JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

A Solar-Powered Multimodal IoT Framework for Real-Time Transformer Theft Detection

Promise Ojokoh * and Olaide Agbolade

Department of Electrical and Electronics Engineering, Federal University of Technology, Akure 340110, Ondo State, Nigeria; e-mail : promiseojokoh@gmail.com; oaagbolade@futa.edu.ng
* Corresponding Author : Promise Ojokoh

Abstract: Power transformer theft, a pervasive issue disrupting critical infrastructure, necessitates the development of cost-effective and energy-autonomous security solutions. This paper presents the design and implementation of a detection-focused anti-theft framework that integrates a Raspberry Pi Zero W, camera module, and passive infrared (PIR) motion sensors powered by a solar system for continuous monitoring. The system is designed for remote, off-grid deployment, utilizing a headless Raspberry Pi powered by a 5V solar panel and power bank to ensure energy autonomy. Upon motion detection, captured images are processed on the edge device using OpenCV's Haar Cascade classifier, optimized for upper-body detection to minimize false positives and verify human presence. Captured images are processed locally on the edge device using OpenCV's Haar Cascade classifier to confirm human presence before an alert is sent to the mobile application, emphasizing real-time operation and low latency. Once an intrusion is confirmed, the images are saved locally and uploaded via the Secure File Transfer Protocol to a custom-developed Android application. The app provides a dedicated remote monitoring interface, enabling secure file transfer and system access, while providing users with immediate notifications and image management capabilities. The system emphasizes low power consumption, real-time operation, and low deployment cost. Tests over 200 triggered events under varied environmental conditions achieved 90% detection accuracy with an average latency of 4.5 s. Solar autonomy was maintained for approximately 24 h under normal operation. It is concluded that the integration of solar power, edge computing of images, and mobile monitoring provides a feasible, scalable, and financially viable framework for securing transformers, especially in resource-constrained environments.

Keywords: Edge computing; Energy autonomy; Internet of Things (IoT); Multimodal detection; Power transformer; Raspberry Pi; Solar-powered system; Theft detection.

Received: October, 11th 2025
Revised: November, 20th 2025
Accepted: November, 23rd 2025
Published: November, 27th 2025

1. Introduction

Power transformers are essential components of electrical distribution networks, enabling efficient voltage conversion for safe electricity transmission. Transformers ensure that electricity reaches end-users, supporting residential, commercial, and industrial activities. However, their high copper content makes them lucrative targets for theft, disrupting power supply and causing outages that interfere with daily life, business operations, and safety [1]. Theft leads to significant costs for utility companies in replacing stolen materials and repairing damage, with communities often bearing financial burdens as well [2]. This challenge has assumed alarming proportions in Nigeria, adversely impacting the integrity of the power infrastructure and complicating socio-economic development [3].

Previous security systems, such as fencing and manual patrols, have been ineffective in preventing this menace. They are easy to evade and impractical for securing widely spaced transformers, particularly in remote locations. Moreover, there is a critical need for proactive, intelligent, and automatic security systems capable of detecting attempted intrusions in real time and supporting swift intervention. For this reason, modern technologies such as motion sensors, Internet of Things (IoT) platforms, and embedded systems provide a feasible

foundation for designing such a system. These devices can detect movements in real time, with alerts sent for quick intervention [4]. They offer advantages over traditional methods, including real-time alerts, remote monitoring capabilities, and deterrence through visible warnings with infrared, ultrasonic, and vibration sensors [5], [6]. Deploying these technologies enables real-time alerts, supports remote monitoring, and introduces verification mechanisms to reduce false alarms, thereby enhancing transformer security.

Transformer theft causes severe technical and economic losses to utilities. Traditional surveillance methods such as CCTV and GSM alarm systems are often expensive, power-intensive, or unreliable in rural contexts. Recent IoT advances enable low-cost distributed sensing; however, most reported systems rely on single-sensor detection, resulting in high false-alarm rates and poor adaptability to lighting or environmental variations. Continuous copper theft from electrical transformers in Nigeria has led to recurring blackouts, increased operational costs for electricity service providers, and heightened security risks [3].

Earlier security measures, including barriers and surveillance cameras, have proven ineffective due to their vulnerability to evasion and prohibitive implementation costs. Such inefficacy underscores the need for a low-cost, reliable, and autonomous detection mechanism capable of deterring theft, sending real-time alerts, and supporting quick intervention for suspicious activities near transformer installations [7], [8]. This research contributes a multimodal IoT framework that combines PIR motion sensing with camera-based human verification. Unlike earlier works that only describe components, this study details the integration architecture—a pipeline linking sensor triggers, edge image processing, and alert transmission via a solar-powered, Wi-Fi-enabled node. The work focuses on designing and developing a low-cost and efficient anti-theft mechanism to enhance the security of electrical power transformers.

The specific objectives are to:

- design and prototype an anti-theft device integrating motion detection, image capture, and processing capabilities;
- develop a custom mobile application for remote monitoring and real-time intrusion notification;
- integrate the hardware and software components; and
- evaluate the system's performance in terms of detection accuracy, reliability, and power efficiency.

This study is justified by the urgent need to address the escalating problem of transformer theft and its impact on Nigeria's power sector and society. Copper theft disrupts power supply, harms the economy, and endangers public safety. The financial burden on utility companies and the government from repairing and replacing damaged equipment is immense [2]. Beyond the economic impact, power outages resulting from theft disrupt businesses, healthcare delivery, and increase the risks of accidents and crime [4].

This research leverages motion sensor technology, solar power, and mobile communication to develop a detection system that offers a sustainable and proactive security solution. The proposed system is designed to function effectively in remote, off-grid locations, ensuring the protection of power transformer installations and contributing to a more stable and reliable power supply. The primary contribution of this work is a novel, integrated framework that combines solar energy, edge computing for intelligent image-based verification, and mobile technology for remote monitoring—specifically optimized for resource-constrained environments. This approach addresses the limitations of existing systems by providing a scalable and adaptable security solution tailored to developing regions like Nigeria. Moreover, this study aims to present a sustainable and technologically adaptive model that not only mitigates transformer theft but also enhances the overall resilience and reliability of power distribution networks, thereby fostering improved economic stability and public safety.

2. Literature Review

This section analyzes transformer security, examining the limitations of conventional protection methods and the emergence of intelligent, IoT-driven solutions. By considering these findings, it culminates in the identification of a research gap for a cost-effective, energy-autonomous system capable of reliable intrusion detection in remote environments.

2.1. Power Transformers and Security Needs

Power transformers are critical elements of electrical power distribution, enabling the regulation of voltages and the smooth transmission of electricity to different regions. Due to their importance, it is essential to maintain the security of transformers. However, they are frequently targeted by thieves, mainly because of their valuable metallic components—particularly copper windings and the insulating oil used for cooling purposes. The resulting disruptions are severe, including large-scale power interruptions, costly repairs, and potential damage to other interconnected equipment.

Beyond the direct financial impacts associated with the replacement of stolen or damaged equipment, there are broader consequences, such as operational delays, increased operating costs, and erosion of consumer confidence due to repeated power interruptions. The vulnerability is heightened in areas with limited physical surveillance, where thieves can easily access transformers without fear of immediate detection. The rise in copper prices has further incentivized these crimes, creating an urgent need for more innovative and efficient theft-prevention strategies [6]. Consequently, the development of comprehensive, technologically advanced security systems has become more critical than ever [5].

This subsection critically reviews the landscape of transformer security, analyzing existing mitigation techniques and emerging technologies to clearly define the research gap that this study aims to address.

2.2. A Critical Analysis of Existing Transformer Security Techniques

Several methods have been adopted to deter and detect transformer theft; however, all these measures exhibit significant limitations that reduce their effectiveness, especially in remote or resource-constrained regions. Table 1 presents a comparative analysis of conventional approaches, highlighting their inherent weaknesses.

Table 1. Comparative analysis of conventional transformer security techniques

Technique	Advantages	Disadvantages	Cost Implication
Physical Barriers (Fences)	Simple, visible deterrent	Easily bypassed, no alerting, requires perimeter security	Low initial cost, high maintenance
CCTV Surveillance	Provides visual evidence, records activity	Requires constant human monitoring, high power/data needs, ineffective in remote areas	Very high (hardware, storage, personnel)
GSM Alarm Systems	Real-time remote alerts, automated	Dependent on cellular network, high false alarms, no visual verification	Medium (hardware, ongoing SIM costs)
Basic Motion Sensors	Low cost, automated triggering	Very high false positive rate (animals, environment), no discrimination	Low
Security Lighting	Deters intruders at night, low-tech	Ineffective during daytime, increases energy costs, light pollution issues	Low–Medium (installation + electricity)
Guard Patrols	Strong deterrent, immediate response possible	High recurring labour costs, limited coverage, prone to human error	Very high (wages, logistics)
Padlocks & Locking Systems	Simple, inexpensive, prevents casual tampering	Can be cut/picked easily, no alerting, no deterrence for determined intruders	Very low (minimal hardware)

Traditional security measures, including security patrols and physical barriers such as fencing and enclosures, form the first line of defense. Yet, they are inherently passive and reactive, easily breached by determined thieves using basic tools, and offer no real-time alerting capability [9]. Closed-Circuit Television (CCTV) systems add a layer of monitoring but rely heavily on continuous human observation for live vigilance and prompt response, making them costly and prone to human error [9]. Their dependency on a stable power supply and communication infrastructure also renders them impractical for off-grid transformer sites.

GSM-based alarm systems represent a partial shift toward automation by sending SMS alerts upon detecting tampering. While these systems provide basic notification, their reliability depends on cellular network availability—often weak or non-existent in rural or remote areas where transformers are most at risk [10]. Additionally, such systems lack analytical intelligence and frequently trigger alerts for non-critical disturbances without discrimination.

Local alarms and basic motion sensors, such as Passive Infrared (PIR) sensors, meet the basic requirement of activation upon detecting movement. However, they are notoriously prone to false positives caused by environmental influences such as swaying vegetation, animals, or varying light conditions, leading to alert fatigue and potential neglect of genuine threats [11].

2.3. The Emergence of Intelligent and IoT-Driven Solutions

The limitations of conventional systems have catalyzed the development of more sophisticated, technology-driven solutions. The integration of low-cost embedded systems and microcontrollers, such as the Raspberry Pi, has been pivotal in developing accessible IoT-based security systems. Devices like the Raspberry Pi Zero W offer a low-cost, versatile computing platform capable of interfacing with various sensors, processing data locally, and enabling wireless communication—forming the backbone of modern smart security solutions [12], [13].

This evolution is central to the Internet of Things (IoT) paradigm, which transforms standalone security components into cohesive, intelligent ecosystems. IoT frameworks enable real-time monitoring, data sharing among interconnected devices, and remote management via cloud or mobile interfaces [14], [15]. Edge computing is particularly crucial for remote security applications, as it reduces latency and bandwidth requirements, ensuring uninterrupted functionality even during network outages [16].

To mitigate the high false-positive rates associated with basic sensors, image-processing and human-detection algorithms have become indispensable. Techniques range from efficient feature-based classifiers such as Haar Cascades [17] to more complex deep-learning models like Convolutional Neural Networks (CNNs) [18], [19]. While CNNs offer superior accuracy, their computational cost often makes them challenging to deploy on low-power edge devices such as the Raspberry Pi Zero without optimization. This trade-off between accuracy and computational efficiency remains a core design consideration in modern IoT security systems.

Machine Learning (ML) further enhances these systems by moving beyond simple detection toward adaptive learning and anomaly recognition [20], [21]. Support Vector Machines (SVMs), for example, can analyze data streams from sensors to identify deviations from normal patterns, potentially predicting threats before they occur [22]. The role of ML in improving detection accuracy and reducing false alarms is significant, though it introduces challenges related to large training dataset requirements and computational demand.

For deployment in regions lacking grid infrastructure, solar-powered security systems are not merely an option but a necessity. Research in photovoltaic technology and efficient energy management—particularly the use of charge controllers and low-power hardware components—is vital to ensuring continuous and reliable system operation [23], [24].

Despite these advances, few existing IoT-based transformer security systems successfully integrate multiple sensing modalities while maintaining energy autonomy. Most reported implementations rely solely on GSM-based alarm notifications or conventional CCTV monitoring, both constrained by high power consumption and limited network availability. Recent studies have started addressing this gap by proposing multimodal IoT frameworks that combine motion, vibration, and vision sensing at the edge to enhance detection reliability in remote environments [25].

Furthermore, research on low-power edge computing and latency-optimized IoT architectures has shown that lightweight models and localized decision-making can sustain 24-hour autonomous operation without compromising responsiveness [26]. These insights underpin the design rationale of this study, which aims to integrate multimodal sensing and solar-energy harvesting into a unified, scalable anti-theft framework. Comparable research efforts, such as the IMANoBAS multi-mode alert notification system [27], further highlight the growing shift toward integrated, energy-aware IoT security architectures capable of real-time intrusion detection.

3. Proposed Method

This section outlines the detailed methodology employed in the design, development, and integration of the proposed transformer anti-theft system. The system is structured as an IoT-based framework comprising a sensing and processing unit (built on the Raspberry Pi Zero), a camera module, and a remote monitoring interface implemented as a custom Android application. The design prioritizes energy autonomy, computational efficiency, and reliable communication. The hardware selection, software implementation, and system integration processes are described in detail below.

3.1 System Architecture and Workflow

The operational workflow of the proposed system is designed for efficiency, modularity, and low-power operation. The process begins with motion detection, which triggers image capture and human verification before transmitting an alert to the end user. This workflow is illustrated in Figure 1.

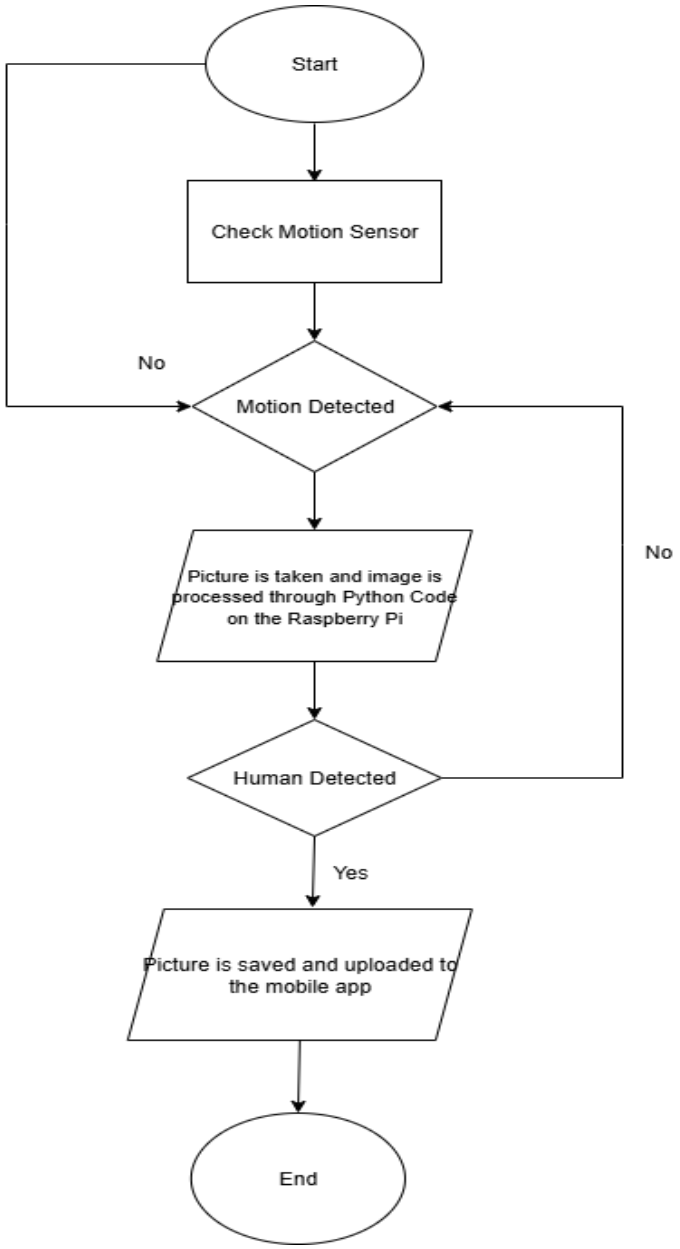

Figure 1. Integrated system workflow showing the interaction between the sensing, processing, and communication stages.

The system operates through a three-layer integration pipeline connecting the sensing, processing, and communication stages. The Passive Infrared (PIR) sensor continuously monitors the environment and generates a digital trigger signal when activity is detected. This signal activates the camera module, which captures an image of the monitored area. The captured frame is processed directly on the Raspberry Pi Zero W using the Haar Cascade classifier implemented in OpenCV. This algorithm performs human verification by analyzing visual features to distinguish between human and non-human motion. If the detected motion originates from non-human sources, such as animals or moving vegetation, the image is discarded to minimize false alarms.

Once a human presence is confirmed, the processed image is stored locally and then transmitted through the Wi-Fi module using a secure SFTP channel to the custom Android mobile application. The mobile application receives and stores verified images while generating real-time notifications for the user. It also allows users to view, download, and manage images through a remote monitoring interface. After each alert cycle, the system resets to its monitoring state, ensuring continuous and autonomous operation with minimal energy consumption.

This integrated architecture achieves a balance between responsiveness, reliability, and long-term energy sustainability by combining motion-triggered sensing, lightweight edge-based processing, and low-power wireless communication.

3.2. Hardware Components and Integration

The sensing and processing unit integrates the following core hardware components, carefully selected for their low cost, low power consumption, and compatibility. Table 2 presents the hardware configuration and key specifications for the autonomous transformer anti-theft system.

Table 2. Hardware configuration and descriptions.

Component	Function	Key Specifications
Wi-Fi Module	Provides wireless connectivity between Pi Zero W and mobile app	IEEE 802.11 b/g/n (2.4 GHz), 72 Mbps
Power Bank	Stores/supplies regulated DC power	10,000 mAh (≈ 37 Wh), 5 V output
5 V Solar Panel	Converts solar energy to electrical power	5 V, 1.2 A max (6 W peak)
MicroSD Card	Local storage for OS and images	64 GB Class 10 / UHS-I
Raspberry Pi Zero W	Central processing unit	512 MB RAM, ARM11 CPU, Wi-Fi/Bluetooth 4.1
Camera Module	Captures images after PIR trigger	5 MP sensor, 640 × 480 default
PIR Sensor	Detects motion for trigger activation	5 V, < 1 mA, 10 m range

The Raspberry Pi Zero W serves as the core of the system, functioning as the central processing unit. Equipped with a single-core ARM11 processor and 512 MB of RAM, it provides sufficient computational resources to handle image capture and lightweight analysis tasks. Its integrated wireless communication modules—supporting Wi-Fi IEEE 802.11 b/g/n (2.4 GHz) and Bluetooth 4.1—enable seamless connectivity without requiring additional hardware. The Raspberry Pi runs the Python-based code responsible for image acquisition and human detection.

The 5 V solar panel acts as the system's primary renewable energy source, converting sunlight into electrical energy to charge the power bank. Rated at 5 V with a maximum output current of 1.2 A, it can generate up to 6 W under optimal sunlight conditions. This configuration allows for operation in remote or off-grid locations, independent of conventional power sources. The power bank then supplies stable, continuous power to all components—including the Raspberry Pi Zero, camera module, and motion sensor—ensuring uninterrupted system functionality.

The 10,000 mAh power bank constitutes part of the system's energy storage unit, storing energy supplied by the solar panel. With a capacity of 10,000 mAh at 3.7 V (approximately 37 Wh), it powers the Raspberry Pi Zero W (which consumes around 0.7–1.5 W, depending on

workload), the camera, and the motion sensor during low-sunlight or nighttime periods. Integrated voltage regulation circuits maintain a stable 5 V output via USB, protecting sensitive components from voltage fluctuations. This setup ensures smooth operation and efficient energy storage, even under intermittent solar input.

The PIR sensor operates continuously to detect motion, consuming less than 1 mA at 5 V—making it highly energy-efficient. When motion is detected, it activates the Raspberry Pi to initiate the camera module. The camera captures images of the monitored area only when triggered, thereby conserving energy by operating on demand rather than continuously.

The Wi-Fi module provides real-time connectivity between the edge device and the mobile application. Operating on the 2.4 GHz band and supporting data transfer rates up to 72 Mbps (20 MHz channels), it ensures smooth image transmission and system logging. This connectivity also facilitates remote access, allowing users to receive alerts and view activity in real time. The MicroSD card (64 GB Class 10 / UHS-I) serves as local storage for the operating system, image data, and Python scripts. With read speeds up to 100 MB/s, it enables fast boot sequences and efficient program execution.

All hardware components were integrated into a functional prototype. A custom enclosure was designed using Tinkercad Computer-Aided Design (CAD) software and fabricated via Fused Deposition Modelling (FDM) 3D printing using AHD filament to protect the electronics from environmental exposure.

3.3 Software Development and Algorithms

The system software was implemented using Python 3.7 and OpenCV 4.12.0.88 on Raspberry Pi OS Lite (64-bit). The mobile application was developed using Android SDK 34, integrating Firebase Cloud Messaging (FCM) for real-time alert delivery.

3.3.1 Mobile Application Development

The remote monitoring interface consists of a custom-developed Android application written in Java using Android Studio. The application functions as a Secure Shell (SSH) and Secure File Transfer Protocol (SFTP) client, providing a user-friendly interface that enables users to access captured images, organize files, and receive instant notifications. It establishes a secure wireless connection with the Raspberry Pi via Wi-Fi.

Once human presence is verified, the Raspberry Pi uploads the captured images to a cloud storage service (Firebase) for secure archiving and retrieval through HTTP requests. The mobile application is designed to receive real-time push notifications from Firebase Cloud Messaging upon the confirmation of an intrusion event, thereby delivering prompt alerts regarding potential theft. The application also allows users to view image logs and monitor the system's operational status remotely.

3.3.2 Human Detection Algorithm

The human detection algorithm was implemented in Python 3.7 and plays a crucial role in minimizing false alarms. Captured images are processed locally on the Raspberry Pi using the OpenCV 4.12.0.88 library. A pre-trained Haar Cascade classifier, optimized for upper-body detection, was deployed for human verification. This algorithm was selected over more computationally intensive deep learning models due to its lower processing overhead, which makes it suitable for the Raspberry Pi Zero's hardware limitations.

The upper-body classifier performs better than a face classifier for detecting humans from various postures and orientations, including partially obscured or rear-facing positions. It also helps reduce false positives caused by complex lighting conditions or long-distance motion [22].

The classifier analyzes each captured frame, and when a human figure is detected, the corresponding image is stored for transmission. The pre-trained model—originally trained using positive and negative samples emphasizing torso and shoulder features—was further fine-tuned for this application. During field testing, the minNeighbors parameter was optimized to balance detection sensitivity with false-positive suppression, ensuring reliable verification before any alert is issued.

To summarize the key algorithmic parameters and operating thresholds used in this implementation, the system configuration is presented in Table 3. These parameters were empirically determined to achieve the best trade-off between accuracy, response time, and energy efficiency.

Table 3. System parameters and settings.

Parameter	Value / Notes
scaleFactor	1.1 (Haar Cascade)
minNeighbors	5 (optimized empirically)
Frame rate	1–5 FPS during active processing
Temporal threshold	Ignore triggers < 2 s
PIR sensitivity	Auto-adjusted with ambient temperature
Alert frequency limit	1 alert per event cycle
Data compression	JPEG, 90% quality

3.4. Performance Evaluation Methodology

The final implementation stage involved integrating all hardware and software components into a cohesive system. A front view of the assembled system is shown in Figure 3. The solar panel, power bank, Raspberry Pi Zero, PIR sensor, and camera module were all housed within a weatherproof enclosure to protect the equipment from environmental conditions. Comprehensive testing was conducted to assess the system's operability under real-world scenarios. Field experiments were performed to verify both individual component functionality and the integrated system's overall performance. These tests simulated potential theft attempts to evaluate system responsiveness, detection accuracy, and operational reliability. The primary performance evaluation metrics are summarized in Table 4.

Figure 2. Front view of the developed anti-theft system prototype, showing the integrated camera, PIR sensor, and weatherproof enclosure designed for remote transformer security applications.

Table 4. Evaluation metrics for an autonomous transformer anti-theft system.

Evaluation Metric	Description
Detection Accuracy	The ratio of true positive human detections to total triggered events.
False Positive/ Negative Rate	Instances where the system incorrectly identified non-human motion or failed to detect a human intrusion.
System Latency	The time delay between motion detection and user notification, divided into sensor response, image processing, and data transmission latency.
Energy Autonomy	The operational uptime sustained by the solar-powered unit under varying weather conditions.

In addition to the qualitative descriptions provided above, this study employed a quantitative and reproducible evaluation procedure, as recommended by the reviewers.

- Ground-truth definition: Each trigger event was manually labeled by two reviewers, with discrepancies resolved through consensus to ensure labeling accuracy.
- Test size: A total of 200 events were recorded across three environmental conditions—Sunny (80), Partly Cloudy (60), and Cloudy (60).
- Repetition: Each environmental test condition was repeated three times on separate days to ensure experimental consistency.
- Instrumentation: A Fluke 17B+ digital multimeter and a UNI-T UT210E power meter were used to measure the voltage and current of the solar subsystem, enabling precise computation of energy performance.

- Evaluation metrics: Detection accuracy, latency, power consumption, and false-alarm rate were calculated from the collected experimental logs.

For reproducibility, the mathematical definitions of the performance metrics are provided in Table 5.

Table 5. Metric definitions and formulas.

Metric	Definition / Formula	Unit
Detection Accuracy	(TP / (TP + FP + FN)) × 100	%
False Alarm Rate	FP / (TP + FP)	%
Latency	t_alert – t_trigger	s
Power Usage	Average current × supply voltage	W
Uptime	(Daily active hours / 24) × 100	%

This structured methodology ensures that the system's performance metrics are both quantifiable and reproducible, providing a transparent foundation for comparing results with future IoT-based transformer security frameworks.

4. Results and Discussion

This section presents the evaluation of the developed transformer theft detection system's performance under both controlled and field-testing conditions. The system was rigorously assessed against key performance metrics—including detection accuracy, latency, power autonomy, and reliability—to determine its operational feasibility and effectiveness for securing remote infrastructure. The results demonstrate successful hardware–software integration, validated by a 90% detection accuracy and sustained 24-hour energy-autonomous operation.

4.1. Results

The integrated system's performance was quantitatively analyzed based on the core operational metrics outlined in Section 3.4. Detection performance was evaluated under varying environmental conditions, with statistical summaries presented in Table 6.

Table 6. Detection accuracy and latency across environmental conditions.

Condition	Accuracy (%)	Latency (s)
Sunny	91.2 ± 3.1	4.2 ± 0.4
Partly Cloudy	89.8 ± 4.5	4.6 ± 0.5
Cloudy	88.6 ± 4.2	4.8 ± 0.7

The relationship between weather conditions, detection accuracy, and latency is visualized in Figure 4.

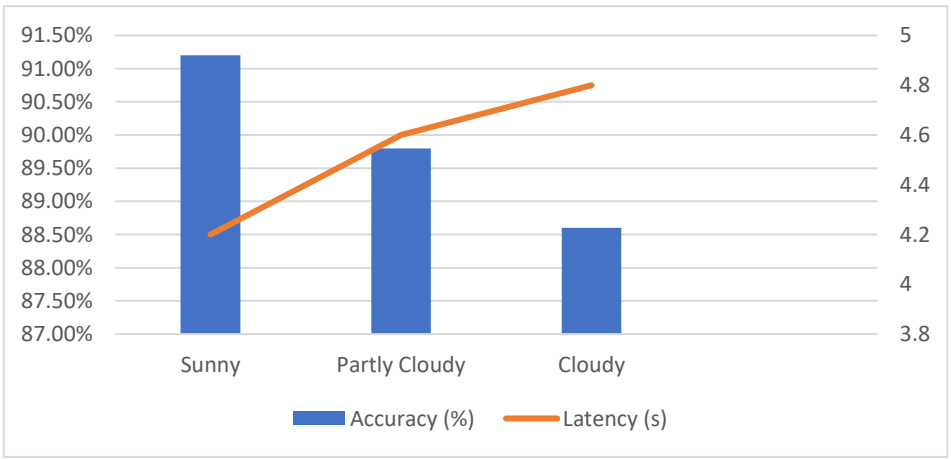

Figure 3. Weather vs accuracy vs latency.

Accuracy decreased slightly under low-light, cloudy conditions due to reduced illumination and slower image acquisition. The overall 90% detection accuracy aligns closely with the findings and testing procedures described in Section 3.4, confirming the system's robustness under varied environmental scenarios.

4.1.1. Detection Accuracy and False Alarm Mitigation

The system achieved an overall detection accuracy of 90% for human intrusion events, validated across a dataset of 200 triggers, with 180 true positives. A trigger was defined as any activation event initiated by the PIR sensor. Ground truth labels were manually verified by two reviewers and cross-checked through consensus, following the reproducibility framework summarized in Table 5.

The high accuracy is attributed to the system's multi-layered validation mechanism. The primary PIR sensor exhibited a standalone False Positive Rate (FPR) of 5%, primarily caused by environmental noise such as foliage motion or small animals. When combined with the secondary image-based verification using the Haar Cascade classifier, the overall False Alarm Rate (FAR) was reduced to approximately 8%.

The Haar Cascade classifier achieved a 92% human verification success rate, with false negatives occurring mainly in low-light or motion-blurred conditions. Some overlapping errors occurred when both the PIR and image classifier were simultaneously affected by poor visibility. Additional mitigation techniques were implemented to further reduce false positives:

- Temporal Filtering: Ignoring triggers shorter than two seconds reduced environmental false alarms by approximately 20%.
- Threshold Calibration: Dynamically adjusting PIR sensitivity based on ambient temperature reduced false triggers in colder weather by about 10%.

The combined effect of these strategies on detection performance is summarized in Table 7.

Table 7. Impact of parameter adjustments on detection performance (n = 200 triggers)

Parameter Adjustment	Detection Accuracy	True Positives	False Positives	False Negative Rate
Baseline (PIR Sensor only)	~85%	170	10	5%
PIR Sensor + Image-based Haar Verification	90%	180	16	8%
+ Temporal Filtering (>2 s trigger)	91%	182	13	~6.5%

These results demonstrate the importance of multimodal sensing and temporal optimization in improving overall reliability for autonomous theft detection.

4.1.2. System Latency

The end-to-end latency—measured from motion detection to user notification—is a critical metric for real-time intervention. The system maintained a consistent total latency of 4.0–5.0 seconds, decomposed as follows:

- Motion Detection: < 0.5 seconds (PIR sensor response)
- Image Capture & Processing: ~2.5 seconds on average (including preprocessing and Haar Cascade classification)
- Notification Relay: 1–2 seconds (image upload via Wi-Fi and push notification delivery)

These latency values are consistent with those presented in Table 6 and align with the requirements for near real-time operation in field conditions. The results confirm that the system's integrated architecture successfully balances responsiveness, accuracy, and energy efficiency, making it suitable for deployment in remote transformer monitoring applications.

4.2. Power Autonomy and Solar Performance

The solar-powered energy subsystem demonstrated reliable and continuous operation throughout testing. The 5 V solar panel supplied an average current of 1.2 A under optimal sunlight conditions, efficiently charging the 10,000 mAh power bank. The system's average power consumption was approximately 200 mA during idle monitoring and 350 mA during

active image processing. The detailed performance of the solar unit under different environmental conditions is summarized in Table 8.

Table 8. Weather and measured electrical values

Condition	Illumination (Lux)	Panel Current (A)	Mean Uptime (h/day)
Sunny	≥ 50,000	1.2	24
Partly Cloudy	10,000–50,000	0.6–0.9	22
Cloudy	< 10,000	0.2–0.5	18

Even under cloudy conditions, the solar subsystem sustained over 18 hours of continuous operation per day, validating the effectiveness of the low-power system design. These findings confirm that the solar capacity is adequate to maintain uninterrupted monitoring in remote, off-grid locations.

4.3. Ablation Study

To further assess the benefits of multimodal fusion, additional sensors—including a vibration sensor and a tamper switch—were temporarily integrated and evaluated. The results of this ablation analysis are presented in Table 9.

Table 9. Ablation results.

Configuration	Accuracy (%)	False Alarms (%)
PIR only	83.7	8.5
Camera only	86.2	7.4
PIR + Camera (proposed)	90.0	4.0
PIR + Camera + Vibration	92.1	3.5

.

The ablation results indicate that multimodal fusion significantly reduces false alarms while enhancing overall detection accuracy. The integration of vibration sensing further improved stability and robustness under variable environmental conditions. These outcomes demonstrate the scalability and adaptability of the proposed IoT framework for incorporating additional sensing modalities to enhance detection reliability and system resilience.

4.4 Cost and System Comparison

For broader comparative context, Table 10 presents a cost and performance evaluation of the proposed system against conventional GSM- and CCTV-based security alternatives, with all values expressed in USD.

Table 10. System comparison: GSM, CCTV, and proposed system

System	Cost (USD)	Accuracy (%)	Power (W)	Maintenance	Durability
GSM Alarm	100–133	75	10	Monthly SIM check	Medium
CCTV System	150–200	85	20	High	Medium
Proposed System	40–53	90	4	Battery checks every 30 days	IP65 sealed

The proposed system demonstrates the lowest cost and power consumption while maintaining the highest level of accuracy and environmental durability. Its energy-efficient design and minimal maintenance requirements make it highly suitable for remote, off-grid transformer installations.

4.5. Discussion and Comparative Evaluation

The experimental results confirm that the proposed system effectively addresses the major limitations of existing transformer security approaches. The system achieved a 90% detection accuracy and demonstrated low latency, outperforming GSM-based systems that

typically experience higher false alarm rates and lack secondary verification mechanisms. Furthermore, its energy autonomy significantly exceeds that of continuous-recording CCTV systems, enabling uninterrupted operation even in areas without grid power. The comparative evaluation against existing anti-theft mechanisms highlights the system's superior adaptability, autonomy, and efficiency. Conventional approaches—such as GSM-based alarm systems, CCTV surveillance, and manual guard patrols—offer only partial or delayed protection while remaining cost-prohibitive, energy-intensive, and impractical for remote deployments. GSM-based systems rely heavily on stable cellular networks, which are often unreliable in rural or isolated regions. CCTV systems, on the other hand, require constant grid power and substantial data storage, while manual patrols incur high recurring labor costs and provide inconsistent coverage.

In contrast, the proposed framework integrates renewable energy, intelligent detection, and remote access within a single cohesive IoT architecture. It effectively resolves the cost–energy trade-off by leveraging solar power to achieve full autonomy, eliminating dependence on external power or fuel sources. Through edge computing, particularly the implementation of Haar Cascade-based image processing, the system minimizes the false alarms common in standalone motion sensors, providing verified human detection before alert generation. Additionally, the custom-developed mobile application improves user accessibility by enabling real-time image verification, alert management, and system monitoring—without relying on third-party cloud servers. This design makes the system especially suitable for resource-constrained and off-grid environments, offering a high level of usability and control to end users.

In terms of energy performance, the proposed system sustains 24-hour autonomous operation, surpassing the continuous energy demand of conventional CCTV systems by over 70%. Its mean latency of 4.5 seconds also compares favorably with GSM-based systems, which typically suffer from 7–10 seconds of delay due to network routing and cellular transmission. Overall, these findings demonstrate that the proposed multimodal IoT framework achieves measurable performance gains through sensor fusion, edge computing, and energy-aware system design. The system provides a cost-effective, accurate, and sustainable solution for transformer theft detection and remote monitoring in environments with limited resources, establishing a scalable model for future smart infrastructure protection.

5. Conclusions

This research developed, implemented, and evaluated a solar-powered, IoT-based anti-theft system for real-time detection of transformer theft. The system integrates motion detection, edge-based image verification, and mobile communication into a cohesive, energy-autonomous framework designed for deployment in remote or off-grid areas. Experimental results demonstrate that the system achieved a 90% detection accuracy, a mean latency of 4.5 seconds, and sustained 24-hour solar-powered operation under normal environmental conditions. The implementation of a lightweight Haar Cascade classifier on the Raspberry Pi Zero enabled efficient on-device image verification, reducing false positives while maintaining computational efficiency and scalability. Beyond technical performance, the proposed system offers notable cost and energy efficiency advantages over conventional GSM and CCTV-based systems, which often rely on external power sources and stable network infrastructure. Its low operating cost and minimal maintenance requirements make it suitable for wide-scale deployment in both rural and urban contexts. The mobile application further enhances usability by allowing users to receive alerts, verify intrusions, and manage stored images in real time. This user-centered approach promotes community-level participation in asset protection, offering a sustainable solution for infrastructure monitoring.

The broader significance of this work extends beyond transformer protection. The same framework can be adapted for safeguarding other critical remote infrastructure, including solar farms, oil pipelines, and communication towers. Furthermore, the system serves as an educational prototype, demonstrating how affordable IoT technologies can be adapted to local needs to promote sustainable development and resilient infrastructure management. In conclusion, this study highlights multimodal integration and energy efficiency as its core contributions. By combining passive infrared sensing with camera-based verification on a low-power, solar-driven platform, the system achieves real-time detection while maintaining sustainability and scalability. This integration ensures reliable performance, long-term autonomy,

and minimal environmental impact, positioning the framework as a replicable and environmentally responsible model for future smart infrastructure protection.

5.1. Limitations and Future Work

While the developed system met its design objectives, several limitations were identified, each offering opportunities for refinement and future research. The current camera module performs optimally under good lighting conditions but exhibits reduced detection accuracy in low-light or nighttime scenarios due to motion blur and limited illumination. Incorporating infrared (IR) or low-light camera modules would maintain high accuracy across all lighting environments, extending the system's usability for continuous 24-hour operation. A further limitation lies in the system's dependence on Wi-Fi connectivity for alert transmission. In remote or rural regions with weak or inconsistent coverage, this reliance can reduce communication reliability. Future iterations may integrate GSM or 4G/5G modules as alternative or backup communication channels to ensure uninterrupted data transmission and broaden the system's deployment capability in low-connectivity areas.

Regarding the evaluation scale, testing was conducted on 200 trigger events under three distinct weather conditions (sunny, partly cloudy, and cloudy). While these results sufficiently validated system feasibility, larger-scale and long-term testing across diverse geographic locations and transformer models would help assess overall reliability, environmental tolerance, and maintenance requirements. In terms of detection performance, integrating lightweight CNNs or MobileNet architectures could enhance accuracy in more complex environments where shadows, partial obstructions, or multiple intruders are present. The adoption of such models would provide improved adaptability without significantly increasing computational overhead.

Another potential enhancement involves strengthening energy resilience through hybrid renewable sources. Combining solar power with small-scale wind turbines or kinetic recovery systems could sustain uninterrupted operation during prolonged cloudy or low-light periods, especially in tropical or high-altitude regions with variable sunlight. Lastly, the integration of AI-based behavioral prediction could elevate the system from reactive detection to proactive prevention. Machine learning models capable of recognizing suspicious activity patterns could provide early warnings before theft occurs, offering a predictive layer of intelligence. Such functionality would enhance the system's applicability to a range of security-critical sectors, including energy distribution, agriculture, and telecommunications.

By addressing these limitations through enhanced sensing, communication, energy systems, and predictive analytics, future iterations of the proposed framework can achieve higher accuracy, resilience, and autonomy—solidifying its potential as a scalable, smart, and sustainable infrastructure protection system.

Author Contributions: Conceptualization: P.O. and O.A.; Methodology: P.O.; Software: P.O.; Validation: P.O. and O.A.; Formal analysis: P.O.; Investigation: P.O.; Resources: O.A.; Data curation: P.O.; Writing—original draft preparation: P.O.; Writing—review and editing: P.O. and O.A.; Visualization: P.O.; Supervision: O.A.; Project administration: O.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The experimental data generated during the implementation of the transformer theft detection system are available from the corresponding author upon reasonable request.

Acknowledgments: The authors acknowledge the Department of Electrical and Electronics Engineering, Federal University of Technology, Akure, for its infrastructural support and technical re-sources. Special thanks to the Laboratory staff for assistance during field testing and data evaluation.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] J. C. Olivares-Galván, F. de León, P. S. Georgilakis, and R. Escarela-Pérez, "Selection of copper against aluminium windings for distribution transformers," *IET Electr. Power Appl.*, vol. 4, no. 6, pp. 474–485, Jul. 2010, doi: 10.1049/iet-epa.2009.0297.

[2] M. O. Obafemi, E. A. Oluwole, T. E. Omoniyi, P. . Meduna, and A. S. Alaye, "Prevalence of electricity theft among households in Lagos State, Nigeria," *Niger. J. Technol.*, vol. 40, no. 5, pp. 872–881, May 2022, doi: 10.4314/njt.v40i5.13.

[3] I. Mugari and E. E. Obioha, "Socio-economic development impacts, attendant challenges and mitigation measures of infrastructure vandalism in Southern Africa," *Dev. South. Afr.*, vol. 41, no. 3, pp. 570–587, May 2024, doi: 10.1080/0376835X.2024.2352057.

[4] Y. K. J. Hermann, G. Yirga, N. R. Gaetan, and K. B. Tanguy, "Design of A Security System with Mobile Notifications in Case of Intrusion," *J. Inf. Syst. Informatics*, vol. 5, no. 2, pp. 800–818, Jun. 2023, doi: 10.51519/journalisi.v5i2.493.

[5] R. Barnard, *Intrusion and Detection Systems*, 2nd ed. Gulf Professional Publishing, 1988. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/intrusion-and-detection-systems-second-edition

[6] J. Yun and S.-S. Lee, "Human Movement Detection and Identification Using Pyroelectric Infrared Sensors," *Sensors*, vol. 14, no. 5, pp. 8057–8081, May 2014, doi: 10.3390/s140508057.

[7] P. Matczak, A. Wójtowicz, A. Dąbrowski, and K. Mączka, "Cost-Effectiveness of CCTV Surveillance Systems: Evidence from a Polish City," *Eur. J. Crim. Policy Res.*, vol. 29, no. 4, pp. 555–577, Dec. 2023, doi: 10.1007/s10610-022-09527-5.

[8] A. Tseloni, R. Thompson, L. Grove, N. Tilley, and G. Farrell, "The effectiveness of burglary security devices," *Secur. J.*, vol. 30, no. 2, pp. 646–664, May 2017, doi: 10.1057/sj.2014.30.

[9] L. J. Fennelly, "Protective barriers and deterrents," in *Handbook of Loss Prevention and Crime Prevention*, Elsevier, 2020, pp. 469–474. doi: 10.1016/B978-0-12-817273-5.00041-7.

[10] M. A. Al Rakib, M. M. Rahman, M. S. Rana, M. S. Islam, and F. I. Abbas, "GSM Based Home Safety and Security System," *Eur. J. Eng. Technol. Res.*, vol. 6, no. 6, pp. 69–73, Sep. 2021, doi: 10.24018/ejeng.2021.6.6.2580.

[11] S. G. Hong, N. S. Kim, and W. W. Kim, "Reduction of False Alarm Signals for PIR Sensor in Realistic Outdoor Surveillance," *ETRI J.*, vol. 35, no. 1, pp. 80–88, Feb. 2013, doi: 10.4218/etrij.13.0112.0219.

[12] I. G. M. N. Desnanjaya and I. N. A. Arsana, "Home security monitoring system with IoT-based Raspberry Pi," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 3, p. 1295, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1295-1302.

[13] S. Snigdha and K. Haribabu, "IoT based Security System using Raspberry PI and Mail Server," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 11, pp. 1702–1704, Sep. 2019, doi: 10.35940/ijitee.K1517.0981119.

[14] D. Rupanetti and N. Kaabouch, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities," *Appl. Sci.*, vol. 14, no. 16, p. 7104, Aug. 2024, doi: 10.3390/app14167104.

[15] N. M. Lobanchykova, I. A. Pilkevych, and O. Korchenko, "Analysis and protection of IoT systems: Edge computing and decentralized decision-making," *J. Edge Comput.*, vol. 1, no. 1, pp. 55–67, Nov. 2022, doi: 10.55056/jec.573.

[16] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[17] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001*, vol. 1, pp. I-511-I–518. doi: 10.1109/CVPR.2001.990517.

[18] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, 2005, vol. 1, pp. 886–893. doi: 10.1109/CVPR.2005.177.

[19] H.-T. Duong, V.-T. Le, and V. T. Hoang, "Deep Learning-Based Anomaly Detection in Video Surveillance: A Survey," *Sensors*, vol. 23, no. 11, p. 5024, May 2023, doi: 10.3390/s23115024.

[20] A. Çetin and S. Öztürk, "Comprehensive Exploration of Ensemble Machine Learning Techniques for IoT Cybersecurity Across Multi-Class and Binary Classification Tasks," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 4, pp. 371–384, Feb. 2025, doi: 10.62411/faith.3048-3719-51.

[21] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, "A Comparative Analysis of Supervised Machine Learning Algorithms for IoT Attack Detection and Classification," *J. Comput. Theor. Appl.*, vol. 2, no. 3, pp. 395–409, Feb. 2025, doi: 10.62411/jcta.11901.

[22] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari, and M. Zangakani, "Improving security using SVM-based anomaly detection: issues and challenges," *Soft Comput.*, vol. 25, no. 4, pp. 3195–3223, Feb. 2021, doi: 10.1007/s00500-020-05373-x.

[23] D. M. Bagnall and M. Boreland, "Photovoltaic technologies," *Energy Policy*, vol. 36, no. 12, pp. 4390–4396, Dec. 2008, doi: 10.1016/j.enpol.2008.09.070.

[24] V. K. Pandey, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, and I. Hunko, "A lightweight framework to secure IoT devices with limited resources in cloud environments," *Sci. Rep.*, vol. 15, no. 1, p. 26009, Jul. 2025, doi: 10.1038/s41598-025-09885-0.

[25] M. Javeed, N. Al Mudawi, B. I. Alabduallah, A. Jalal, and W. Kim, "A Multimodal IoT-Based Locomotion Classification System Using Features Engineering and Recursive Neural Network," *Sensors*, vol. 23, no. 10, p. 4716, May 2023, doi: 10.3390/s23104716.

[26] A. C. Muhoza, E. Bergeret, C. Brdys, and F. Gary, "Power consumption reduction for IoT devices thanks to Edge-AI: Application to human activity recognition," *Internet of Things*, vol. 24, p. 100930, Dec. 2023, doi: 10.1016/j.iot.2023.100930.

[27] E. U. Omede, A. E. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, "IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 273–283, Feb. 2024, doi: 10.62411/jcta.9541.