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

Volume 7, Issue 2, 364-371

# Cost-Efficient Automated Intrusion Detection and Reporting System for Homes in Nigeria

Olaitan AFOLABI[1], Osekhonmen ABHULIMEN[2], Joanah AMOS[3]

*Department of Information and Communication Engineering, Elizade University, Ilara-Mokin, Ondo State, Nigeria*
olaitan.afolabi@elizadeuniversity.edu.ng/osekhonmen.abhulimen@elizadeuniversity.edu.ng/
joanah.amos@elizadeuniversity.edu.ng

*Corresponding Author:* olaitan.afolabi@eizadeuniversity.edu.ng, +2348036496177
*Date Submitted:* 14/05/2024
*Date Accepted:* 20/09/2024
*Date Published:* 24/09/2024

***Abstract**: Substantial investments are made to mitigate the persistent threat to lives and assets posed by various forms of intrusion. Automated security systems have emerged as crucial tools for safeguarding homes against intrusions in recent times. A major advantage of this is its independent ability to report human activities around homes without direct observation. However, the cost of implementing the system is not pocket-friendly to an average Nigerian given the prevailing economic situation. This research therefore seeks to develop and implement an intrusion detection and reporting system using low cost materials while maintaining a balance between quality and cost at the same time. The system architecture employs the passive infrared sensor (PIR) for motion detection, the ultrasonic sensor measures intruders' location from the home entrance while the NodeMCU ESP8266 microcontroller is responsible for coordinating the reception and relaying of signals within the system. The system was implemented with varying distances of human presence from the security device. Reports of potential intrusion alerts were obtained within reasonable time frames (between 11 seconds and 49 seconds) on the homeowner's mobile phone via the Blynk application. This performance demonstrates the reliability of the system for home security. The system is equally cost-efficient relative to most similar state-of-the art IoT based home security systems considered in this work. Our work therefore contributes to knowledge by proposing an affordable home security solution for a low budget Nigerian user.*

***Keywords:** Cost Efficient, Home Automation, Security, Intrusion Detection, Internet of things (IoT).*

## 1. INTRODUCTION

Intrusion is an act of disrupting the regular flow of a system by compromising the integrity and confidentiality of the system [1]. Security systems are mainly deployed in residences and properties to prevent intrusion that informs thefts and damages. While the use of human security guards may not be completely dependable, these systems may serve as a reliable alternative. Home automation is the use of technology to remotely control and operate connected home devices through a smartphone app, iPad, or other network device [2]. Automated intrusion detection systems deployed to protect properties are designed to mitigate unauthorized access to such. An intrusion detection alarm system may function autonomously or as an integrated part of a security solution to detect the presence of intruders and send notifications in the case of a security event [3]. To facilitate communications between these alarm systems; web services such as the Internet of Things (IoT) are often employed to exchange information between them and end users with the use of mobile applications [4, 5]. IoT is currently the in-thing in virtually all sectors of human endeavours to automate healthcare, agriculture, transportation, and industries for socio-economic development. Devices can send and receive data from each other when connected to the internet using IoT infrastructures [6, 7]. The IoT system is a giant network that consists of varieties of network-enabled devices such as actuators and sensors that exchange diverse types of data through the private network and internet infrastructure [8, 9]. Products compatible with both wired and wireless connection technologies have advanced over years to remotely monitor, detect and control security systems. These automated technologies has improved human lifestyles by securing homes and important facilities [10].

Several researchers have proposed solutions for home automation, intrusion detection and monitoring systems. Rao et al. [11] developed an IoT based home automation system using Raspberry Pi microprocessor to integrate surveillance cameras and motion sensors into a web application. Pujaria et al. [12] presents a home automation system based on NodeMCU ESP32 with IoT that facilitates remote device control from an android-based mobile app. Gunawan et al. [13] built a solar powered home automation and intrusion detection using Arduino Mega2560 as the central controller. Saravanan et al. [14] designed and implemented a prototype of home door lock and unlocking system using Arduino Uno ATmega328p microcontroller board. Taiwo et al. [15] introduced an intelligent home automation system for appliances control and environmental monitoring with the aid of deep learning model to classify motion pattern recognition to mitigate false alert. The components of the system include surveillance camera, sensors, an ESP8266 microcontroller and a relay module. In Ambalkar et al. [16] an Arduino Uno based multiple home automation system for soil irrigation, access control, light control, water reservoir filling, door control security and environmental monitoring and reporting system was developed. Aydin et al. [17] utilized optical wireless communication technology to remote control home devices like door locks, electric light, sound systems, air conditioner and security cameras. In [18], a home based smart security system was developed using Arduino Uno microcontroller for the coordinating signals sent by the ultrasonic sensor and reception of the security alert on GSM module. Sayeduzzaman et al. [19] leveraged IoT technology to facilitate automated home door lock with voice activation in addition to monitoring and alert system on Blynk application. The system is NodeMCU ESP8266 and Arduino Uno microcontrollers based among other components. We present a summary of the reviewed works in Table 1 with a comparative presentation of cost efficiency, energy efficiency and ease of microcontroller programming.

Table 1: Summary of related works

| Ref. | Functionality | Cost Efficiency | Energy Efficiency | Ease of Microcontroller Programming |
|---|---|---|---|---|
| [11] | A Raspberry Pi based system equipped camera surveillance, motion sensor and a web application for security alert. | No | No | No |
| [12] | A NodeMCU ESP32 based home appliances mobile application control system. | No | No | No |
| [13] | A solar powered home automation and intrusion detection system. | No | Yes | No |
| [14] | A door lock control system through a smartphone using Bluetooth as the communication protocol and Arduino Uno ATmega328p microcontroller. | No | No | No |
| [15] | A home devices control and security with deep learning model for motion pattern recognition to mitigate fake alerts. | No | No | No |
| [16] | Arduino Uno based multiple home automation and alert system. | No | No | No |
| [17] | Secure home devices management in using optical data transmission network | No | No | No |
| [18] | Home based smart security system using IoT technology | No | No | No |
| [19] | IoT based door locking and home monitoring system. | No | No | No |
| Proposed | Monitors and reports movement in homes to homeowners with NodeMCU ESP8266 microcontroller automated system. | Yes | Yes | Yes |

However, acquisition of a home based automated IoT security systems of these sort might not be realistic for low-income persons in Nigeria due to the cost of development, power consumption and programming expertise requirement. According to Vanguard online report, the current operational electricity tariff for urban consumers rose by 300% from the previous rate in 2024 [20]. In addition, the inflation rate is reportedly on the rise on a yearly basis [21]. To this effect, there is a need for pocket-friendly life sustainability resources for an average Nigerian.

This work proposes a NodeMCU ESP8266 microcontroller based automated home intrusion detection and reporting system which is cost efficient for a low budget user. Unlike most of the microprocessors employed in the reviewed literatures, NodeMCU ESP8266 microcontroller-based system is relatively less expensive to deploy. The microcontroller being a key component of the system can determine its affordability. It costs $5 on the average and consumes around 70 mA and 10 µA during signal transmission/reception and idle mode respectively. In addition, the simplicity of programming the microcontroller on the user-friendly Arduino independent development environment (IDE) can save significant time used in learning and programming other complex microcontrollers [22, 23, 24]. The automated system integrates a hardware and a software module for its functionality, where NodeMCU ESP8266 microcontroller serves as the central controller. The system monitors a home environment with a motion detection sensor and sends an alert to the Blynk application on a mobile device to notify the homeowner. Details of the process of implementation of this work are discussed in the sections that follow. Section 2 documents the materials and methods, Section 3 bothers on results and its discussion, conclusions are drawn in Section 4 based on the outcome of the results.

## 2. MATERIALS AND METHODS

### 2.1. Materials

The system architecture comprises a smartphone, Blynk application, and hardware components. The hardware component of the system include; NodeMCU ESP8266 Microcontroller unit, Passive Infrared Ray (PIR) Sensor, Ultrasonic Sensor, Light Emitting Diode (LEDs), Universal Serial Bus (USB) charging port, Resistor, and the Li-ion 3.7V rechargeable batteries. Functionalities of the hardware components are detailed as follows:

1. **NodeMCU ESP8266:** The NodeMCU ESP8266 chip is an IoT platform consisting of firmware and hardware. Interfacing objects are connected on the sockets of the microcontroller and data transfer takes place using a Wi-Fi protocol. It is a System-on-a-Chip (SoC) that incorporates components such as a 32-bit microcontroller, switches, filters, power amplifier, power management module, antenna, and standard digital peripheral interfaces into a small package [25, 27]. The choice of the microcontroller is due to its suitability for IoT applications of this sort and affordability for a common man. Figure 1 shows the pictorial representation of the microcontroller.

2. **Ultrasonic Sensor:** Figure 2 presents the picture of an Ultrasonic sensor. The sensor measures the distance of a non-contact target object from the sensing device [25, 26]. It emits sound waves above 20000Hz and receives reflected waves in return. The time of reflection is the basis for distance estimation. It calculates the distance of the object from the sensor at the speed of sound. Time taken by the pulse is actually for to-and-fro travel of ultrasonic signals, but only half of this is required. Therefore, time is taken as time/2, speed of sound at sea level = 343 m/s; then is calculated as given as in Equation (1).

$$Distance = \frac{Speed\ of\ sound\ X\ Time}{2} \quad (1)$$

Figure 1: NodeMCU ESP8266 microcontroller [27]

Figure 2: Ultrasonic sensor [25]

3. **PIR Sensor:** The passive infra-red (PIR) sensors detect human movement in a certain range [27]. They are basically made of a pyroelectric sensor, which can easily detect different levels of infrared radiation. The PIR sensor consists of an infrared sensitive crystal and a processing circuit. The plastic structure over the sensitive crystal serves as lens that focuses the infrared light on the sensors. The sensor works with a dual sensing mechanism; as such the processing through the pair of lenses must be balanced correctly. To ensure the correct configuration of the sensing elements, the respective single signal output voltage (SSOV) must be evaluated using Equation (2):

$$Balance = \frac{|V_a - V_b|}{|V_a + V_b|}\ X\ 100\% \quad (2)$$

Where, $V_a$ = Sensitivity of side A (mV peak to peak), $V_b$ = Sensitivity side B (mV peak to peak)

4. **Light Emitting Diodes (LEDs):** LEDs are electric components light source that are based on semiconductor mechanism [27]. They are used as indicators in this work, when current passes through them the electrons recombine with holes emitting light in the process.

Figure 3: PIR sensor [24]

Figure 4: Light emitting diodes [24]

## 2.2 Methods

This work was conducted on a HP computer, with core i3 processor, 4GB of RAM and 64bit Windows Operating System. The program was written using C language. The methods of the system constitute the hardware and software modules development.

1. **Hardware Module:** The hardware components were integrated as shown in the circuit diagram presented in Figure 5 while Figure 6 shows the coupling process of the hardware module. Figure 7 and Figure present the views of the position of the PIR and Ultrasonic sensors on the coupled hardware device.

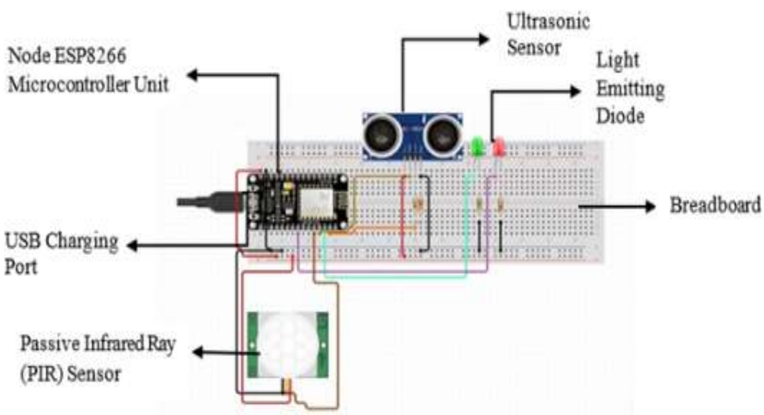


Figure 5: Circuit diagram of the hardware design

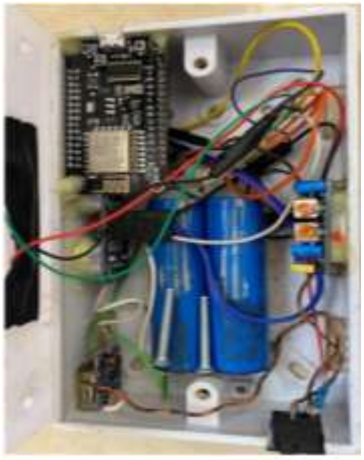

Figure 6: Coupling process of the hardware module

Figure 7: A View of the PIR sensor on the hardware device

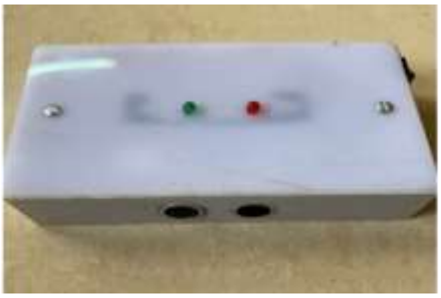

Figure 8: A view of the ultrasonic sensor on the hardware device

2. **Software Module:** The software module consists of the Blynk application and Arduino Independent Development Environment (IDE).
   i. Arduino Independent Development Environment (IDE): Arduino IDE is an open-source platform used for writing, compiling, and uploading codes to Arduino boards [10] takes place. It is used as an IDE for other compatible boards such as the Node ESP8266 microcontroller.
   ii. The Blynk Application: Blynk App provides a platform where a user can interact with connected devices. The Blynk application consists of three components namely; the Blynk app, Blynk server and Blynk libraries. The Blynk app provides a dashboard for users to design an interface for interacting with the hardware device. The Blynk server is responsible for all the communications between the smartphone and hardware. Blynk libraries

enable communication with the server and process all the incoming and out coming commands. Table 2 presents the algorithm that drives the operation of the cost-efficient intrusion detection and reporting system.

Table 2: Algorithm of the Cost-Efficient Intrusion Detection and Reporting System.

***1: Initialize Libraries and Configuration:***

- *Include necessary libraries (ESP8266WiFi, BlynkSimpleEsp8266).*
- *Define WiFi credentials (auth, ssid, pass).*
- *Define GPIO pins for ultrasonic sensor, PIR sensor, and LED.*

***2: Setup Phase:***

- *Begin serial communication (Serial.begin(9600)).*
- *Initialize Blynk with the provided WiFi credentials.*
- *Configure GPIO pins:*
  - *PIR sensor as INPUT.*
  - *Ultrasonic sensor trigger as OUTPUT and echo as INPUT.*
  - *LED as OUTPUT.*
- *Write initial values to Blynk virtual pins (V1, V2).*

***3: Main Loop Execution:***

***PIR Sensor Monitoring:***

- *Read the state of the PIR sensor.*
- *If motion is detected (PIR_SENSE == 1) and the flag is 1:*
  - *Print "INTRUDER'S ALERT" to the serial monitor.*
    - *Send a notification via Blynk.*
    - *Turn on the LED.*
    - *Set flag to 0.*
- *If no motion is detected (PIR_SENSE == 0) and the flag is 0:*
  - *Print "scanning" to the serial monitor.*
    - *Send a notification via Blynk.*
    - *Turn off the LED.*
    - *Reset the flag to 1.*
- ***Ultrasonic Sensor Measurement:***
  - *Set the trigger pin LOW, wait for 2 microseconds.*
  - *Set the trigger pin HIGH for 10 microseconds, then LOW.*
  - *Measure the echo pin duration using pulseIn().*
  - *Calculate distance in cm (distance = (duration / 2) / 29.1).*
  - *If the distance is less than 4meters:*
    - *Turn on the LED.*
    - *Send an intruder alert via Blynk.*
    - *Turn on the virtual LED on Blynk.*
  - *If the distance is greater than 4meters:*
    - *Turn off the virtual LED.*
    - *Turn off the physical LED.*

  *Print the measured distance to the serial monitor.*
  *Write distance and PIR sensor values to Blynk virtual pins (V1, V2).*
- ***Blynk Run:***
  *Continuously run the Blynk process to handle updates and events.*

***4: Ultrasonic Sensor Standalone Setup:***

- *Configure pins for trigger and echo.*
- *Calculate the distance based on sound velocity and print both cm and inches values to the serial monitor.*

***5: PIR Sensor Standalone Setup:***

- *Configure a digital pin for the PIR sensor input and another for the status output.*
- *Continuously monitor the PIR sensor:*

*If motion is detected, print "INTRUDERS ALERT" and turn on the status LED.*

***6: End of Algorithm***

3. **System Implementation:** The system begins the process by initializing the sensors (that is the PIR and ultrasonic sensors). The PIR sensor checks for motion around the home environment, if a motion is sensed, the ultrasonic sensor also checks if the object is within a specified range. If this is the case, the system sends an alert notification to the Blynk application on the mobile phone of the home owner to notify him or her of the security threat. This procedure is also represented in the form of a flowchart in Figure 9.

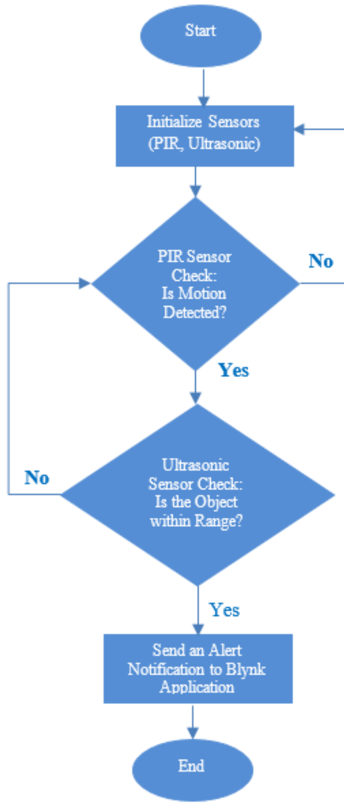


Figure 9: Flowchart automated of the intruder detection and reporting system

## 3. RESULTS AND DISCUSSION

Values of varying distances of an intruder from the security device with respect to time a homeowner received a security alert on his mobile phone were taken. Table 3 shows the values taken for six experiments. The result shows that the alert notification time increases with increasing distances of the intruder from the security device. This can only imply that the sensitivity of the sensors directly depends on the distance of the sensed object. The minimum response time recorded is 11 seconds and 49 seconds at the most. These short latencies justifies the efficiency of the system. Compared to other related works which are based on Raspberry Pi, ATmega328p, Fiber optics wireless connectivity and the likes; a NodeMCU ESP8266 microcontroller based system can be considered a better choice due to its affordability and ease of programming. It comes with an in-built WiFi for connectivity and works on lower energy.

Table 3: Experimental readings of the intrusion detection system

| S/N | Time Frame Between Intrusion and Notification (Second) | Intruder Distance from Home Entrance (Meter) |
|---|---|---|
| 1 | 11 | 2.61 |
| 2 | 15 | 2.68 |
| 3 | 31 | 2.73 |
| 4 | 39 | 3.10 |
| 5 | 47 | 3.53 |
| 6 | 49 | 3.89 |

## 4. CONCLUSION

This research presents a cost-efficient automated intrusion detection and reporting system for homes in Nigeria. The system was developed using IoT technology. The system responded satisfactorily by sending notification alerts to the mobile Blynk application at varying distances when implemented in a home environment. This demonstrates a successful implementation. By implication, the prompt responses of the system to intrusion detection can help users to take mitigating actions against a potential security threat as well as serve as a deterrence to a potential intruder. This work contributes to knowledge by proposing an intrusion detection and reporting system that eases manual security of homes. In addition, the design is cost efficient compared with many state-of-the art designs considered in this work which makes it affordable for low income users to implement. Our future work in this research area seeks to improve the system by incorporating an audio-visual camera that can capture and send images alongside the mobile notifications to the connected mobile device. We intend to also deploy artificial intelligent technique to differentiate types of persons reported to the home owners by the system to mitigate false alarm in the future version of this research.

## ACKNOWLEDGMENT

The authors acknowledge all the professionals whose knowledge, expertise, and experiences directly or indirectly serves as the basis for this work, and also the Department of Information and Communication Engineering, Elizade University, Nigeria for access to the laboratory resources used in the development of this research.

## REFERENCES

[1] Wanda, P., & Jie, H. J. (2020). A survey of intrusion detection system. International Journal of Informatics and Computation, 1(1), 1-10.
[2] Alghayadh, F. & Debnath, D. (2021). A hybrid intrusion detection system for smart home security based on machine learning and user behavior. Advances in Internet of Things, 11, 10-25. https://doi.org/10.4236/ait.2021.111002.
[3] Makhija, H. & Mathur, A. (2020). Design and implementation of home automation system using Google Assistant and Blynk. International Research Journal of Engineering and Technology (IRJET), 7(7), 4281-4284. Retrieved on 25.07.2024 from https://www.irjet.net/archives/V7/i7/IRJET-V7I7746.pdf.
[4] Sinchangreed, V., Watanyulertsakul, E., & Onrit, S. (2022). Web services performance evaluation on single board computers for mobile applications and IoT devices. Suranaree Journal of Science and Technology, 29(2). https://doi.org/10.1109/ACCESS.2016.2615181.
[5] Wiboonrat, M. (2022). Energy loss model for tier 2 and tier 3 data centers. Science & Technology, 29(1), 1-8.
[6] Khanna, A., & Kaur, S. (2020). Internet of things (IoT), applications and challenges: a comprehensive review. Wireless Personal Communications, 114, 1687-1762.
[7] Li, H., Ota, K., & Dong, M. (2018). Learning IoT in edge: Deep learning for the Internet of Things with edge computing. IEEE network, 32(1), 96-101. https://doi.org/10.1109/MNET.2018.1700202.
[8] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys and Tutorials, 22(2), 1191-1221. https://doi.org/10.1109/COMST.2019.2962586.
[9] Kamolklang, T., & Uthansakul, M. (2021). Real-time automatic beam-tracking for NB-IOT. Suranaree Journal of Science and Technology, 28(3):010054(1-9). https://doi.org/10.1109/iciteed.2019.8929983.
[10] Rianmora, S., Sarakichpreecha, I., Eiawsakul, P., & Klaewthanong, V. (2021). The automated cabinet for supporting security storage with passlock system and automatic transportation. Suranaree Journal of Science and Technology, 28(6):010079(1-17).
[11] Rao, G. J., Vinod, A., Priyanka, N., & Kumar, C. H. (2019). IOT based web controlled home automation using Raspberry PI. International Journal of Scientific Research in Science, Engineering (IJSRSET), 6(2), 229-234. https://doi.org/10.32628/ijsrset196246.
[12] Pujari, U., Patil, D., Bahadure, D., & Asnodkar, M. (2020). Internet of Things based integrated smart home automation system. In 2nd International Conference on Communication and Information Processing (ICCIP). https://doi.org/10.2139/ssrn.3645458.
[13] Gunawan, T. S., Yaldi, I. R. H., Kartiwi, M., Ismail, N., Za'bah, N. F., Mansor, H., & Nordin, A. N. (2017). Prototype design of smart home system using internet of things. Indonesian Journal of Electrical Engineering and Computer Science, 7(1), 107-115. https://doi.org/10.11591/ijeecs.v7.i1.pp107-115.
[14] Saravanan, S. K., Nainar, A. M., and Marichamy, S. V. (2019). Android based smart automation system using multiple authentications. IRE Journal, 3(6), 60-65. Retrieved on 16.4. 2024 from: https://www.irejournals.com/paper-details/1701790.
[15] Taiwo, O., Ezugwu, A. E., Oyelade, O. N., & Almutairi, M. S. (2022). Enhanced intelligent smart home control and security system based on deep learning model. Wireless communications and mobile computing, 2022(1), 9307961.
[16] Ambalkar, C., Sontakke, H., Bidkar, P., Raut, K., & Kalore, N. (2024). Development of smart home automation system. SSGM Journal of Science and Engineering, 2(1), 53-56.
[17] Aydin, H., Aydın, G. Z. G., & Aydın, M. A. (2024). The potential of light fidelity in smart home automation. Bulletin of Electrical Engineering and Informatics, 13(5), 3155-3166.

[18] Abiodun, O. J., & Okpe, O. A. (2024). Smart home security using Arduino-based Internet of Things (IoTs) intrusion detection system. World Journal of Advanced Research and Reviews, 2024, 22(03), 857–864. https://doi.org/10.30574/wjarr.2024.22.3.2000.

[19] Sayeduzzaman, M., Hasan, T., Nasser, A. A., & Negi, A. (2024). An internet of things-integrated home automation with smart security system. Automated Secure Computing for Next-Generation Systems, 243-273.

[20] Vanguard (2024). FG hikes electricity tariff from N68/KwH to N225. Retrieved on 18.08.2024 from: https://www.vanguardngr.com/2024/04/nerc-hikes-electricity-tariff-from-n68-to-n225-kwh/).

[21] NBS: National Bureau of Statistics Report (2024). CPI and Inflation Report July 2024. Retrieved on 18.08.2024 from: https://nigerianstat.gov.ng/elibrary/read/1241542.

[22] Raju, K. L., Chandrani, V., Begum, S. S., & Devi, M. P. (2019). Home automation and security system with node MCU using internet of things. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 1-5. https://doi.org/10.1109/ViTECoN.2019.8899540.

[23] Akintade, O. O., Yesufu, T. K., & Kehinde, L. O. (2019). Development of power consumption models for esp8266-enabled low-cost iot monitoring nodes. Advances in Internet of Things, 9(01), 1. doi: 10.4236/ait.2019.91001.

[24] Amazon.com (2024). Computer components. Retrieved on 21.08.2024 from: https://www.amazon.com/s?k=nodemcu+esp8266&crid=NIPU63GKNP3F&sprefix=nodemcu+%2Caps%2C660&ref=nb_sb_ss_pltr-xclick_1_8.

[25] GeekPub (2022). Sensor Wiki: Ky-050 / Hc-Sr04 ultrasonic sensor. Retrieved on 22.06. 2024 from: https://www.thegeekpub.com/.

[26] Durani H., Sheth M., Vaghasia M., & Kotech S. (2018). Smart automated home application using IoT with Blynk app. In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 393-397. https://doi.org/10.1109/icicct.2018.8473224.

[27] Rajeshkumar, G., Rajesh Kanna, P., Sriram, S., Sadesh, S., Karunamoorthi, R., & Mahudapathi, P. (2022). Home automation system using Nodemcu (ESP8266). In International Conference on Advanced Communications and Machine Intelligence, 293-302. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-2768-5_28.