UNIABUJA Journal of Engineering and Technology

https://ujet.uniabuja.edu.ng/
Special Issue

Development of a Mobile Integrated Smart Intrusion Detection System for Critical Power Assets

Tolulope Christiana ERINOSHO[1], Oluwaseun Ibrahim ADEBISI[1], Abdultaofeek ABAYOMI[2], Abiola Rachael OWOSIBO[3], Mathew SIMEON[1], Peter Olayemi OLAOGUN[1], Esso GOODNESS[1]

[1]*Department of Electrical and Electronic Engineering, Federal University of Agriculture, Abeokuta, Nigeria.*
[2]*Department of Information Technology, Summit University, Offa, PMB 4412, Offa 250101, Kwara State. Nigeria.*
[3]*Bells University of Technology, Ota, Ogun State, Nigeria.*

erinoshotc@funaab.edu.ng, adebisioi@funaab.edu.ng, taofeek.abayomi@summituniversity.edu.ng, owosiboabiola@gmail.com, simeonmathew@funaab.edu.ng, olaogunpo@funaab.edu.ng, goodnesseso2018@gmail.com

Abstract
Power system infrastructure such as substations and transformers is frequently targeted by criminals and vandals due to the high value of copper cables and other equipment. Existing security measures often fail due to slow response times, false alarms, and limited monitoring capabilities. To address this menace, a mobile-integrated smart intrusion detection framework is designed to safeguard critical power infrastructure against the growing threats of physical and cyber intrusions, vandalism, energy theft, and sabotage. This framework combines advanced sensing technologies and artificial intelligence (AI) to provide real-time, comprehensive, and adaptive protection. At its core, the system utilizes a Raspberry Pi microprocessor as the central hub for data acquisition, processing, and communication. The framework leverages AI-based image recognition to ensure high detection accuracy while minimizing false positives for anomaly detection between rodents and humans. The system's mobile integration enables real-time alerts and remote management through a Telegram-based bot, empowering security personnel to respond swiftly to security threats. This approach enhances the security posture and resilience of critical power infrastructure against evolving threats. This framework offers a scalable, cost-effective, and intelligent solution, making it suitable for widespread adoption. By providing real-time monitoring and high detection accuracy, this framework enables security personnel to respond quickly to security breaches, protecting critical power assets from various threats.

Keywords: *Infrastructure, Telegram, Intrusion, Security, Computer vision, Bot*

1.0 Introduction

Computer Vision (CV), a branch of digital signal processing (DSP), is an evolving field at the overlap of computer science and smart technology, dedicated to enabling computers to see, interpret, and understand information from digital images or videos to duplicate the usefulness of human visual systems (Kalluri *et al.*, 2025; Che *et al.*, 2024). CV systems perform fundamental tasks such as image classification and real-time object detection (Mokayed *et al.*, 2023; Turay and Vladimirova, 2022), with applications in different fields of research.

Critical power infrastructure serves as a foundation for societal stability and national development, powering healthcare, industry, and communication sectors (Escobar *et al.*, 2021). In many developing regions, these facilities are increasingly susceptible to intrusion, vandalism, and sabotage due to their remote locations and insufficient on-site surveillance (Akashdeep *et al.*,*2022*). The consequences of such breaches can be severe, ranging from regional power outages to substantial economic losses and equipment damage. Despite widespread use, traditional security mechanisms such as physical locks, human patrols, and analog surveillance cameras are often reactive, resource-intensive, and limited in effectiveness. These systems typically lack real-time alert capabilities and intelligent threat assessment, allowing many incidents to go undetected or unaddressed until significant damage or loss has occurred (Nadiya *et al., 2021*).

Several studies in the literature have sought to incorporate recent technological advancements to address this challenge. Nwosu and Emecheta (2022), for instance, developed an IoT-based intrusion detection model for energy facilities, which showed promise but suffered from high false alarm rates and lacked intelligent decision-making capabilities. In terms of communication systems, many existing systems use GSM modules

Received: 27-05-2026 / Accepted: 11-06-2026 / Published: 20-07-2026

https://doi.org/10.70118/ujet.2026.sp01.06

for sending SMS alerts. While this was effective in earlier designs, such as in the GSM-based system (Aditi *et al.,* 2023; Ojo *et al.,* 2022; Rakib *et al.,* 2021), these methods are limited in terms of speed, image transmission, and remote control. More recent systems leverage internet-based platforms like Telegram, which allows developers to build interactive bots that can send messages, images, and even receive commands in real-time (Aprianto *et al.,* 2024; Abu *et al.,* 2023; Faqihah *et al.,* 2022; Nizam Rakib *et al.,* 2022; Khan *et al.,* 2021 and Mfundo *et al.,* 2021), which significantly improves the responsiveness and flexibility of intrusion detection systems.

Recent advances in artificial intelligence (AI), embedded systems, and mobile communication technologies offer promising solutions to modern security challenges. (Sowmya *et al.,* 2023) demonstrated that convolutional neural networks (CNNs) are particularly effective for recognizing human activity in video surveillance, minimizing false detections caused by non-human movements. (Patil *et al.,* 2021 and Lee *et al.,* 2021) also emphasized the role of AI in smart grid security, highlighting how AI can help distinguish between genuine threats and environmental noise. The hardware that supports these systems has also evolved. Low-cost microcontrollers, especially Raspberry Pi, have become the preferred platform for implementing intelligent surveillance solutions. Attou et al. (2023) illustrated how Raspberry Pi combined with OpenCV enables real-time video monitoring and local image processing, making it suitable for security applications in remote or resource-constrained environments. In summary, while prior works have introduced elements like sensor-based detection and GSM alerts (Ambekar *et al.,* 2025; Mazunga *et al.,* 2021; Jabu, 2021), there remains a clear gap in integrating AI-powered visual recognition with modern, mobile-friendly communication platforms for enhanced performance.

This work filled that gap by combining AI-enabled, camera-based, image intrusion detection with Telegram-based alerting or notification, creating a smart, scalable, and mobile-integrated security framework suitable for critical power infrastructure. The proposed system utilizes a smart camera-based detection mechanism managed by a Raspberry Pi and provides real-time alerts through a Telegram bot. This mobile integration ensures that system administrators and security personnel can receive and respond to physical intrusion incidents promptly, even when off-site, thus enhancing overall situational awareness and decision-making using the Telegram Bot API, 2024. By integrating intelligent surveillance with mobile communication, this project aims to provide a cost-effective, responsive, and scalable solution to the pressing security challenges faced by critical power infrastructure. We structured the rest of this paper as follows: in Section 2, the materials and methods applied are presented, whilst Section 3 outlines the results and discussion. Section 4 presents the conclusion of the paper.

2.0 Materials and method

This section describes the detailed methodology adopted in the development of the proposed smart intrusion system.

2.1 System overview

The Mobile Integrated Smart Intrusion Detection system operates through the seamless interaction of three core functional components: the image capture unit, the processing and decision unit, and the alert unit, as depicted in Figure 1. The image capture unit, primarily a high-resolution camera, serves as the system's "eyes," utilized to continuously acquire real-time visual input from designated monitoring areas around critical power assets. This visual data is then fed into the processing and decision unit, powered by a Raspberry Pi that hosts an on-device Artificial Intelligence (AI) model. This AI model is specifically trained for object detection, particularly to recognize human presence, allowing for immediate analysis of incoming images right at the source, and minimizing latency. If the AI model identifies a human presence, indicating a potential intrusion, it instantaneously triggers an alarm and the alert unit, which is implemented as a Telegram bot. This bot immediately dispatches a real-time notification to authorized personnel through a pre-configured Telegram chat. This integrated workflow ensures rapid detection, immediate contextual awareness, and enables swift remote assessment and response from security teams, regardless of their location.

https://doi.org/10.70118/ujet.2026.sp01.06

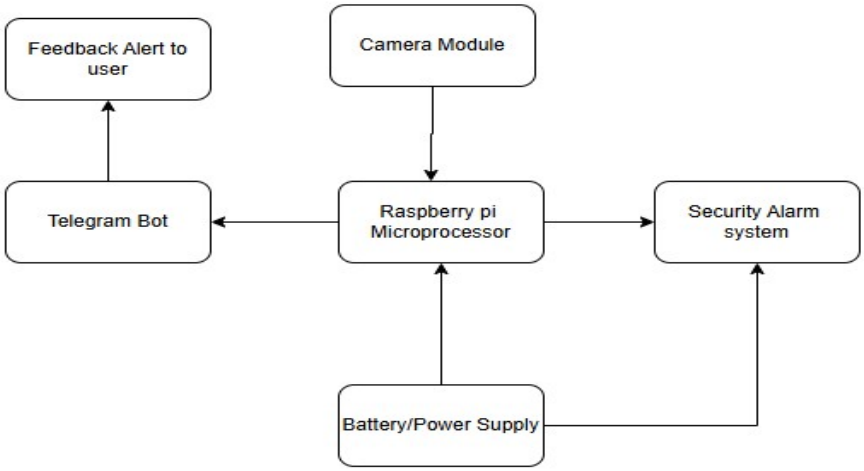

Figure 1: Block diagram of the mobile integrated smart detection system

2.2 Hardware components

The hardware components, which are the backbone of the smart intrusion detection system, primarily consist of a webcam, a Raspberry Pi, a lithium battery for power, and a buzzer for local alerts. The webcam, serving as the system's input unit, is chosen for its ability to continuously capture clear visual frames from the monitored environment and provide the raw data essential for intrusion detection. This visual stream is then processed by the Raspberry Pi, which functions as the central processing and decision-making unit. Selected for its compact size, energy efficiency, and sufficient computational power, the Raspberry Pi is responsible for running the embedded AI model that analyzes the camera feed in real-time, towards identifying the presence of humans. Powering these crucial components, particularly in remote or intermittently supplied locations, is a lithium battery to ensure a reliable and continuous operation of the system. Finally, a buzzer is integrated to provide an immediate, audible local alert upon intrusion detection, complementing the remote notifications sent via the Telegram bot. Together, these elements form the on-site intelligence, resilient power supply, and multi-modal alerting capability, enabling immediate capture, analysis, and notification of potential intrusion events directly at the critical power asset location.

2.3 Control unit

The control unit of the smart intrusion detection system is primarily embodied by the Raspberry Pi, which serves as the central processing and decision-making hub of the entire system, as depicted in the flowchart in Figure 2. This compact yet powerful single-board computer is responsible for orchestrating the core functions: it receives continuous visual input from the webcam, executes the embedded AI model (Tensorflow Lite) to analyze these frames for human presence, and, based on the detection outcome, triggers the appropriate response. Beyond merely processing data, the Raspberry Pi effectively manages the workflow from sensing to alerting, therefore acting as the intelligent core that interprets information and directs actions, including sending notifications via the Telegram Bot and activating the local buzzer. This is to ensure a seamless and autonomous operation of the intrusion detection process.

https://doi.org/10.70118/ujet.2026.sp01.06

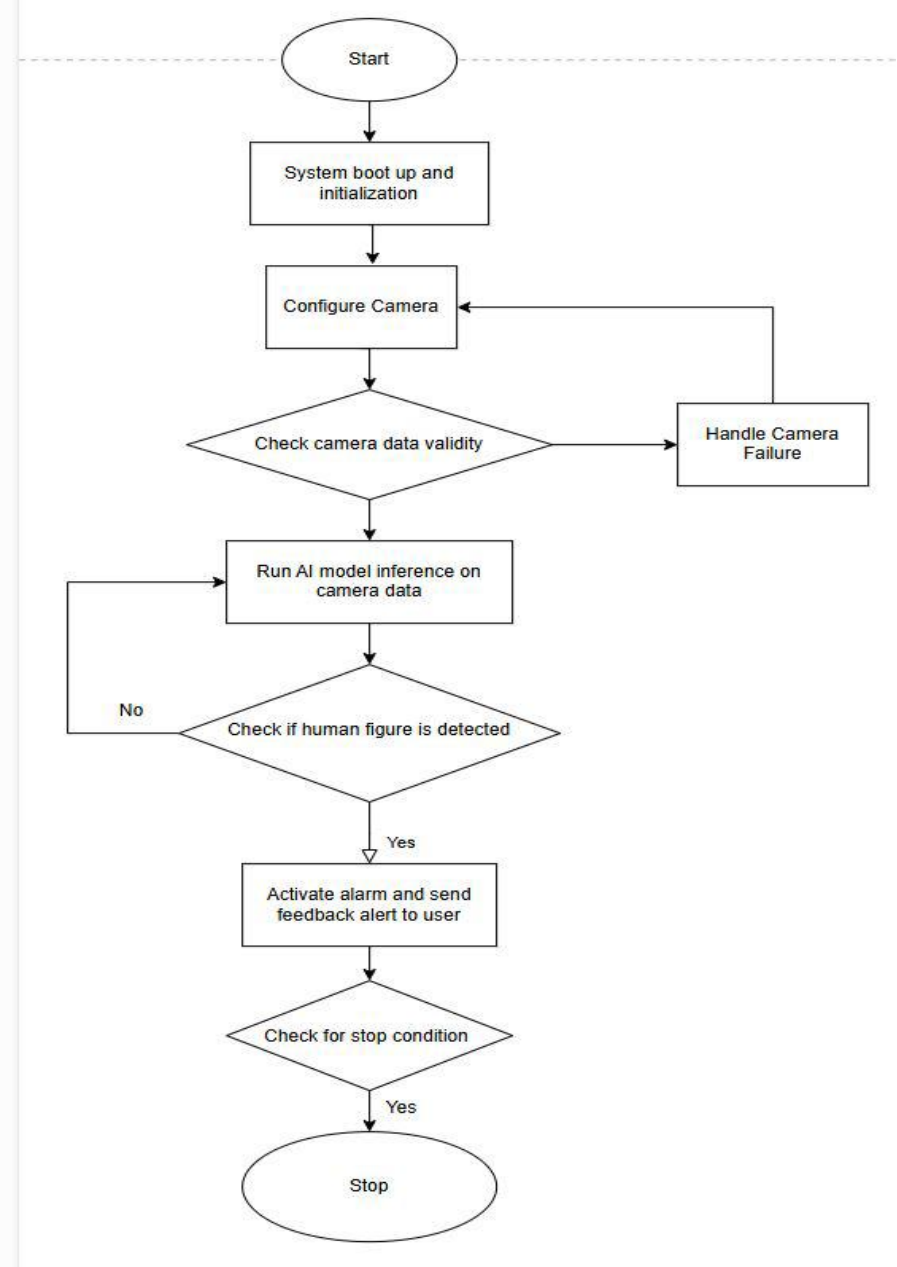

Figure 2: Flow chart for the operation of the proposed system

Figure 3. Plate of the internal circuitry of the proposed intrusion detection system

https://doi.org/10.70118/ujet.2026.sp01.06

2.4 AI Model Development and Dataset

For real time human detection, the intrusion detection system employed a fine-tuned TensorFlow based Single Shot Detector (SSD) MobileNet object detection model deployed on a Raspberry Pi. The selection of TensorFlow Lite for the system was based on its high computational efficiency and suitability for edge devices with constrained processing power, enabling low-latency inference while maintaining acceptable detection performance.

The object detection model was developed using a 1650 publicly available online dataset comprising images of humans captured under diverse environmental conditions including variations in skin tone, body posture, viewing angle, background complexity, and illumination from Kaggle machine learning repository. The data is splitted into an 80:10:10 ratio for training, validation, and testing. With such diversity, the model has the capability to generalize effectively to practical surveillance scenarios typically found around critical power infrastructure.

A pre-trained SSD MobileNet model was adopted through transfer learning and subsequently fine-tuned using the Kaggle dataset to improve its capability for real-time human detection. During fine-tuning, the network weights were updated using the labelled training images while preserving the robust feature representations learned from large-scale image datasets. The optimized model was then converted to the TensorFlow Lite format to enable efficient inference on the Raspberry Pi without compromising real-time performance.

When interference occurs, the camera continuously acquires video frames, resized and processed through the SSD model to detect objects in real time. The model then predicts the location of each detected object together with its corresponding confidence score and class label. It is worthy to mention that only detections classified as 'human' are considered valid intrusion events. When the confidence score exceeds the predefined detection threshold, the event is classified as a potential intrusion prompting the Raspberry Pi to activate the inbuild local buzzer and transmit notification immediately to authorized personnel via the Telegram Bot.

2.6 Experimental Evaluation

To assess the effectiveness of the developed IDS prototype under realistic operating conditions, the device was experimentally evaluated at a distribution transformer substation in Abeokuta, Ogun State, Nigeria. A total of fifty (50) experimental trials were conducted comprising both human intrusion events and non-human movements including birds and related environmental disturbances. During each trial, the camera continuously monitored the protected area while the Raspberry Pi executed the TensorFlow Lite SSD model to detect human presence in real time. System performance was evaluated using standard metrics like detection accuracy, confidence score, false detections, notification latency and successful alert delivery through the preset Telegram Bot.

Model effectiveness was measured using standard classification metrics which are

1. Accuracy:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

1. Precision:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

3. Recall:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

4. F1-Score:

$$F1 = \frac{2*Precision*Recall}{2TP+FP+FN} \quad (4)$$

where TP, TN, FP and FN connote true positives, true negatives, false positives and false negatives, respectively.

3.0 Results and discussion

Figure 3 shows the internal circuitry of the smart intrusion system. To ensure that the proposed system works as designed, it was thoroughly tested at a selected distribution transformer site in Abeokuta, Ogun State, Nigeria, covering key areas. The system's power management, user interface functionality, core component operations, and overall performance were meticulously assessed to ensure its reliability and effectiveness. Functional testing was conducted to verify that the system performs as expected, including confirming that it can correctly detect potential intrusions and respond accordingly.

https://doi.org/10.70118/ujet.2026.sp01.06

The system was then tested in a real-life intrusion scenario, as shown in Figure 4, in which the camera captures an image and determines whether it is a human using a pre-trained object detection model built with TensorFlow Lite and SSD (Single Shot Detector). When this occurs, the alarm sounds, and a message is sent to the user via an in-built Telegram Bot incorporated in the system, as portrayed in Figure 5. This step helps confirm that all the components and system parts work together smoothly during an actual security event. User Acceptance Testing was also carried out by having potential users utilize the system to ensure that it is easy and simple to use and effective in protecting their concerned item or property. Their feedback assisted in improving the overall design and functionality.

Firstly, a power consumption test was performed to monitor how much power the system uses in different modes of operation. This test is important to evaluate the efficiency of the lithium battery and estimate how long the system can run without needing a recharge or replacement. The power supply unit was confirmed to efficiently deliver the required voltage of 12.6V for system operation, verified using a digital multimeter. Raspberry Pi consumes 5V; the buzzer also consumes 5V. The developed control logic and communication routines, using Python, and the final firmware were uploaded to the microprocessor using the Thonny IDE. The code handled all the key tasks, including camera input reading, event detection, alert triggering, and power switching.

The smart intrusion detection system (SIDS) underwent rigorous testing at a simulated distribution substation to evaluate its performance and reliability under realistic conditions. Key functionalities, including intrusion detection and alert delivery, were thoroughly assessed.

One crucial evaluation was the human detection test. This involved a camera equipped with TensorFlow Lite, continuously capturing and analyzing video frames in real-time. A computer vision library, OpenCV, processed the camera feed, allowing the system to identify human shapes and movements based on predefined classes, ensuring accurate human detection. As depicted in Table 1, out of 50 iterations, 84% human detection accuracy and about 77.6% confidence level were obtained. The system was also able to discriminate non-human presence when birds came around the site by sending no message when this occurred, as shown in Figures 5 and 6.

Another important assessment was the Alert Speed Test, which measured the time between intrusion detection and the delivery of an alert via a Telegram bot. Multiple trials showed an average delay ranging from 3 to 7 seconds, depending on the internet network conditions. This response time was deemed acceptable for a real-time alert system.

Figure 4. Performance testing of the developed system at a typical substation with the developed intrusion detection system installed

https://doi.org/10.70118/ujet.2026.sp01.06

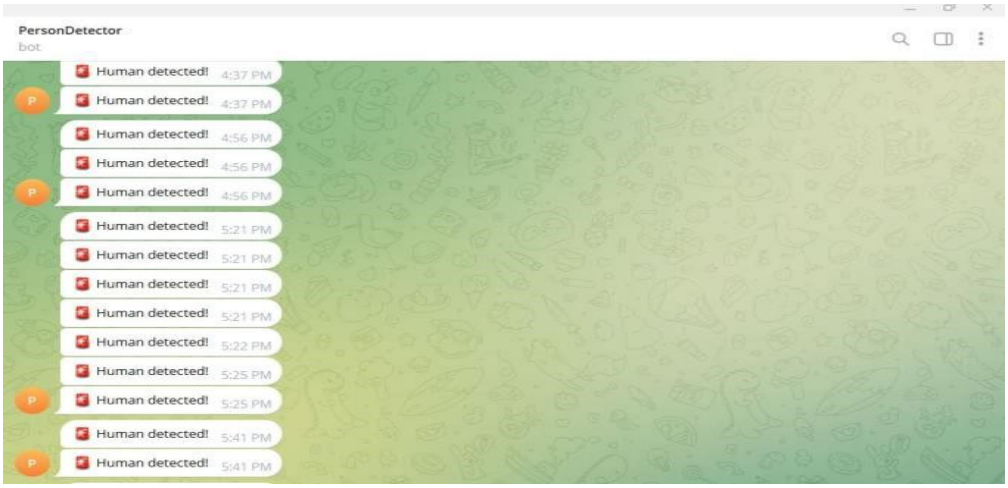

Figure 5. Plate of the developed Telegram Bot alert system

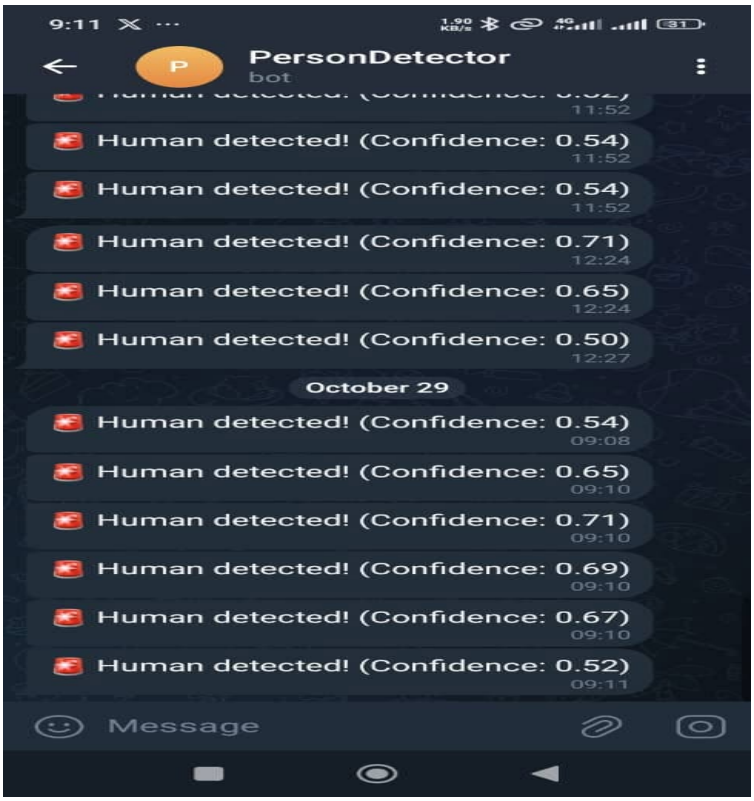

Figure 6: Display of the Telegram Bot alert of the proposed intrusion detection system

3.1 Result of the Model Performance and Accuracy

Table 1 below depicts the result obtained on the intrusion detection model using standard performance metrics described in equations (1) to (4) after several iterations

Table 1: Results of the model performance using standard metrics

Metric	Value
Accuracy	84%
Precision	89%
Recall	84%
F1-score	86%
False Positive Rate	12%
Mean confidence	77.60%
Average inference time	6.47s

https://doi.org/10.70118/ujet.2026.sp01.06

The average response time and outcome of the performance evaluation tests carried out on the system are presented in Table 2.

Table 2: Table showing the results of the different tests carried out on the smart intrusion detection system

Test Scenario	Expected Outcome	Actual Outcome
Motion Detection	Immediate detection	Detected in < 3 sec
Telegram Notification	Delivered within 10 seconds	Avg. 6.5 seconds
Power Failover	No interruption in operation	Passed

It is evident from these results that compared with conventional sensor systems, the AI-enhanced system demonstrated improved accuracy and reduced false alarms significantly.

Table 3 Performance comparison of the developed intrusion system with previous studies

Author	Sensing technique	Mobile Alert	Accuracy	Real Deployment
Ojo et al., 2022	No	GSM	70%	No
Saha et al., 2023	Sensor	SMS	75%	No
Current study	SSD + AI	Telegram	84%	Yes

Comparing the results with previous similar systems (Victor and Idowu, 2024; Saha *et al.,* 2023; Ojo *et al.,* 2022) as shown in table 3, this approach is an enhanced technology by integrating intelligent surveillance with mobile communication, thereby providing a more responsive and scalable solution to the pressing security challenges faced by critical power infrastructure security.

4.0 Conclusion

The development and deployment of the smart intrusion detection system proved that it is both feasible and effective for securing power infrastructure and other critical assets using a low-cost IoT-based solution. The combination of AI, wireless communication, and automation achieved the goal of early detection and immediate alerting in the event of unauthorized access.

Using Telegram as a communication platform was particularly beneficial because it allowed the system to bypass GSM-related network limitations and deliver alerts quickly and reliably. This adjustment made the system more practical for use in rural and off-grid locations, where mobile signals are often inconsistent. In summary, the experiments and results obtained in this study demonstrated that, with proper planning, locally available resources, and the right mix of software and hardware, a smart security solution can be created to address the real problems of intrusion detection in power-critical infrastructure. The proposed system is scalable, adaptable, and suited to the Nigerian context, making it a promising approach to protecting power infrastructure.

However, the limitations of the developed IDS are that it can only work in daytime, has only one camera, limitation in Raspberry Pi computational capability and can only work only when internet is available. Future works can focus on using YOLOv8 Nano for enhanced capacity, multi-camera fusion, explainable AI to enhance model trust and integrate night vision ability in the design. Furthermore, the modular nature of the system also allows for future expansion, such as integrating more sensors, upgrading the camera for higher resolution images, or deploying AI tools to improve detection accuracy and clean energy sources for enhanced energy sustainability. The hardware enclosure should also be constructed using robust materials to withstand harsh weather, falling and other physical tampering, towards ensuring longevity and protection in field conditions.

AI-Use Disclosure

The authors used AI tools, such as Grammarly and Perplexity, for assistance in editing, grammar enhancement, and spelling checks; all technical content and conclusions were authored and verified by the authors.

References

Abu, Z. M., Abdullah, R., Ismail, S. I., and Dzulkefli, N. N. (2023). "IoT-based emergency alert system integrated with a Telegram bot". In 2023 IEEE International Conference on Automatic Control and

https://doi.org/10.70118/ujet.2026.sp01.06

Intelligent Systems (I2CACIS), 126-131.

Aditi, G., Gupta, D., Roy, S., Al Ahasan, M. A., and Haque, M. A. (2023). "GSM based home security alarm system using Arduino, using mobile call". In 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 0268-0274.

Akashdeep, B., Kaushik, K., Bharany, S., Elnaggar, M. F., Mossad, M. I., and Kamel, S. (2022). Comparison of IoT communication protocols using anomaly detection with security assessments of smart devices. Processes, 10(10), 1952.

Ambekar, P., Kamble, T., Bahurashi, K., Gedam, S., and Thakare, V. (2025). "Implementation of automated doorlock for ATM with SMS alert and calling using GSM". International Journal of Engineering Development and Research, 13(3), 169-178.

Aprianto, F., Kusnadi, A., Tobing, F. A., Pane, I. Z., Wijaya, N., Nabilah, S. M., Wicaksono, P. A., and Andrasito, F. N. (2024). "Enhancing home security with Telegram bots: Bridging facial recognition technologies for real-time alert systems". In 2024 9th International Conference on Mechatronics Engineering (ICOM), 13-19.

Attou, H., Mohy-eddine, M. M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., and Almusallam, N. (2023). "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing". Applied Sciences, 13(17), 9588.

Babu, J. R. (2021). "Design, implementation, and field-testing of a distributed intrusion detection system for smart grid SCADA network". Master's thesis, Iowa State University.

Cao, Y. (2024). "Design and implementation of multi-sensor integrated intelligent alarm based on Arduino". In 2nd International Conference on Mechatronic Automation and Electrical Engineering (ICMAEE 2024), 73-78.

Che, C., Zheng, H., Huang, Z., Jiang, W., and Liu, B. (2024). "Intelligent robotic control system based on computer vision technology". arXiv preprint arXiv:2404.01116.

Escobar, M., Jaime, J., Matamoros, O. M., Padilla, R. T., Reyes, I. L., and Espinosa, H. Q. (2021). "A comprehensive review on smart grids: Challenges and opportunities". Sensors, 21: 6978.

Faqihah, M. F., Mazlan, S. S., and Mohamed, N. (2022). "Development of surveillance system with automated email and Telegram notification using open-source application programming interphase (API)". International Journal of Infrastructure Research and Management, 10(2), 39.

Hosmer, P. (2004). Use of laser scanning technology for perimeter protection. IEEE Aerospace and Electronic Systems Magazine, 19(8), 13-17.

Kalluri, P. R., Agnew, W., Cheng, M., Owens, K., Soldaini, L., and Birhane, A. (2025). "Computer-vision research powers surveillance technology". Nature, 643(8070), 73-79.

Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., Pitropakis, N. and Buchanan, W. J. (2021). "A deep learning-based intrusion detection system for MQTT enabled IoT". Sensors, 21(21), 7016.

Lee, D., Lai, C., Liao, K., and Chang, J. (2021). "Artificial intelligence assisted false alarm detection and diagnosis system development for reducing maintenance cost of chillers at the data centre". Journal of Building Engineering, 36, 102110.

Mazunga, F., Romosi, T., and Guvhu, R. (2021). "Manhole intrusion detection system with notification stages". Scientific African, 12: e00819.

Mfundo, Z., Owolawi, P. A., Malele, V., Odeyemi, K., Aiyetoro, G., and Ojo, J. S. (2021). "Intrusion detection system using Raspberry Pi and Telegram integration". In Proceedings of the International Conference on Artificial Intelligence and its Applications, 1-7.

Mokayed, H., Quan, T. Z., Alkhaled, L., and Sivakumar, V. (2023). "Real-time human detection and counting system using deep learning computer vision techniques". In Artificial Intelligence and Applications, 1(4), 205-213.

Nadiyah, R. S., Samah, K. A., Ahmad, M. H., and Riza, L. S. (2021). "IoT based accident detection and tracking system with Telegram and SMS notifications". In 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), 6, 1-5.

Nizam, O. M., Ismail, M. H., Sedek, K. A., Othman, N. A., and Maghribi, M. (2022). "A low-cost home security notification system using IoT and Telegram bot: A design and implementation". Journal of Computing Research and Innovation, 7(2), 327-337.

Nwosu, J. and Emecheta, C. (2022). "A comparative study of communication protocols in IoT-based alarm systems". Journal of Network and Communication Technologies, 9(3), 67-74.

Ojo, T. P., Akinwumi, A. O., Ehiagwina, F. O., Ambali, J. M., and Olatinwo, I. S. (2022). "Design and implementation of a GSM-based monitoring system for a distribution transformer". European Journal of Engineering and Technology Research, 7(2), 22-28.

Patil, M. A., Parane, K., Poojara, S., and Patil, A. (2021). "Internet-of-things and mobile application-based hybrid model for controlling energy system". International Journal of Information Technology, 13(5),

https://doi.org/10.70118/ujet.2026.sp01.06

2129-2138.

Rakib, A., Abdullah, M., Rahman, M. M., Rana, M. S., Islam, M. S., and Abbas, F. I. (2021). "GSM based home safety and security system". European Journal of Engineering and Technology Research, 6(6), 69-73.

Saha, A., Hasan, T., Ahmed, F., Shuvo, I. H., and Mondal, S. (2023). "Design and development of low-cost smart safety system for residence". In International Conference on Intelligent Systems Design and Applications, 90-100. Springer Nature Switzerland.

Sowmya, C. S., and Vibin, R. (2023). "Enhancing smart grid security: Detecting electricity theft through ensemble deep learning". In 2023 8th International Conference on Communication and Electronics Systems (ICCES), 1803-1810.

Turay, T., and Vladimirova, T. (2022). "Toward performing image classification and object detection with convolutional neural networks in autonomous driving systems: A survey". IEEE Access, 10, 14076-14119.

Victor, A., and Idowu, L. (2024). "Multi-sensor intrusion detection system". arXiv preprint arXiv:2406.05137.

https://doi.org/10.70118/ujet.2026.sp01.06