Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 10 ~ Issue 1 (2024) pp: 38-44
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Design and Implementation of a Wireless Network Smart Campus System

[1]Ayeni, M. O.
Electrical Engineering Department, The Polytechnic, Ibadan, Nigeria

[2]Adejumobi, O. K.
Computer Engineering Department, The Polytechnic, Ibadan, Nigeria

ABSTRACT
This paper presents, 'Designand Implementation of a Wireless Network Smart Campus System' aimed at augmenting safety measures and operational efficiency at The Polytechnic, Ibadan, Oyo State, Nigeria. The system integrates a variety of sensors (motion and flame/fire), which are strategically deployed to capture real-time data such as intrusion and smoke or fire incidents. The collected data are transmitted wirelessly to the Nodes namely; the Office, Fixed (security Post), and Mobile, as text messages for prompt actions. The primary objectives of this study include enhancing campus security, optimizing infrastructure protection, and providing a responsive emergency management framework.The model is capable of monitoring selected offices and areas on the campus against intruders and fire outbreaks. The alarm system is also activated to alert nearby people for necessary action. The office owners can also contact the Central Monitoring Unit (CMU) with one button click. This action will automatically inform the security personnel of prompt action. It should be noted that all selected locations are already pre-registered on the CMU and the Mobile Security Patrol Unit for easy identification of affected areas. In conclusion, it is recommended that more areas be captured and smart cameras be embedded in the design to capture images of intruders.

KEYWORDS: *Wireless Network, Smart Campus Technology, Sensors, Central Monitoring Unit and Mobile Security Patrol Unit*

***R**eceived 28 Jan., 2024; **R**evised 08 Feb., 2024; **A**ccepted 10 Feb., 2024 © The author(s) 2024.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

In today's world of higher education, integrating cutting-edge technologies has become essential to creating productive and safe campus environments. Among these technical paradigms, the Wireless Network Smart Campus System has attracted a lot of interest. Intelligent monitoring systems specifically designed for educational environments have been made possible by the growing ubiquity of wireless connectivity, Internet of Things (IoT) sensors, and smart device prevalence. By providing institutions with real-time insights, these solutions enable them to optimize numerous operational aspects, guarantee the well-being of the campus community, and manage resources proactively.Over time, the concept of a smart campus system has changed to meet the ever-changing demands of educational institutions as well as the ever-changing technological world. Closed-circuit television (CCTV) cameras and basic sensors were first added to traditional security systems. However, the emergence of IoT and wireless networks has made it possible to develop increasingly complex, networked, and data-driven monitoring systems.A strong wireless network infrastructure is essential to a smart campus system's efficacy. The campus is home to a multitude of sensors and gadgets that communicate with one another more easily when connected via wireless technology. This infrastructure makes it possible to gather and transmit data in real time, which promotes an adaptable and linked ecosystem.Studies show that adding wireless networks to smart campus systems improves their cost-effectiveness, scalability, and adaptability [1]. These networks provide the framework for the integration of various sensors, such as security cameras and environmental monitoring equipment, forming an intelligent mesh that continuously gathers and processes data.The widespread adoption of sensor technology is a crucial component of campus monitoring systems with intelligence. Numerous sensors, including sound, motion, and environmental detectors, add to the thorough observation of events and circumstances on campus. Decision-makers can take immediate action based on the

real-time processing of the data gathered by these sensors.Research has shown that sensor integration is crucial for efficient campus security, as it plays a part in guaranteeing safety as well as efficient use of resources and promotion of environmentally friendly behaviours [2].Advanced analytics are required for meaningful interpretation due to the massive amount of data generated by smart campus systems. Finding patterns, anomalies, and trends through the integration of machine learning algorithms and data analytics tools facilitates the process of making well-informed decisions.Researchers have investigated how machine learning approaches may be used to analyze data from smart campus devices, showing that these techniques can be effective in both minimizing energy use and anticipating and averting security issues [3].Advances in wireless networks and electronic devices give rise to the development of low-power sensors and the deployment of large-scale wireless sensor networks. With the abilities of pervasive monitoring, sensor networks have attracted important attention in many application areas, such as object tracking, environment monitoring, military, habitat monitoring, smart environments, and disaster management [4]. The main purpose of sensor networks is to collect the monitoring raw data and provide basic information and decision support for the base station [5]. Wireless sensor technology makes life easy and interacts with the physical environment. Soon, tiny and dirt-cheap sensors can be orderly deployed into the roads or machines, creating a digital output that senses a variety of physical events, and detects forest architecture to help rapid emergency response [6]. The surveillance of homes or industrial places through sensors and the prevention of problems via prediction is of vital importance for the safety of these areas. This paper shows how to increase wireless sensor network (WSN) techniques by composing new design methods and improving low-cost industrial and home safety systems. To guarantee and present accurate solutions to the system, not only temperature and humidity sensors but also flame and gas sensors were used in this study [7]. Security has been defined as precautions to guard against crime, attack, sabotage, espionage, etc. [8]. The alarming crime rate in various homes and offices around the globe has necessitated the installation of surveillance security systems in most establishments. Security threats ranging from armed robbery, kidnapping, and recent bomb blasts have kept the entire region on their toes to the extent that no one can be sure of his/her security in the next moment. Surveillance is the systematic investigation or monitoring of the actions or communications of one or more persons in a place [9].

II. METHODOLOGY

The research is divided into Hardware and Software Sections.
The Hardware comprises of:

1. **Nodes**

a. Office Node: The node is comprised of a smoke sensor, a motion sensor, a microcontroller, a radio, and an energy source.

b.Mobile Nodes (Security Personnel): The mobile node can be installed in the Patrol vehicle or a piece of handheld equipment to be held by the security personnel. The node is comprised of buttons, a GPS module, a display module, a buzzer, a microcontroller, a radio, and an energy source

c. Security Post node: This node will be installed at the Security Posts within the campus. This node comprises of keypad, a display module, a buzzer, a microcontroller, a radio, and an energy source

2. Two Repeaters with Sub-Control/Monitoring Unit: The repeater relays the message from nodes to the Gateway where the signal is not covered. Security post is an integral part of the Repeater and in this research andit is also known as aControlMonitoring Unit (CMU)

3. Gateway/Coordinator with Central Control/Monitoring Unit: The Gateway in this research is also called Coordinator. It is connected to 3G & internet. All the messages from allnodes come to It can make an automatic phone call & send SMS to the Fire and Police Station.

The function of the Gateway/Coordinator is as follows:

- Receives/Sends messages/signals from all Repeaters
- Receives/Sends messages to all nodes
- Relay all messages from all nodes to the Security Node for necessary action
- Security post is an integral part of the Gateway and in this context, we call it the Central Control & Monitoring Unit (CMU)

3.1 Network

The Gateway, repeaters, office nodes, mobile nodes, and CMU form the campus Nodes Network. The nodes have bidirectional communication with the Gateway. Where the Gateway network cannot cover, the repeaters relay the information to the gateway and vice versa

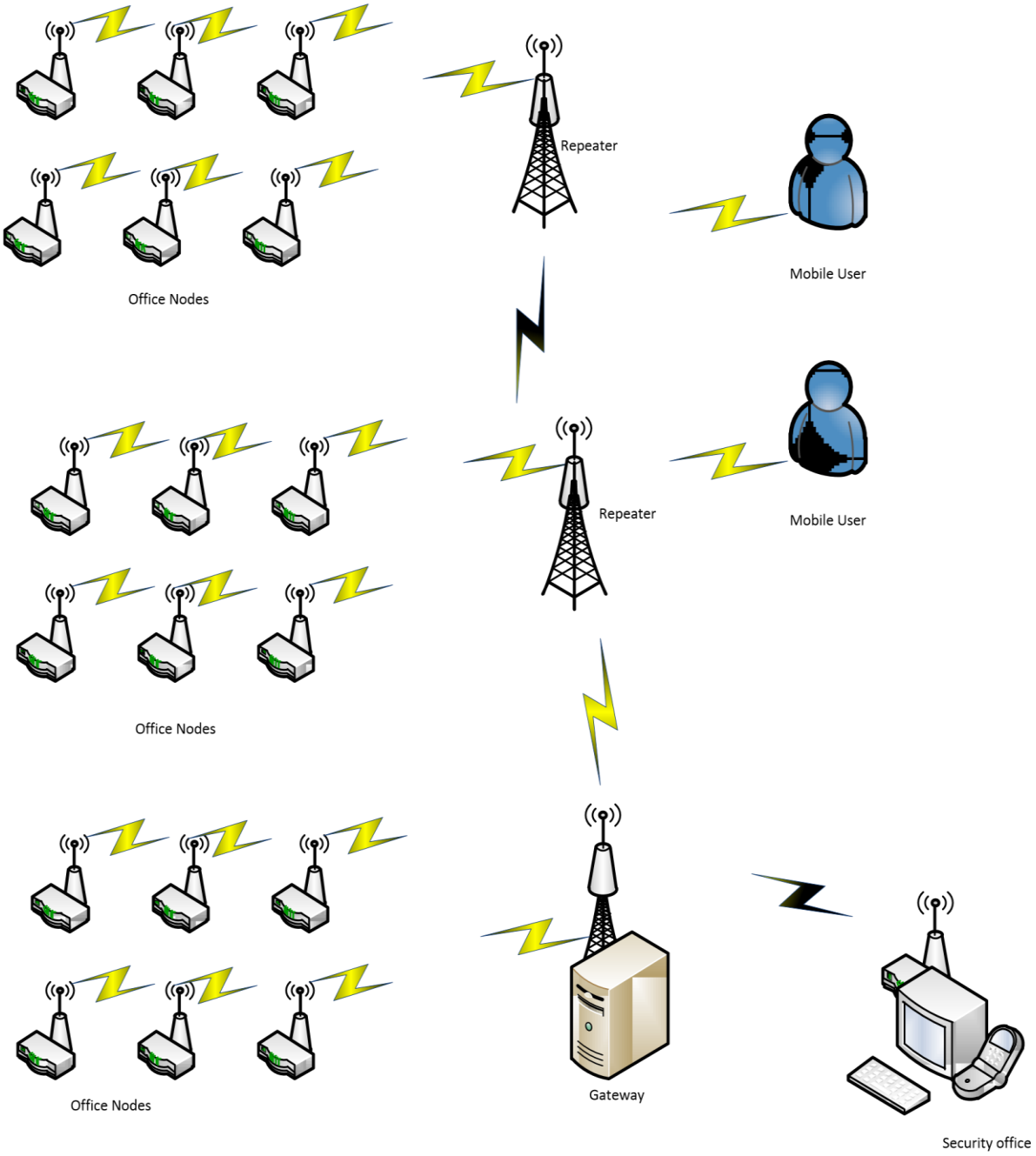

Figure 1: Campus Nodes Network

3.2 Office Node

Each office should be installed with Office Node. The node is comprised of a smoke sensor, a motion sensor, a light sensor, a microcontroller, and a radio and energy source

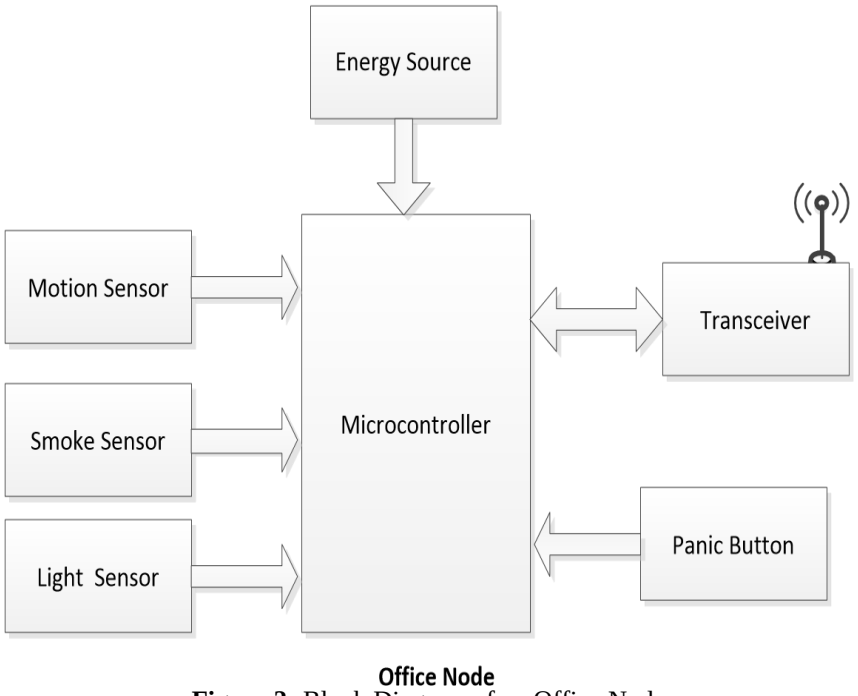

Figure 2: Block Diagram of an Office Node

3.3 Mobile Node

The mobile node can be installed in the Patrol vehicle or hand-held equipment to be held by the security personnel. The node is comprised of buttons, a GPS module, a display module, a buzzer, a microcontroller, and a radio and energy source

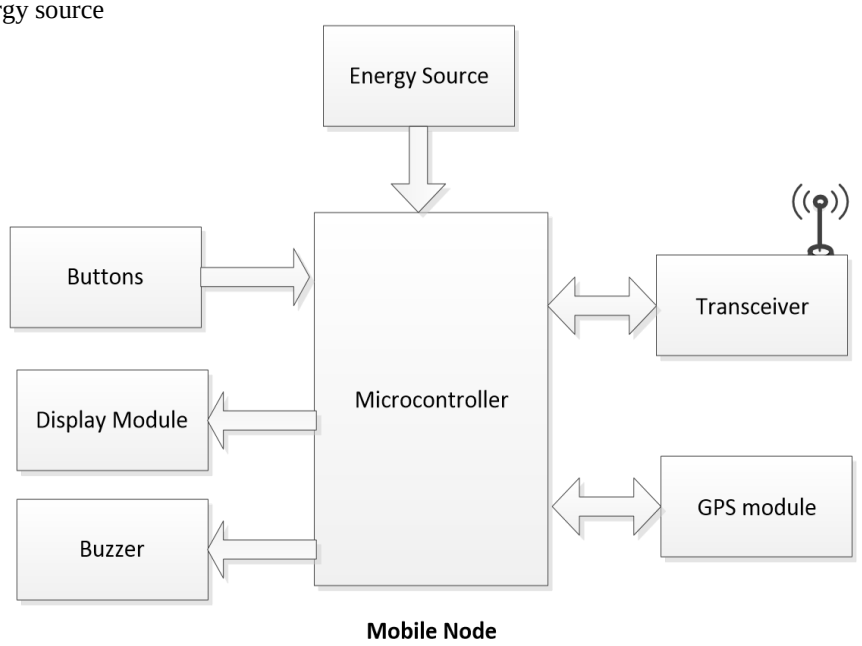

Figure 3: Block Diagram of a Mobile Node

3.4 Security Post Node

This node will be installed at the Security Posts within the campus. It comprises of keypad, a display module, a buzzer, a microcontroller, a radio, and energy source

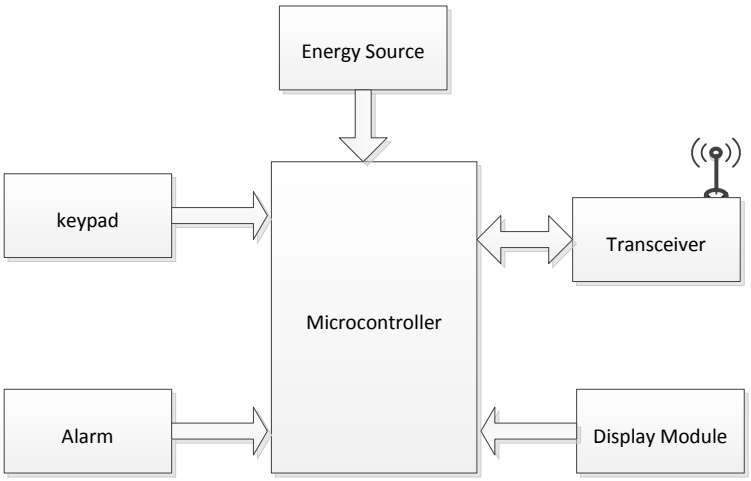

Figure 4: Block Diagram of a Security Node

3.5 Repeater

The repeater relays the message from nodes to the Gateway where the signal is not covered. Security post is an integral part of the Repeater and in this research, it is known asthe Control & Monitoring Unit (CMU).
The circuit diagram of the Wireless Network Smart Campus System is shown in Figure 5.

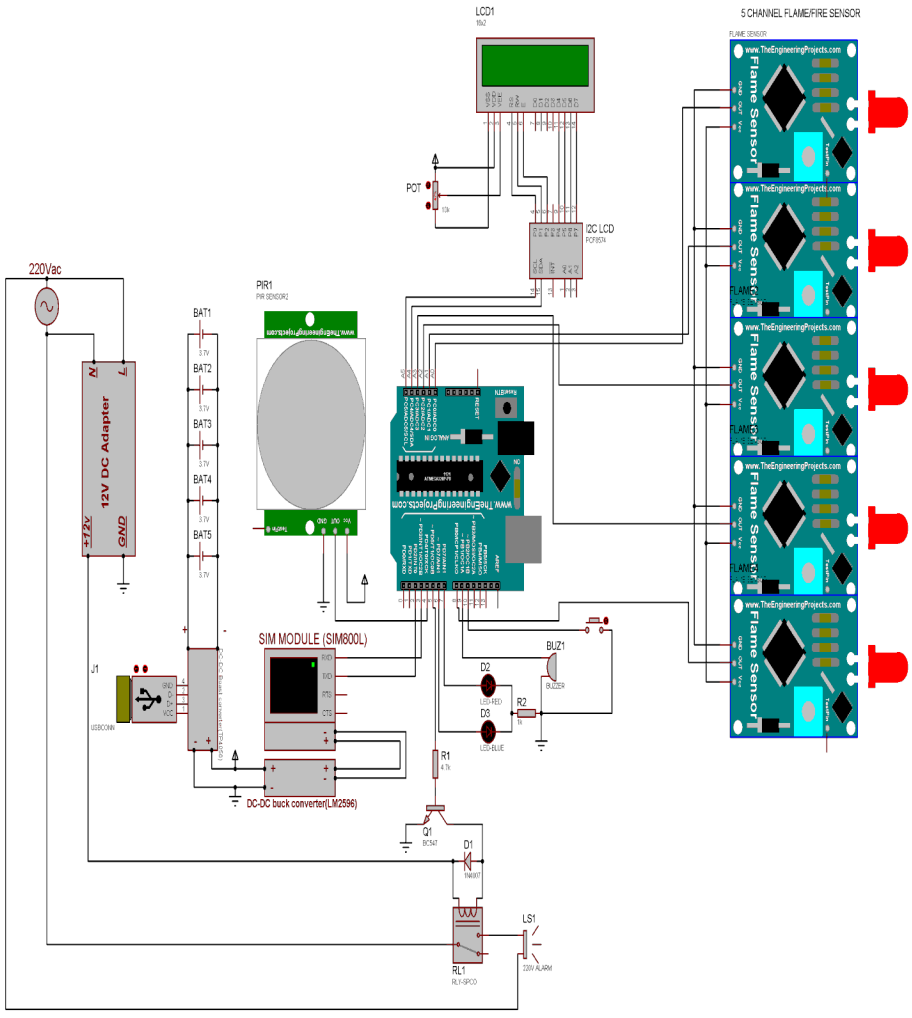

Figure 5: Circuit Diagram of the Wireless Network Smart Campus System.

2. Software Section

The Software is comprised of:

1. Algorithm/Flowchart (see Figure 6).
2. Micro-C programming and
3. Arduino IDE

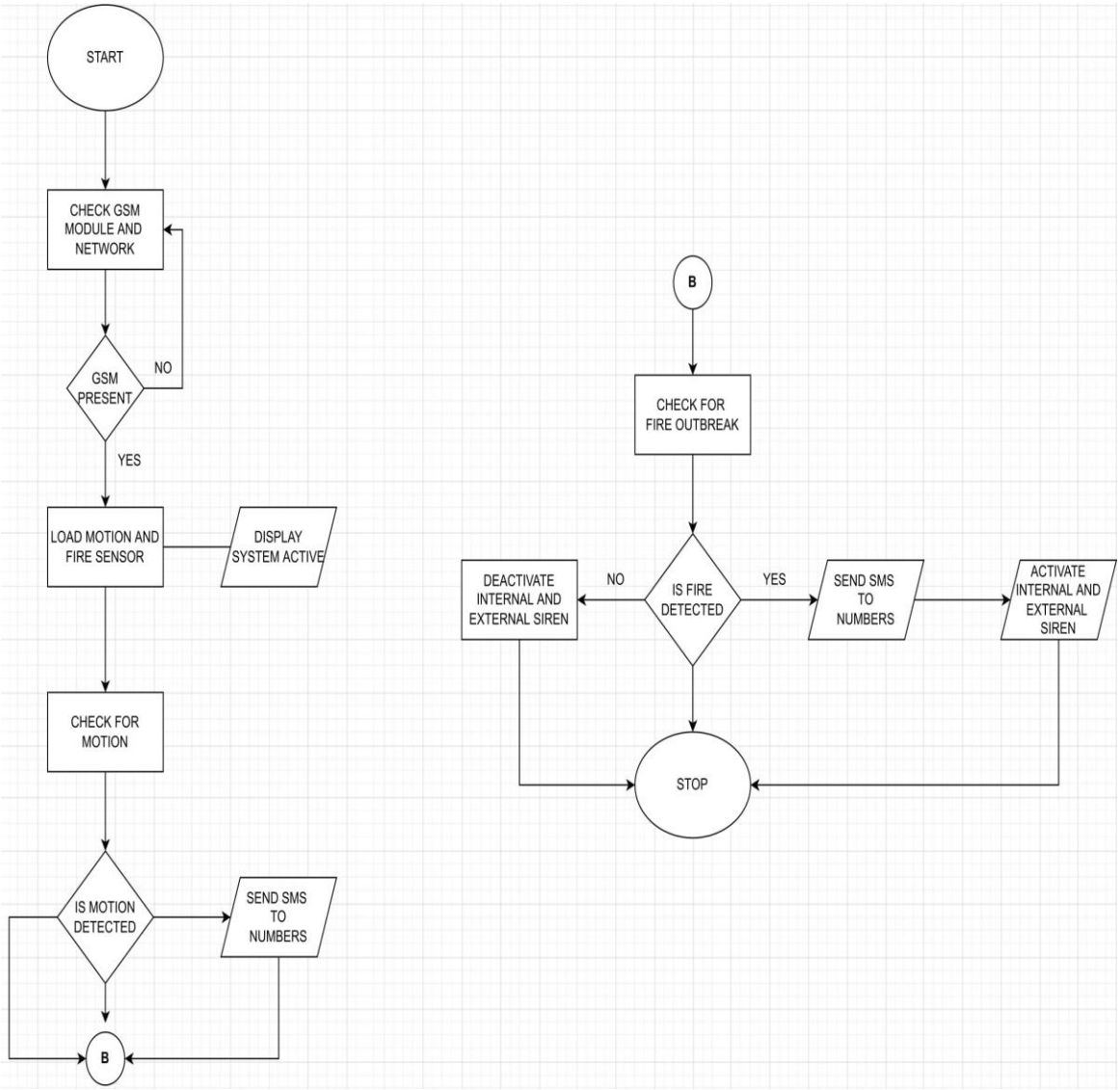

Figure 6: Flow Chart of the Smart Campus System.

III. RESULTS AND DISCUSSION

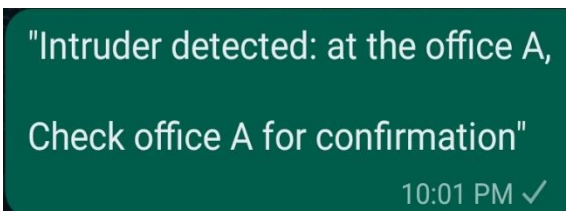

Figure 7a: Intruder Alert message

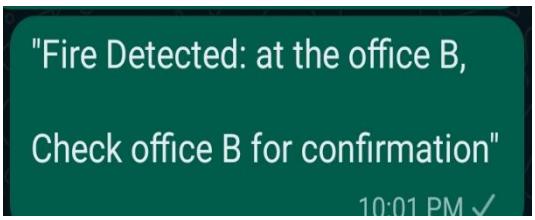

Figure 7b: Fire Alert Message

Tests were carried out on the project and the results are shown in Figures 7a & 7b. When there was an intrusion in office A, a message as shown in Figure 7a was sent to the Central Monitoring Unit and Mobile Security Patrol Unit for prompt action. Likewise, when there was a fire outbreak in office B, a message was also sent to the Central Monitoring Unit and Mobile Security Patrol Unit for prompt action.

The Motion Sensor & Smoke/Fire Sensor Section of the research as shown in Figure 5 uses 5V and 12V regulated power supply. The 5V is used to power the Arduino Uno board, motion sensor, LCD, buzzer, sim Module, as well as LED. While the 12V is used to switch on the relay which activates the external Alarm.The Microcontroller board used is Arduino Uno capable of handling many input and output devices due to many GPIO pins. All programs are saved on this board, it is responsible for sending information to the LCD, receiving signals from the push button,fire/smoke, and motion sensor as well as activating the sending of SMS and Alarm system. The smoke/fire sensor detects flame over a broad range (>120 degrees) and has an operating voltage of 3.3V - 9V. It recognizes the fire using five independent sensors arranged with 30 degrees of separation. The module outputs both an analogue signal (value varies with the intensity of sensed flame) and also a digital signal well suited to microcomputer applications. The motion sensor is used in sensing intruders, once it detects motion, it sends a signal to the microcontroller which interns activates a portion of the code to send SMS to an array of numbers using the GSM Module. The DC-DC buck converter (LM2596) is a DC-to-DC power converter that steps up voltage (while stepping down current) from its input (supply) to its output system) and it is used to power the GSM Module which requires a stable voltage of 3.5 - 4.4Vdc and a current of 2A. For this research, a SIM Module (Sim800L) GSM module was used for sending and receiving information. Also, the GSM Module was used to establish communication between a mobile device or a computing machine and a GSM or GPRS system. A 16x2 LCD was used to show internal processes and information to the user. I2c Lcd was used with this LCD to avoid the wastage of pins.

IV. CONCLUSION

The Wireless Network Smart Campus System is a revolutionary method for augmenting the security, effectiveness, and durability of academic establishments. The amalgamation of wireless networks, sensor technologies, and data analytics endows campuses with the ability to adjust to the dynamic technological terrain and anticipate the particular obstacles they encounter.

ACKNOWLEDGEMENT

This Project is sponsored by TETFUND through the IBR Programme at The Polytechnic, Ibadan, OyoState, Nigeria.

REFERENCES

[1]. X. Wang, Y. Xing, and X. Guan, "Wireless sensor network in intelligent campus: A survey," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2017, pp. 179-184.

[2]. M. S. Hossain, "A comprehensive study of smart campus: A case study of Kyungpook National University," *2016 18th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, South Korea, 2016, pp. 493-497.

[3]. Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, "Game theory in wireless and communication networks: Theory, models, and applications," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 39, no. 3, pp. 533-546, May 2009.

[4]. Sabri, N., Aljunid, S.A., Ahmad, B., Yahya, A., Kamaruddin, A. and Salim, M.S.. (2011): "Wireless sensor actor network based on fuzzy inference system for greenhouse climate control," Journal of Applied Sciences, vol.11, no.17, pp.3104–3116.

[5]. Feng-R., Yuan, H., Hai-Ning, L., Chuang, (2003): "Wireless Sensor Networks," Journal of Software, vol. 14, No.7, pp. 1282-1291.

[6]. Estrin, D. Culler, D., Pister, K. and Sukhatme, G. (2002): "Connecting the physical world with pervasive networks", IEEE Pervasive Computing, pp 59–69, January 2002.

[7]. Karwan Muheden, Ebubekir ErdemaAnd Sercan Vançøn (2016): "Design and Implementation of the Mobile Fire Alarm System Using Wireless Sensor Networks". 17th IEEE International Symposium on Computational Intelligence and Informatics • 17–19, Budapest, Hungary.

[8]. Christine Ammer (2015): "Security". The American Heritage Dictionary of Idioms. APA (AmericanPsychologicalAssociation): Dictionary.com website: http://dictionary.reference.com/browse/security.

[9]. Franck, L. (2001): "Encryption and Cryptosystems in Electronic Surveillance: A Survey of the Technology Assessment Issues". Peggy Becker. Vol. 1, pp 99-106.