Sumerianz Journal of Scientific Research, 2024, Vol. 7, No. 4, pp. 39-47
ISSN(e): 2617-6955, ISSN(p): 2617-765X
Website: https://www.sumerianz.com
DOI: https://doi.org/10.47752/sjsr.74.39.47

Original Article Open Access

Surveillance System for Electrical Transformer Security: An Identification Technology-Based Approach

Emewu B. M.*
Department of Computer Science, Ebonyi State University, P.M.B. 053, Abakaliki, Ebonyi State, Nigeria

Nweze C.
Department of Computer Science, Ebonyi State University, P.M.B. 053, Abakaliki, Ebonyi State, Nigeria

Onwudebelu U.
Department of Computer Science/Informatics, Alex Ekwueme Federal University Ndufu Alike (FUNAI), P.M.B. 1010, Abakaliki, Ebonyi State, Nigeria
Email: anelectugocy@yahoo.com

Ofiah I. T.
Department of Computer Science, Ebonyi State University, P.M.B. 053, Abakaliki, Ebonyi State, Nigeria

Article History

Received: 2 September, 2024

Revised: 3 November, 2024

Accepted: 6 November, 2024

Published: 9 November, 2024

How to Cite

Emewu B. M, Nweze C, Onwudebelu U and Ofiah I. T. Surveillance System for Electrical Transformer Security: An Identification Technology-Based Approach. *Sumerianz Journal of Scientific Research, Vol. 7, No. 4, pp. 39-47.*

Abstract

Power distribution companies in Nigeria incur losses of billions due to the vandalization of transformers, electrical cables, and other valuable electrical components. To combat this abnormality, an Internet of Things (IoT)-based Surveillance Security System is proposed. The aim is to provide better security services for electrical transformers. The proposed system, called the ITB-Approach, integrates Internet of Things (IoT) and Radio Frequency Identification (RFID) technologies to offer enhanced security services for electrical transformers. The system has the capability to distinguish between EEDC staff and intruders by reading their identification codes, names, and other details on the RFID card through the RFID card reader and sending them as IoT notifications to stakeholders, including the location of the transformer, date, and time. The system uses the ESP8266 NodeMCU Wi-Fi module as the central microcontroller and RFID technology for identification and access control for EEDC staff whose identity is verified by the system. The microcontroller is programmed with embedded C++ to perform all logic and computations. The system is connected to the internet through the wireless technology integrated into the NodeMCU and an IoT platform called Blynk. With the Blynk application, the system can monitor the state of the transformer and send notifications to the registered phone numbers of security agents. It is hoped that the ITB-Approach system, when adopted, will help reduce or prevent the vandalization of electrical transformers.

Keywords: Surveillance System; Electrical Transformer Security; Identification Technology-Based; ITB-Approach.

1. Introduction

A transformer is a device that transfers electrical energy from one circuit to another through magnetic coupling without requiring relative motion between its parts [1]. Electrical transformers are core components in electrical systems, and their primary function is to transfer electric energy from one alternating current circuit to another. They also work to increase or reduce power voltages as electricity travels from one component to another. These, among other vital functions and contents of transformers, make them the chief components of the electrical system, hence the need to safeguard them.

In general, vandalism occurs when a person or group deliberately destroys or damages private or public property. The electricity sector has incurred significant losses as a result of vandalism, with transformers being the most affected equipment. This was confirmed by staff at the Afikpo branch of the Enugu Electricity Distribution Company (EEDC), which was also used as the case study for this work. After interviewing some of them, they attested that most of the vandals' criminal activities target power transformers due to insecurity, and such criminal activity results in energy loss. According to Shokoya and Raji [2], electricity is one of the main drivers of any progressive economy around the world. Each time vandalism of transformers and other electrical components occurs, both the customers in the affected areas and the power company incur significant losses. It also poses serious dangers to human lives, as these illegal acts may result in the electrocution of citizens or vandals by the transformer itself. According to Ola and Adewale [3], many people have lost their lives because of this illegal activity. This has also contributed to the loss of income and jobs for many innocent citizens who rely on electricity as their primary source of power for their businesses, leading to hunger and starvation. Additionally, in some areas, when vandals are caught, they are burned by angry mobs. In a news release by Amechi [4], three suspected electricity transformer vandals were burned alive in Igweledoha Amagu in Ikwo Local Government Area of Ebonyi State. Despite these terrible consequences, the vandals persist in their activities. Research has shown that several efforts have been made to reduce the rate of transformer vandalism, including the use of local security vigilantes, military and paramilitary security personnel, youths, and the fencing and wiring of transformer locations. Yet, the problem persists.

According to Abdullahi [5], Ilorin, the capital of Kwara State has witnessed an upsurge in the vandalization of electric transformers and cables. This development has thrown residents of some areas in the Ilorin metropolis into darkness for some months. It is therefore obvious to say that vandalization of transformers and other electrical components is a very big challenge facing the power holding company of Nigeria at large. Consequently, in this article, we focus on proffering a better solution on safe guiding electrical transformers by integrating IoT and radio frequency identification technology based surveillance system for electrical transformer security services. In a more precise term, the problems of transformer vandalism has become an alarming issue that calls for an urgent attention, with the under listed but not limited to the following problems:

i. It has led the citizens to suffer setbacks in businesses and other activities that involve the use of light and make living so boring;

ii. Replacing and repairing of vandalized transformers has imposed financial burden to the community as well as the power distribution companies;

iii. Many lives have been lost through electrocution in an attempt to vandalize transformers.

The aim of this research work is to develop a transformer security surveillance system using IoT and RFID (Radio Frequency Identification) technologies, for the purpose of rendering a better security services to the electrical transformers. We carried out the following objectives to achieve our aim:

a. To develop an electrical transformer surveillance system that uses the combination of IoT and RIFD capabilities;

b. To develop a system that can dictate motion;

c. To build a system that has the capability of reading the EEDC staff identity information (name and staff number) in the RFID card through the RFID card reader and send the same including the location of the transformer visited, through IoT notification to the stakeholders;

d. To detect when it is day or night using light dependent resistor (LDR);

e. To store and manage data of EEDC staff identity in the cloud saver.

This research is significant for the following reasons, as it will help in:

a. Reducing the rate of electrical power transformer vandalism by offering all time monitoring on the transformer environs regardless of the weather condition and locations;

b. Protecting other electrical components within the transformer unit to ensure continues supply of electricity to the customers;

c. Saving money lost due to vandalism;

d. Saving lives that would have been lost as a result of electrocution, in attempting to vandalize transformers.

2. Literature Review

The issue of protecting electrical transformers in a nation will definitely ensure that a regular and adequate power supply is maintain in such a country which on the other hand demonstrates the hallmark of a developed economy. Owojori, *et al.* [6], reiterated the fact that power instability in Nigeria was caused by overbearing demand of power by consumers and lack of proper maintenance of the power system devices among others. This has pushed the citizens to seek for alternative power sources such as generators, natural gas, biomass energy, solar, typical inverters and other alternative supplies which requires one form of switching or the other to achieve phase selection during power failure. Consequently, Owojori, *et al.* [6], gave a design analysis of an automatic phase selector linking available power supplies. Their design adopts the use of a microcontroller-based system interconnected with other hardware components for proper isolation, switching and visualization of switching conditions but fails short of how these hardware components will be protected from vandalization from criminals. Onochie, *et al.* [7] in their assessment of the Nigeria electric power sector clearly stated that some of the challenges were that the transformers deployed are overloaded in most service areas; bad feeder pillars as well as uneven allocation and distribution of available resources like transformers. Thus, they suggested that there be a reform in power sector of Nigeria due to the effect of inadequate electricity supply, incessant power outages, low generating plant availability and high technical and non-technical losses that have characterized the Nigerian electricity industry.

The issues of electricity theft detection have been the subject matter of many researchers such as Aminu [8], Blazakis, *et al.* [9] and Obafemi, *et al.* [10]. Ali, *et al.* [11], also researched on prevention and detection of electricity theft of distribution network. At times, the power distribution network saddle with the responsibility of delivering electricity to stakeholders as well as consumers in the developing country are faced with the challenge of electricity theft through meter bypassing and hook up connections, causing significant financial inflow problem to the utility company. Thus, Tola, *et al.* [12] presented the design and implementation of an indirect matrix converter for electricity theft mitigation at low voltage distribution network. Their step-down indirect matrix converter was designed and simulated with a frequency range of 10–20 Hz at the converter’s output. In their proposed system, the converter was designed to be connected to the output of the distribution transformer to convert the power frequency to 10 Hz, with another unit incorporated at the consumer end to convert the power frequency back to 50 Hz to make it usable. After analyzing the results, it was observed that using 10 Hz as the worst-case scenario was effective in mitigating electricity issues, with a total harmonic distortion of 204.99% [12]. Finally, their system prevents unregistered clients from using electricity, significantly reducing electricity theft and improving the utility company's bottom line. The key advantage of matrix converters, compared to other methods, is that they do not require a DC-Link capacitor, making them more reliable and suitable for installation at the customer's premises.

In their research, Ifaei, *et al.* [13] discussed the viability of their framework for transporting energy from transformers to the consumer's electric meter and highlighted potential obstacles that must be overcome to expedite energy transformation. The results of their findings showed that off-grid solutions with energy storage systems enhance the efficiency of energy facilities. Furthermore, they observed that bus configurations are commonly used at the distribution level, with standardization rates of 48V and 380V.

3. Proposed Method

It is essential to mention a few things about the current system before discussing the proposed system. In the current system, radio and television are used to educate the public on the dangers of vandalism. Additionally, security measures include the use of village vigilantes, military and paramilitary security personnel, as well as local youths, to safeguard the transformers.

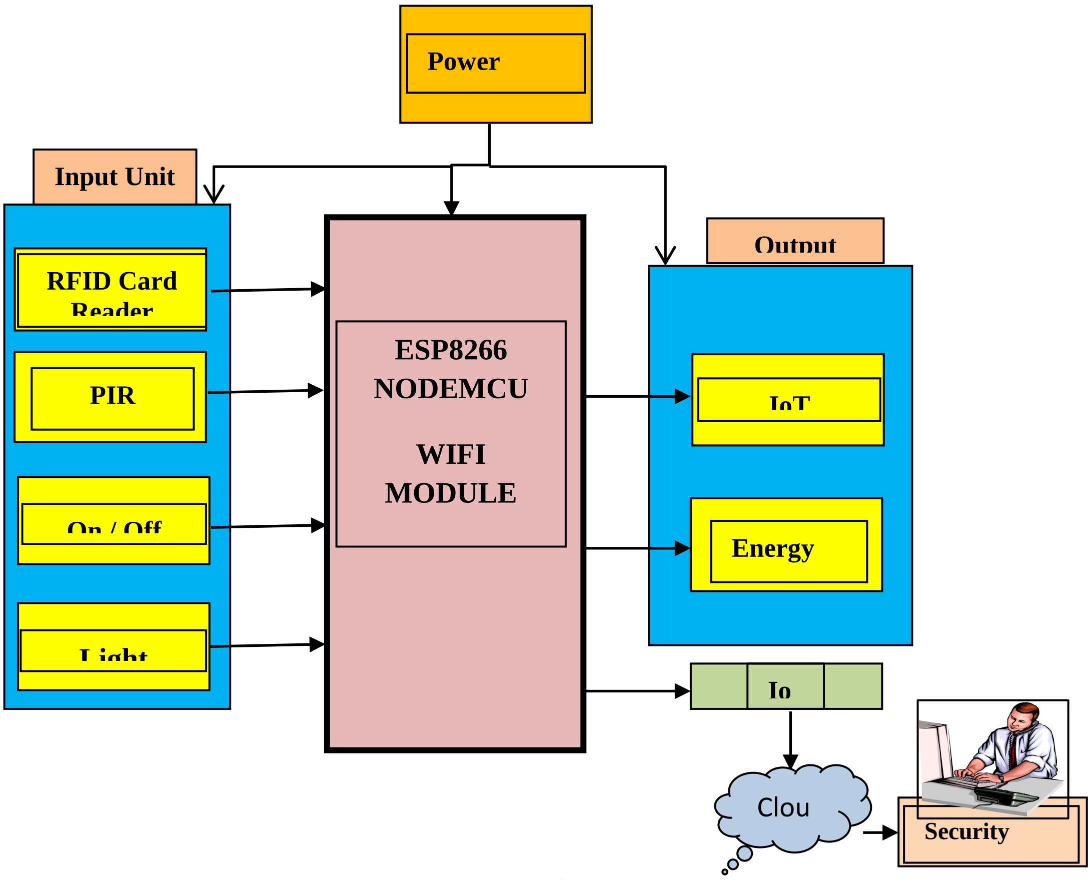


Figure-1. The Block Diagram of an ITB-Approach System

In some locations, walls are built around transformer sites as a security measure to protect the transformers. However, these current systems cannot provide consistent security services, especially for transformers in remote areas. Consequently, there is a need for an identification technology-based approach (ITB-Approach). The block diagram of the system is shown in Figure 1. The ITB-Approach system offers a more effective method for responding to any incidents, including cases where a suspect is found near the transformer. The ITB-Approach detects intruders using a Passive Infrared Sensor (PIR) and sends notifications to the assigned security officers and EEDC stakeholders. Any EEDC staff member who needs to work on the transformer will use their personal RFID card. Once the card is swiped on the RFID reader, the reader will capture the staff ID and send it, along with the date and time of the visit, to the stakeholders as an IoT notification. If an unidentified person approaches the transformer location, the system will send an empty notification (showing no card number) to the stakeholders. With these features, the new system (ITB-Approach) will automatically distinguish between an intruder and EEDC staff. Additionally, a light sensor detects whether it is day or night; it turns off the bulb during the day and turns it on at night.

3.1. Use Case Diagram of the System

Figure 2 shows the interaction between the ITB-Approach system and the outside world. Here, the system and the user are actors. From the use case diagram in Figure 2, the system detects the motion caused by an intruder and triggers the IoT notification to the security units. The system will read the codes in the RFID card. The system is equipped with the ability to detect when it is day or night. This is done with the light dependent resistor (LDR). If it is day, it turns off the bulb and if night, it turns the bulb on.

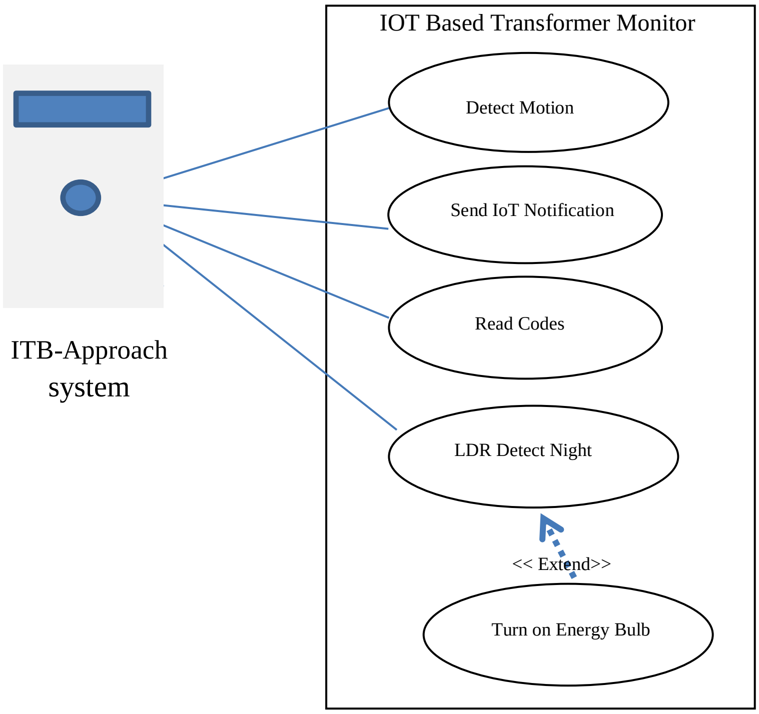


Figure-2. The Use Case Diagram of an ITB-Approach System

4. Analysis of Components

The ITB-approach system involves a detailed analysis of its components to ensure optimal performance and efficiency.

4.1. Control Unit

The ITB-approach system employs ESP8266 NodeMCU. The ESP8266 as shown in Figure 3 is the name of a micro controller designed by Espressif Systems. The ESP8266 is a self-contained Wi-Fi networking solution offering as a bridge from existing micro controller to Wi-Fi and is also capable of running self-contained applications. This module comes with a built in USB connector and a rich assortment of pin-outs. With a micro USB cable, one can connect NodeMCU devkit to his laptop and flash it without any trouble, just like Arduino.

NodeMCU is an open source IOT platform, it includes firmware which runs on the ESP8266 Wi-Fi SoC (System on Chip) from expressif system and hardware which is based on the ESP-12 module. The term " NodeMCU " by default refers to the firmware rather than the device kits. The firmware uses the Lua scripting language Advanced API for hardware IO, which can dramatically reduce the redundant work for configuring and manipulating hardware. NodeMCU Greatly speeds up IoT application developing process. The main advantages of NodeMCU are low cost, ease of use, flexibility, size of the board is reduced as well as less energy consumption. The NodeMCU ESP8266 used in our research has the following specifications:

a. Voltage: 3.3V; b. Wi-Fi Direct (P2P), soft-AP; c. Current consumption: 10uA~170mA;

d. Flash memory attachable: 16MB max (512K normal); e. Integrated TCP/IP protocol stack;

f. Processor: Tensilica L106 32-bit; g. Processor speed: 80~160MHz; h. RAM: 32K + 80K;

i. GPIOs: 17 (multiplexed with other functions); j.Analog to Digital: 1 input with 1024 step resolution; k. +19.5dBm output power in 802.11b mode; l. 802.11 support: b/g/n;

m. Maximum concurrent TCP connections: 5.

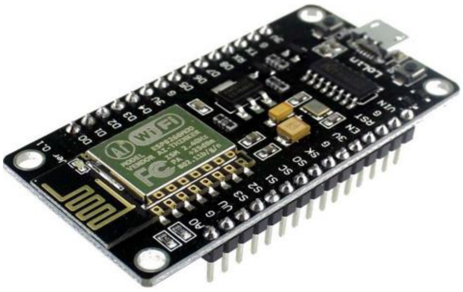


Figure-3. Control Unit (ESP8266 NodeMCU)

4.2. Motion/Movement Sensor

Sensor is a device that measures the physical quantity and converts it into a signal that can be analyzed by an instrument or controller. In our work, we used a Passive Infrared Sensor (PIR). Using the word passive actually means that the PIR device cannot emit an infrared beam but accepts incoming radiation passively. PIR is an electronic device that is used to measure infrared (IR) light radiating objects with its field of view. Passive infrared sensors are technically used to manufacture PIR- based motion detectors. Therefore, this sensor was incorporated into our smart ITB-Approach system, to monitor any apparent movement around the transformer. Figure 4 shows the motion / movement sensor.

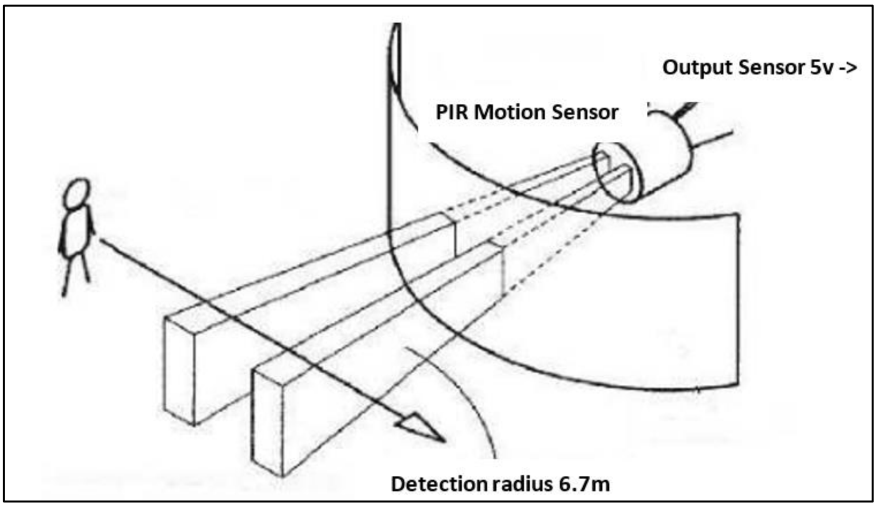


Figure-4. Motion/Movement Sensor Detector

Any object that passes through the infrared rays emits black body radiation. This is the thermal, electromagnetic radiation within a body in thermodynamic equilibrium. Its spectrum and intensity depend only on the temperature of the body. The infrared radiation is invisible to the human eye; however, it can be detected by electronic devices.

4.3. RFID Reader

The ITB-Approach system uses the RFID reader to identify and detect RFID tags as well as extract data stored on the RFID tags such as identification numbers, location information, or other relevant data. The RFID scans and authenticates an RFID tag on a card number and decision will be taken base on the card scanned (see Figure 5). A radio frequency signal is generated and transmitted to the surrounding using antenna by the RFID reader. The RFID reader communicates at 13.56 MHz and it uses SPI communication. The reader is able to read a unique card number and transmit it to the controller for processing.

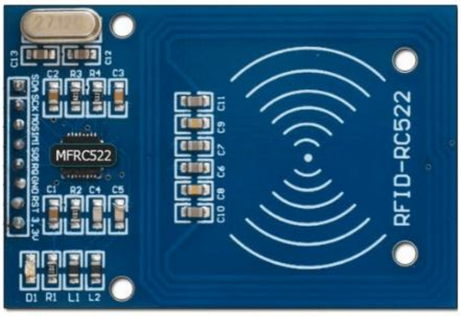


Figure-5. RFID Reader

4.4. The Feedback Unit

The ITB-Approach system uses the feedback unit to give feedback to the stakeholders of EEDC. Blynk provides the platform for building mobile app, cloud service and a library for embedding into IoT hardware as well as web applications for IoT. The system gives feedback to the user through Wi-Fi network technology integrated. The sensor readings are collected, transmitted to the Blynk cloud through the Wi-Fi network connection, and then the officers use the installed Blynk app to receive the readings from the cloud remotely. This enables them to view sensor readings from any location in the world.

4.5. Sensor Data Storage

The sensor readings (RFID Codes) are stored and managed in the cloud server owned by Blynk Company. But the most recent readings in the online server will be displayed on the user's android app. The unique codes of the staff are all stored and retrieved afterwards for further analysis and computation. The sensor storage is shown in Figure 6.

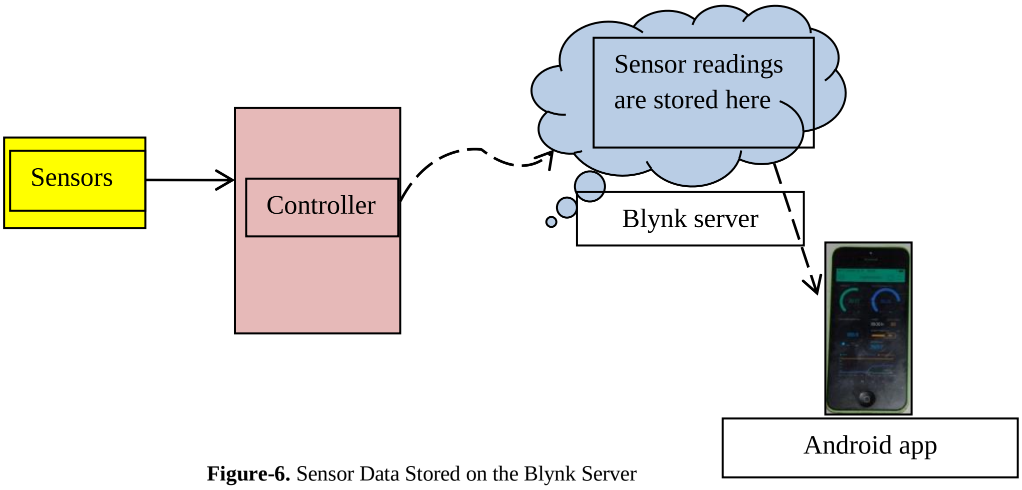


Figure-6. Sensor Data Stored on the Blynk Server

5. System Construction

After modeling the circuit in a software environment called Fritzen, the values of each component were obtained and ordered from the marketers and when they arrived construction began. The construction started with mounting of components on the Vero board; each component was tested before mounting and then soldered to the Vero board. The power supply unit was built first and the voltages from the voltage regulator were tested before going into the next stage. The control unit was soldered and tested. See the system construction and assembling in Figure 7.

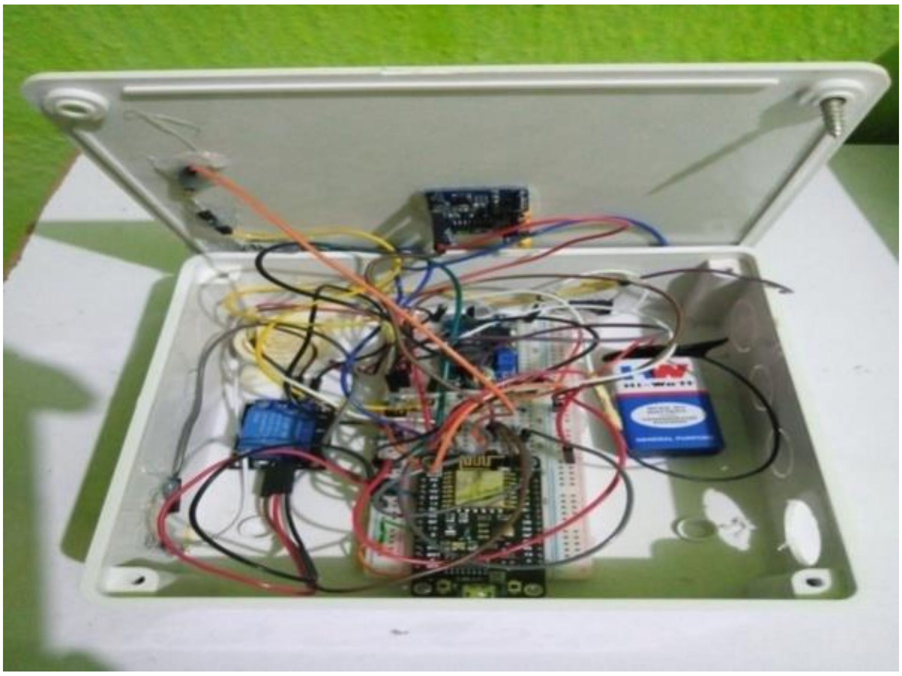


Figure-7. System Construction and Assembly

6. System Implementation

Systems implementation is the process of defining how the information system was built (i.e., physical system design), ensuring that the information system is operational and used, and ensuring that the information system meets quality standard (i.e., quality assurance).

6.1. Main Interface Implementation

The system was implemented by assembling all the electronic components (the sensors, microcontrollers, the actuators and other electronic components) together on the breadboard and packaged all the inner assembly in a casing. The microcontroller was programmed with embedded C++ to carry out all logic and computation. Figure 8 below shows inner assembly of the new system. The RFID Reader, PIR sensor, LDR are all interfaced with the microcontroller board (NodeMCU) for input and output sequencing. The jumpers are used to interface the sensors with the microcontrollers. The LEDs are mounted on the front cover of the casing as indicators. The LM2956 dc-dc buck converter module has been used to reduce the source voltage from the 9v battery to 5v which is useable by the system. All the mounting of electrical components on the casing was done using hand driller, glue gun and screw driver.

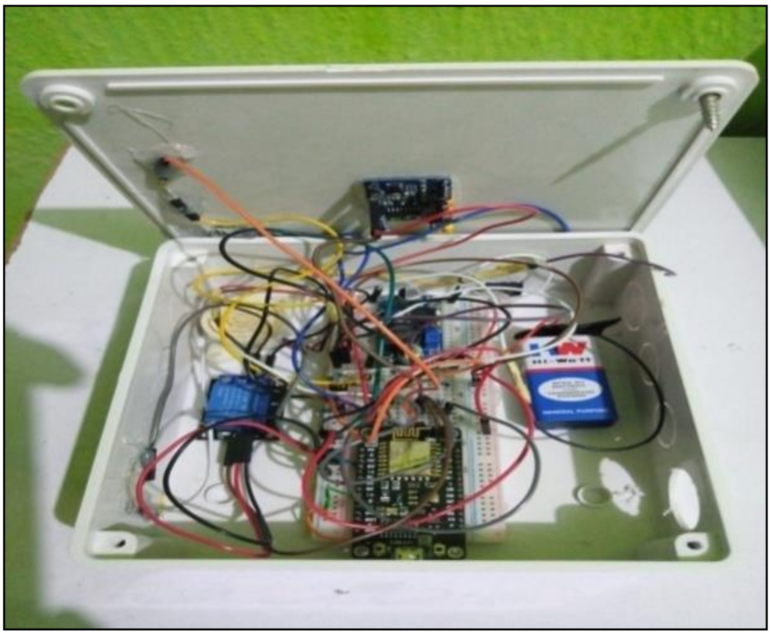


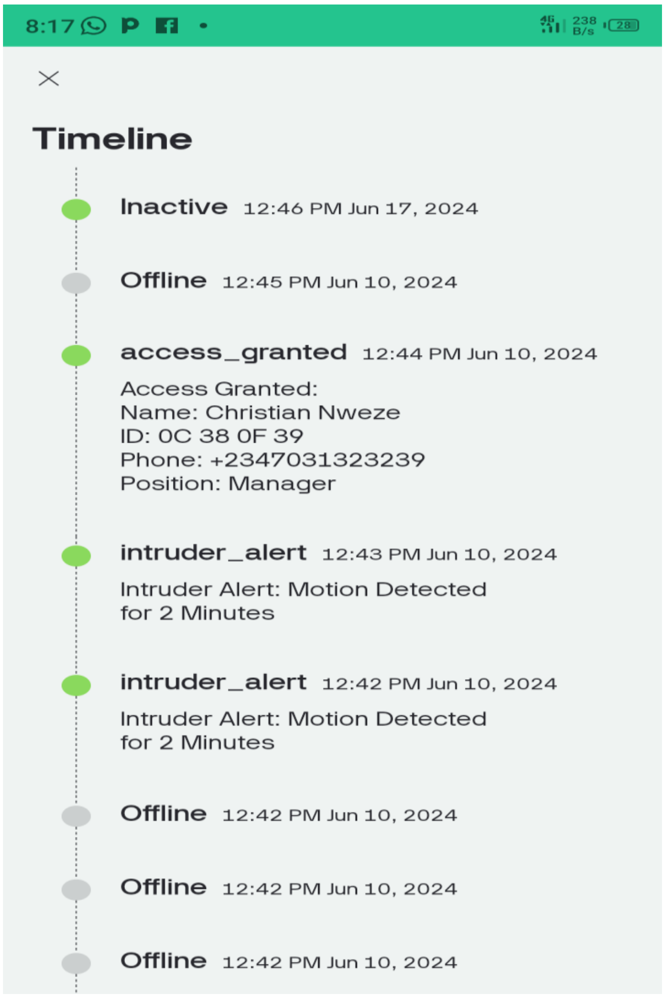
Figure-8. The New System Inner View

6.2. Input Implementation

The inputs to the systems are the sensors which take readings of the specified parameter and communicate them to the microcontroller for processing. The sensors was interfaced with the microcontroller and powered using 9v battery. Also, the motions, staff unique card numbers and darkness are input to the system.

6.3. Output Implementation

The output to the system is the sensor reading on the android phone. Also, the indicator lads mounted on the casing. The microcontroller is integrated with a Wi-Fi network which makes it possible to send sensor data to the stakeholder’s mobile phone or laptop browser window using Blynk cloud. The stakeholders are able to view sensor data and receive notification on their mobile phones. The LDR ensures that the bulb turns on when it is dark. The indicator lads are also used to indicate the booting of the system and change in parameter values. The system also shows where a valid staff has been detected and access granted. The Figure 9 shows the implementation of output Notification on mobile phones using Blynk cloud. The notification of intruder at the transformer location and the notification which shows the output notification of an EEDC staff indicating the staff identity which include: name, staff number, and position.



Timeline

Inactive 12:46 PM Jun 17, 2024

Offline 12:45 PM Jun 10, 2024

access_granted 12:44 PM Jun 10, 2024
Access Granted:
Name: Christian Nweze
ID: 0C 38 0F 39
Phone: +2347031323239
Position: Manager

intruder_alert 12:43 PM Jun 10, 2024
Intruder Alert: Motion Detected
for 2 Minutes

intruder_alert 12:42 PM Jun 10, 2024
Intruder Alert: Motion Detected
for 2 Minutes

Offline 12:42 PM Jun 10, 2024

Offline 12:42 PM Jun 10, 2024

Offline 12:42 PM Jun 10, 2024

Figure-9. Notification on Mobile Phones using Blynk Cloud

From Figure 9, we were able to determine that someone is either an intruder or a legitimate staff by using RFID tag number identification. If someone is not able to provide a valid ID, a notification is sent indicating he is not a staff and hence actions taken. From Figure 9, it can be ascertain that EEDC staff, Christian Nweze, was granted access by 12:44 p.m. on the 10th June 2024 with an ID number: OC 38 OF 39. However, if a valid card number is detected, a notification bearing the person's details is sent hence the individual is allowed access. Also, this new system is able to keep track of the details of staff who had attended to the transformer previous for future use. With this, it is easier to trace who visited the station at what time and hence take certain decision.

7. Conclusion

This research was aimed at enhancing the existing transformer security system. Most of the reviewed works integrated the ability to sense motion and raise continuous alarm to indicate intrusion. However, this research has been able to determine that someone is either an intruder or a legitimate staff by using RFID card number identification. If someone is not able to provide a valid ID, a notification is sent indicating he is not a staff and hence actions taken. The system having being built and test has achieved the aim and objectives for which it was meant and thus, to this effect, the system:

i. Detected a motion through a passive infrared sensor;
ii. Read the details of an EEDC staff identity and send same as IoT notification to the stake holders' android application;
iii. Stored and manage data of EEDC staff identity in the cloud saver;
iv. Sent an empty IoT notification when an intruder is detected within the transformer area.
v. Detected when it is day or night via the LDR.

7.1. Recommendations

i. The system can be improved by integrating the ability to send a captured images of the intruder for further analysis.
ii. Other researchers can integrate the ability to predict the possibility of transformer vandalism and report to necessary offices.

References

[1] Prashant, C., Pukhraj, C., Sunil, K., and Kuldeep, S. R., 2017. "Theory and application of transformer in electrical and electronics circuits." *International Journal of Research,* vol. 4, pp. 2348-6848. Available: https://edupediapublications.org/journals/index.php/IJR/

[2] Shokoya, N. O. and Raji, A. K., 2019. "Electricity theft mitigation in the nigerian power sector." *International Journal of Engineering & Technology,* vol. 8, pp. 467-472. Available: https://doi.org/10.14419/ijet.v8i4.29391

[3] Ola, A. B. and Adewale, Y. Y., 2014. "Infrastructural vandalism in nigerian cities: The case of osogbo, osun state." *Journal of Research on Humanities and Social Sciences,* vol. 4, pp. 49-6. Available: https://www.iiste.org/Journals/index

[4] Amechi, K., 2022. *Transformer vandals burnt alive in Ebonyi*. Radio Nigeria FM.

[5] Abdullahi, O., 2024. "blackout as vandals continue attacks on transformers, Cables In Ilorin." Available: https://leadership.ng/

[6] Owojori, A. O., Akinbolade, A. M., and Akingbade, K., 2022. "Design analysis of an automatic phase selector." *Journal of Engineering Studies and Research,* vol. 27, pp. 51-63.

[7] Onochie, U. P., Egware, H. O., and Eyakwanor, T. O., 2015. "The nigeria electric power sector (opportunities and challenges)." *Journal of Multidisciplinary Engineering Science and Technology (JMEST),* vol. 2, pp. 494-502. Available: www.jmest.org

[8] Aminu, M. A., 2020. "5-hz distribution system for mitigation of energy theft by residential consumers." *Frontiers in Energy Research,* vol. 7, Available: https://doi.org/10.3389/fenrg.2019.00153

[9] Blazakis, K. V., Kapetanakis, T. N., and Stavrakakis, G. S., 2020. "Effective electricity theft detection in power distribution grids using an adaptive neuro fuzzy inference system." *Energies,* vol. 13, Available: https://doi.org/10.3390/en13123110

[10] Obafemi, M. O., Oluwole, E. A., Omoniyi, T. E., Meduna, P., and Alaye, A. S., 2022. "Prevalence of electricity theft among households in Lagos State, Nigeria." *Nigerian Journal of Technology,* vol. 40, pp. 872-881. Available: https://doi.org/10.4314/njt.v40i5.13

[11] Ali, S., Yongzhi, M., and Ali, W., 2023. "Prevention and detection of electricity theft of distribution network." *Sustainability,* vol. 15, p. 4868. Available: https://doi.org/10.3390/su15064868

[12] Tola, O. J., Tsado, J., and Abel, S., 2023. "Electricity theft mitigation at low voltage distribution end using indirect matrix converter." *FUOYE Journal of Engineering and Technology,* vol. 8, pp. 314-318. Available: http://doi.org/10.46792/fuoyejet.v8i3.1074

[13] Ifaei, P., Tayerani, C. A. S., Loy-Benitez, J., Yang, R. J., and Yoo, C., 2022. "A data-driven analytical roadmap to a sustainable 2030 in South Korea based on optimal renewable microgrids." *Renewable and Sustainable Energy Reviews,* vol. 167, p. 112752. Available: https://doi.org/10.1016/j.rser.2022.112752