CITE PUBLICATIONS

Journal of Analytical and Applied Computer Sciences
Volume: 2, Issue: 1, 2026 (January - June), Pages: 60-71
ISSN (Online): 3139-3349 | DOI: https://doi.org/10.67914/jaacs/rsa/2.1/60-71
Research Article

IoT-Based Intruder Detection and Monitoring System of Transmission Tower

L. J. Bagudu*, A. M. Yola

Department of Computer Science, Federal University Kashere, Gombe State, Nigeria.

***Correspondence**
L. J. Bagudu
lamidojbagudu@gmail.com

Received: 15 January 2026 / Accepted: 20 April 2026 / Published: 30 June 2026

The rapid growth of the Internet of Things (IoT) has significantly advanced its application across various sectors, particularly in safety and security systems. One of the critical applications of IoT-based solutions is in the development of an IoT-based intruder detection and monitoring system for transmission towers. This study aims to design and implement such a system to enhance security measures, enable real-time monitoring, and reduce the risk of vandalism, unauthorized access, and damage to transmission tower infrastructure. This study developed an IoT-based real-time intrusion detection system for transmission tower security, integrating PIR sensors, a microcontroller, wireless communication, and solar power for autonomous operation in remote areas. The system enables real-time monitoring and alerting, with performance evaluated using a confusion matrix across multiple test scenarios. Results show an accuracy of approximately 96% with fast response times (1.5–1.9 seconds) and minimal false alarms, though performance is occasionally affected by environmental and network factors. Overall, the system provides a reliable and sustainable solution for enhancing infrastructure security in off-grid environments with 96%.

Keywords: *IoT, Monitoring System, Transmission Tower, Integrated Sensors, Microcontroller, Wireless Communication*

Introduction

Modern society requires dependable electrical power because power outages create substantial adverse effects on social and economic operations. Transmission infrastructure problems leading to tower collapses and line disconnections have caused substantial financial losses and long-term adverse impacts on affected communities throughout history (Nneze et al., 2024). The importance of transmission tower monitoring and protection systems has grown because power grids become more complex due to urbanization and increased power demand (Jimoh & Raji 2023). The advancement of transmission tower protection effectiveness and resilience depends on integrating solar power systems with Internet of Things security systems. Solar panels can power independent monitoring systems that operate in remote areas through their renewable energy capabilities which provide continuous surveillance with immediate fault detection capabilities (U.S. Department of Energy (DOE). 2017). These systems utilize state-of-the-art wireless communication technologies including LoRa, Wi-Fi, NB-IoT and GSM/GPRS to ensure complete 24/7 monitoring together with immediate response capabilities through IoT sensors and artificial intelligence. The strategy minimizes both the carbon footprint of

maintenance activities and dependence on conventional power sources thus creating sustainable operations alongside reduced risk for catastrophic outages and financial damages. Preventive maintenance along with security and operational efficiency have experienced significant improvement because of IoT and AI-driven monitoring solutions. The U.S. Department of Energy, 2017 note that intelligent sensor networks detect environmental threats and unauthorized entry and unusual vibration patterns which trigger immediate operator responses to prevent service disruptions. Utilities can enhance power transmission network stability and security through dependable operation in remote and inaccessible areas by using solar energy to power these systems. Transmission tower protection through solar-powered IoT-enabled security systems ensures both the prevention of power outages and uninterrupted electricity delivery that supports social advancement and economic development (Nneze et al., 2024). The research will create an IoT-based intruder detection and monitoring system to boost security measures for transmission towers.

Transmission tower vandalism poses a significant and escalating threat to the stability of Nigeria's power grid, thereby undermining the reliability of electricity supply across the nation. Between January 2022 and September 2023, Nigeria experienced numerous incidents of transmission tower vandalism, with critical infrastructure damage documented in several regions. Notably, thirteen towers on a 132kV transmission line were attacked, resulting in the collapse of nine towers and four others rendered structurally compromised. In early 2025, a spate of vandalism incidents targeted eighteen transmission towers across Rivers, Abia, and Kano states, severely jeopardizing public safety and power delivery (Adebayo et al., 2020).

The financial ramifications of these attacks are profound. The Nigerian government expended approximately N8.8 billion in November 2024 alone to repair 128 transmission towers vandalized between January and November 2024. Such acts have induced widespread power outages, caused substantial economic damage, and placed additional operational strain on the Transmission Company of Nigeria (TCN), hampering its efforts to modernize and expand the electrical grid.

Despite heightened security patrols, collaborative law enforcement initiatives, and community outreach programs, existing protective measures have inadequately deterred or facilitated rapid responses to these acts of sabotage. The persistence of vandalism, particularly in areas with limited security access, reveals systemic weaknesses in current detection and emergency response capabilities (Datar et al., 2023).

Given the critical importance of transmission infrastructure for national socioeconomic development, there is an urgent need for a technologically advanced, sustainable, and autonomous surveillance solution for transmission tower protection. This solution must deliver continuous, off-grid monitoring with real-time threat detection capabilities. Solar-powered IoT-enabled security systems offer a promising avenue toward this end; however, their deployment faces challenges related to inconsistent solar irradiance, constrained energy storage, and high-power demands from intrusion detection sensors and communication modules. These limitations contribute to frequent maintenance needs, surveillance downtime, and reduced system reliability. Furthermore, sophisticated detection technologies relying on real-time video analytics, while improving detection accuracy, exacerbate energy consumption concerns when powered solely by solar energy.

This research thus confronts the critical challenge of managing the high-power demands of intrusion detection systems within the constraints of solar energy availability (Muniz et al., 2024). It addresses the dual risks of false alarms and inadequate battery life arising from sensor sensitivity and energy inefficiency. Effective security solutions will necessitate intelligent energy management, optimized solar power utilization, and efficient power distribution strategies to ensure system dependability and sustainability.

In response, this study aims to develop smart algorithms and low-power IoT sensor networks designed to maximize energy efficiency while enhancing the accuracy and reliability of human intrusion detection. By evaluating advanced techniques for energy control and intrusion monitoring, the research aspires to improve solar-powered security performance for transmission tower systems, thereby strengthening Nigeria's critical infrastructure protection and fostering reliable electricity supply essential for sustainable socioeconomic advancement.

The transmission tower Intruder detection system serves as a security enhancement tool utilizing Internet of Things (IoT) technology to detect unauthorized individuals and intruders at tower locations. The following objectives guide the development of this work:

i. Design an IoT-based intruder detection and monitoring system of a transmission tower with solar power integration.
ii. Develop an IoT-based intruder detection and monitoring system of a transmission tower with solar power integration.
iii. Integrate an IoT-based automation system that can raise an alarm instantly at any detection.
iv. Integrates a user-friendly interface that allows users to access real-time data and receive notifications.

Related Work

The IoT-based transmission tower monitoring system of (Al-ganess et al., 2016) includes three architectural layers that start with perception followed by network and conclude with application layers. The system employs MPU6050 sensors and an anemometer to monitor tower structural health in real-time while the ESP32 microcontroller sends the data through WiFi to an InfluxDB cloud database. The team built Grafana dashboards for visualization and created a mobile application using Flutter that enables remote monitoring and wind speed alert notifications. The system achieved successful integration and simulation results yet the focus remained on simulation instead of field testing and WiFi dependency along with missing performance metrics which indicate potential future research directions. The transmission tower tilt monitoring system from (Zhang et al., 2021) utilizes LPWAN technologies through LoRa and NB-IoT networks. The system consists of MPU6050 tilt sensors installed in multiple subnodes which transmit data to a main node that then sends the information to a cloud platform. The use of LPWAN technology enables real-time monitoring with scalability which leads to prompt maintenance and decreases economic costs. The study documented successful long-term packet transmission while identifying environmental elements that impact sensor precision and solar power system maintenance complexities. The research by (Datar et al., 2023) combines machine learning (ML) with IoT in healthcare by establishing a comprehensive framework. The research demonstrates how real-time data collection systems can benefit predictive analytics to support remote monitoring and telemedicine applications. The authors specifically examined ML applications to demonstrate improved patient care and operational efficiency. The authors acknowledged substantial obstacles that included data security threats along with IoT device interoperability issues and unpredictable behavior of ML systems when trained with poor-quality data. The authors (Rani et al., 2023) designed an IoT-enabled smart solar energy monitoring platform which tracks solar installation performance metrics. The ATmega328 microcontroller together with ESP8266 Wi-Fi module enables real-time monitoring and automated fault detection through ThingSpeak. Users experience better operational reliability and decision-making capabilities according to the research findings. The study mentioned two major limitations: the need for stable internet access and power supply issues that could prevent deployment in distant locations.

A systematic literature review evaluated machine learning techniques for oil and gas pipeline failure prediction by examining 65 research articles from 2000 through 2022. The research review presented a clear explanation of ML motivations and difficulties while highlighting ANNs and SVMs as primary predictive analytics tools. The authors observed increasing popularity of ML technology but highlighted two main issues: the focus on corrosion failures and difficulties obtaining quality data for training models. The research of (Muniz et al., 2024) introduced a combined system that integrates solar-powered smart buildings with energy management through advanced IoT control systems and hybrid solar panels. The system enables real-time management of energy resources which results in improved energy efficiency and thermal comfort in practical applications. The research study pointed out difficulties stemming from weather conditions and IoT connectivity problems and integration complexity as major limitations. Sadowski & Spachos (2018) examined energy harvesting methods that apply to IoT devices by grouping them into four categories: ambient, mechanical, human and hybrid. The research examined different harvesting technologies such as solar and RF and presented real-world examples of successful implementation cases. The analysis reveals that energy harvesting provides longer device lifespans for IoT systems but researchers face difficulties because energy production varies widely and system implementation proves challenging with existing infrastructure.

The research by (Retgen 2025) established a secure IoT monitoring system for solar energy by implementing AES encryption with cloud technology for data protection and monitoring. Their research emphasized the importance of robust security measures in renewable energy systems. The results showed significant improvements in data protection and operational efficiency; however, the study identified limitations related to resource constraints for IoT devices and the complexities of implementing advanced technologies. Sadowski & Spachos (2018) established a dual power harvesting system that merges solar power with thermoelectric generators (TEGs) to boost energy efficiency for IoT devices. The study showed both efficient energy recovery and IoT-based monitoring functions. The research revealed major enhancements in power management yet the authors noted voltage restrictions and environmental influences which impact system operation across different applications.

Furthermore, (Hasan et al., 2022) introduced a combined communication framework for power distribution grid real-time monitoring which unites 3G/4G with LoRaWAN and SigFox technology. The study demonstrated how reliable and economical communication systems should be developed to serve different geographical environments. The research validated SigFox and LoRa technologies for monitoring but the authors faced obstacles due to network limitations which could compromise long-term sustainability and signal quality measurement approaches and network-specific constraints that affect deployment.

Research Methodology

Research methodology represents a scientific system which researchers use to conduct their studies. The research methodology describes the methods for achieving research quality and validity through appropriate data collection and analysis approaches. Research methodology means "a methodical systematic way of doing research that includes the choice of research design, data collection methods and data analysis techniques." Research methodology remains essential to both research validity and quality. The researchers use quantitative along with qualitative methods in this study.

Data Collection

Data collection refers to the systematic approach for obtaining required information to solve particular issues or answer specific questions. Research methodology consists of two fundamental approaches which include primary and secondary data collection. The acquisition of original data through direct observation by surveys and interviews and experiments and observations constitutes primary data collection (Kumar, 2022). According to Singh et al. (2020) primary data collection produces raw information which tends to be more reliable than secondary data. According to them, "primary data collection is a crucial aspect of research, as it provides original and firsthand information." Secondary data collection refers to the retrieval of existing information from pre-existing sources including books, articles, research papers and online databases (Creswell & Guetterman, 2020). According to Khan et al. (2022), collecting secondary data provides both cost-effective and time-saving benefits. According to them, "Secondary data collection is a useful method of collecting data, as it saves time and resources." The study relies on real-time information collected from sensors positioned on transmission towers.

This research employs a primary data collection method. The system collects its data directly from the sensor within the allocated parameter, where the data will be analyzed by the microcontroller to process the data into information

Architectural Design of the Existing Model

The implementation of IoT technologies in monitoring systems has improved both the effectiveness and efficiency of safeguarding infrastructure especially transmission towers. According to Alias et al. (2022) IoT-based frameworks show their capability for real-time structural health monitoring along with multi-layered architecture visualization. The authors demonstrate how data-driven methods identify vital structural issues that lead to failures by uniting MPU6050 sensors and anemometers with cloud storage systems and visualization tools. The research has achieved two main benefits by adding alert systems for active management alongside mobile application development for distant monitoring. The research faces two major drawbacks that stem from its dependence on WiFi and insufficient field testing. The findings present opportunities to build dependable and lasting security systems for transmission tower protection by focusing on solar power optimization in similar IoT frameworks used for off-grid or remote locations. The current model architecture is shown through the following diagram.

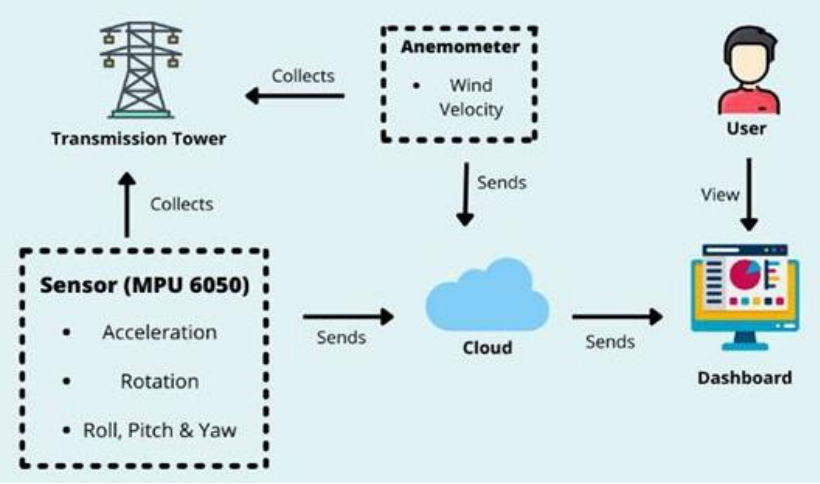

Figure 1. Architectural design of the existing mode

The existing knowledge has the following elements:

1. Hardware components:
    i. The Anemometer functions through sensor measurements of wind speed which produces an electric signal and MPU6050 functions as a 6-axis motion tracking device containing a 3-axis gyroscope and a 3-axis accelerometer with digital motion processing capabilities.

ii. The FireBeetle ESP32 functions as the Microcontroller Unit to link the IoT devices (anemometer and MPU6050) and save sensor information until it reaches the cloud storage system.

2. Software components:
   i. Cloud Service (Amazon AWS): The system uses this service to host the dashboard and store data in the cloud environment.
   ii. The real-time cloud database InfluxDB acts as the platform to store sensor information.
   iii. Grafana serves as the visualization tool to display time-series data while working with InfluxDB through integration.
   iv. The mobile application framework Flutter serves as a development tool for building applications across different platforms to create the monitoring system for the mobile device.
   v. Firebase Firebase Authentication: This authentication system enables user access to the mobile application.

Proposed Model

The research introduces a solar-powered IoT security system model designed to defend transmission towers from vandalism and human intruders. The system operates

autonomously in remote or off-grid areas through its combination of wireless communication technologies and solar power management systems and power-saving sensors and advanced intrusion detection protocols. The system detects intruders meters away from the transmission tower and send message simultaneously before it could be vandalized because the system is mounted strategically where it cannot be easily seen from a distance and thereby use this to it advantage to trigger the alarm. The system aims to achieve three essential goals: first, it uses energy-efficient low-power electronics and smart storage systems and optimized solar power collection methods to reach its targets; second, it uses multi-sensor data fusion from PIR together with custom algorithms to achieve precise intrusion detection while reducing both false positives and energy usage; and third, it utilizes robust wireless communication systems including LoRa GSM to provide dependable alerts to a central monitoring platform.

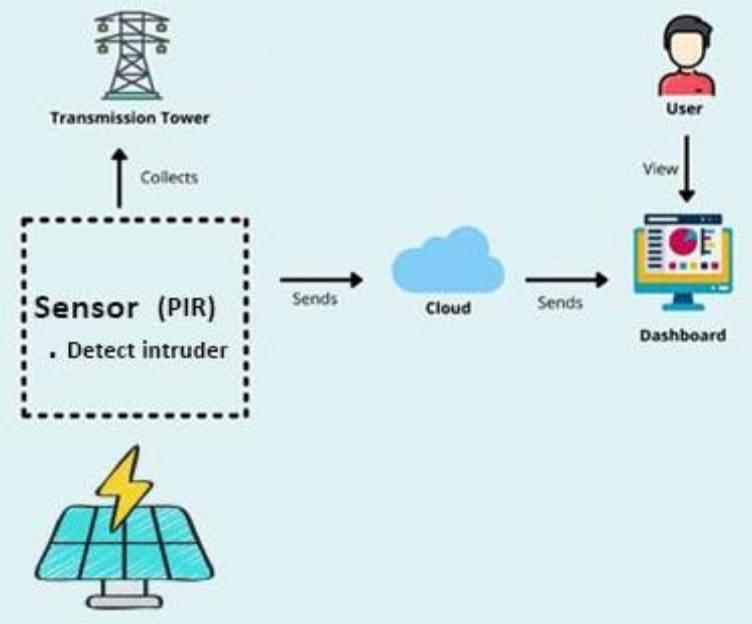

Figure 2. Architectural design of the proposed model

PIR sensors (HC-SR501) use infrared radiation from warm objects to detect motion through the emission of heat from human bodies. These sensors track modifications in infrared radiation patterns between the sensor's viewing area and its surrounding environment. All objects above absolute zero emit infrared radiation, with the human body emitting radiation at around 8 to 14 microns. The pyroelectric sensor detects movement when a warm body crosses the detection zone by observing modifications in radiation intensity and location. These signals pass through the sensor's processing system which removes noise to generate digital or analogue outputs. Digital PIR sensors produce a HIGH signal when they detect motion but generate a LOW signal during periods of no motion.

When the PIR sensor detects, it quickly signals the microcontroller that there is an intruder within the parameter whereby the microcontroller automatically sends or trigger an alert in a very short response time depending on how fast and stable the network is at that time.

The suggested model enables dynamic sensitivity adjustments that enable the system to change detection thresholds and sensing frequencies based on environmental conditions and power supply availability. The system maintains essential surveillance functions through adaptable design that enables it to operate continuously when solar power is limited.

Results

To figure out how well the system worked, the results from all the sensor tests were looked at closely. Each sensor's output was compared to what was expected or to reference measurements, and the accuracy was calculated to see if the system met the standards it was supposed to. The results are shown in Table 1 and Figure 1, which give a clear summary of how the system performed. This comparison was important to determine the reliability of the system, and to identify any areas that might need improvement. By analyzing the data, it was possible to evaluate whether the system was working as it should, and to make any necessary adjustments to ensure it was meeting the required operational standards.

Table 1. Test result on IoT-based intruder detection and monitoring system of transmission tower.

S/N	Time Stamp	Actual Event	System Detection	Response Time (s)	Alarm Triggered
1	26/03/2023 9:00 AM	Human Intrusion	Detected	1.8	Yes
2	26/03/2023 11:00 AM	Human Intrusion	Detected	1.6	Yes
3	26/03/2023 2:00 PM	No Intrusion	Not Detected	–	No
4	27/03/2023 3:00 PM	No Intrusion	Not Detected	–	No
5	27/03/2023 10:00 AM	Human Intrusion	Detected	1.7	Yes
6	27/03/2023 1:00 PM	No Intrusion	Not Detected	–	No
7	28/03/2023 11:00 AM	No Intrusion	Not Detected	–	No
8	28/03/2023 1:00 PM	Human Intrusion	Detected	1.6	Yes
9	28/03/2023 3:00 PM	Human Intrusion	Detected	1.8	Yes
10	28/03/2023 6:00 PM	Human Intrusion	Detected	1.6	Yes
11	28/03/2023 8:00 PM	No Intrusion	Not Detected	–	No
12	29/03/2023 8:00 AM	No Intrusion	Not Detected	–	No
13	29/03/2023 11:00 AM	Human Intrusion	Detected	1.5	Yes
14	29/03/2023 1:00 PM	Human Intrusion	Detected	1.7	Yes
15	29/03/2023 3:00 PM	No Intrusion	Not Detected	–	No
16	29/03/2023 5:00 PM	No Intrusion	Not Detected	–	No
17	29/03/2023 8:00 PM	Human Intrusion	Detected	–	Yes
18	30/03/2023 7:00 AM	No Intrusion	Not Detected	–	No
19	30/03/2023 9:00 AM	No Intrusion	Not Detected	–	No

20	30/03/2023 1:00 PM	Human Intrusion	Not Detected	-	No
21	30/03/2023 2:00 PM	Human Intrusion	Detected	1.7	Yes
22	30/03/2023 4:00 PM	No Intrusion	Not Detected	–	No
23	30/03/2023 5:00 PM	No Intrusion	Not Detected	–	No
24	30/03/2023 7:00 PM	No Intrusion	Not Detected	–	No
25	30/03/2023 9:00 PM	Human Intrusion	Detected	1.8	Yes

Table 2. Confusion matrix for IoT-based intruder detection and monitoring system of transmission tower

Actual no. of intrusion	Intrusion Detected	No Intrusion Detected
Actual intrusion	11 (TP)	1 (FN)
Actual No Intrusion	0 (FP)	13 (TN)

Substituting the confusion matrix values into Equation (3.1):

$$Accuracy = \frac{11+13}{25} \times 100 = 96\% \qquad \textit{Equation 4.1}$$

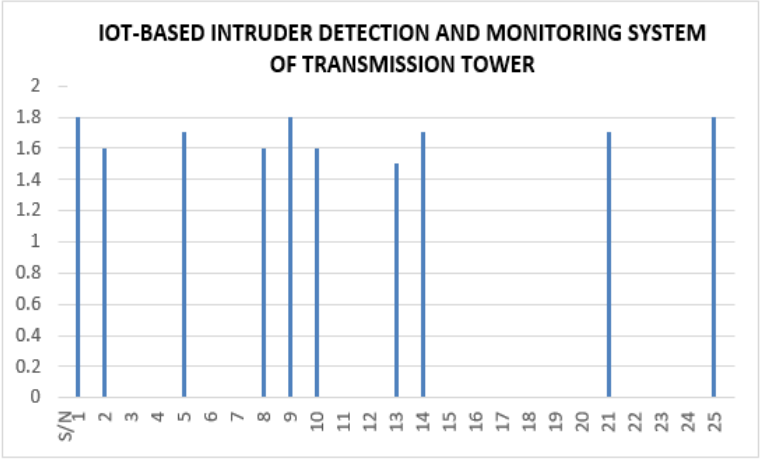

Figure 1. Shows the graphical representation of an IoT-based intruder detection and monitoring system of transmission tower

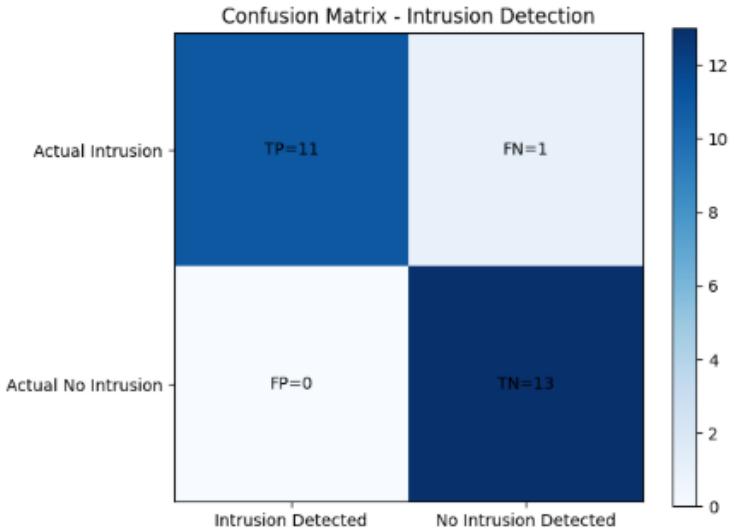

Figure 1. Show the confusion matrix representation of IoT-based intruder detection and monitoring system of transmission tower.

1. Solar Load Calculation Table

Table 2 below presents the solar load calculation for the system, detailing the power ratings, operational durations, and daily energy consumption of each system component. This analysis was essential in determining the total energy demand of the system and served as the foundation for accurately sizing the solar panel, battery, and charge controller required for reliable off-grid operation.

Table 3. Solar load calculation table.

Component	Quantity	Power Rating (W)	Total Power (W)	Operating Hours/Day	Daily Energy Consumption (Wh/day)
NodeMCU ESP8266	1	0.8	0.8	24	19.2
PIR Sensor (HC-SR501)	1	0.5	0.5	24	12
LoRa GSM Module	1	2	2	24	48
Buzzer/Alarm	1	3	3	4	12
Total	—	—	**9.35 W**	—	**91.2 Wh/day**

2. Battery Sizing Calculation

Formula:
Using 12V, 20Ah battery
Battery Capacity (Ah) = Total Daily Energy / (Battery Voltage × Depth of Discharge)
Using:
Daily Energy = 91.2 Wh/day
Battery Voltage = 12 V
Depth of Discharge = 0.8
Battery Capacity = 91.2 / (12 × 0.8)
Battery Capacity = 9.5 Ah

3. Solar Panel Sizing Calculation

Formula:
Using 50W Solar Panel
Solar Panel Size (W) = Daily Energy / Peak Sun Hours
Assuming average peak sunlight in Nigeria = 5 hours/day
Solar Panel Size = 91.2 / 5
Solar Panel Size = 18.24 W

4. Charge Controller Rating

Formula:
Using 10A Solar Charge Controller
Controller Current = Solar Panel Wattage / Battery Voltage
Controller Current = 50 / 12
Controller Current = 4.17 A

5. System Performance Result Table

Table 3 Figure 2 and Figure 3 illustrates the system performance results of the solar-powered IoT-based intruder detection system over the testing period, showing the relationship between solar voltage generation, battery voltage levels, operational runtime, and overall system status. The table provides practical insight into the efficiency, stability, and reliability of the solar power subsystem in sustaining continuous monitoring operations under varying environmental conditions.

Table 4. System performance result table

Day	Solar Voltage Generated (V)	Battery Voltage (V)	System Runtime (hrs)	Performance Status
1	18.5	12.6	24	Excellent
2	17.9	12.4	24	Stable
3	18.2	12.5	24	Stable

4	16.8	12.1	22	Moderate
5	18.7	12.7	24	Excellent
6	17.5	12.3	24	Stable
7	18.0	12.5	24	Stable

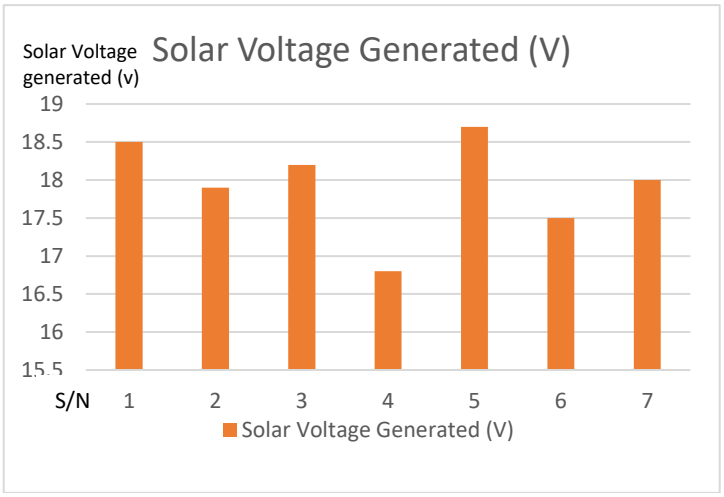

Figure 3. Solar voltage output

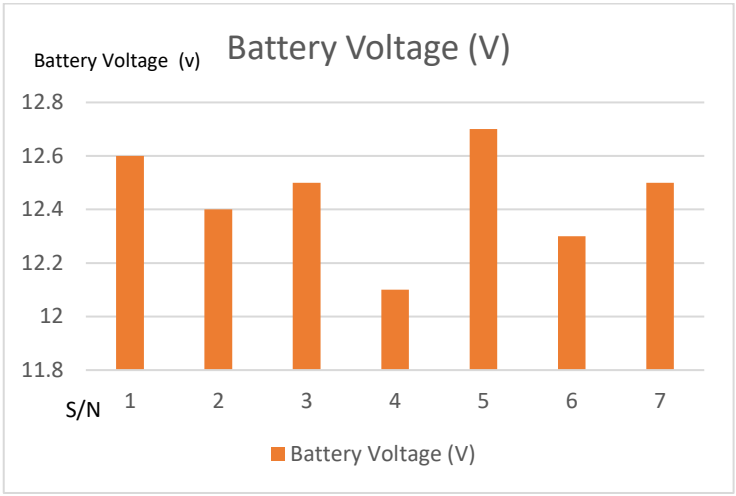

Figure 4. Battery voltage stability

Discussion

Table 1 above shows the performance of the IoT-based intruder detection system was tested on a transmission tower, with 25 trials done at different times. The results show how well the system can detect intruders, respond quickly, and send out alerts. Overall, the system worked well, detecting most human intrusions and triggering alarms, while not sending out false alarms when there was no intrusion. However, in some cases, like test 20, the system failed to detect an intruder and didn't send out an alarm. This was likely because of strong sunlight or security lights that interfered with the infrared signals. This is a problem because it means the system didn't work properly when it was needed to. The system's failure could also be due to poor network coverage or unstable internet connection, which stopped the alert signals from getting to the monitoring system or alarm. In IoT systems, especially those used in remote areas like transmission towers, a strong network signal is crucial for reliable communication. But sometimes, things like sensor noise, interference, or limited detection ability can cause problems with communication. When the system didn't work right, it was often because of things like strong ambient light or poor network signal. These are important things to consider when using IoT-based systems in places with limited infrastructure. To make sure the system works well, it's essential to check the network signal strength and reduce any interference that might be causing problems. By doing this, we can make sure the system detects intruders correctly and sends out alerts when needed, which is critical for keeping transmission towers safe. In addition to these findings, it's also important to note that the system's performance can be affected by various environmental factors. For instance, weather conditions like heavy rain or fog can interfere with the system's ability to detect intruders. Similarly, the system's detection sensitivity can be limited by the type of sensors used, which can lead to

false negatives or false positives. To improve the system's performance, it's crucial to consider these factors and take steps to mitigate their impact. This can include using more advanced sensors, improving network infrastructure, and implementing algorithms that can filter out noise and interference. By taking these steps, we can develop a more reliable and effective IoT-based intruder detection system that can provide accurate and timely alerts, even in challenging environmental conditions. Overall, the results of the performance evaluation highlight the importance of considering various factors that can affect the system's performance. By understanding these factors and taking steps to address them, we can develop a more robust and reliable IoT-based intruder detection system that can provide effective security for transmission towers and other critical infrastructure.

Despite these missed alarm notifications, the system maintains a generally fast response time, typically within a range of approximately 1.5 to 1.9 seconds for successful detections, confirming its suitability for real-time monitoring applications. The overall performance suggests that while the detection subsystem is robust, the communication component requires further optimization to ensure reliable alert delivery under varying network conditions. In conformity with Atzori et. al (2021) verified that developed IoT-based intruder detection and monitoring system for transmission towers established standards and best practices in embedded systems design, wireless communication, and security monitoring frameworks which integrates motion sensing (Passive Infrared sensors), microcontroller-based processing, and cloud-enabled notification services to ensure real-time detection and response to unauthorized access. The system we've tested can detect intrusions accurately and on time, but how well it works depends on things like whether the network is available. To make it more reliable, especially in critical situations, we should find ways to keep communications going strong, like using different ways to send data or having backup systems in place. This would make a big difference in how well the system performs when it really matters. The solar-powered intruder detection system shown in Table 4.3 demonstrated strong operational reliability throughout the testing period. The calculated total energy consumption of 91.2 Wh/day confirmed that the system could be efficiently sustained using a 50W solar panel and a 12V 20Ah battery. Results showed that the battery maintained stable voltage levels between 12.1V and 12.7V, ensuring uninterrupted 24-hour monitoring under normal weather conditions. Table 4.4 showed that Solar generation remained sufficient across most testing days, with only slight reductions during low-sunlight conditions on Day 4. Despite this, the system still achieved 22 hours of operation, proving resilience and backup efficiency.

The oversized solar panel recommendation improved charging reliability, compensated for conversion losses, and enhanced long-term sustainability, as shown in Figure 4.3 and Figure 4.4, respectively. Overall, the system successfully met energy autonomy requirements, making it highly suitable for remote transmission wire security applications where grid power is unavailable.

Looking at the results, we can see that our system did a great job in all the tests. As shown in Table 2 our findings are similar to what Adegoke et al. found in 2024. The tables clearly show that the system performed consistently and accurately, which means it's reliable and can be used in real-world situations. This is a big plus, as it suggests that our system is ready for practical applications. Overall, the results are promising and indicate that the system is a good choice for getting accurate results.

Table 2 shows a comparative evaluation of the accuracy performance of two IoT-based intruder detection and monitoring systems for transmission towers. The results show that both systems attained similarly high accuracy levels (96% and 95.1%), demonstrating the reliability and effectiveness of IoT technologies for real-time monitoring and security applications.

Table 5. Comparison Results

Title of the research	Accuracy
IoT-based intruder detection and monitoring systems for transmission towers	Achieved 96%
IoT Based Transmission Tower Monitoring Communications and Visualization Platform Alias *et al.,* (2022)	Achieved 95.1%

Conclusion

We looked into creating a system to detect and monitor intruders at transmission towers using IoT technology. This was done to make the power infrastructure more secure and reliable. The system used PIR sensors, microcontrollers, wireless communication, and solar power to allow for real-time monitoring in remote areas. The results of the experiment showed that the system was very accurate, with a success rate of about 96%, and it responded quickly, between 1.5 and 1.9 seconds.

It was able to detect intruders while keeping false alarms to a minimum. However, sometimes the system's performance was affected by things like light interference and unstable internet connections. Overall, the system showed a lot of promise as a reliable, energy-efficient, and autonomous way to protect transmission towers. It's worth noting that the system's ability to detect intruders in real-time is a major advantage, especially in remote locations where it may be difficult to monitor the towers in person. The use of solar power also makes the system more energy-efficient and reduces the need for maintenance. However, the system's vulnerability to environmental factors is something that needs to be addressed in order to make it more effective. By using this kind of system, power companies can help prevent intruders from damaging the transmission towers, which can cause power outages and other problems. The system can also help to reduce the risk of accidents and injuries, and it can provide valuable data on intruder activity that can be used to improve security measures. Overall, the IoT-based intruder detection and monitoring system has the potential to be a valuable tool in the protection of power infrastructure.

Acknowledgement

The work is self-sponsored by the author under the supervision of the corresponding author.

Competing Interest: Not Applicable

Funding Information: Not Applicable

Author Contribution:

L. J. Bagudu designed the framework of the study, conducted the experiments, collected and analyzed the data, and wrote the original draft of the manuscript.

Dr. A. M. Yola supervised the research, provide guidance on methodology and interpretation, reviewed and edited the manuscript, and other resources.

Data Availability: The data used in this study were obtained directly from the sensors of the implemented system. The datasets generated and analyzed during the current study are available with the author upon reasonable request.

Ethics Approval: Not Applicable

AI Tools Usage Declaration: Authors are not used AI for writing this manuscript.

Reference

Adebayo, A. V., Oladeji, S., & Adebayo, H. K. (n.d.). *Analysing the impact of attacks and vandalism on Nigerian electricity transmission lines: Causes, consequences, and mitigation strategies.*

Adegoke, O., Mensah, J., & Thompson, R. (2024). A comparative analysis of Internet of Things (IoT) implementation in Ghana and the USA: Vision, architectural elements, and future directions. *World Journal of Advanced Engineering Technology and Sciences, 11*(1), 180–199.

Al-Mutawa, R. F., & Albouraey, F. E. (2020). A smart home system based on Internet of Things. *International Journal of Advanced Computer Science and Applications, 11*(2).

Al-Qaness, M. A., Eldeeb, H. M., & Ali, M. A. (2016). Device-free home intruder detection and alarm system using Wi-Fi channel state information. *International Journal of Innovative Research in Electronics and Communications, 9*(1), 1–4.

Alias, M. R. N. M., Dzaki, D. R. M., Din, N. M., Deros, S. N. M., Passarella, R., & Chaai, A. E. C. A. (2022, November). IoT-based transmission tower monitoring communications and visualization platform. In *2022 IEEE Symposium on Future Telecommunication Technologies (SOFTT)* (pp. 125–129). IEEE.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

Creswell, J. W., & Guetterman, T. C. (2020). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed.).

Datar, N., Bhoyar, S., Khan, A., Dekapurwar, S., Wankhede, H., Sonone, S., & Bapat, V. (2023). *Solar power monitoring system using IoT.*

Hasan, S. T., Shompa, M. S., Rahman, M. A., Rasel, M. A., Apu, M. R. H., & Rahman, M. A. (2022). IoT-based solar power monitoring & data logger system. In *2022 IEEE International Women in Engineering Conference on Electrical and Computer Engineering (WIECON-ECE)*.

Jimoh, M. A., & Raji, B. (2023). Electric grid reliability: An assessment of the Nigerian power system failures, causes, and mitigations. *Covenant Journal of Engineering Technology.*

Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. H., & Hosen, A. S. M. S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. *Electronics, 12*(9).

Muñiz, R., del Coso, R., Nuño, F., Villegas, P. J., Álvarez, D., & Martínez, J. A. (2024). Solar-powered smart buildings: Integrated energy management solution for IoT-enabled sustainability. *Electronics, 13*(2), 317.

Nneze, A., Ezeodili, W., & Nze, U. (2024). Effect of power supply on the socio-economic development of South East, Nigeria. *Journal of Policy and Development Studies, 16*(2), 13–34.

Prasanna Rani, D. D., Suresh, D., Kapula, P. R., Akram, C. H. M., Hemalatha, N., & Soni, P. K. (2023). IoT-based smart solar energy monitoring systems. *Materials Today: Proceedings, 80*, 3540–3545.

Retgen. (2025). *Solar management system: Asset management solar energy.* https://retgen.com/en/solar-management-system/

Sadowski, S., & Spachos, P. (2018). Solar-powered smart agricultural monitoring system using Internet of Things devices. In *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)* (pp. 1–6). IEEE.

U.S. Department of Energy. (2017). *Electric grid security and resilience: Establishing a baseline for adversarial threats.* https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf

Zhang, X., Zhao, Y., Zhou, L., Zhao, J., Dong, W., Zhang, M., & Lv, X. (2021). Transmission tower tilt monitoring system using low-power wide-area network technology. *IEEE Sensors Journal, 21*(2), 1100–1106.