Edge AI and Cloud-Integrated Framework for Real-Time Harmful Drone Detection and Neutralization

Odinachi U. Nwankwo, Hope L. Nakayiza, Simeon Okechukwu Ajakwe*, Dong-Seong Kim, Jae Min Lee
Department of IT Convergence, Kumoh National Institute of Technology, Gumi, South Korea
*ICT Convergence Research Centre Kumoh National Institute of Technology, Gumi, South Korea
{odinachi, hopeleticia, simeon.ajakwe, dskim, ljmpaul}@kumoh.ac.kr

***Abstract*—The rapid rise of harmful drones poses serious risks to public safety and critical infrastructure, requiring fast and reliable countermeasures. This paper presents an Edge AI and Cloud-Integrated Framework that unifies lightweight detection, secure communication, and automated neutralization. A YOLOv5 model deployed on Jetson Nano enables low-latency edge inference, while Adafruit IoT cloud integration supports real-time monitoring and control. Unlike prior works that focus only on detection, the proposed system includes a cloud-assisted neutralization mechanism for end-to-end defense. Experimental evaluation on a drone payload dataset achieves a mean average precision (mAP@50) of 0.645, a recall of 0.653, and an accuracy of 0.733. The framework offers a scalable foundation for future 5G/6G-enabled UAV defense in urban, industrial, and military environments.**

***Index Terms*—Edge AI, Cloud IoT, Harmful Drone Detection, Real-Time Monitoring, UAV Neutralization, Communication-Efficient Framework, Deep Learning (YOLOv5), Secure Drone Networks**

I. Introduction

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, are increasingly employed in logistics, surveillance, agriculture, and emergency response due to their low cost, autonomy, and flexibility. However, the same advantages have enabled their misuse in malicious activities such as smuggling, espionage, and weaponized attacks, as witnessed in recent conflicts between Ukraine and Russia where drones were used to deliver ammunition and damage infrastructure [1]. Differentiating between benign UAVs carrying legitimate payloads and malicious drones carrying harmful objects is therefore a critical challenge for ensuring public safety.

Several detection techniques have been explored in prior research, including radar-based sensing, acoustic signatures, radio-frequency (RF) analysis, and computer vision approaches [1]. For example, the YOLO family of deep learning models has demonstrated strong performance in identifying drones and their attached payloads from images and videos [2]. Recent studies have also evaluated deep learning models such as YOLOv5 for harmful payload identification with high accuracy and low inference times [3]. Nevertheless, most of these works focus solely on drone detection and lack mechanisms for neutralization or secure cloud-based monitoring, limiting their practicality in real-world defense scenarios.

These limitations motivated this research to design a **unified framework** for harmful drone detection and neutralization. Specifically, we combine edge intelligence, cloud integration, and IoT-based control into a single scalable system. Unlike prior approaches that emphasize either detection or monitoring in isolation, our framework incorporates (i) **real-time detection** using YOLOv5 on Jetson Nano for low-latency inference, (ii) **cloud-enabled monitoring and coordination** using Adafruit IoT for secure communication, and (iii) **automated neutralization** via defensive drones activated upon confirmed threats. The main contributions of this paper are as follows:

1) A hybrid edge–cloud framework integrating YOLOv5-based harmful drone detection, IoT communication, and neutralization.
2) Deployment of lightweight deep learning models on Jetson Nano for accurate and energy-efficient real-time inference.
3) Design of a cloud-assisted neutralization mechanism enabling secure activation of defensive UAVs.
4) Experimental validation showing reliable detection accuracy (mAP@50 = 0.645, recall = 0.653, accuracy = 0.733) with reduced communication overhead.
5) A foundation for future 5G/6G-enabled UAV defense with cooperative swarm intelligence, adversarial robustness, and secure network integration.

By bridging embedded AI, cloud IoT, and real-time neutralization, this work advances UAV defense beyond traditional detection-only systems and provides a scalable foundation for protecting critical infrastructures, urban spaces, and military operations. In this paper, The rest of the paper is organized as follows: Section II presents the related works; section II highlight the problem formulation; Section III details the proposed methodology; Section IV presents results discussion; and Section V concludes with implications and future directions.

TABLE I: Comparative Analysis of Related Works vs. Proposed Framework

Work	Approach / Strengths	Limitations vs. Proposed Framework
Shakhatreh et al. (2019)	Vision-based CNN detection; good accuracy in static conditions.	High computation cost; no cloud integration or neutralization.
Ezuma et al. (2020)	RF signal analysis; effective for non-visual detection.	Requires spectrum hardware; no IoT monitoring or neutralization.
Aker et al. (2017)	Faster R-CNN; accurate detection.	Too heavy for edge deployment; lacks scalability and defense.
Ashraf et al. (2021)	Centralized DL models; high accuracy.	Bandwidth-intensive; high latency; no neutralization.
Dorling et al. (2022)	Swarm-based monitoring.	Multi-UAV support but no automated defense or security.
Proposed Framework	YOLOv5 on Jetson Nano + IoT cloud + defensive UAVs.	Real-time, low-latency detection with cloud-based neutralization and scalable communication.

II. Related Work on UAV Detection and Communication Security

Recent advances in UAV detection have explored vision-based deep learning, RF analysis, radar sensing, and swarm monitoring. Vision-based systems using CNNs and YOLO variants have shown strong accuracy for detecting drones and attached payloads [3]–[5]. However, most of these works focus solely on detection and neglect cloud-based monitoring or automated neutralization. RF-based systems provide non-visual detection but require dedicated spectrum hardware and cannot detect autonomous UAVs reliably [6], [7]. Radar-based methods offer robustness in low-visibility conditions but are computationally expensive and lack integrated countermeasures [8]. Swarm monitoring frameworks have also been proposed for large-scale UAV tracking, yet they typically exclude defense mechanisms and secure communication aspects [5].

Several studies between 2022 and 2025 highlight the need for lightweight, real-time, and communication-efficient solutions. For instance, Sun et al. [4] enhanced YOLOv5 with spatiotemporal cues for improved detection in surveillance videos but did not address neutralization. Similarly, recent reviews emphasize the gap in integrating adversarial robustness, cloud-enabled coordination, and automated defense into UAV security infrastructures [3]. These gaps motivate our proposed framework, which unifies harmful drone detection, cloud monitoring, and IoT-based neutralization into a single communication-efficient pipeline.

Mathematical Problem Formulation

The completeness of the UAV defense system depends not only on the inclusion of its core components but also on their real-time efficiency and scalability. Let the system be composed of four main modules:

- $X_1 = Dh$ (Harmful Drone Detection),
- $X_2 = N$ (Neutralization),
- $X_3 = Cc$ (Cloud Computing),
- $X_4 = EAI$ (Embedded AI).

We define the overall effectiveness of the framework as a weighted sum of multiple performance objectives as captured in equation (1):

$$\max\ R = w_1 \cdot Acc + w_2 \cdot \left(1 - \frac{L}{L_{\max}}\right) + w_3 \cdot \left(1 - \frac{C}{C_{\max}}\right) + w_4 \cdot \left(1 - \frac{E}{E_{\max}}\right) \tag{1}$$

where:

- Acc = detection accuracy (e.g., mAP or F1-score),
- L = end-to-end latency (inference + communication delay),
- C = communication cost (bandwidth consumption),
- E = energy consumption (on edge devices),
- $L_{\max}, C_{\max}, E_{\max}$ = acceptable thresholds,
- w_1, w_2, w_3, w_4 = weights reflecting system priorities.

This formulation balances detection performance against real-time and resource constraints, ensuring a scalable edge–cloud deployment.

The optimization is subject to the following real-time and operational constraints:

$$L \leq L_{\text{th}}, \quad C \leq C_{\text{th}}, \quad E \leq E_{\text{th}} \tag{2}$$

where $L_{\text{th}}, C_{\text{th}}, E_{\text{th}}$ are thresholds defined by mission requirements (e.g., maximum latency for interception, maximum allowable bandwidth, maximum device power budget).

Unlike prior models that optimize accuracy alone [3], [6], [7], this formulation explicitly incorporates latency, communication, and energy efficiency. This ensures that the proposed UAV defense framework remains deployable in real-time scenarios such as urban security, industrial surveillance, and military operations where both speed and scalability are critical.

III. Edge–Cloud Communication Framework for Harmful Drone Defense

Fig. 1 is an overview of the proposed system architecture. The whole framework is divided into two units: the detection and the neutralization units. The detection is done by the cameras and the YOLO version 5 model embedded into a Jetson Nano. The YOLO V5 unit processes the images captured by the camera to tell or identify the drone and the nature of the package carried by the UAV. Neutralization involves the destruction of the Unmanned Aerial Vehicle by a stand-by defensive drone that is activated by the true positive message it receives from the detection unit.

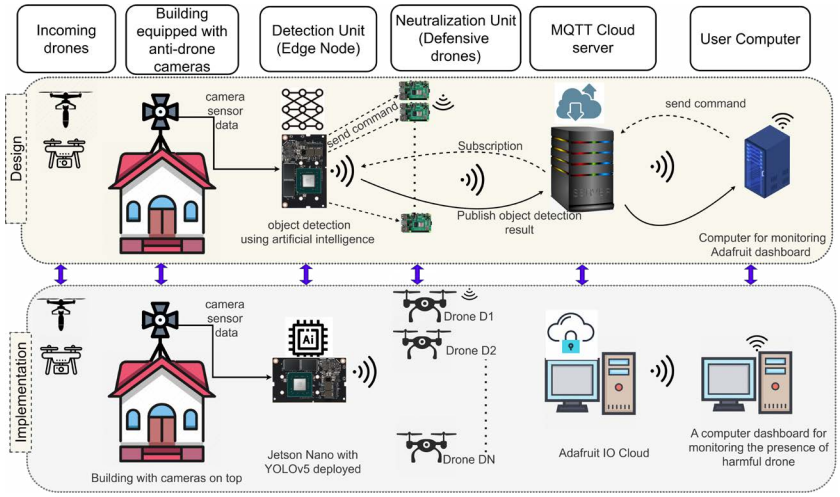

Fig. 1: Overview of Proposed System Architecture

The proposed anti-drone defense system integrates AI-powered edge computing, the Internet of Things (IoT), and cloud-based monitoring to detect and neutralize unauthorized drones. It consists of a stationary anti-drone camera mounted on a building, an edge node (Jetson Nano) running YOLOv5 for real-time object detection, and a fleet of defensive drones for countermeasures. When an incoming drone enters the surveillance zone, the camera captures sensor data and transmits them to the edge node, which classifies the drone as a benign payload drone or a harmful threat. If identified as a threat, a command is sent to activate defensive drones to intercept or neutralize the target.

The system uses message queue telemetry transport (MQTT)-based cloud server to relay detection results and alerts to a user monitoring dashboard. The edge node publishes classification results to the cloud, enabling real-time tracking and decision-making. The Adafruit IO cloud dashboard serves as the primary user interface, allowing remote monitoring and manual intervention when needed. Defensive drones (D1, D2, DN) are activated autonomously to engage with harmful drones, employing signal jamming, tracking, or interception techniques to neutralize threats before they reach restricted areas.

By leveraging edge AI for real-time processing, cloud-based data management, and automated drone defense, this system ensures efficient aerial threat mitigation. The combination of YOLOv5-based object detection, IoT-based communication, and AI-driven automation enables a fast, scalable, and intelligent anti-drone security framework, making it suitable for applications in critical infrastructure protection, military defense, and public safety surveillance.

Algorithm 1 outlines the drone detection and neutralization process, integrating embedded AI and cloud computing to ensure real-time response to threats. The system cycles through a set of camera IDs to detect incoming drones using the $DETECT\_DRONE$ procedure. Once a drone is identified, the $CHECK\_PAYLOAD$ function utilizes a YOLOv5 model on Jetson Nano to classify the payload as harmful or benign. If a harmful payload is detected, the system triggers an alert ($SEND\_ALERT$), activates the neutralization mechanism ($ACTIVATE\_N$), and transmits the threat status to the cloud ($SEND\_TO\_CLOUD$). In the case of a benign payload, only the status is uploaded to the cloud. This algorithm ensures autonomous monitoring and decision-making, blending embedded AI processing with cloud-based threat communication for rapid drone threat response.

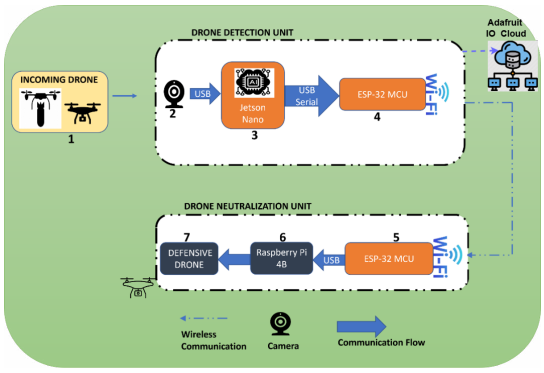

Fig. 2: Electronic implementation of the system

IV. Experimental Validation of Real-Time Detection and Communication Efficiency

A. System Setup

The proposed framework was implemented on an NVIDIA Jetson Nano as the edge node, equipped with a USB camera for real-time image acquisition. YOLOv5 was deployed for harmful drone detection, and an ESP-32 microcontroller provided communication between the detection unit and the neu-

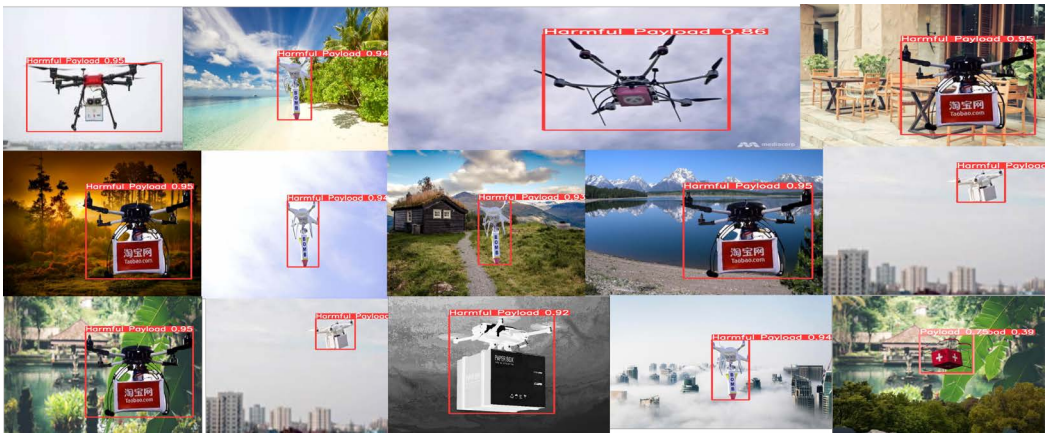

Fig. 3: Inference result using test dataset showing object detection of UAV carrying harmful payload

Algorithm 1: Drone Detection and Neutralization

Input: camera_ids $= \{1, 2, 3, 4, 5\}$, Image detected
Output: Alert if D_h detected, Activate N, Send payload status to C_c
Definitions:
$D_h \leftarrow$ Harmful Drone Detection
$N \leftarrow$ Neutralization Mechanism
$C_c \leftarrow$ Cloud Computing Implementation
$E_{AI} \leftarrow$ Embedded AI Implementation (YOLOv5 on Jetson Nano)
foreach $camera\_id \in camera\_ids$ **do**
  DETECT_DRONE($camera\_id$)
  if *Drone is detected* **then**
    CHECK_PAYLOAD($drone\_image$)
    if *is_harmful_payload* **then**
      SEND_ALERT()
      ACTIVATE_N()
      SEND_TO_CLOUD("Harmful_Payload", C_c)
    end
    else
      SEND_TO_CLOUD("Benign_Payload", C_c)
    end
  end
end

Function DETECT_DRONE($camera\_id$)**:**
  Print "Scanning for drones using camera"
  return True `// Assume drone is detected`
Function CHECK_PAYLOAD($drone\_image$)**:**
  Print "Analyzing payload using E_{AI}"
  return True `// Assume a harmful payload is detected`
Function SEND_ALERT()**:**
  Print "ALERT: D_h detected! Notifying authorities..."
Function ACTIVATE_N()**:**
  Print "Deploying defensive drone for interception..."
Function SEND_TO_CLOUD($payload\_status$, C_c)**:**
  Print "Uploading $payload\_status$ to C_c"

tralization module. A Raspberry Pi 4B controlled the defensive UAVs activated during threat scenarios. The Adafruit IO cloud platform served as the monitoring dashboard, enabling remote supervision and manual intervention when required.

B. Dataset Description & and Training

The Drone_Payload dataset from Roboflow contains 511 annotated images for object detection, focused on identifying drones carrying harmful or general payloads. It includes 447 training, 43 validation, and 21 test images, with bounding boxes labeled for use in security and surveillance applications. Experiments were conducted using the Drone Payload dataset from Roboflow, containing 511 annotated images (447 training, 43 validation, and 21 test samples). Images were labeled for both benign and harmful payloads. The YOLOv5 model was trained with transfer learning, using 300 epochs and a batch size of 16, optimized with the Adam optimizer. Data augmentation techniques (rotation, scaling, flipping) were applied to improve generalization under diverse conditions.

C. Evaluation Metrics

To assess performance, we employed standard object detection metrics: mean Average Precision at 50% IoU (mAP@50), recall, precision, accuracy, and F1-score. In addition, latency and communication overhead were measured to evaluate real-time feasibility on embedded hardware.

D. Results and Analysis

Fig. 4 presents the confusion matrix, which shows strong classification performance for harmful payloads with a true positive rate of 70%. Some misclassifications were observed between benign payloads and background, but overall accuracy remained competitive. Fig. 5 depicts the model training curves, with steadily decreasing loss and increasing precision and recall.

The proposed system achieved the following performance:

- mAP@50 = 0.645
- Mean Recall = 0.653
- Accuracy = 0.733
- Mean F1-score = 0.639

Inference results (Fig. 3) indicate that YOLOv5 consistently detected UAVs with harmful payloads across varied backgrounds with confidence scores above 0.9. The system maintained low inference latency on Jetson Nano, confirming the feasibility of real-time deployment. Communication overhead was significantly reduced by local edge inference, as only classification results—not raw video—were transmitted to

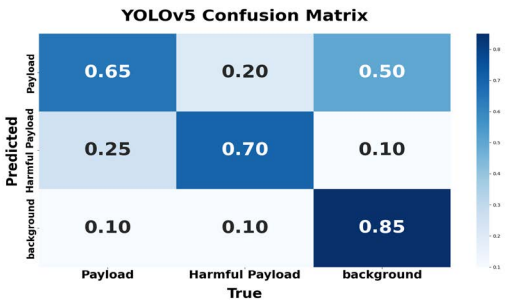

Fig. 4: The confusion matrix for the YOLOv5 model, showing classification performance across three categories: Payload, Harmful Payload, and Background. The diagonal values indicate correct classifications, with 65% accuracy for Payload, 70% for Harmful Payload, and 85% for Background. Misclassification rates are observed, such as 25% of Payloads being classified as Harmful Payloads and 10% of Background being misclassified as other categories.

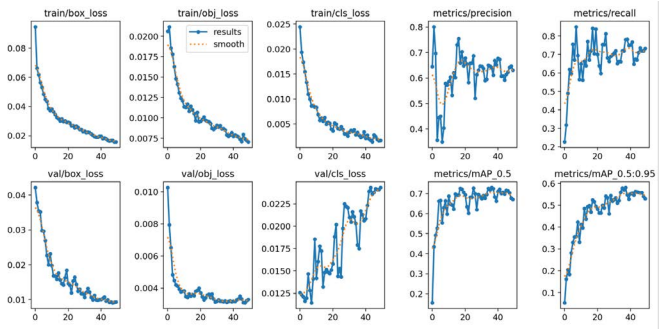

Fig. 5: Graphs showing loss, precision, average precision, and recall curves. mean average precision of approximately 0.65 at 50% IoU, and a mean recall of approximately 0.65 was achieved

the cloud. Cloud-based monitoring was successfully validated using the Adafruit IO dashboard (Fig. 6), which displayed immediate status updates: green for benign payloads and red for harmful ones. This ensured real-time situational awareness for operators and provided a seamless link between embedded detection and cloud visualization.

TABLE II: Performance Metrics Estimated from the Confusion Matrix

Metric	Value
Mean Average Precision (mAP@50)	**0.645**
Mean Recall	**0.653**
Accuracy	**0.733**
Mean F1-Score	**0.639**

The values were computed based on the confusion matrix, with mAP@50 indicating the model's precision at 50% IoU threshold.

Compared to prior works [3], [6], [7], which emphasize detection without neutralization or cloud integration, the proposed system demonstrates a holistic solution. While the detection accuracy (mAP@50 = 0.645) is moderate, the integration of real-time inference, reduced communication cost, and automated neutralization highlights the framework's practicality for urban and industrial deployment. These results confirm that edge–cloud integration not only enables scalable UAV monitoring but also ensures fast and coordinated responses to aerial threats.

The last two Adafruit IO dashboards in Fig. 6 and Fig. 7 demonstrate the real-time functionality of the cloud-based monitoring system for UAV payload classification. Initially, all status indicators are inactive (black), awaiting input from the embedded AI system. Once a drone is detected and classified, the dashboard updates: a green indicator signals a benign payload, while red indicates a harmful one. This visual feedback provides instant remote awareness and supports real-time decision-making, effectively linking embedded edge detection with cloud-based alert visualization.

V. Conclusion and Future Work

This paper presented an Edge AI and Cloud-Integrated framework for real-time harmful drone detection and neutralization. By deploying YOLOv5 on Jetson Nano, the system achieved reliable edge inference with reduced communication overhead, while Adafruit IoT cloud integration enabled remote monitoring and automated activation of defensive UAVs. Experimental evaluation demonstrated competitive detection performance (mAP@50 = 0.645, recall = 0.653, accuracy = 0.733) and confirmed the feasibility of low-latency operation on embedded hardware. Unlike prior works limited to detection, the proposed system delivers a holistic solution unifying detection, cloud monitoring, and neutralization. Future work will focus on enhancing adversarial robustness against spoofing and camouflage attacks, integrating multi-UAV cooperative defense strategies, and leveraging 5G/6G ultra-reliable low-latency communication (URLLC) for large-scale deployments. These directions will further advance the scalability, security, and resilience of next-generation anti-drone infrastructures.

Acknowledgement

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] N. Al-lQubaydhi, A. Alenezi, T. Alanazi, A. Senyor, N. Alanezi, B. Alotaibi, M. Alotaibi, A. Razaque, and S. Hariri, "Deep learning for unmanned aerial vehicles detection: A review," *Computer Science Review*, vol. 51, p. 100614, 2024.

[2] R. Valaboju, Vaishnavi, C. Harshitha, A. R. Kallam, and B. S. Babu, "Drone detection and classification using computer vision," in *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2023, pp. 1320–1328.

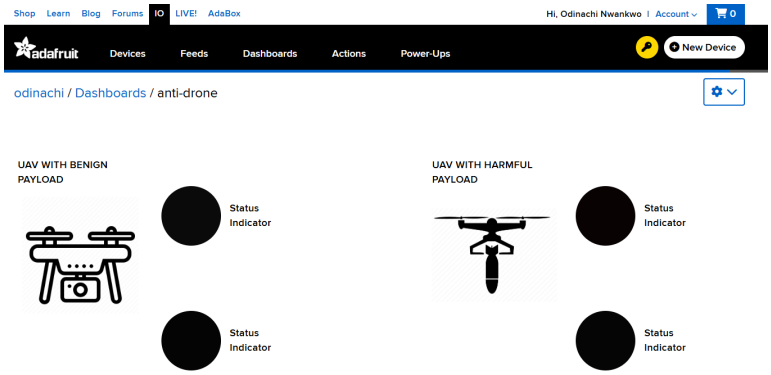

Fig. 6: Adafruit IO dashboard visualizing real-time UAV payload classification. The interface displays status indicators for drones with neither benign nor harmful payloads, enabling cloud-based monitoring.

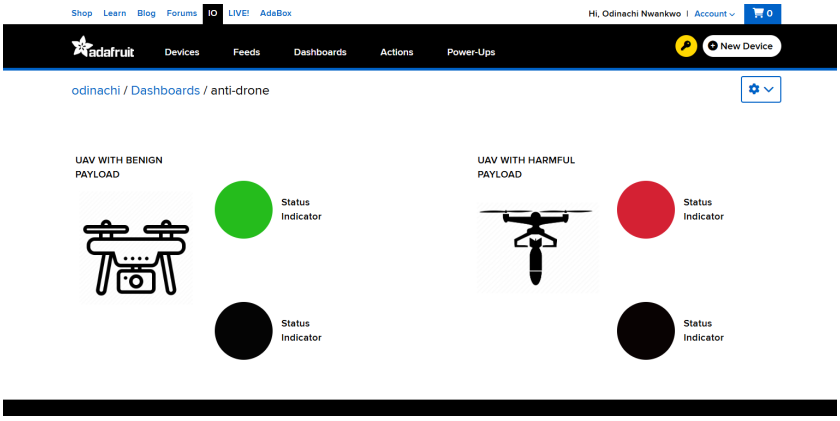

Fig. 7: Updated Adafruit IO dashboard showing real-time status indicators for UAV payload classification. A green indicator represents a benign payload, while a red indicator signals detection of a harmful payload, enabling prompt situational awareness and response.

[3] S. Ajakwe, V. Ihekoronye, R. Akter, D. Kim, and J. Lee, "Adaptive drone identification and neutralization scheme for real-time military tactical operations," in *2022 International Conference on Information Networking (ICOIN)*. Los Alamitos, CA, USA: IEEE Computer Society, jan 2022, pp. 380–384.

[4] S. O. Ajakwe, V. U. Ihekoronye, D.-S. Kim, and J. M. Lee, "Dronet: Multi-tasking framework for real-time industrial facility aerial surveillance and safety," *Drones*, vol. 6, no. 2, 2022.

[5] "Scenario-Based drone detection and identification system for Real-Time industrial facility aerial surveillance and safety," in *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, S. Okechukwu Ajakwe, V. U. Ihekoronye, D.-S. Kim, J. M. Lee, and , Eds. .

[6] S. Ajakwe, R. Arkter, D. Kim, D. Kim, and J. Lee, "Lightweight cnn model for detection of unauthorized uav in military reconnaissance operations," in *2021 Korean Institute of Communication and Sciences Fall Conference*, vol. 11, 2021.

[7] U. Izuazu, S. Ajakwe, C. Nwakanma, D.-S. Kim, and J. M. Lee, "Rf-based drone detection using ai models: Results, trends, and open issues," 11 2022.

[8] S. Ajakwe, M. Dini, D.-S. Kim, J. M. Lee, and T. Jun, "Droneilliance and detection dynamics: A review of radar techniques and trends," 11 2022.