S. Susmitha, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Advanced Security Monitoring System Using LoRa/LoRaWAN by Raspberry Pi

S. Susmitha[1], V. Hema Sri Durga[2], K. Sandeep[3], M. Bulliraju[4], T. Sunil Abhishek [5], R.L.R. Lokesh Babu[6],

Undergraduate Student [1,2,3,4,5], Asst. Professor [6], Dept. of ECE, Sri Vasavi Engineering College (A), Tadepalligudem [1,2,3,4,5,6]

Abstract- A comprehensive approach is developed for the design and implementation of a solar-powered, Raspberry Pi-based edge processing perimeter alert system capable of detecting unmanned aerial vehicles (UAVs) and enhancing security monitoring. This system is intended to protect key areas such as borders, private property, and critical buildings. The setup uses a Raspberry Pi equipped with Artificial Intelligence (AI) to recognize drones and helicopter sounds. Including PIR motion sensors, microwave radar, and microphone are integrated to detect movement and changes in the monitored area. For long-distance communication, the system employs LoRa/LoRaWAN technology, which operates with very low power, supports long-ranges, and can transmit signals over few meters. The entire unit runs on a solar-charged battery, enabling operation in remote locations without access to electricity. This makes system eco-friendly and suitable for continuous 24/7 security monitoring. Field testing under controlled conditions demonstrates high reliability and precision in UAV detection, validating the feasibility of combining edge AI processing, renewable energy, and low-power communication technologies for decentralized security applications. This architecture provides a scalable, energy-efficient, and environmentally sustainable solution for aerial threat detection and prevention of unauthorized access.

Keywords — Raspberry Pi, solar power, edge computing, LoRa, LoRaWAN, UAV detection, perimeter security, AI-based monitoring.

I. INTRODUCTION

The increasing availability and low cost of unmanned aerial vehicles (UAVs), commonly known as drones, have led to their widespread use across civilian and commercial applications. However, this rapid growth has also introduced serious security concerns, as drones can be misused for unauthorized surveillance, privacy invasion, smuggling, and threats to public safety and critical infrastructure[5],[6]. Existing drone detection methods such as camera-based surveillance, radar systems, and radio-frequency (RF) signal monitoring are widely used, but each of these approaches has important limitations [1]. Vision-based systems are strongly affected by lighting conditions, weather, and line-of-sight constraints, while radar-based solutions are costly, energy-intensive, and difficult to deploy in remote environments. RF-based detection fails when drones operate autonomously without active communication links. Moreover, many current solutions rely on continuous internet connectivity and centralized cloud processing, which limits their applicability in rural and isolated locations. To address these challenges, this work proposes an advanced, internet-independent drone detection and security monitoring system that combines edge computing, acoustic sensing, and long-range wireless communication. The system employs a Raspberry Pi for local signal processing, enabling real-time decision-making at the deployment site.

Drone detection is primarily achieved using an I2S MEMS microphone that captures the characteristic acoustic signatures of drone propellers, supported by microwave radar and PIR sensors to improve detection reliability. Alert information is transmitted over long distances using low-power LoRa communication, making the system suitable for large-area monitoring with minimal energy consumption [10]. By integrating edge intelligence, multi-sensor validation, and sustainable power sources such as batteries and solar panels, the proposed system offers a scalable, cost-effective, and practical solution for drone detection in remote and public environments where conventional methods are ineffective [9].

II. LITERATURE SURVEY

Recent advancements in UAV detection systems focus on enhancing security against unauthorized drone activities using techniques such as acoustic sensing, RF analysis, and radar detection [1]. Hybrid approaches combining RF and acoustic features with deep learning models improve detection accuracy but require high computational resources [1]. Acoustic-based drone identification using sound signatures is effective but sensitive to environmental noise conditions [8]. Deep learning techniques, particularly 1D CNNs, are suitable for time-series and audio signal processing in real-time applications [2]. Acoustic analysis methods have also been used for aerial object detection, though performance may degrade due to background noise [3]. Environmental studies highlight the impact of UAV noise, emphasizing the need for robust detection systems [4]. Security risks such as surveillance and attacks on critical infrastructure further increase the importance of UAV monitoring [5]. Comprehensive reviews stress the need for scalable and efficient drone detection and countermeasure systems [6]. IoT-based smart monitoring solutions enable collaborative and intelligent UAV detection frameworks [9]. Additionally, LPWAN technologies like LoRa provide low-power, long-range communication suitable for remote monitoring applications [10].

III. PROPOSED METHODOLOGY

Raspberry Pi Pico2 Hardware Description: The Raspberry Pi Pico 2 is a compact and efficient microcontroller board built on the RP2350 dual-core Arm Cortex-M33 processor, operating up to 150 MHz. It has 520 KB of SRAM and 4 MB of flash memory, providing enough performance for real-time processing and lightweight AI tasks [2] .

In this project, it acts as the main controller, collecting data from sensors, processing signals, running DL algorithms, and sending alerts through the LoRa module. It supports multiple interfaces such as UART, ADC, and I2S, allowing easy connection with the MEMS microphone, PIR sensor, and radar module. The Pico 2 operates at 3.3V and includes low-power modes, making it suitable for solar-powered security systems. Its combination of high performance, low power use, and flexibility makes it ideal for intelligent and long-range monitoring applications.

Figure1: raspberry pi pico2 Pinout diagram

Blynk Cloud: Blynk is an IoT cloud platform, it is used to provide the remote access and instant updates for the drone detection and security monitoring system [9].

Real-Time Monitoring and Data Logging: Blynk provides instant live updates of drone detection status on mobile dashboard and it records the detection events and system activity for future analysis and performance evaluation.

Remote Access: Users can monitor the security system from anywhere without being physically present at the monitoring system.

Secure Authentication: Blynk uses unique Auth Tokens to ensure secure and authorized device access.

Push Notifications: Instant alerts are sent to the users mobile when a drone is detected.

Dashboard Visualization: Blynk dashboard provide the indicators such as LED widgets, status displays and event logs for monitoring system.

Figure2: Cloud Platform

MEMS Microphone: A MEMS (Micro-Electro-Mechanical Systems) microphone is a compact and energy-efficient microphone that integrates a tiny mechanical sensing element and signal processing circuitry on a single silicon chip. MEMS microphone is used to capture the acoustic signatures of drone. The microphone converts sound waves into electrical signals, which are then digitized internally using a built-in Analog-to-Digital Converter (ADC) [3],[8]. The digital audio data is transmitted to the microcontroller raspberry pi pico2 through the I2S interface, ensuring clear, low-noise, and high-quality sound capture.

Figure3: MEMS Microphone

Microwave Radar Sensor: The HLK-LD2420 is a 24 GHz millimeter-wave radar sensor used for motion detection. It operates using Frequency Modulated Continuous Wave technology to detect both moving and stationary objects with high accuracy [1]. HLK-LD2420 can detect human presence, micro-movements, and object motion even in complete darkness. The sensor typically operates at 3.3V–5V and communicates via UART interface, making it easy to integrate with microcontrollers like the Raspberry Pi Pico 2. The HLK-LD2420 radar sensor enhances system reliability by providing secondary motion confirmation alongside acoustic detection, thereby reducing false alarms and improving overall drone detection accuracy. It offers higher sensitivity and better environmental adaptability.

Figure4: Microwave Radar

PIR Sensor: The Passive Infrared Sensor is a motion detection device that detects changes in infrared radiation emitted by living beings such as humans and animals. It typically operates at 3.3V–5V and provides a simple HIGH/LOW output, making it easy to interface with microcontrollers like the Raspberry Pi Pico 2. While the primary detection of drones is achieved through acoustic sensing (MEMS microphone) and radar validation (HLK-LD2420), the PIR sensor provides additional motion confirmation by detecting infrared radiation changes caused by moving objects within its range. When motion is detected, the PIR sensor sends a digital signal to the Raspberry Pi Pico 2.

The system then correlates this input with radar and acoustic data before generating an alert, which can reduce false alarms and increase the accuracy.

Figure5: PIR Sensor

LORA MODULES (RA-02): LoRa is a low-power, long-distance wireless communication technology designed for Internet of Things applications [10]. It uses a special modulation technique called Chirp Spread Spectrum (CSS), which allows reliable data transmission over long distances with very low power. LoRa operates in ISM frequency bands (such as 433 MHz, 868 MHz, and 915 MHz depending on the country).

RA-02 transmitts up to the 10kms in open environments and 15kms by using the helical antenna. When the Raspberry Pi Pico 2 confirms drone presence using acoustic and sensor validation, it sends an alert message to the LoRa transmitter module. The transmitter wirelessly sends this data over long distances without dependence on Wi-Fi or cellular networks. The LoRa receiver, placed at the monitoring station, captures the transmitted signal, processes it by using esp8266 and forwards it for display on lcd for further action [9],[10].

Figure6: LORA Module

Solar Panel: The solar panel serves the sustainable power source for the drone detection and security monitoring system. Since the system is designed for remote and outdoor environments where continuous electrical supply may not be available, the solar panel provides renewable energy to charge the battery and power the Raspberry Pi Pico 2, sensors, and LoRa module. The system becomes energy-efficient, cost-effective, and suitable for long-term deployment in off-grid locations such as border areas, agricultural fields, industrial perimeters, and rural infrastructure sites.

Figure7: Solar Panel

ESP8266 Hardware Description: ESP8266 is a low-cost Wi-Fi microcontroller module used for IoT applications. It features a 32-bit processor running at 80 MHz, built-in Wi-Fi. It operates at 3.3V and provides multiple GPIO pins supporting UART, I2C and ADC interfaces. It process the received signal from the lora receiver module and gives the output. ESP8266 is used to provide optional Wi-Fi communication and cloud connectivity (Blynk) for remote monitoring when internet access is available.

Figure8: ESP8266 Pinout diagram

LCD: The LCD (Liquid Crystal Display) is an output display device used to visually show system information in text format. It typically operates at 5V. The LCD displays status messages such as Drone Detected, No Drone Activity after signal get processed. The LCD helps us to easily monitor the system locally without needing a phone or computer.

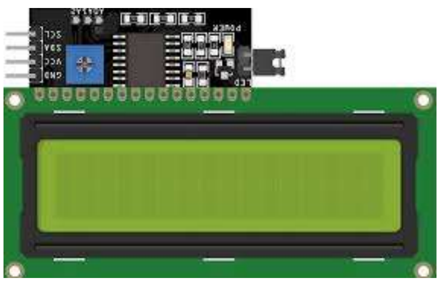


Figure9: LCD Display

LED and Buzzer: The led and buzzer are used to know the status of the drone detection at the receiving station. If the drone is detected the led will blink and the buzzer will buzz or produce the beep sound. If the drone was not detected, no action takes places.

Figure10: LED

Figure11: Buzzer

Connecting Esp8266 To Blynk Cloud For Remote Drone Monitoring

Blynk Platform Setup:
Create Blynk Account: First, create an account in the Blynk IoT platform. This acts as the cloud interface for remote monitoring.

Create a New Template: Set up a new device template for the drone detection system. Blynk generated an Auth Token, which is required for secure communication between the ESP8266 and the Blynk cloud.

Designing Dashboard: Design the dashboard by adding the widgets such as led indicator, buzzer, Event log, status display. These will shows the real time drone detection updates.

ESP8266 Setup (Arduino IDE):
Board Configuration:
Install ESP8266 board support in Arduino IDE to program the hardware.

Install Blynk Library:
Install the Blynk library for ESP8266, which enables the communication between the device and the cloud.

Wi-Fi Credentials:
Enter Wi-Fi SSID, password, and Blynk Auth Token in to the code to allow the secure cloud connection.

Connection and Working Process
Wi-Fi Connection: ESP8266 connects to the available Wi-Fi network.

Cloud Authentication: Using the Auth Token, the ESP8266 securely connects and authenticates with the Blynk cloud server.

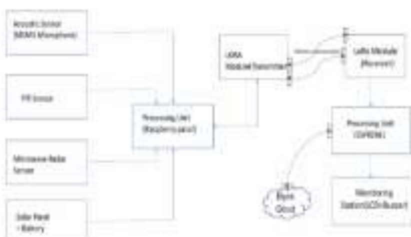
Data Reception and Cloud Update: When the LoRa receiver receives a drone detection alert, the ESP8266 processes and sends the detection status to the cloud.

User Notification: Blynk application instantly updates the dashboard and sends the push notifications.

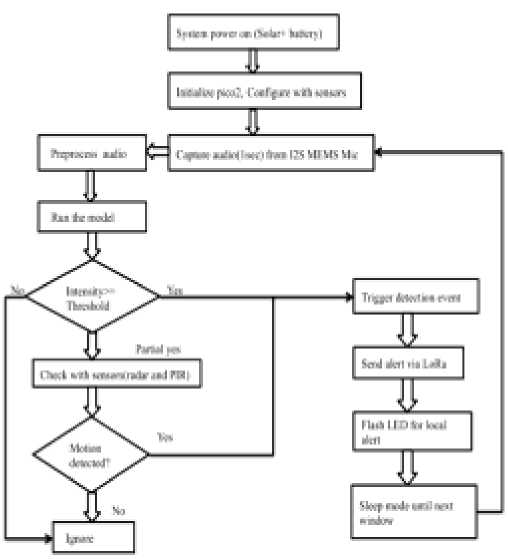
Figure: Device Creation

Figure: At the receiver side

IV. BLOCK DIAGRAM



V. FLOWCHART



Integration of DL to the model:

Data Collection:

Current dataset (used to train drone_final_project_inferencing) consists of:

Classes: 2

Drone: Speaker-playback of drone sounds (from ~5 drone models)

Noise: Real environment recordings (home/quiet backgrounds)

Recordings:

Drone audio: ~5 minutes total (5 models, played through speaker)

Noise: ~6 minutes total (background noise, likely home environment)

Processing:

Window: 1 second slices

Stride: 250 ms overlap (for continuous inference)

Sample rate: 16 kHz

Features: MFCC/MFE (Mel Filter Bank Energy)

Total samples after slicing:

~1,000–2,000 windows (exact depends on overlap and exact recording lengths)

Send data to the cloud: The collected sensor and acoustic data is temporarily buffered in ESP8266 and transmitted via MQTT/HTTP over Wi-Fi to the Blynk cloud, enabling real-time monitoring and instant remote alerts.

Data Preprocessing: The collected acoustic data is processed using the Edge Impulse platform, where Digital Signal Processing techniques are applied before model training. Mel-filterbank energy extraction is used to convert raw audio signals in to the Mel spectrogram features, capturing the frequency characteristics of drone sounds. The audio is segmented into the short frames, transformed using the FFT, to reduce the background noise. These processed Mel features are used as input to the CNN model for accurate results.

Model Selection: The 1D Convolutional Neural Network is used to automatically learn the acoustic patterns from the Mel-filtered features without requiring manual inputs. It highly suitable for real-time processing on embedded and edge devices.

Model Training: Training is the process of enabling the 1D-CNN model to learn and recognize drone sounds from Mel-filtered acoustic features. During this phase, the network is provided with labelled audio samples and repeatedly analyses them to identify distinguishing patterns. With each training cycle, the model adjusts its internal parameters (weights) to reduce prediction errors and minimize loss. Over multiple iterations, the network progressively improves its learning capability. As a result, the trained model becomes capable of performing accurate and reliable real-time drone sound classification.

Deployment: The trained model is converted to Arduino C format, suitable for deployment on the ESP8266 microcontroller. It allows the device to perform real time monitoring without relying on the internet.

Monitoring and Alerts: Once the model deployed, the model processes the data and gives the results.

- Visual LED and Buzzer are activated at the receiving station.
- Alerts are sent to the mobile dashboard through SMS.
- Advantages of this work:
- It consumes low power and transmits signals to long distances.
- It reduces the false alarms.
- It works in remote areas even though unavailability of internet.

Results: The accuracy of the real-time system,

VI. CONCLUSION

This project presents an intelligent drone detection and security monitoring system using acoustic sensing, 1D CNN based edge AI, and LoRa communication. The system enables real-time drone detection and transmits alerts through LoRa while providing remote monitoring using the Blynk platform. The proposed approach offers a cost effective, scalable, and efficient solution for security monitoring in restricted and remote areas.

REFERENCES

1. Frid, A.; Ben-Shimol, Y.; Manor, E.; Greenberg, S., “Drones Detection Using a Fusion of RF and Acoustic Features and Deep Neural Networks,” Sensors, vol. 24, 2024, 2427.
2. Cacciari, I.; Ranfagni, A., “Hands-On Fundamentals of 1D Convolutional Neural Networks—A Tutorial for Beginner Users,” Applied Sciences, vol. 14, 2024, 8500.
3. Yu, L.; Yu, L.; Wang, R.; Wei, C.; Xu, K.; Wang, R., “Passive Sound Detection of the Helicopter in the Far-Field with a Spectral Coherence Decomposition Method,” Mechanical Systems and Signal Processing,vol.185,2023,109754.
4. Škultéty, F.; Bujna, E.; Janovec, M.; Kandera, B., “Noise Impact Assessment of UAS Operation in Urbanised Areas: Field Measurements and a Simulation,” Drones, vol. 7, 2023,314.
5. Adnan, W.H.; Khamis, M.F., “Drone Use in Military and Civilian Application: Risk to National Security,” Journal of Media and Information Warfare, vol. 15, 2022, 60–70.
6. Chamola, V.; Kotesh, P.; Agarwal, A.; Naren; Gupta, N.; Guizani, M., “A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques,” Ad Hoc Networks, vol. 111, 2021, 102324.
7. Gupta, A.; Afrin, T.; Scully, E.; Yodo, N., “Advances of UAVs toward Future Transportation: The State-of-the-Art, Challenges, and Opportunities,” Future Transportation, vol. 1, 2021, 326–350.
8. Kolamunna, H.; Dahanayaka, T.; Li, J.; Seneviratne, S.; Thilakaratne, K.; Zomaya, A.Y.; Seneviratne, A., “DronePrint: Acoustic Signatures for Open-set Drone Detection and Identification with Online Data,” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol.5,20.
9. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Almalki, F.A., “Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities,” IEEE Access, 2021.
10. Raza, U.; Kulkarni, P.; Sooriyabandara, M., “Low Power Wide Area Networks: An Overview,” IEEE Communications Surveys & Tutorials, 2017.