IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153118

An IoT-Driven Intrusion Detection and Autonomous UAV Surveillance System with Edge-AI Verification

Blessan B Kuriakose[1], Aswin Prakash[2], Krishnajith K S[3], Githu Manoj[4], Parvathy R Nair[5]

Student, Electrical and Computer Engineering, College of Engineering Kidangoor, Kottayam, India[1-5]

Assistant Professor, Electrical and Computer Engineering, College of Engineering Kidangoor, Kottayam, India[6]

Abstract: Traditional home and commercial security systems relying solely on static CCTV cameras are highly vulnerable to physical tampering, often resulting in critical surveillance blind spots during targeted intrusions. Furthermore, conventional alarms suffer from high false-positive rates, leading to alarm fatigue. This paper proposes a robust, Internet of Things (IoT) driven, multi-layered security framework designed to provide uninterrupted monitoring through autonomous robotic response. At the core of the architecture, a localized edge-computing Ground Control Station (Laptop GCS) processes real-time video feeds, executing deep-learning algorithms for facial recognition and continuous pixel-variance analysis to mathematically detect sudden camera blackouts. In the event of a compromised camera, the system initiates a distributed, dual-tier response mechanism. Bypassing vulnerable local networks, the GCS publishes a low-latency execution payload to a secure HiveMQ Cloud MQTT broker. An Unmanned Aerial Vehicle (UAV), equipped with an onboard Raspberry Pi 5 companion computer and a Pixhawk flight controller, intercepts this payload, activates onboard hardware deterrents, and launches into an autonomous waypoint patrol, restoring visual oversight via a 5.8GHz analog video transmitter. Crucially, the system employs a secondary artificial intelligence verification loop; the GCS scans the incoming aerial feed for human silhouettes. Using adaptive decision-making, the system routes a high-priority alert and live video stream to a custom Flutter mobile application only upon visually confirming a human threat. Experimental results demonstrate a visual feed restoration time of under 14 seconds and near-zero false positives, providing a cost-effective, intelligent framework for next-generation smart security systems.

Keywords: Intrusion detection, Autonomous UAV, Edge Computing, MQTT, HOG algorithm, False-alarm mitigation, Smart home security.

I. INTRODUCTION

Accidents, burglaries, and targeted intrusions in residential and commercial buildings pose a severe threat to human life and property. Traditional methods of securing premises predominantly rely on static CCTV cameras and passive alarm units. While effective at deterring casual trespassers, these conventional systems possess a critical vulnerability: a stationary and highly predictable Field of View (FoV). Once an intruder maps the camera locations, the system becomes highly susceptible to physical sabotage, such as lens masking, wire-cutting, or spray painting.

When a camera experiences a blackout, the security system is essentially blinded, creating a severe surveillance gap precisely when situational awareness is most critical. Furthermore, conventional alarm systems lack intelligent decision-making; a camera blinded by a fallen tree branch triggers the exact same panic response as a camera destroyed by a burglar, resulting in high false-positive rates and subsequent alarm fatigue for homeowners and local law enforcement.

Recent advancements in the Internet of Things (IoT), Edge Computing, and Unmanned Aerial Vehicles (UAVs) have provided unprecedented opportunities to revolutionize physical security. In this context, this paper proposes an active, self-healing intrusion detection and aerial verification system referred to as "ActiveShield." Unlike traditional systems, ActiveShield integrates heavy edge-computing on the ground with an intelligent onboard companion computer (Raspberry Pi 5) mounted on a custom quadcopter. The system detects sabotage in real-time, autonomously deploys the UAV to the compromised sector, and utilizes a secondary AI computer-vision loop to visually verify the presence of a human threat before alerting the user via a mobile application.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026
DOI: 10.17148/IJARCCE.2026.153118

II. RELATED WORKS

A. IoT-Based Security Systems The application of IoT in home security has been extensively studied to facilitate remote monitoring. Early systems employ distributed IoT sensor networks (PIR sensors, magnetic door contacts) to monitor perimeter breaches. While these systems provide instant push notifications, they lack dynamic visual verification. If a sensor is tripped in a blind spot, the user receives an alert but no actionable visual data to assess the threat level.

B. AI-Based Intrusion Detection Significant improvements have been made in Artificial Intelligence, particularly in computer vision. Edge-computing models utilizing Convolutional Neural Networks (CNNs) and Histogram of Oriented Gradients (HOG) are commonly used to detect human patterns in video feeds. While highly accurate, most AI-based camera systems are designed to work independently as static nodes. If the node is physically destroyed, the AI is rendered offline, offering no secondary backup or evacuation of the data..

C. Autonomous UAVs in Surveillance
UAVs have been heavily researched for disaster management and border patrol. Various optimization algorithms have been applied to drone path-planning for emergency response. However, commercial drone security solutions are often cost-prohibitive, rely on heavy, proprietary ground stations, and generally require a human-in-the-loop to pilot the drone to the point of interest after an alarm is triggered, introducing massive latency.

D. Cloud-Edge Integrated Architectures
The integration of Cloud MQTT brokers with edge devices has resulted in the development of highly scalable smart-city systems. Some studies have proposed triggering drones via cloud networks; however, these systems often rely on cellular GSM modules that introduce 5-to-8 second dialing delays, or they lack the onboard companion computing required to make split-second hardware relay decisions (like activating sirens) during flight.

E. Comparative Analysis
From the existing literature, it is evident that IoT alarms lack dynamic visual backup, AI cameras are vulnerable to physical blinding, and UAV systems lack automated, localized trigger integration. Furthermore, almost no existing systems address the issue of false-alarm mitigation during hardware failure. The proposed ActiveShield system addresses these challenges by incorporating real-time mathematical sabotage detection, global MQTT IoT triggering, autonomous MAVLink flight generation, and a secondary mobile-verified AI loop within a single unified framework.

III. PROPOSED SYSTEM

The proposed system provides an intelligent, AI-driven active response to physical security breaches. It combines edge-based computer vision, global IoT communication, and autonomous robotics.

Stationary CCTV cameras continuously monitor the perimeter of a building. A centralized Laptop Ground Control Station (GCS) processes these video streams using highly optimized Python scripts, tracking authorized faces and monitoring structural pixel integrity. If an intruder attempts to blind the system, the GCS mathematically detects the camera blackout. Instead of triggering an immediate local siren, the GCS publishes an encrypted payload to a HiveMQ Cloud MQTT broker. An autonomous quadcopter, resting on a designated launchpad and equipped with a Raspberry Pi 5 companion computer, receives this signal. At that instant, the Pi activates an onboard GPIO relay to trigger physical deterrents (high-intensity lights) and commands the Pixhawk flight controller to launch.

The UAV navigates to the compromised zone and streams an analog aerial video feed back to the GCS via a 5.8GHz transmission link. The GCS subjects this new aerial feed to a secondary HOG human-detection algorithm. This dual-tier approach helps confirm real intrusions and prevents false detections caused by environmental camera blockages. Finally, the GCS routes the safest decision to the homeowner's Flutter mobile application, sending a high-priority alarm and live video stream only if a human is verified.

IV. SYSTEM ARCHITECTURE

The architecture of ActiveShield is designed for highly distributed processing, ensuring low-latency responses without overloading any single hardware node. The system consists of four primary layers:

1. **Input Layer (Sensory Node):** Consists of the stationary CCTV cameras streaming RTSP video to the central processor, and a 5.8GHz OTG Video Receiver waiting to capture aerial backup feeds.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026
DOI: 10.17148/IJARCCE.2026.153118

2. **Central Processing and Decision Engine Layer (GCS):** A standard Laptop acts as the heavy edge-computing hub. It runs OpenCV and face_recognition models to analyze the input layer. It is responsible for biometric matching (using a 128-dimension encoding array with a strict 0.45 tolerance) and computing mean frame brightness to detect sabotage.
3. **Agent Controller Layer (UAV Payload):** Consists of the Raspberry Pi 5 companion computer, the Pixhawk 2.4.5 flight controller, a 5V GPIO relay, and a 600mW 5.8GHz VTX. The Pi handles the translation of cloud MQTT payloads into localized MAVLink flight commands.
4. **Output Layer (Mobile Application):** A custom mobile application developed using the Flutter framework (Dart). It subscribes to a local Mosquitto MQTT broker (Port 1883) to receive real-time JSON telemetry (altitude, armed status, flight mode) and the multipart JPEG live video feed, providing the user with an intuitive command dashboard.

V. METHODOLOGY

A. AI-Based Sabotage Detection

The initial stage is passive monitoring. The Laptop GCS continuously converts the incoming CCTV feed to grayscale to compute the mean pixel intensity (μ). To filter out transient events like a bird flying past the lens, a debounce algorithm is utilized. If μ drops below a critical threshold of 50 for 20 consecutive frames (approximately 0.66 seconds at 30 FPS), the system definitively validates a "Blackout" event.

B. Alert and UAV Activation

Upon validating the blackout, the GCS transitions from passive to active mode. It opens a secure TLS connection to the HiveMQ Cloud broker (Port 8883) and publishes an "autostart" payload. The onboard Raspberry Pi receives this payload and immediately sets GPIO Pin 17 to HIGH, activating the drone's external hardware deterrent. Simultaneously, it sends the vehicle.armed = True and simple_takeoff(3.0) MAVLink commands directly to the Pixhawk.

C. Autonomous Aerial Monitoring

Once the drone reaches its target altitude, it switches to AUTO mode, executing a pre-loaded waypoint mission towards the blinded camera. During flight, its analog FPV camera feeds raw video directly to the 600mW VTX. On the ground, the Laptop GCS dynamically releases the dead RTSP stream and captures the \dev\video1 USB port connected to the 5.8GHz OTG receiver, instantly restoring visual oversight of the property.

D. Decision Making (Secondary Verification)

The system enters its secondary AI phase. The Laptop GCS subjects the newly acquired aerial feed to a cv2.HOGDescriptor specifically tuned for full-body human detection. If a human silhouette is detected near the compromised sector, the system flags the intrusion as "Verified." If the drone patrols the area and detects no human presence, the blackout is categorized as an environmental anomaly (e.g., a power failure or severe weather).

E. App Alerting and Guidance

Based on the secondary verification, the GCS communicates with the user via the local Mosquitto broker. If verified, an alarm_active: true JSON payload is published. The Flutter application instantly overrides the user's phone silencer, sounds an intrusion alarm, and displays the live aerial feed, allowing the user to immediately dispatch law enforcement. If no human is detected, the alarm is suppressed, a silent log is generated, and the drone automatically executes a Return to Launch (RTL) command to conserve battery.

VI. RESULT AND DISCUSSION

The proposed system was implemented and tested under various real-world and simulated intrusion scenarios to assess its effectiveness in edge processing, cloud communication latency, and false-positive mitigation.

A. Latency and Response Time

The response time of the system was measured across its distributed network. Unlike traditional GSM-based systems that introduce up to 8 seconds of dialing delay, the integration of HiveMQ Cloud MQTT demonstrated an average payload delivery time of 150 to 250 milliseconds.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153118

Event / Processing Stage	Measured Latency
Mathematical Blackout Detection (20 Frames)	~0.66 s
GCS Software Detection to HiveMQ Cloud Publish	0.15 s
Raspberry Pi Reception to GPIO Relay Activation	0.10 s
MAVLink Arming Command Received by Onboard Pixhawk	0.20 s
UAV Takeoff to Target Hover (10m distance)	~12.0 s
Total Time to Restore Visual Feed on App	**< 14.0 s**

From Table I, it is clear that the software detection of a blackout occurs in ~0.66 seconds. The entire sequence—from physical sabotage, cloud triggering, drone spool-up, and flight—results in a total visual feed restoration time of less than 14 seconds on the mobile application. This represents a massive improvement over traditional human-dispatched drone systems.

B. AI Accuracy and Mitigation

The vision module was tested against varying environmental conditions. By skipping heavy facial recognition (processing 1 in every 15 frames) and prioritizing the HOG human-detector on the aerial feed, the Laptop GCS maintained stable CPU loads without thermal throttling.

Tolerance Level	True Positive	False Positive	Security Assessment
0.60 (Library Default)	98%	12%	High risk of unauthorized bypass
0.45 (ActiveShield)	**92%**	**<1%**	**Strict security, optimal balance**
0.35	70%	0%	Too strict, high false rejection

The experimental results demonstrate that the system possesses exceptional logic routing. In tests where the camera was manually covered with a cloth but no human stood in the patrol zone, the secondary verification successfully suppressed the Flutter app alarm 100% of the time, executing an automatic RTL. This dual-tier verification definitively solves the industry-wide issue of smart-home alarm fatigue.

Test Scenario	Secondary Vision Result (Aerial)	Final System Action
CCTV Lens Covered (Intruder Present)	HOG Positive (Human Detected)	UAV Deployed, Mobile Alarm Triggered.
CCTV Lens Covered (No Human Present)	HOG Negative (No Human)	UAV Deployed, Alarm Suppressed, RTL Executed.
Authorized Resident walks past CCTV	Face Recognized (0.45 Tolerance)	Passive Monitoring Continued.

VII. FUTURE SCOPE

While the current architecture provides a highly robust, self-healing security net, it lays the groundwork for advanced commercial scalability:

1. **Thermal Vision Integration:** Upgrading the analog aerial camera to a FLIR (Forward Looking Infrared) payload would allow the UAV to detect human heat signatures in pitch-black environments or dense foliage, providing 24/7 tactical monitoring.
2. **Automated Precision Charging:** For complete, zero-touch autonomy, a wireless inductive charging launchpad utilizing ArduCopter IR beacons could be integrated, allowing the drone to land, recharge, and hold standby indefinitely.
3. **Smart Home Ecosystems:** Because the Mosquitto MQTT backend is the industry standard for home automation, the blackout triggers could be linked to existing hubs (like Home Assistant) to automatically lock digital doors and activate perimeter floodlights during an aerial deployment.

VIII. CONCLUSION

This project successfully shifts the paradigm of property security from passive observation to active, self-healing robotic deterrence. By bridging heavy edge computing on the ground with an intelligent onboard companion computer, the ActiveShield system completely neutralizes the blind-spot vulnerabilities of static CCTV networks. The implementation of a multi-layered MQTT architecture ensures sub-second deployment times, while the secondary aerial AI verification

DOI: 10.17148/IJARCCE.2026.153118

loop virtually eliminates false alarms. Ultimately, the integration of autonomous UAV navigation with IoT-driven threat analysis proves to be a highly effective, scalable, and cost-efficient solution for next-generation smart building security.

REFERENCES

[1]. M. N. A. Khan and S. Sharma, "Survey Paper on IoT based Intrusion Detection System: Datasets and Techniques," *2022 3rd International Conference on Computing, Analytics and Networks (ICAN)*, 2022, pp. 1-6.

[2]. V. R. S. et al., "AI and IoT based Intrusion Detection System for Cybersecurity," *2023 International Conference on Data Science and Network Security*, 2023, pp. 1-5.

[3]. A. Kumar, S. Patel, and R. Singh, "Implementation of an IoT Based Intrusion Detection System for Smart City Applications," *2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST)*, 2024, pp. 1-6.

[4]. N. F. M. et al., "AERO: AI-Enabled Remote Sensing Observation with Onboard Edge Computing in UAVs," *Remote Sensing*, vol. 15, no. 7, p. 1873, 2023..

[5]. P. N. A. R. and K. Lee, "Advanced Feature Processing for IoT-Based Intrusion Detection System," *2023 IEEE International Conference on Advanced Trends in Information Theory*, 2023, pp. 120-125.

[6]. A. Al-Shabibi et al., "EagleEYE: Aerial Edge-enabled Disaster Relief Response System," *2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-7.

[7]. Y. Li, S. Hassairi, and C. Liang, "Energy efficient strategy for uninterrupted mission execution via automatic drone replacement," *2020 IEEE International Systems Conference (SysCon)*, Montreal, QC, Canada, 2020, pp. 1-7.

[8]. M. H. Rehmani, E. Ahmed, and A. Jamalipour, "Amateur Drone Surveillance: Applications, Architectures, Enabling Technologies, and Public Safety Issues," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 66-67, April 2018.

[9]. N. K. et al., "Near-Edge Computing Aware Object Detection: A Review," *IEEE Access*, vol. 11, pp. 15243-15260, 2023.

[10]. S. J. et al., "YOLO-Powered Deep Learning Framework for Smart Drone Surveillance in Emergency Rescue Operation," *2024 IEEE International Conference on Autonomous Systems*, 2024, pp. 45-51.

