JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Design and Implementation of a Cost-Effective, AI-Enabled Smart Security System for Real-Time Threat Detection in Nigerian Rural Communities

Aliyu Abdul-Quadri Hujatullahi, A. E. Airoboman
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna

ABSTRACT
This study presented the design and implementation of a cost-effective, AI-enabled smart security system tailored for real-time threat detection in Nigerian rural communities. The system integrated an ESP32-CAM microcontroller, a Passive Infra-Red (PIR) Camera Sensor Module, and a Global System for Mobile Communications (GSM) module, employing a quantized MobileNet model for edge-based classification and Short Message Service (SMS) alert transmission without internet dependency. The methodology involved developing a lightweight MobileNet model trained on a 226-sample dataset, achieving a 97.35% training accuracy, and simulating system performance with 30 test instances, resulting in a 93.3% classification accuracy. The key performance metric included a 0.5-second motion-to-capture time, 60–77ms classification time (post-1s load), and an average 3.2-second SMS alert delivery. Results demonstrated robust threat distinction between threats and non-threats, and was validated by a confusion matrix showing 9 True Positives, 19 True Negatives, 1 False Positive, and 1 False Negative. The system, with an estimated cost of less than ₦30,000, was shown to be more affordable and adaptable to resource-constrained areas than many of the current alternatives. The system's performance confirms its potential as a scalable, intelligent security solution for rural Nigeria, despite the fact that it is simulation-based, which restricted real-world environmental testing.

ARTICLE INFO
Article History
Received: August, 2025
Received in revised form: September, 2025
Accepted: November, 2025
Published online: December, 2025

KEYWORDS
Design, Implementation, Cost-Effective, AI-Enable, Smart Security System, Real-Time, Threat Detection, Nigerian Rural Communities

INTRODUCTION

The global rise in population and the expansion of urban settlements into rural areas have intensified security challenges, particularly in underdeveloped regions. In Nigeria, these challenges are worsened by the increase in burglary, unauthorized access, and more recently, violent encroachments by armed herdsmen. These attacks have resulted in the loss of over 5,000 lives and have directly affected an estimated 7.5 million people through displacement, destruction of farmlands, and loss of property [1]. Rural communities, in particular, remain disproportionately exposed due to the lack of intelligent, responsive, and cost-effective surveillance systems capable of providing timely alerts and threat classification [2].

Unfortunately, most existing security solutions fall short of this need. Conventional tools in rural areas, such as simple alarms and local vigilante patrols, are inefficient and prone to false alarms due to their inability to accurately differentiate between real threats and harmless disturbances like wind or animals [3]. Advanced commercial systems, while effective in urban settings, are typically too expensive, power-intensive, and heavily reliant on internet infrastructure, making them impractical for deployment in remote or off-grid areas [4]. Consequently, millions of rural dwellers remain

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

without reliable security coverage, increasing their vulnerability to attacks and economic losses.

The aim of this study is to design and implement a cost-effective AI-Enabled Smart Security System for Real-Time threat Detection in Nigerian Rural Communities. The system will integrate a compact ESP32-CAM microcontroller with a PIR motion sensor, a quantized MobileNet-based image classifier for on-device inference, and a GSM module for SMS alert transmission in order to detect motion, capture visual data, classify potential intruders, and transmit real-time alerts via GSM, all without dependence on internet connectivity. This will be achieved through the design and simulation of the complete system architecture, focusing on its ability to accurately detect, classify intrusions as human, animal, or non-threatening objects, while minimizing false positives. System performance is evaluated in terms of classification accuracy, response time, and alert reliability. A cost and feasibility analysis further demonstrates the advantages of the proposed solution over existing alternatives, particularly in settings with limited infrastructure and power supply.

While the system is designed for robust field application, this initial study is limited to simulation-based testing. It does not account for environmental variability such as lighting, weather, or terrain. Vision coverage is constrained to a fixed camera angle, and alert delivery is dependent on GSM network availability, which may be unreliable in some areas. Additionally, the system lacks advanced geolocation features and its classification accuracy may vary with the quality and diversity of the training data.

In essence, the proposed solution addresses a pressing gap in rural security infrastructure by combining affordability, intelligence, and offline operation. It offers a promising direction for future deployment and serves as a foundation for broader research in embedded, autonomous surveillance systems

LITERATURE REVIEW

Several attempts have been made to address these challenges using low-cost microcontrollers, Passive Infra-Red (PIR) motion sensors, and Global System for Mobile Communications (GSM) modules. The review to choose these particular materials were done in Table 1 which showed a comparative analysis of several components which could be combined together to give a cost-effective security solution for rural locations in Nigeria.

Table 1: Comparative Analysis of Materials, Models, and Design Choices for Smart Security Systems

Component	Best Low-Cost Option	Best Performance Option	Accuracy/Efficiency	Scalability	Cost Range (₦)
Microcontroller	ESP32-CAM	Raspberry Pi 4	60–95% depending on MCU	Moderate–High	7,700 – 92,400
Imaging	Low-cost ESP32 camera	USB HD Camera / Thermal	Medium–High	Moderate–High	Included – 308,000
Motion Sensors	PIR Sensor	mmWave Radar	Low–High depending on sensor	Low–High	1,540 – 61,600
ML Algorithm	Lightweight CNN	YOLOv5/v8	70–98%	High	Training-only – 123,200
Alert System	Console Simulation	GSM Module / IoT Cloud	Low–Very High	Low–Very High	Free – 15,400 (monthly for cloud)

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Figure 1 and Figure 2 show the Passive Infra-Red (PIR) sensor and the ESP32-CAM microcontroller considered for the research.

Figure 1. PIR- Camera Sensor Module

Figure 2: ESP32 CAM

A review of related works by authors highlights their attempts in providing a solution to cost effective security problems for rural areas in Nigeria. A GSM-based home security system using PIR sensors and cameras was developed by [5], while [6] incorporated solar power to enable off-grid functionality. Similarly, [7] designed a smart alarm system, and [8] integrated PIR detection with SMS alerting. Although these systems offered affordability and energy efficiency, they were limited by their reliance on motion-only detection, vulnerability to false positives, absence of intelligent classification, and poor adaptability to environmental conditions.

Others that leveraged Internet of Things (IoT) and cloud connectivity (e.g., [9] and [10] provided remote monitoring but were unsuitable for rural environments due to their dependence on stable internet access. Consequently, the persistent lack of scalable, intelligent, and offline-capable surveillance leaves rural populations vulnerable.

This study addresses these gaps by designing and simulating a cost-effective AI-enabled Smart Security System for rural Nigerian communities. The system integrates an ESP32-CAM with a Passive Infra-Red (PIR) motion sensor, a quantized MobileNet classifier for on-device inference, and a Global System for Mobile Communications (GSM) module for Short Message Service (SMS) alerting. By enabling on-device classification of intrusions into human as threat, and animals or other objects as non-threat categories, the design minimizes false alarms and reduces messaging costs. Unlike prior works, it provides visual verification, operates offline without internet connectivity, and supports modular scalability. With energy-optimized operation through deep-sleep cycles and potential solar integration, the proposed system is practical for off-grid deployments.

MATERIALS AND METHOD.

Material Selection

This research adopts a design–simulation–evaluation methodology to simulate and test the proposed intelligent, cost-effective, offline-capable intrusion detection system for rural Nigerian communities. The approach combines hardware selection from the comparative analysis in Table 1, which lead to the choice of an ESP32-CAM microcontroller which has an integrated camera module as well as a Passive Infra-Red (PIR) motion sensor with an embedded machine learning model integration, and GSM-based communication to produce a surveillance solution that minimizes false alarms, reduces dependency on internet infrastructure, and operates efficiently in resource-constrained environments.

To test and evaluate the suggested simulation program, an image dataset was created from openly accessible internet sources. These photos were found via search engine queries and open-access platforms, and they were used only for academic, non-commercial purposes. Utilizing publicly accessible data ensures cost-effectiveness and accessibility while reflecting the real-world environment in which such systems function.

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

System Design

The proposed system design combines a PIR motion sensor, an ESP32-CAM microcontroller with an integrated camera module, an embedded AI classification model, and a GSM communication unit to deliver an efficient, low-power intrusion detection solution. The design prioritizes high detection reliability, minimal false alarms, adaptability to changing environmental conditions, and optimized energy consumption. Functionally, the system operates as a chain of interconnected subsystems: the sensing unit detects motion through the PIR sensor and activates the camera for image capture; the feature extraction and classification module processes the image using a lightweight AI model to identify whether the object is a threat (human in this case) or non-threat (animal and non-living objects); the decision and control logic triggers alerts only when genuine threats are detected; the communication module transmits alerts and images to predefined recipients via GSM; and it is simulated in this manner in order to minimize resource usage to enable real-time operation in resource-constrained environments

Mathematical Modeling

Motion Detection

The motion detection subsystem employs a Passive Infrared (PIR) sensor to detect thermal changes caused by moving objects. The raw sensor output $S(t)$ is a binary signal:

$$S(t) = \begin{cases} 1 & \text{if motion detected at time } t \\ 0 & \text{otherwise} \end{cases} \quad \text{(EQ. 1)}$$

To mitigate false triggers from environmental noise $\eta(t)$, a filtered decision signal $D(t)$ is computed:

$$D(t) = \begin{cases} 1 & \text{if } S(t) - \eta(t) > \theta_m \\ 0 & \text{otherwise} \end{cases} \quad \text{(EQ. 2)}$$

where:

1. $\eta(t) \sim \mathcal{N}(0, \sigma_\eta^2)$ model's sensor noise as a zero-mean Gaussian process.
2. θ_m is a calibrated threshold tuned to the deployment environment (i.e the rural setting).

To further reduce transient false positives (e.g., wind-blown foliage), a persistence validation stage requires motion to be detected for k consecutive samples before triggering the camera:

$$D_{\text{valid}}(t) = \begin{cases} 1 & \text{if } \sum_{i=t-k+1}^{t} D\,(i) = k \\ 0 & \text{otherwise} \end{cases}$$

(EQ. 3)

Image Capture and Preprocessing

When $D_{\text{valid}}(t) = 1$, the **ESP32-CAM** module captures an image $I(x, y)$ with resolution $M \times N$. To optimize computational efficiency for edge-AI processing, the image undergoes:

Spatial Down sampling:

$$I_{\text{down}}(x, y) = \text{resize}(I(x, y), \quad \text{dimensions} = \alpha M \times \alpha N \quad (0 < \alpha < 1)$$

(EQ. 4)

where α is a scaling factor (e.g., $\alpha = 0.25$ for a 4× reduction).

Illumination Normalization:

$$I'(x, y) = \frac{I_{\text{down}}(x,y) - \mu_I}{\sigma_I} \quad \text{(EQ. 5)}$$

Here, μ_I and σ_I denote the mean and standard deviation of pixel intensities, respectively. This step ensures robustness to varying lighting conditions common in rural environments.

Feature Extraction

The preprocessed image $I'(x, y)$ is analyzed by a **lightweight CNN** (e.g., quantized MobileNetV2) for real-time threat classification.

Convolutional Feature Extraction: For each filter k in the CNN's first layer, a feature map f_k is computed via:

$$f_k = \sigma\left(\sum_{i=1}^{M} \sum_{j=1}^{N} I'\,(i, j) \cdot w_{ij}^{k} + b_k\right) \quad \text{(EQ. 6)}$$

where:

1. f_k = extracted feature map for filter k
2. w_{ij}^{k} = weight of the convolution kernel
3. b_k = bias term
4. $\sigma(\cdot)$ = activation function (ReLU in this design)

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Classification Model

The classification output vector $\mathbf{p}$ is produced via a softmax function:

$$p_c = \frac{e^{z_c}}{\sum_{j=1}^{C} e^{z_j}}, \quad c \in \{1,2,\ldots,C\} \qquad \text{(EQ.7)}$$

where:

1. C = number of classes (Human, Animal, No Threat)
2. z_c = logit value for class c

Decision rule:

$$\hat{y} = \underset{c}{\operatorname{argmax}}\ p_c \qquad \text{(EQ. 8)}$$

An SMS alert is triggered via GSM **only** if:

$$P(\text{threat} \mid I') > \theta_{\text{threat}} \quad (\theta_{\text{threat}} = 0.9) \qquad \text{(EQ. 9)}$$

Decision and Alert Model

The decision logic $A(t)$ for sending an alert is:

$$A(t) = \begin{cases} 1 & \text{if } \hat{y} = \text{Human and } p_{\text{Human}} \geq \theta_c \\ 0 & \text{otherwise} \end{cases} \qquad \text{(EQ. 10)}$$

where θ_c is the classification confidence threshold.

GSM Communication Model

If $A(t) = 1$, the GSM module sends an SMS alert with image attachment:

$$T_{\text{alert}} = T_{\text{proc}} + T_{\text{tx}} \qquad \text{(EQ. 11)}$$

where:

3. T_{proc} = AI processing time
4. T_{tx} = GSM transmission time (depends on network conditions)

To optimize GSM costs in simulation:

a. **Duty Cycling**: Alerts are batched during high-threat periods (e.g., nighttime).
b. **Contextual Filtering**: Non-human motion (e.g., animals) is suppressed using temporal consistency checks (e.g., require threat probability $>$ θ_{threat} for 2+ consecutive frames).

Power Consumption Model

The total system power consumption P_{total} is given by:

$$P_{\text{total}} = P_{\text{idle}} + P_{\text{motion}} \cdot \alpha + P_{\text{AI}} \cdot \beta + P_{\text{GSM}} \cdot \gamma \qquad \text{(EQ. 12)}$$

where:

1. P_{idle} = standby power consumption
2. P_{motion} = power for motion sensing
3. P_{AI} = power for AI inference
4. P_{GSM} = power for GSM transmission
5. α, β, γ = duty cycle factors for each component

The entire System design is summarized in the form of a flowchart in Figure 3.

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

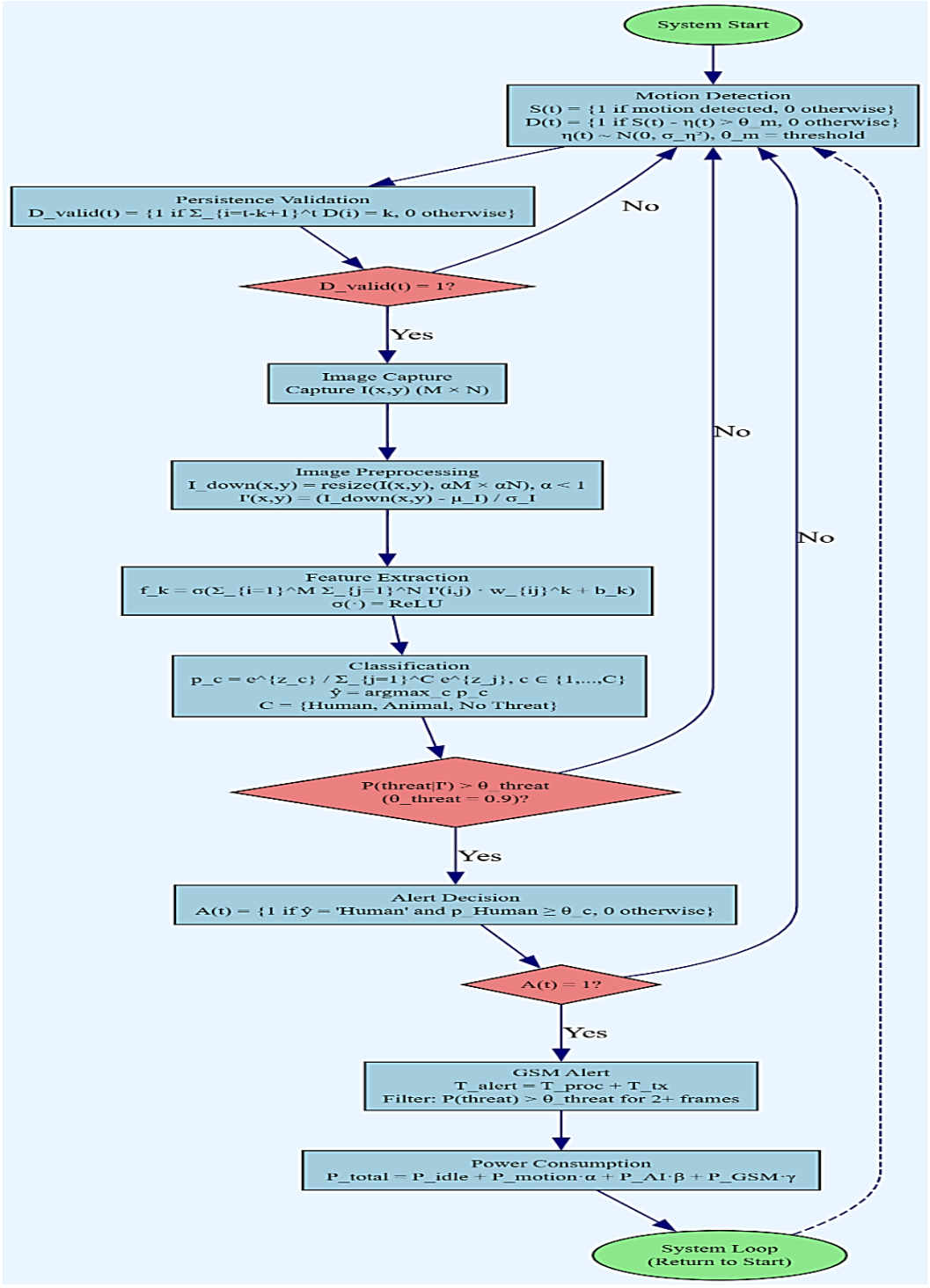

Figure 3: Flowchart describing the summary of the system architecture from motion detection to alert system

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

System Simulation

To validate the feasibility of the proposed design prior to hardware implementation, a software-based simulation was developed in Python. The simulation emulates the behavior of each subsystem, motion detection, image capture, AI classification, and GSM alert transmission, within a controlled environment.

Simulation Setup

The simulation was developed in Python 3.13, utilizing TensorFlow for the Convolutional Neural Network model inference (CNN) and Open-Source Computer Vision (OpenCV) for image preprocessing. A trained lightweight CNN model, saved as threat_detector.keras, was integrated into the system to classify captured images into two categories: *dThreat* and *non-Threat*. For testing, multiple sample images, such as test.jpeg, were sequentially used to emulate visual inputs from the ESP32-CAM. The simulation ran for five monitoring cycles, during which the PIR sensor's output was randomly determined. If motion was detected, the CNN model analyzed and classified the corresponding image; otherwise, the system remained idle.

Simulation Workflow

The simulation emulated motion detection using a pseudo-random function to replicate PIR sensor activity, alternating between "motion" and "no motion." When motion was detected, a test image was captured, preprocessed by resizing and normalization, and then passed to the CNN model for inference. The decision logic evaluated the classification confidence, and if it exceeded a predefined threshold (≥ 0.9 for "Threat"), the system simulated triggering an alert. Instead of relying on an actual GSM modem, the simulation printed SMS-like alerts to the console, mimicking message dispatch to security personnel. This entire process was repeated across multiple cycles to reflect continuous real-world monitoring. The block diagram of the simulation workflow is highlighted in Figure 4 and the summary of the system simulation is illustrated in the flowchart in Figure 5.

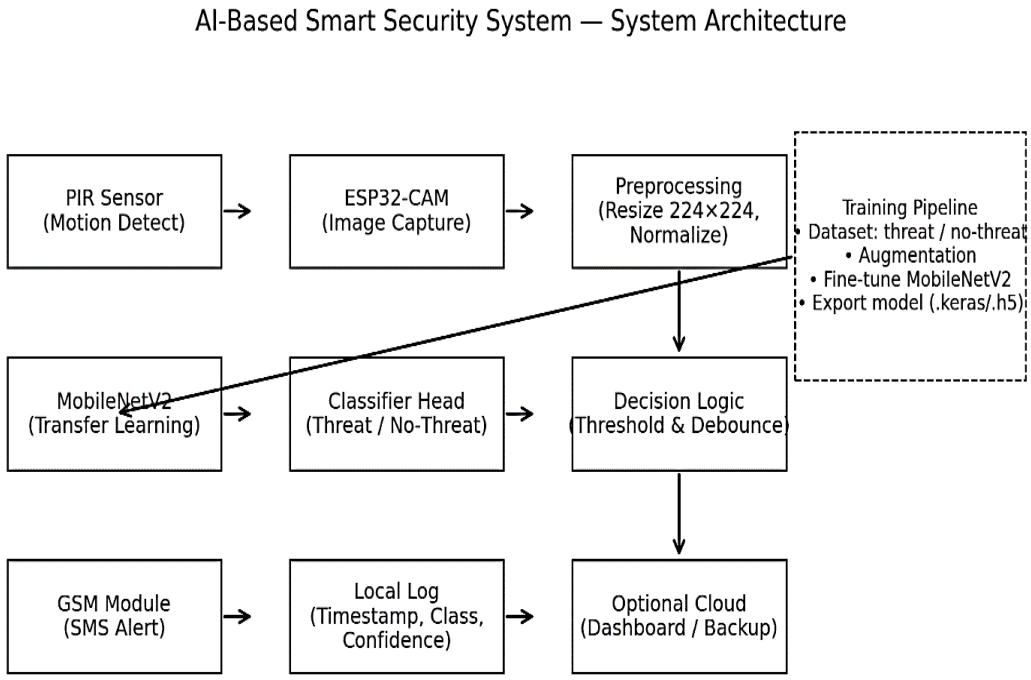

Fig 4: Block Diagram of the simulation

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

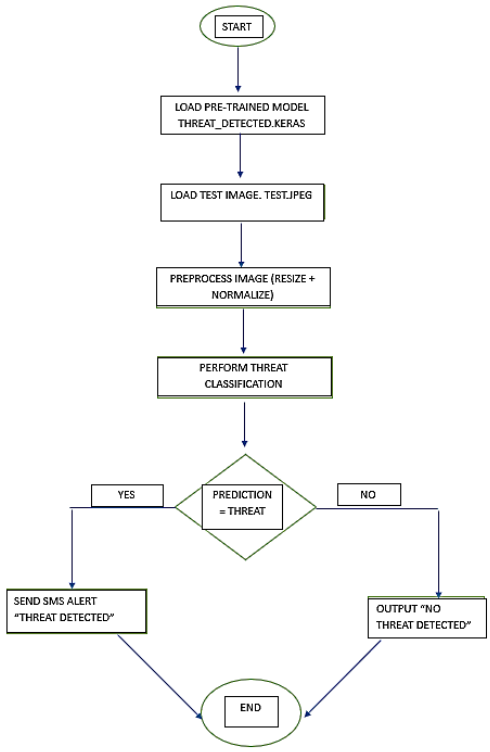

Figure 5: Flowchart representing the motion detection → image capture → CNN classification → alert generation of the simulated system.

Performance Metrics

The performance of this smart security system will be calculated based on standard classification metrics derived from the confusion matrix, as they provide quantitative measures of accuracy and reliability. The metrices being used are; Accuracy, Precision, Recall (Sensitivity), Specificity, and F1-Score, which collectively ensure that the proposed model's performance can be objectively compared against existing approaches and validated for real-world deployment. The formulas to be used are:

Accuracy

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{(EQ 13)}$$

Precision (Threat class)

$$\text{Precision} = \frac{TP}{TP+FP} \quad \text{(EQ 14)}$$

Recall (Threat detection / Sensitivity)

$$\text{Recall} = \frac{TP}{TP+FN} \quad \text{(EQ 15)}$$

Specificity (non-threat detection)

$$\text{Specificity} = \frac{TN}{TN+FP} \quad \text{(EQ 16)}$$

F1-Score

$$\text{F1} = \frac{2 \cdot Precision \cdot Recall}{Precision+Recall} \quad \text{(EQ 17)}$$

RESULTS AND DISCUSSION.

Model Training Results

The training and evaluation of the developed smart security system model were carried out to assess its ability to learn from the dataset, generalize to unseen data, and maintain robustness in real-world deployment. During this process, both training and validation metrics were continuously monitored across multiple epochs to evaluate the system's convergence behavior and stability. Key performance indicators, including accuracy, loss, precision, recall, specificity, and F1-score, were employed to provide a comprehensive understanding of the model's strengths and limitations. Visual representations such as learning curves, scatter plots, confusion matrices, and Receiver Operating Characteristic (ROC) curves were generated to interpret these results in detail.

The graph in Figure 6 shows how the model's training process was assessed using accuracy and loss curves. Training accuracy rose from 77% at epoch 0 to 94% by epoch 4, while validation accuracy remained consistently high at 97% across all epochs. This stability indicates strong generalization with no evidence of overfitting. Training loss declined sharply from 0.50 to 0.15, confirming effective parameter optimization, while validation loss remained lower throughout, reducing from 0.14 to 0.09. The consistently superior validation performance suggests the validation set was less complex than the training set but also highlights the model's robustness on unseen data. Overall, the results

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

demonstrate efficient convergence, high predictive reliability, and suitability of the model for deployment in practical intrusion detection scenarios.

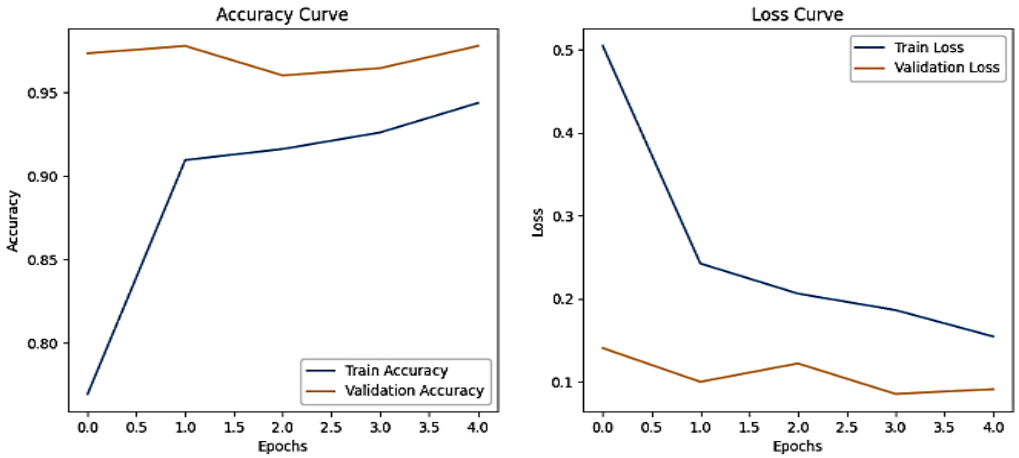

Figure 6. Graph showing Accuracy and Loss curves.

The scatter plot in Figure 7 illustrates the correspondence between true labels (blue) and predicted labels (orange) for the binary classification task. The overlap between the two distributions confirms strong predictive alignment, with the majority of class 0 and class 1 samples classified correctly. Misclassifications are limited to a few isolated points, indicating localized errors likely caused by overlapping features or underrepresented data patterns. This distribution demonstrates good generalization and high classification accuracy, but the small variations point to possible improvements through improved feature extraction, dataset balancing, or additional hyperparameter tuning.

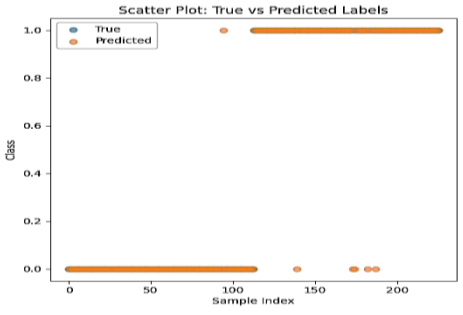

Figure 7. Graph showing the Scatter plot True values vs Predicted Labels

The confusion matrix in Figure 8 summarizes the classification results of the intrusion detection model across the two classes: Threat and Non-threat. Out of 226 test samples, the model correctly classified 112 actual threats as threats (True Positives) and 108 non-threats as non-threats (True Negatives), while only 1 false negative and 5 false positives were recorded. These results correspond and are verified based on the formulas for performance metrics (from chapter 3 EQN 13 – 17) to an overall accuracy of 97.35%, precision of 95.73%, recall of 99.12%, specificity of 95.58%, and an F1-score of 97.38%. The very low false negative rate highlights the system's strong capability to capture genuine threats, while the small number of false positives indicates only a minor trade-off in terms of unnecessary alerts.

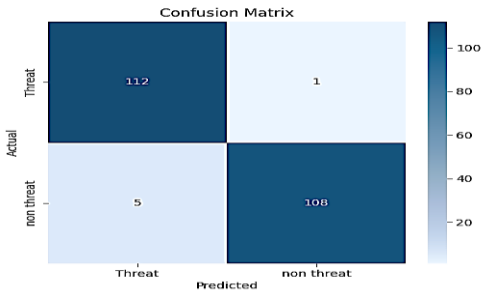

Figure 8. Confusion Matrix results

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Overall, these metrics demonstrate that the developed intrusion detection model achieves a robust balance between sensitivity and specificity, making it highly reliable for practical deployment. The Receiver Operating Characteristic (ROC) curve in Figure 9, quantitatively assessed the classifier's performance by plotting True Positive Rate (TPR) against False Positive Rate (FPR) across thresholds. A random model yields AUC = 0.5, while perfect classification corresponds to AUC = 1.0. In this evaluation, the model achieved AUC = 0.99, with the curve positioned near the top-left corner. At a representative threshold, the classifier attained TPR = 0.98 (i.e., 98% of actual positives correctly identified) and FPR = 0.01 (only 1% of negatives misclassified as positives). Similar performance is observed across multiple thresholds, confirming stable discriminatory power.

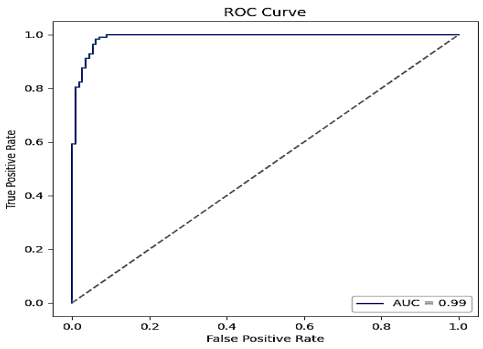

Figure 9. Graph of the ROC Curve and the AUC value.

These values demonstrate excellent accuracy and robustness in distinguishing between the two classes with minimal error, validating the model's suitability for the classification task under study. Nonetheless, the near-ideal AUC necessitates caution, as results evaluated solely on training or non-diverse data may indicate overfitting rather than genuine generalization.

Simulation Results

The simulation of the proposed system integrated a Passive Infrared (PIR) sensor for motion detection, a camera for image capture, a classification model to identify threats, and a GSM module to send alerts spanned 30 iterations, which followed a clear and logical sequence for each run. It began with a "Waiting for motion..." phase, simulating the PIR sensor's idle state, followed by "Motion detected! Triggering camera...", indicating the sensor has detected movement and activated the camera. This step effectively mimicked a real-world scenario where the PIR sensor triggers the system upon detecting an intruder or object.

Once triggered, the camera captures an image from the `simulation_images` directory, with the file path logged for traceability, using subfolders (`non threat` and `dThreat`) to handle categorized input data. The captured image is then processed with a classification step, followed by the processing time, resulting in a classification label (`non threat` or `dThreat`) with an associated probability. If the classification labels an image as `dThreat`, the system triggers a GSM alert with "Threat detected! Sending GSM alert to stakeholder..." and "ALERT: Intrusion detected! Immediate action required...", simulating notification to a stakeholder.

Each simulation concludes with a debug log for validation, and the process ends with an overall accuracy calculation, demonstrating a robust pipeline from motion detection to alert generation suitable for a real-time security system. The speed of the system varies across simulations, providing insight into its responsiveness. The first simulation shows a significant delay with `1s 1s/step`, likely due to model loading or initial image processing overhead, suggesting a one-time startup cost. From Simulation 2 onward, the processing time drops dramatically to `0s 60ms–77ms/step`, with examples like 67ms for `o1.jpeg` and 74ms for `dog4.jpeg`, indicating that once initialized, the system processes each image in approximately 60–77 milliseconds. This fast response is well-suited for real-time applications.

The "Waiting for motion..." phase includes a random delay of `1–3 seconds`, simulated with `time.sleep(random.uniform(1, 3))`, mimicking the PIR sensor's reaction time and

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

adding realism to test the system's behavior under varying conditions. Combining the motion detection delay with image capture and classification, the total response time per simulation ranges from approximately 1.06 to 3.077 seconds, which is reasonable for a security system, allowing quick detection and alerting. The consistent 60–77ms processing times across most simulations, with an occasional outlier like 425ms in Simulation 2 possibly due to I/O operations, highlight stable performance after the initial run.

Overall, the system's response is efficient for a simulated environment, with the PIR trigger and camera activation occurring seamlessly, followed by rapid classification. The GSM alert generation is instantaneous once a threat is detected, suggesting the alert mechanism would function well in a real-world deployment with a connected GSM module. The random delay in motion detection tests the system's ability to handle intermittent triggers, while the sub-100ms classification times demonstrate its capability for near-real-time operation. The initial 1-second delay is a minor aspect, likely addressable in a production setup, making the proposed PIR-Camera-Classification-GSM alert system a promising framework for security applications based on this simulation. The graphs of the overall system performance are shown in Figure 10, Figure 11, Figure 12 and Figure 13.

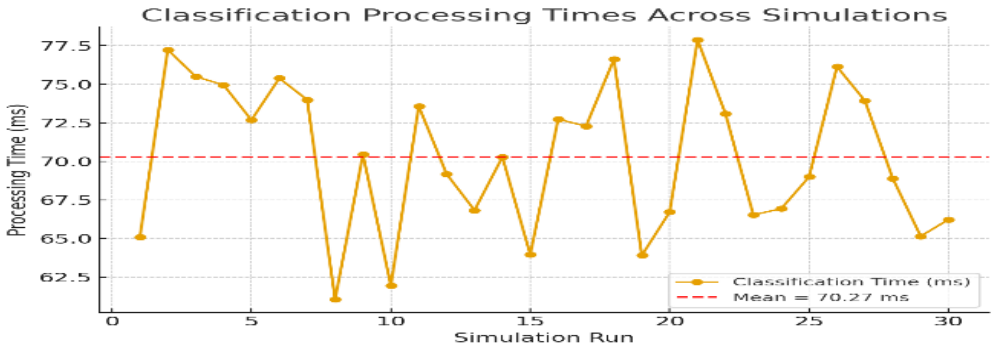

Figure 10: Graph of Classification Processing Times Across Simulations

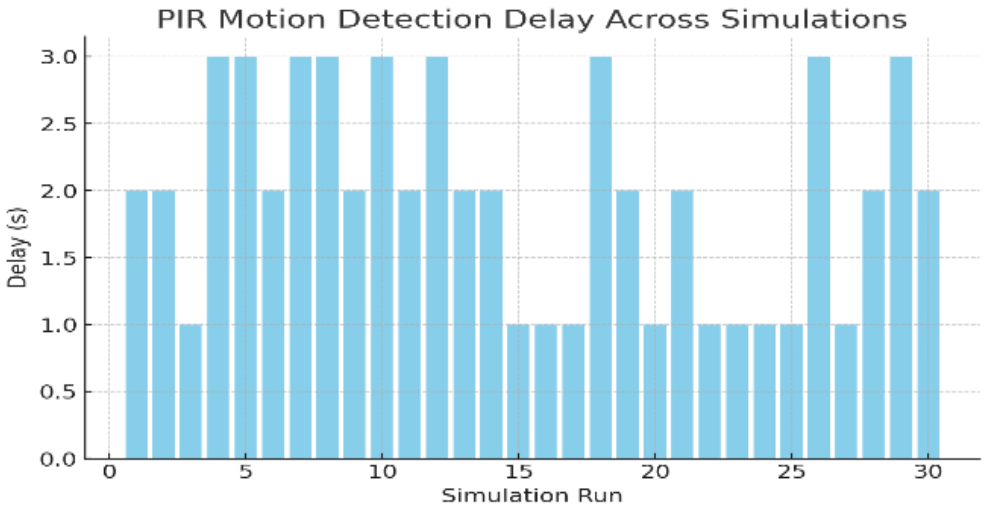

Figure 11: Graph of PIR Motion Detection Delay Across Simulations

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
✉ ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

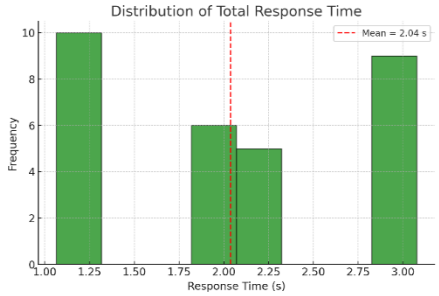

Figure 12: Graph of distribution Total Response Time

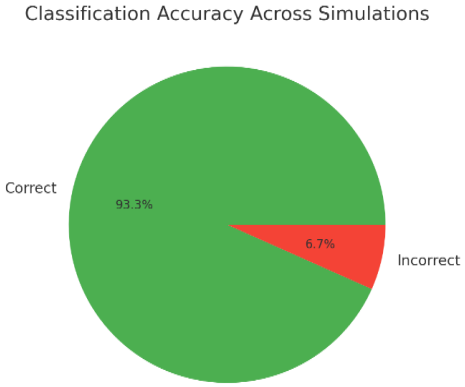

FIG 13: Graph of Classification Accuracy Across Simulations

Performance of the developed Classification

The performance of the developed classification system was evaluated using a dataset of thirty test instances, as summarized in the updated confusion matrix below, reflecting the recent code rerun. Out of the total, the model correctly classified twenty-eight cases, achieving an overall accuracy of 93.3%. Specifically, the outcomes indicate that non-threat samples were reliably detected, with nineteen instances accurately identified as non-threat (True Negatives), while nine genuine threat samples were successfully classified as threats (True Positives). Misclassifications were reduced, with one non-threat sample incorrectly flagged as a threat (False Positive) and one threat sample overlooked and labeled as non-threat (False Negative).

From these results, the classifier achieved a precision of 90% in identifying threats, meaning that nine out of every ten instances predicted as threats were correct. The recall, or sensitivity, reached 90%, indicating that the model captured nine-tenths of the actual threats present in the test set. Similarly, the specificity was calculated at 95%, confirming enhanced reliability in recognizing benign inputs. The balance between precision and recall is reflected in an F1-score of 90%, suggesting a highly effective performance with improved harmony. These results are summarized in the confusion matrix of Figure 14.

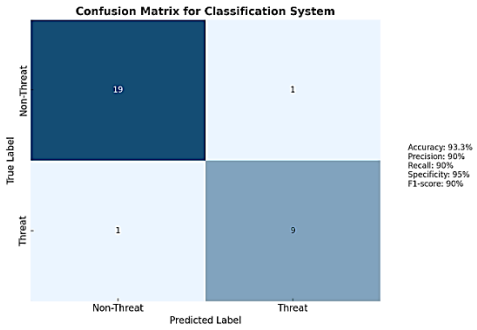

FIG 10: Confusion Matrix of the simulated system

A direct comparison between the confusion matrix of training model and simulation model demonstrates a strong potential for real-world deployment, with results indicating a high level of reliability in distinguishing threats from non-threats. Achieving an overall accuracy of 93.3% and an F1-score of 90%, the system exhibits a balanced performance between precision and recall, reflecting its ability to minimize both false positives and false negatives. Compared to earlier iterations, the classification results highlight the system's robustness in addressing the common challenge of false alarms, which often undermines the effectiveness of low-cost rural security solutions.

Nonetheless, while the outcomes confirm that the model can operate effectively in practice, further refinement and extensive testing on larger, more diverse datasets are necessary to validate its adaptability to broader rural scenarios

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(4), DECEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

and ensure consistent sensitivity across varying environmental conditions.

DISCUSSION OF FINDINGS

The comparative analysis between the proposed system and other alternatives from the literature based on performance, efficiency, affordability, deployment in rural Nigerian setting as well as the systems advantages and disadvantages to these alternatives is well highlighted in Table 3. Based on the comparison, the proposed system is highly suitable for rural Nigerian settings and resource-constrained regions, with a revised 93.3% AI classification accuracy significantly outperforming basic detection in systems of [5], [7] and [8] and rivaling video-based of [6], or the multi-sensor system of [9]. Efficiency excels with 0.5s motion-to-capture, 60–77ms classification (post-1s load), and PIR-camera power conservation with possible solar expansion, surpassing network-dependent delays in [9] and [10] and fixed cycles in [11].

Affordability at ~₦30,000 (ESP32-CAM, PIR, GSM) remains competitive, matching [9], [11], and undercutting [6], with lightweight MobileNet adding value without cost increases. Deployment benefits from offline GSM, addresses rural power/network challenges better than WiFi-limited communication in [9], [10], with 93.3% accuracy minimizing false alarms effectively. Minor delays and simulation-based testing are drawbacks, but the system's cost-effective, intelligent design makes it not only good enough but a robust, reliable solution for rural security needs. The comparative analysis is summarized in Table 3.

Table 3: Comparative Analysis of Proposed System vs Alternatives from Other works

Reference	Performance vs. Proposed System	Efficiency vs. Proposed System	Cost Comparison	Rural Deployment Suitability	Key Advantages of Proposed System	Key Disadvantages
[5]	Proposed system has far higher accuracy (93.3%) and better threat classification	Faster alerts, lower dependence on network	Cheaper (~₦30,000 vs. ₦50,000–₦100,000)	Better for unstable power and offline use	High accuracy, low cost, efficient	No fingerprint; simulation limits
[6]	Comparable detection but more intelligent classification	More power-efficient though less continuous	Much cheaper (~₦30,000 vs. ₦100,000–₦200,000)	Offline GSM and solar-ready	High accuracy, offline operation	No continuous video stream
[7]	Much higher performance due to camera + AI	More efficient alert pipeline	Slightly higher cost but justified	More suitable due to GSM and solar	High accuracy, remote alerts	Higher cost than basic systems
[8]	Major accuracy improvement over PIR-only systems	Faster alerts and power conservation	Slightly higher cost	Better offline deployment	Superior accuracy and speed	Higher complexity
[11]	Outperforms PIR-only and long alert cycles	Much faster and more efficient	Comparable cost	More adaptable via solar/GSM	High accuracy and rural-fit	Slightly higher cost

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

Reference	Performance vs. Proposed System	Efficiency vs. Proposed System	Cost Comparison	Rural Deployment Suitability	Key Advantages of Proposed System	Key Disadvantages
[9]	Higher precision with AI classification	Lower power and offline capability	Comparable cost	Better than WiFi-only for rural	High accuracy and power savings	Slight delay vs. realtime
[10]	Better coverage and accuracy	Lower energy use	Higher cost but more features	Offline and solar-friendly	High accuracy and offline alerts	Startup delay and cost

CONCLUSION

The design and simulation of the AI-enabled smart security system marked a significant step towards addressing the security challenges faced by rural Nigerian communities. The simulated system successfully integrated the ESP32-CAM, PIR-Camera Sensor Module, and GSM technology to provide real-time threat detection and alert transmission without relying on internet infrastructure. The achieved 93.3% classification accuracy, highlights its responsiveness, while the estimated cost of under ₦30,000 showed potential affordability of the overall system. The system also outperformed many existing alternatives in affordability and adaptability to resource-constrained environments. Despite its simulation-based nature, which limits real-world environmental testing, the system's performance validates its potential as a scalable, intelligent security solution for rural Nigeria.

RECOMMENDATIONS

To further enhance the proposed system, several recommendations are suggested. Firstly, expanding field testing by conducting real-world trials across diverse rural settings is essential to assess performance under varying lighting, weather, and terrain conditions, thereby addressing the current limitation of simulation-based evaluation. Additionally, improving dataset diversity by increasing the training dataset beyond 226 samples to encompass a broader range of rural-specific scenarios, such as night conditions and animal movements, could potentially boost accuracy beyond the current 93.3%. Enhancing GSM reliability through the integration of a backup communication method, such as LoRa, is advised to ensure alert delivery in areas with poor GSM coverage, particularly in remote locations. Furthermore, optimizing solar integration by developing a standardized solar panel and battery configuration would fully leverage the system's solar-compatible design, reducing dependency on external power sources. Adding geolocation features by incorporating GPS modules to provide location data with alerts would improve response coordination in large rural areas. Lastly, refining model tuning by adjusting the MobileNet model to minimize the 1-second initial load and reduce the single false positive/negative would enhance real-time performance and reliability.

REFERENCES

[1] K. Ohazuruike, F. A. Elechi, and P. N. Eze, "Impact of herdsmen and community clashes on national integration in nigeria," south east political science review, vol. 9, no. 1, 2024. https://journals.npsa-se.org.ng/index.php/SEPSR/article/view/211

[2] A. M. M. I. Chowdhury and E. S. Hasan, "Smart Surveillance Systems: Trends, Challenges and Future Directions," *Indonesian Journal of Computer Science*, vol. 14, no. 2, pp. 1-10, 2025.

[3] N. J. M. I. I., S. G. Oladele and S. I. O. U. K., "Design and Implementation of Farm Monitoring and Security System," *International Journal of Computer Applications*, vol. 182, no. 31, pp. 31-36, 2018.

[4] B. N. Mohapatra, S. S. Taware, and P. P. Parab, "Smart Security Alarm System using PIR Sensor," Perspectives in Communication, Embedded-systems and Signal-processing -

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.

PiCES (pices), vol. 5, no. 9, pp. 90-92, Jan. 2022, doi: 10.5281/zenodo.5867913.

[5] H. Ahmadu, A. D. Jiya, H. Usman, and I. Yusuf, "Efficacy of a Remote Home-Based Security System on Residential Estate Safety in Minna Metropolis, Niger State, Nigeria," *FNAS Journal of Computing and Applications (FNAS-JCA)*, vol. 2, no. 2, 2025.

[6] P. G. Gopinath, M. Harika, K. Chandu, K. B. Reddy, B. K. Chandrika, and P. Gurucharan, "Development of GSM-based surveillance system in remote areas using solar power," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 11, no. 4, pp. 1–10, Apr. 2024. https://www.jetir.org/papers/JETIR2404690.pdf

[7] B. N. Mohapatra, S. S. Taware, and P. P. Parab, "Smart security alarm system using PIR sensor," *pices*, vol. 5, no. 9, pp. 90–92, Jan. 2022.

[8] S. A. Akinwumi, A. C. Ezenwosu, T. Omotosho, and O. Adewoyin, "Arduino based security system using passive infrared (PIR) motion sensor," *IOP Conference Series: Earth and Environmental Science*, vol. 655, no. 1, p. 012039, Feb. 2021, doi: 10.1088/1755-1315/655/1/012039.

[9] K. Likhitha, S. Malineni, N. Jampani, and N. L. Prasanna, "Home security system using PIR sensor-IoT," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 5, no. 2, pp. 497–500, Mar.–Apr. 2019, doi: 10.32628/CSEIT195272.

[10] V. Kothandapani, P. Kodidela, and P. Gurram, "IoT based smart intruder detection system for smart homes," *International Journal of Scientific Research in Science and Technology*, Jul. 2021, doi: 10.32628/IJSRST218410.

[11] O. E. Ikpenyi, O. E. Abumere, and J. A. Amusan, "Construction of GSM based home security alert system using passive infrared sensor," *World Journal of Advanced Research and Reviews*, vol. 14, no. 2, pp. 648–657, May 2022, doi: 10.30574/wjarr.2022.14.2.0447.

[12] A. R. Axay and A. Purohit, "IoT-based motion sensor camera surveillance system with Telegram control using ESP32-CAM," 2025. doi: 10.13140/RG.2.2.11183.24484.

[13] C. Azubuike and O. Obiefuna, "Wireless communication: The impact of GSM on the economic lives of the Nigerian rural users," *J. Educ. Soc. Res.*, vol. 4, no. 7, pp. 79–86, 2014, doi: 10.5901/jesr.2014.v4n7p79.

[14] P. Dutta, U. K. Garapati, B. Sridharan, and V. Agarwal, "A comprehensive review of embedded system design aspects for rural application platform," *Int. J. Comput. Appl.*, vol. 106, no. 11, pp. 39–44, 2014, doi: 10.5120/18567-9819.

[15] E. Edozie, V. H. U. Eze, M. Imaculate, and W. Janat, "Design and implementation of a smart surveillance security system," *Int. J. Comput. Eng. Technol.*, vol. 14, no. 1, pp. 28–36, 2023.

[16] F. Kristensen, H. Hedberg, H. Jiang, and P. Nilsson, "An embedded real-time surveillance system: Implementation and evaluation," *J. Signal Process. Syst.*, vol. 52, no. 1, pp. 75–94, 2008, doi: 10.1007/s11265-007-0100-7.

[17] K. Ohazuruike, F. A. Elechi, and P. N. Eze, "Impact of herdsmen and community clashes on national integration in Nigeria," *South East Political Science Review*, vol. 9, no. 1, 2024. [Online]. Available: https://journals.npsa-se.org.ng/index.php/SEPSR/article/view/211

[18] S. G. Oladele and S. I. O. Uk, "Design and implementation of farm monitoring and security system," *Int. J. Comput. Appl.*, vol. 182, no. 31, pp. 31–36, 2018.

[19] V. N. Pamadi and P. Singh, "Edge AI vs Cloud AI: A comparative study of performance, latency and scalability," *Int. J. Eng. Emerg. Technol.*, vol. 13, no. 3, 2025.

[20] A. Rana, T. Kumar, and N. Puri, "Design of GSM-based fire detection system using microcontroller and sensors," in *Advances in Manufacturing Technology and Management: Proc. 6th Int. Conf. Advanced Production and Industrial Engineering (ICAPIE)*, Nov. 2022, pp. 557–568, Springer. doi: 10.1007/978-981-16-9523-0_62.

[21] A. F. Santamaria, P. Raimondo, M. Tropea, F. De Rango, and C. Aiello, "An IoT surveillance system based on a decentralised architecture," *Sensors*, vol. 19, no. 6, p. 1462, 2019, doi: 10.3390/s19061462.

[22] P. H. M. Sá, R. B. Loureiro, F. V. N. Lisboa, and R. M. Peixoto, "Efficient deployment of machine learning models on microcontrollers: A comparative study of quantization and pruning strategies," in *Proc. IX Simpósio Internacional de Inovação e Tecnologia (SIINTEC)*, Oct. 2023. doi: 10.5151/siintec2023-305873.

Corresponding author: Aliyu Abdul-Quadri Hujatullahi
ahaliyu@nda.edu.ng
Electrical/Electronic Engineering, Nigerian Defence Academy Kaduna.