

Smart Vandalism Detection and Monitoring System for Power Transmission Lines Using Multi-Sensor Integration and GSM/IoT Communication

Obianke F. I¹, Obianke G. U² & Obianke E. C³

¹Department of Electrical & Electronics Engineering, Delta State Polytechnic, Otefe-Oghara, Delta State, Nigeria.

²Atlantic Exhibition Nigeria Limited, Magboro, Ogun state, Nigeria

³Evertch Packaging Solutions Nigeria. Ltd, Agbor, Delta State, Nigeria

Received: 11.05.2026 / Accepted: 03.06.2026 / Published: 01.07.2026

*Corresponding author: Obianke F. I

DOI: [10.5281/zenodo.21080830](https://doi.org/10.5281/zenodo.21080830)

Abstract

Original Research Article

Power infrastructure vandalism remains a serious problem that threatens the reliability and stability of electricity supply, particularly in developing countries. This paper presents the design and implementation of a cost-effective vandalism monitoring system for power transmission lines using embedded systems and GSM /IoT communication technology.

The proposed system integrates vibration, motion, and current sensor to identify unauthorized interference or tampering activities. In the system design, the PIR sensor detects human presence, the SIM800L module transmits SMS alert notifications, the IoT is the internet connectivity/cloud synchronization while the micro-controller coordinates and monitors the overall operation of the system. Once suspicious activity is detected, real-time alerts are immediately sent to authorized personnel for prompt intervention. The developed system helps to improve response time, minimize energy losses, and strengthen power grid security. It is efficient, reliable, low-cost, and offers scalable solution for securing power transmission infrastructure against vandalism and theft.

Keyword: GSM Communication, IoT Security, Microcontroller, Power Transmission Lines, Sensors, Vandalism Detection.

Copyright © 2026 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

1.0 Introduction

Electric power is the driving force behind industrialization. More than just an important factor, it is the fundamental backbone of industrial growth and socioeconomic development. It is widely recognized across the world that electricity remains one of the strongest driving forces behind the economic growth and industrial development in any nation.

According to Odili and Mokuwonye (2003), no

country has successfully transformed from a subsistence economy into an industrialized nation or achieve sustainable economic growth without first establishing a reliable and adequate electricity infrastructure capable of meeting its energy demands. In Nigeria, however, the state of electricity supply has remained a major concern for over four decades due to persistent instability and inadequate power delivery.

Today, one of the greatest challenges facing our society is insecurity. Human lives are



increasingly endangered, while valuable properties and national assets are continuously destroyed through acts of vandalism. The power sector has been heavily affected by this menace, Adenikinju (2003). Criminals and unscrupulous individuals vandalize electrical power installations, transmission lines, oil pipelines, and other critical infrastructures for personal gains. These destructive activities have repeatedly contributed to the collapse of the national grid, resulting in frequent power outages, epileptic electricity supply, and some cases total blackout across the country. The consequences have been severe, leading to economic hardship, unemployment, poverty, hunger, reduced industrial productivity, and even loss of lives. Power transmission systems are vital infrastructures that must be safeguarded against vandalism and theft. In many parts of the world, intentional destruction of cables, transformers, and other electrical facilities results in frequent power outages, economic losses, and reduced system reliability.

Many industries and manufacturing companies have been forced to shut down operations, while others have relocated to neighbouring countries because they can no longer sustain the high cost of generating electricity independently. The cost of petroleum products used to power generators has also become excessively high, making production more difficult and expensive.

Despite the Nigerian government spending hundreds of billions of Naira annually on the maintenance, monitoring, and protection of power infrastructure, electricity supply in the country remains unreliable and constantly threatened by vandalism. Even after the privatization of electricity agencies such as NEPA and PHCN, the situation has not significantly improved, as numerous cases of vandalism continue to be recorded. In 2021 alone, the national grid reportedly collapsed five times due to attacks on power transmission facilities.

A notable incident occurred on April 8, 2022, at about 6.30 pm, when the national grid dropped drastically and eventually collapsed after transmission tower number 104 at Oku Iboku in Akwa Ibom state was vandalized along the 330 kV Ikot Ekpene - Odukpani transmission line.

Similarly, in March 2022, the 330 kV Sapele - Benin transmission line experienced a shutdown after repeated acts of vandalism damaged several towers along the route.

A transmission tower on the 132 kV Enugu - Benue power line was vandalized and severely damaged, almost leading to its collapse. During the incident, one of the suspected vandals was electrocuted. Similarly, near Oshogbo in Osun state, vandals reportedly used welding machines to cut down two towers on the newly constructed 330 kV Osogbo - Akure transmission line, causing significant delays in the completion of the project. In Ogun state, three transmission towers on the 132 kV line collapsed due to vandalism, while Akwa Ibom and Cross River states recorded about five separate cases of attacks on power infrastructure. In Delta state, ten transmission towers were damaged and had to be repaired consecutively as a result of repeated vandalism activities, Daily Trust, (2022).

Following these disturbing incidents, the then minister of power, Abubakar D. Aliyu, raised concerns over the growing energy crisis caused by the vandalism of transmission facilities. After the attack on the Oku Iboku section of the 330 kV Odukpani (Cross River) -- Ikot Ekpene (Akwa Ibom) transmission line, he directed the Nigerian Electricity Regulatory Commission (NERC) to investigate the situation thoroughly.

In a related development, the Managing Director of the Transmission Company of Nigeria (TCN), Dr Sule Abdulaziz, while addressing journalists, appealed to Nigerians to actively support efforts aimed at combating the vandalism of power infrastructure across the country, Daily Trust, (2022).

Traditional methods used for monitoring power transmission lines mainly involve manual inspections and routine patrols by utility personnel. Several other methods have been applied and reviewed but power theft is not reduced. Furthermore, many current systems cannot simultaneously detect physical intrusion and electrical abnormalities, making them less reliable in practical deployment.

The approaches are often ineffective because transmission lines usually cover long distances

and are located in remote or inaccessible areas. They are expensive to deploy, dependent on internet connectivity, or limited to single sensor detection technique.

They have their own challenges to interpretation of data regarding power, efficiency, delay fault reporting, false alarm, lack real-time monitoring and accuracy to pinpoint the location of vandals.

As a result, vandalism incidents are sometimes detected too late, leading to prolonged outages and expensive repairs. With the advancement of IoT, embedded systems, smart sensors, GSM communication technologies, more intelligent approaches for remote monitoring and fault detection have been developed. Such systems can automatically monitor transmission infrastructure, identify suspicious activities, and immediately notify utility operators before severe damage occurs.

Considering the increasing rate of vandalism and the fact that conventional methods of monitoring power lines and providing security have proven inadequate, there is a growing need for more intelligent, efficient, and reliable monitoring systems capable of detecting multiple forms of vandalism, operating effectively in remote environments, providing rapid alerts, and improving the overall security of power transmission infrastructure.

It is against this background that this work, titled vandalism detection and monitoring system of power transmission lines using multi-sensors fusion with GSM/IoT technologies was developed to provide an effective solution for detecting and preventing vandalism of electrical power infrastructure in Nigeria. The proposed system is designed to be safe, reliable, and highly efficient in monitoring and protecting power transmission facilities.

The aim of the research work is to design and implement an intelligent vandalism detection and monitoring system for power transmission lines using multi-sensor fusion, embedded processing, and GSM communication technology for real-time detection and alert generation.

The specific objectives of the study are;

- a) To design a vandalism monitoring architecture for transmission lines using embedded systems technology
- b) To develop a multi-sensor detection system using vibration sensor, PIR motion sensor, and current sensor.
- c) To integrate a GSM based communication module for instant SMS alert transmission.
- d) To develop the hardware and software components of the proposed system using Arduino Uno and embedded programming
- e) To evaluate the performance of the developed system
- f) To compare the developed system with existing vandalism monitoring approaches to establish its novelty and effectiveness.

2.0. Related literature Review

In Nigeria, voltages of 330 kV and 132 kV are transmitted, while voltages of 33 kV, 11kV and 0.45 kV are being distributed, Adesina, L.M. et al. (2020). The power generation, transmission lines and distribution lines have a lot of operational losses, the amount of these losses is increasing at a high rate in several countries in the world.

Several researchers have examined vandalism and theft in power and utility systems with emphasis on improving security and monitoring. Olaoluwa O. G. (2017) discussed the effects of electricity theft on power quality in Nigeria and highlighted the need for effective control measures to reduce losses and improve electricity supply reliability. Mohammed Shafeeq k. k. & Maqbool Thoufeeq T, (2018) developed a GSM and GPS-based vehicle anti-theft system for remote monitoring and vehicle tracking. Similarly, Ogujor, et al. (2013) proposed a micro-controller based anti-pipe line vandalism system that detect attacks on pipe line and send alert to operators.

Suliman A. S. et al. (2022) further introduced an IoT based monitoring system for high-voltage power lines using sensors and GPS technology to improve maintenance planning and system reliability.

Kumar K. K, et al. (2017), Recommended the use of passive infra-red (PIR) sensors for motion detection due to their high sensitivity to infrared changes. Fezari M. and Dahoud A. A. (2019), Antinus A. et al. (2015), and Dasgupta Ruythm (2017) demonstrated the application of Raspberry pi and camera systems for surveillance, motion detection, image processing and live video streaming.

Eluwande and Ayo (2016) developed a UAV based pipeline surveillance system for real-time monitoring of oil pipelines, although the system was costly to maintain.

Abdulhamid Musa, (2023) concluded that internet of things-based power line vandalism monitoring system improves the security and resilience of power networks through real-time alerts and data monitoring. Furthermore, Thisday Newspaper (2016) and Bayo (2016) identified the market for stolen electrical materials and the scrap value of power cables as major factors encouraging vandalism.

Zulu, C. L, and Dzobo, O, (2023) developed a real-time power theft monitoring system using embedded monitoring techniques to detect abnormal current behaviour. Similarly, Walendra, D. M, (2021) proposed a GSM based electricity theft detection system for remote alert transmission. Although these systems improved theft detection, they focused mainly on electrical abnormalities without addressing physical vandalism or intrusion detection.

Researchers have also developed GSM based transformer monitoring systems for remote fault reporting and operational monitoring. Salauddin, B. et al, (2023), Kumar, M. S, et al, (2014), and Aniebiet, I, (2020) utilized GSM technology to monitor transformer conditions such as current and voltage variations. In addition, Kirunguru, E. et al, (2018) proposed a vandalism monitoring system for transformer protection. However, these systems lacked integrated multi-sensor intelligence for comprehensive transmission line monitoring.

Recent studies have explored IoT and wireless sensor network (WSN) technologies for transmission line monitoring. Zhang, Y. et al, (2021) and Ahmed & Mahmood (2020) developed an IoT-based smart Grid monitoring

system, while Lin, J, et al, (2014) and Li, L, et al, (2015) demonstrated WSN based monitoring system for fault detection and surveillance. Akyildiz et al.(2002) investigated wireless sensor network architectures for industrial monitoring applications and highlighted the advantages of distributed sensing in remote environments.

Gungor and Hancke (2009) developed industrial wireless sensor network for real-time monitoring and fault detection in smart grid systems. Olwal et al. (2018) proposed IoT-based utility monitoring systems capable of cloud synchronization and remote asset management for electrical infrastructure protection.

Although previous works demonstrated the usefulness of wireless monitoring technologies, many existing systems rely on single-sensor architectures which are vulnerable to environmental noise and false triggering. Furthermore, some systems lack integrated GSM emergency communication for rapid response.

The present work addresses these limitations through multi-sensor fusion combined with GSM and IoT communication for improved detection accuracy and remote accessibility.

Although these systems improved remote monitoring, they suffer from internet dependency, high deployment complexity, and increased maintenance cost. Therefore, this research proposes a low-cost multi-sensor vandalism monitoring system integrating vibration sensing, PIR motion detection, current anomaly analysis, embedded processing, and GSM communication for improved detection accuracy and smart-grid security.

3.0 Methodology

The principle and method adopted in this work are based on the development of an intelligent monitoring system made up of several important units working together to ensure effective surveillance and protection of power transmission lines. The proposed system consists of the following subsystems as illustrated in fig 1.

Multi-sensor detection unit for sensing and detecting intrusion or suspicious activities

around the power infrastructure.

1. Embedded processing unit which serves as the brain of the system, coordinates and manages all system operations and decision-making processes
2. GSM communication subsystem that sends and receive notifications between the system and the authorized personnel

3. IoT cloud communication subsystem which work in conjecture with the GSM
4. Alarm and notification subsystem is for local alarm generation to alert the personnel
5. Power management subsystem that supplies the energy to the system.

The system architecture enables continuous monitoring of transmission infrastructure and automatic reporting of suspicious activities.

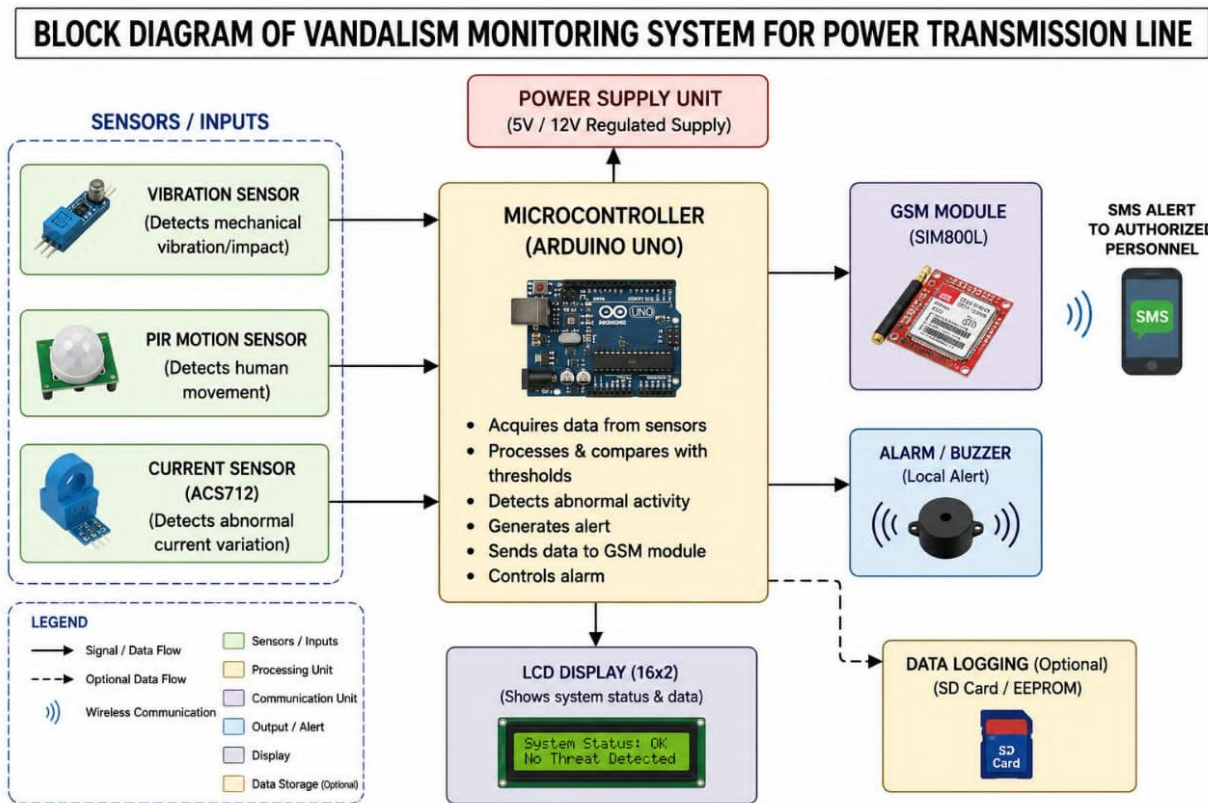


Fig 1 illustrating the block diagram of power transmission line vandalism monitoring system.

3.1 Multi-Sensor Detection Unit

The sensing subsystem integrates Vibration sensor, PIR motion sensor, Acoustic sensor and current sensor.

The vibration sensor detects tower climbing and metal cutting activities, while the PIR sensor detects human movement within restricted areas. The acoustic sensor identifies abnormal sounds associated with vandalism activities such as drilling or hammering.

3.2 Embedded Processing Unit

An ESP32 micro-controller was selected due to its integrated Wi-Fi capability, low power consumption, dual-core architecture, and multiple GPIO interfaces.

The processor performs: Sensor data acquisition, Signal filtering, Amplification, Noise suppression, ADC conversion, Threshold analysis, Sensor fusion, Alarm generation, GSM communication, and cloud synchronization.

The data fusion algorithm system uses weighted

decision logic:

$$D = w_1S_1 + w_2S_2 + w_3S_3 + \dots + w_nS_n$$

Where D represents the decision output,

W represents sensor weight,

S represents individual sensor signal.

Alarm is triggered when the decision output exceeds a predefined threshold limit, vandalism is confirmed.

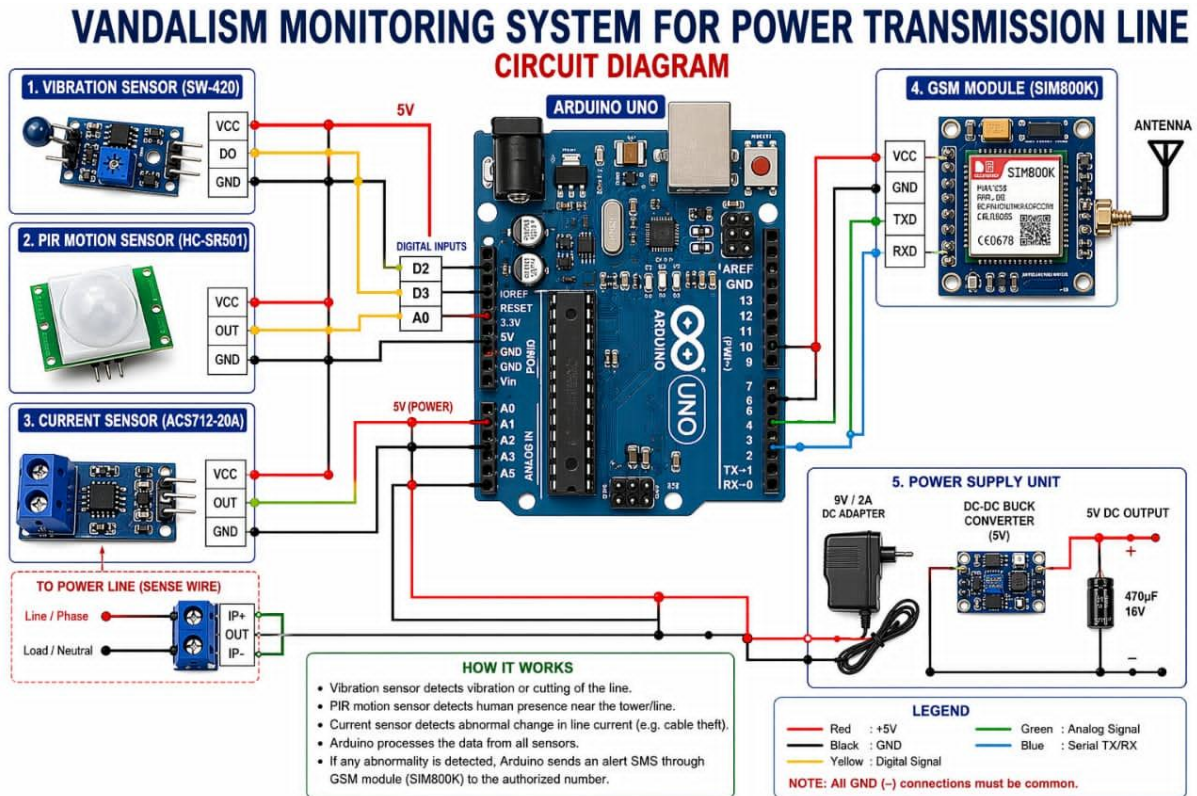


Fig 2 illustrating the circuit diagram of power transmission line vandalism monitoring system.

4. Hardware Construction (System development and prototype implementation)

The hardware implementation involved the design and integration of all electronic modules into a compact prototype system.

4.1 Components Used.

Component	Function
ESP32	Main controller
SIM800L	GSM communication
PIR Sensor	Motion detection
Vibration Sensor	Mechanical disturbance detection
Current sensor	Current monitoring
Buzzer	Alarm notification
LCD Modules	Local display

The signals from the sensors are connected to the digital input pins of the micro controller, where they are processed for appropriate system response as show in fig 2.

The control unit serves as the central processing core of the system. It is built around a micro-controller that continuously monitors inputs, coordinates system operations and ensures proper integration of all components. It also handles status display on the LCD, detects human presence and triggers SMS alerts to the relevant authorities when necessary.

For this project, the ESP32 micro-controller is used. It is a 32-bit Xtensa dual-core, 0 - 240MHz frequency with average power consumption because of Wi-Fi and blue-tooth, it supports both digital input/output operation and built in analog-to-digital conversion. The single-chip controller integrates a microprocessor with several functional features, including multiple analog and digital input pins, flash memory with read-write capability, SRAM storage and wide range of input/output lines for system interfacing. It also includes more advanced and required understanding of networking, serial communication modules such as USART, SPI, and I2C, as well as a 12-bit ADC with multiple channels. The device operate within a voltage range of 2.3V to 3.6V and supports clock of frequencies up to 240MHz with built in Wi-Fi and Bluetooth, hence it can connect directly to cloud services, mobile apps, IoT platforms, and wireless sensors.

To ensure safe handling and ease of maintenance, an IC socket was used to mount the micro-controller on the vero board. This allows the chip to be easily inserted or removed without risk of damage, especially during soldering and

future upgrades or replacements.

4.2 Power Supply Design

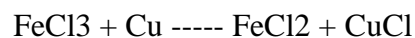
The power subsystem was designed to support solar- powered deployment for remote transmission environments and it consists of Step-down transformer, Rectifier circuit, Filter capacitors, Voltage regulators and Rechargeable battery backup.

5 PCB Fabrication

PCB development was carried out using Proteus and KiCad design environments. The fabrication procedure included Schematic capture, Component placement, PCB routing, Toner transfer, Chemical etching, Drilling and Component soldering.

Ferric chloride solution was used during the etching process.

Chemical reaction:



6. Software Development

The embedded software was developed using Arduino IDE with C/C ++ programming language.

The software performs the following operations, System initialization, Sensor acquisition, Signal conditioning, Sensor fusion, Decision making, GSM communication, and IoT cloud update.

The software algorithm continuously monitors sensor state and activates alarms whenever suspicious activities are detected.

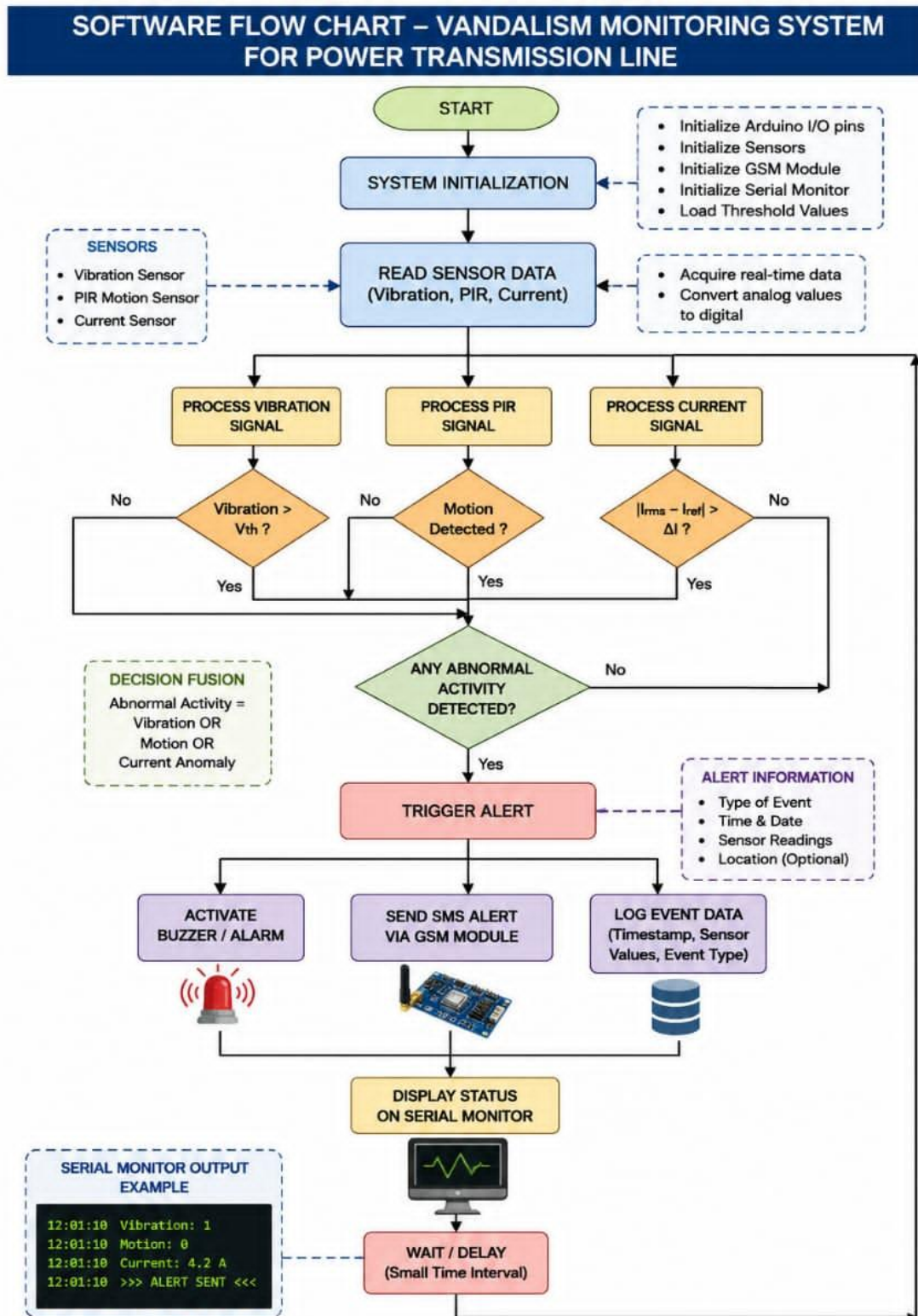


Fig 3 illustrating the flowchart diagram of power transmission line vandalism monitoring system.

The micro-controller program is designed to run a set of instructions in a strict sequence, ensuring the system operates smoothly and without errors. Because of this the code must be carefully structured so that each task is executed in the

correct order, preventing any form of miscommunication or improper coordination between system components during operation. The flowchart shown in fig 3 illustrates the main steps of the program and how the micro-

controller processes them sequentially. The communication flow such that the sensor detects anomaly, micro-controller processes data, GSM sends SMS, IoT uploads data to cloud and Dashboard updates in real time.

Figure 4 presents the full circuit diagram of the smart monitoring system, showing how all the components are connected and integrated to work together effectively.

The system is powered using a regulated 5V/12V supply. Once power is applied, the sensing unit becomes active and continuously monitors the surrounding environment. The motion detection sensor tracks activity around the transmission line and identifies any nearby human presence. When movement is detected close to the monitored area, it sends a signal to the control unit, which then initiates further verification through the sensing module to confirm any unusual activity around the line. If no intrusion is detected, the micro-controller maintains a normal standby state without

initiating any action. However, once a human present is confirmed within or near the protected area, the system immediately responds by activating the GSM module, alarm and the camera units. This results in real-time SMS alerts and image or video capture being sent to the appropriate authorities for prompt response and necessary action.

7. Experimental Implementation

The prototype system was experimentally tested on a simulated transmission tower environment.

The following vandalism scenarios were simulated, Tower climbing, Metal cutting, Hammer impact, Unauthorized access and environmental noise disturbances.

The measured parameters are: Detection time, Detection accuracy, False alarm rate, Communication latency and power consumption.

Experimental Results

The obtained confusion matrix results are summarized below

Parameter	Value
True Positive TP	94
True Negative TN	92
False Positive FP	4
False Negative FN	10

Additional system measurements are shown below:

Parameter	Value
Average Detection Time	1.8 s
GSM Alert Delay	5.2 s
IoT Synchronization Delay	2.4 s
Power Consumption	6.5 w
System Uptime	98%

8. Performance Evaluation

Accuracy.

The system accuracy is computed as;

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Substituting experimental values

$$\text{Accuracy} = \frac{94 + 92}{94 + 92 + 4 + 10}$$

Accuracy = 93%

Precision

$$\text{Precision} = \frac{TP}{TP + FP}$$

Precision = 95.9%

Recall

$$\text{Recall} = \frac{TP}{TP + FN}$$

Recall = 90.4%

False Alarm Rate

$$\text{False Alarm Rate} = \frac{FP}{FP + TN}$$

False Alarm Rate = 4.17%

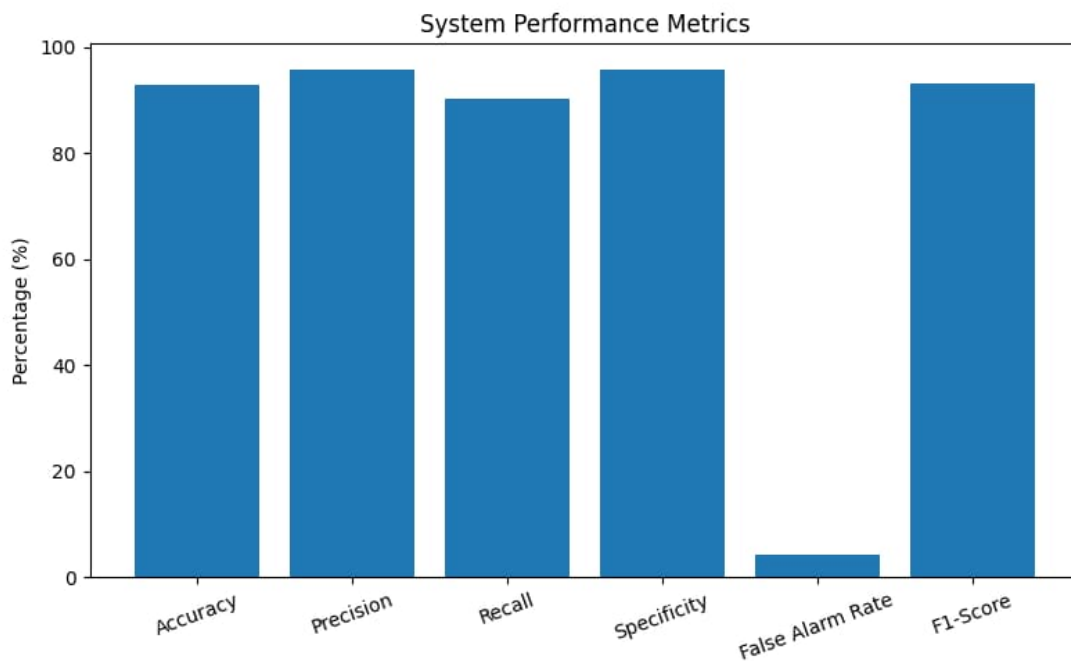


Fig 4 illustrating the graphical representation of the system.

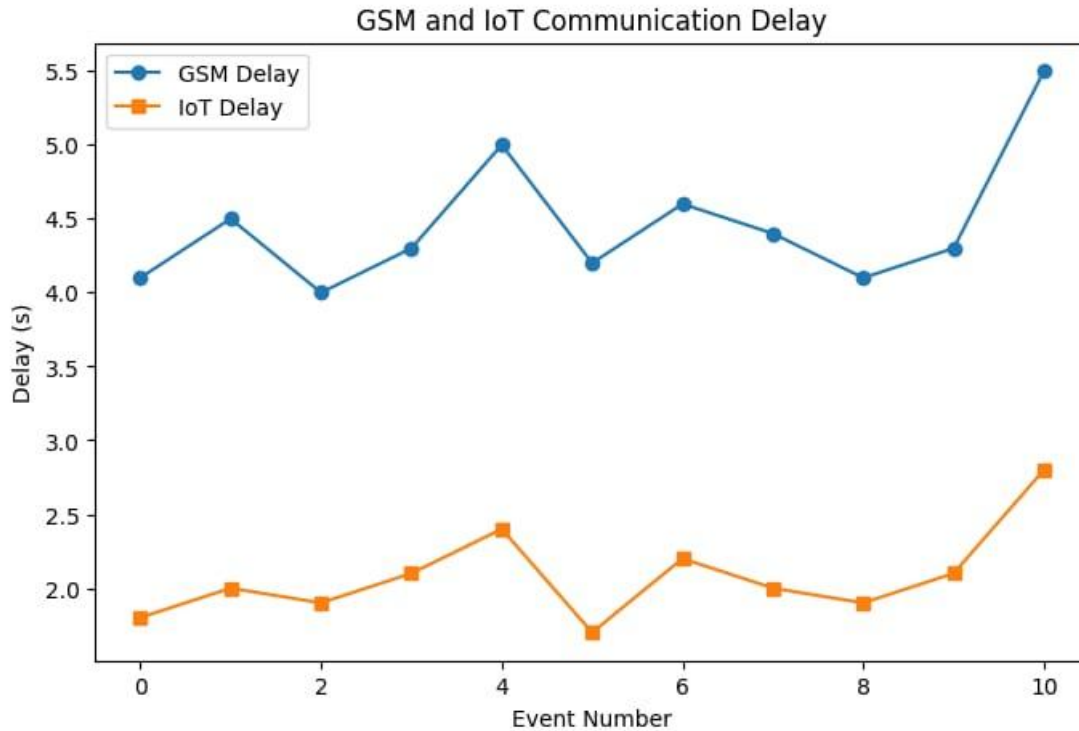


Fig 5 illustrating the GSM and IoT communication delay.

9. Discussion of Results

Figures 4 and 5 illustrates the graphical representation of the system performance metrics and GSM/IoT communication delay. The developed system demonstrated high detection performance under varying vandalism scenarios. The integration of multiple sensors significantly improved detection reliability and reduced false alarms compared to single-sensor approaches.

The vibration and acoustic sensors showed excellent sensitivity during metal cutting and climbing simulations, while the PIR sensor effectively detected unauthorized movement around the monitored area.

The GSM communication subsystem successfully transmitted emergency SMS notifications within an average delay of 5.2 seconds. Similarly, the IoT subsystem achieved near real-time cloud synchronization with an average delay of 2.4 seconds.

The overall system accuracy of 93% confirms the effectiveness of the proposed multi-sensor fusion architecture for transmission infrastructure security applications.

10. Conclusion

This paper presented the design and implementation of a smart vandalism detection and monitoring system for power transmission lines using multi-sensor integration and GSM/IoT communication technologies.

The developed system successfully combines intelligent sensing, embedded processing, wireless communication, and cloud monitoring into a reliable security platform capable of detecting unauthorized activities in real time.

Experimental results demonstrated high detection accuracy, low false alarm rate, fast communication response, and stable system operation. The proposed system provides a practical and scalable solution for enhancing power transmission infrastructure security, especially in remote and vandalism-pron environments.

Future work may include machine learning-based intrusion classification, drone-assisted surveillance integration, and edge-computing optimization for autonomous smart grid protection.

References.

- Abdulhamid Musa, (2023). Implementation of a power line vandalism monitoring system via the internet of things, International journal for research in applied science & engineering technology (IJRASET) ISSN: 2321-9653: IC value: 45.98: SJ Impact Factor: 7,538 volume 11 Issue IV Apr 2023- Available at www.ijraset.com
- Adenikinju, A. F. (2003). Electric infrastructure failures in Nigeria; a survey-based analysis of the costs and adjustment responses, Elsevier, vol. 31(14) pp 1519-1530. Energy policy 2003.
- Adesina, L. M. Ajenikoko, G. A. Ogunbiyi O. and Oluwafemi. T. S. (2020). Symmetrical components of Transmission line parameters based on the installed tower ground resistivity, International journal of recent technology and engineering (IJRTE), ISSN: 2277-3878. Volume-8, Issue-6. Pp 1987-1994.
- Ahmed, S., & Mahmoud, A. (2020). Smart Monitoring System for Electrical Infrastructure, International Journal of Smart Grid, (Theoretical and Empirical Researches in Urban Management), vol. 4(2(11)), pp 87-94.
- Akyildiz, I. F, Su W, Sankarasubramaniam, Y, and Cayirci, E. (2002), "Wireless sensor Network ; A survey" IEEE communication s magazine, vol 38, no.4, pp. 393-422.
- Aniebiet, I. & Sunday Fidelix (2020). Design and Implementation of GSM-enabled remote Sensor for monitoring Power Transformer Operation. American Journal of Electrical and Computer Engineering. Science Publishing Group. ISSN 2640-0480, Vol 4, Issue 2, pp 62.
- Antonius A., Triyanto D., & Ruslianto I., (2015). Penerapan Pangolahan Citra Dengan Metode Adaptive Motion Detection Algorithm Pada Sistem Kamera Keamanan Dengan Push Notification Ke Smartphone Android. Coding Jurnal Komputer dan Aplikasi 3(2) 2015
- Bayo, (2016). The cost of vandalizing public properties. Retrieved January 19, 2019, from punchng: <https://punchng.com/the-cost-of-vandalizing-public-properties/>
- Daily Trust 2022, <https://dailytrusr.com/how-vandalism-may-hamper-10000mw-grid-tatget/>
- Dasgupta Rhythm, (2017). Motion activated wireless surveillance security camera using Raspberry pi, 10.13140/RG.2.2.31134.02886. 2017.
- Eluwande A. D. and Ayo, O. O. (2016). Above ground pipe line monitoring and surveillance drone reactive to attacks; 3rd International conference on African development tissues (CU-ICADI), vol. 5, no. 1. Pp. 437-443. 2016.
- Espressif Systems "ESP32 Technial Reference Manual 2023
- Fezari M, Dahoud A. A., (2019). Internet of things (IOT) using Raspberry pi . Retrieved from <https://www.researchgate.net/publication/330513589> Internet of Things IOT using Raspberry pi (Terakhir dikunjungi 20 september 2019).
- Gungor V. C, and Hancke G.P. (2009), "Industrial wireless sensor Network: Challenges, Design, Principles and Technical Approaches," IEEE Transactions on industrial Electronics, vol, 56, no 1o, pp, 4258-4265
- Kirunguru, E., Huang, Q., & Ayambire, P. N. (2018). Design and Implementation of a transformer vandalism monitoring system. International Journal of Sensors and Sensor Network. Science Publishing Group, Vol 5, Issue 6.
- Kumar K. K, Natraj H. & Jacob T. P. (2017). Motion activated security camera using Raspberry pi. In 2017 International conference on communication and signal processing (ICCSP) (pp. 1598-1601).IEEE. April, 2017.
- Kumar M, S., Prasanna K., R. & Jebaseelem S. D. (2014). Monitoring and Protection of remote Area Transformer using GSM Technology. International Journal of Engineering Research & Technology (IJERT). ISSN 2278-0181, Vol 3, Issue 2.
- Li, L. & Zhao H. (2015). Power line monitoring data transmission using wireless sensor Network. Journal of Power and Energy Engineering. www. Scrip.org, Vol 3, No 8.
- Lin, J., Zhu, B., Zeng, P. & Xiao Y. (2014). Monitoring power transmission lines using a wireless sensor Network , Wireless Communications and Mobile Computing , www.researchgate.net, Vol 15(14)

Mohammed Shafeeq K. K. & Maqbool Thoufeeq T, (2018). Android Board based intelligent car anti-theft system through face recognition using GSM and GPS. Journal of Applied Informational Science, 6(2), 01-05. 2018

Odili and Mokwunye (2003), Minimizing fuel wood consumption through the evolution of hot-stone cooker as an alternative domestic energy supply. Retrieved sept. 12, 2011 from <http://www.ajol.info/index.php/jasr/article/view/File/2785/11352>

Ogujor, E, Inegbenosa S. U. and Esenogho, E, (2013). Implementation of a prototype microcontroller based anti-pipe line vandalization system ; International journal of emerging technologies in engineering research, vol. 2 no 1. Pp. 1- 14. 2013.

Olaqluwa, O. G.(2017). Electricity theft and power quality in Nigeria; International journal of engineering research & technology (IJERT). June 2017. 6(6)

Olwal, T. O, Kurien A. M, and Abu-Mahfouz, A, M.(2018). IoT-Based utility monitoring for Smart Grid Applications IEEE Access, vol.6, pp. 27589-27601

Salauddin B., & Jamil Hossain M (2023). Power transformer monitoring and controlling using GSM, www.researchgate.net.

Doi:10.13140/RG.2.2.18607.71844

SIMCom Wireless Solutions, SIM800L Hardware Design guide.2022

Suliman A. S. Ahmed B. M., Elareefi M. B., Abdulwahab M. M ,, Arbab E. A. (2022). Monitoring system for overhead power transmission lines in smart grid system using internet of things. University of Khartoum Engineering Journal. 12(1) pp 1-5

Vandalism and the Power Sector (2016, May 9), Retrieved january 19, 2019 from thisday; <https://www.thisdaylive.com/index.php/2016/05/09/vandalism-and-the-power-sector/>

[Walendra D. M. \(2021\). GSM-based model to detecting Electrical theft and Iregular usage across Globe. International Journal of Engineering Research and technology \(ijert.org\). doi: //10.17577/IJERTCON9ISO4008. ISSN 2278-0181, Vol 09, Issue 04](#)

[Zhang, Y., Wang, L., & Sun, W. \(2021\). IoT-based Smart Grid Monitoring, IEEE Internet of Things Journal. Energy Reports, 7, 452-463.](#)

[Zulu,C. L. & Dzobo O. \(2023\). Real-time power theft monitoring and detection system with double connected data capture system. Springer Electrical Engineering, Vol 105, pp 3065-3083, https://link.springer.com.](#)