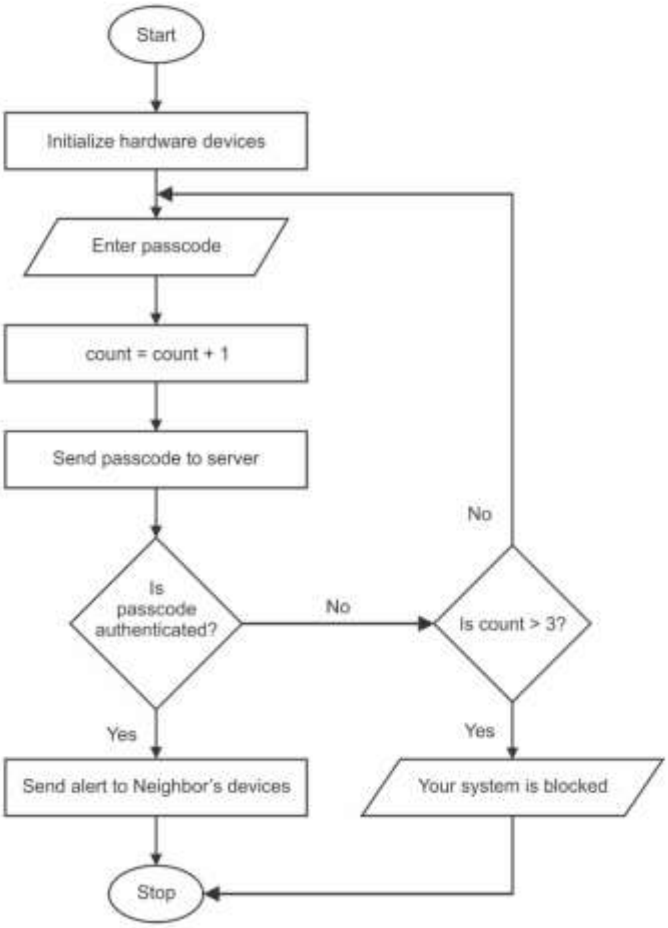

Figure 4: Flow chart description of the proposed system

3. RESULTS AND DISCUSSIONS

3.1 Implementation and Testing

1) Web application

The web application is developed using JavaScript programming language which serves as a platform for virtual quick response to an embattled resident and data repertoire using MongoDB database. The web application also provides an optimized Application Programming Interface (API) that allows the hardware system to communicate with the server.

2) Client registration page

The client registration page is an online form that records the user's data resident in a community so that the data can be stored and processed for later retrieval in case of emergency. Figure 5 shows the user or client registration page. One of the text fields contains a User Unique Identity (UUID) which is by default automatically assigned to users.

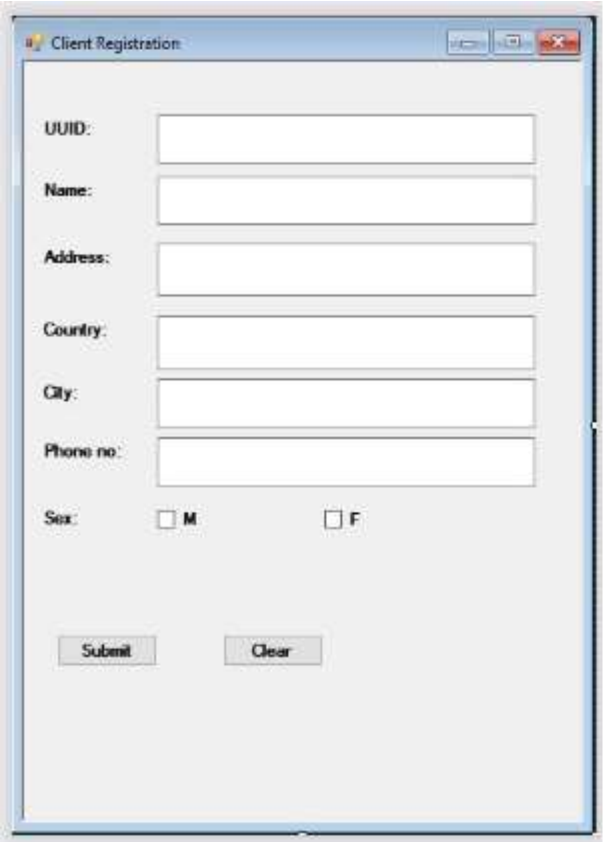

Figure 5: Snapshot of user registration page

3) Google map

The Google Map (GM) data obtained from cloud is deployed on the web application with the help of Google Map Application Interface(API).The API automatically controls access to GM servers. Figure 6 shows the location on Google Map obtained in Ward 3 community, Umuahia North Local Government Area of Abia State with labyrinth of streets during the testing phase of this work.

Again, Table 2 contains some extracts of the residents' information capture during the testing operations carried out in different locations of the neighbourhood.

Table 2: Ward 3 neighbourhood captured data

S/n	Uuid	Name	Phone n0.	Location
1	20	Emeka Elijah	07061225025	Lat.(5.54),Long.(7.49)
2	21	Peter Imoh	09083755505	Lat.(5.54),Long.(7.49)
3	22	Tunde Ayodele	07064672406	Lat.(5.53),Long.(7.49)
4	23	Nelson Nnamdi	08030408397	Lat.(5.54),Long.(7.49)

From this same test, some irregularities were observed in the delivery of the Short Messaging Service (SMS) as shown in Table 3. Despite this, it can be deduced that the success probability of SMS delivery is approximately 75 percent, taking into account some unavoidable data transmission issues like weak network and switched-off phones.

Table 3: SMS Delivery rate

SN	Successful Delivery	Failed Delivery	Success rate
1	3	1	0.75
2	4	0	1
3	2	2	0.5

4) Short messages service (SMS)

To reduce hardware complexity and cost of implementation of the system, no Global System for Mobile Communication (GSM)/General Packet Radio Service (GPRS) module was interfaced to the system. Rather an online Short Message Service (SMS) gateway was deployed to alert users in the community through a display on their system's Liquid Crystal Display (LCD) and mobile phones. A distinct feature of this design is the attachment of a link with the SMS so that users can access the location or address of the neighbourhood or person in distress.by using Google map on their phones as shown in Figure 7.

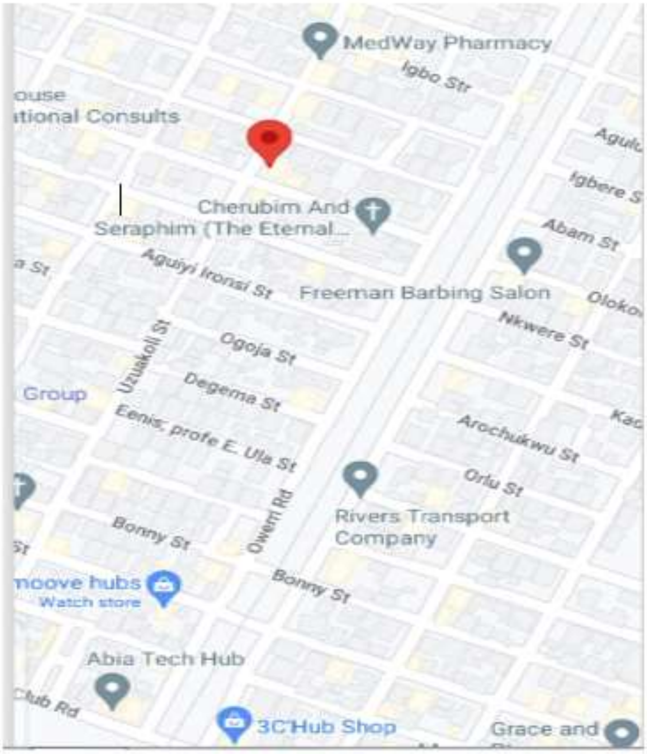

Figure 6: Google map location of the building in distress

Figure 7: Snapshot of a mobile phone message alert with location hyperlink

5) Completed Hardware System Display

Figure 8 shows the system display when a user enters a wrong passcode. This display comes out when the number of failed attempt is less than 4. As explained earlier, there is a maximum number of 3 attempts when entering the system passcode. If this maximum number is exhausted, the system displays a message with the text "You've have been blocked" which require the user to consult the administrator to unblock the system. On the other hand, figure 9 depicts a system display when the passcode is successfully verified and message alert is then delivered to neighbours.

Figure 8: Wrong passcode supply display

Figure 9: Correct passcode supply display

4. CONCLUSION

The paper proposed and implemented an IoT based neighbourhood alert system using fewer components to achieve the desired functionality and affordability.

The proposed system leveraged on cloud resources as a preference over a message-alert hardware device, like the GSM module, and the location-identification hardware device (GPS module) to reduce components count while mitigating the defects associated with the use of a GPS hardware device against the impact of indoors terrestrial satellite interference and other communication systems.

From the system design and implementation, it can be inferred that the use of a self-contained NodeMCU with internet capability was indeed pivotal in the development of this system as it allows for multiple alert to improve notification within and outside the neighbourhood. Thus, this system is functionally reliable and cost effective.

ACKNOWLEDGMENT

We wish to thank the staff of Computer Engineering department and our reputable institution, Michael Okpara University of Agriculture Umudike (MOUAU}, for her unalloyed support towards the completion of this work.

REFERENCES

[1]. Rogers, P. (2010). Losing Control: global security in the first century (3rd Ed.). London: Pluto Press ISBN 9780745329376
[2]. Gibilisco, S. (2001). The Illustrated Dictionary of Electronics. 8th ed. New York: McGraw Hill
[3]. Olanuyan, O.U., Ogudu, U.C. & Subair, J.A. (2021). Implementation of a Microcontroller Based GSM Alert Distress System. LAUTECH Journal of Computing and Informatics (LAUJCI)-ISSN: 2714-4194 volume2, issue1; www.laujci.lautech.edu.ng
[4]. Vignesh, S., Ramya, G. & Morrisha, R. (2021). Implementation of GSM Based Remote Home Monitoring Model. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS). Volume: 3 Issue 3 e-ISSN2582-5208
[5]. Durgashree, K. & Sreepathin, B. (2018). IoT Based Smart Home Security System. International Journal of Engineering Research in Computer Science and Engineering (IJERSCE) Vol. 5, No.4, ISSN (online) 2394-2320.
[6]. Jayashri, B. & Arvind, S. (2013). Design and Implementation of Security System for Smart Home based on GSM technology. International Journal of Smart Home. Vol.7, No.6, pp.201- 208. http://dx.doi.org/10.14257/ijsh.2013.7.6.19

[7]. Khalid, H. J., Niaz, M., Rahman, M.K., Shahjahan, A., Himanghu, K G. (2017). Development of a Versatile and Intelligent Home Security System. IJ. Engineering and Manufacturing (IJEM), MECS. Vol. 4, No.6, pp. 60-72.
[8]. Rachel, P. (2018). Power Button: A History of Pleasure, Panic and the Politics of Pushing, MIT Press, ISBN 9780262038232, reviewed in David Trotter, "Making doorbells ring", *London Review of Books 22 November 2018*
[9]. Taha, S. (2023). What is Node.js: A Comprehensive Guide. Available online At: https://www.simplilearn.com/tutorials/Nodejs-tutorial/what-is-nodejs
[10]. Ahsan, A. (2023). Build Faster with a New Optimized Solutions and Step-Step-Guidance. Available online at https://cloud.google.com/blog/products/maps-platform/build-faster-new-optimized-solutions-and-step-step-guidance.Accessed February 15, 2023.