International Journal of Data Informatics and Intelligent Computing (IJDIIC)
Vol. 5, No. 3, September 2026, pp. 21~49
DOI: 10.59461/ijdiic.v5i3.298

An Integrated IoT–AI–UAV Swarm Architecture for Intelligent Autonomous Airport Security

Rexcharles Enyinna Donatus[1]
[1]Aerospace Engineering Department, Air Force Institute of Technology, Kaduna, Nigeria.

Article Info

Article history:

Received June 18, 2026
Revised August 20, 2026
Accepted August 27, 2026

Keywords:

Airport Security
Internet of Things
UAV Swarms
Edge Computing
Aviation Safety
Artificial Intelligence

ABSTRACT

Airport security faces escalating challenges from perimeter intrusions, runway incursions, wildlife hazards, unauthorized drone activity, and cyber-physical threats. Conventional surveillance systems based on closed-circuit television (CCTV), radar, and human patrols provide essential monitoring capabilities but remain constrained by fragmented situational awareness, limited mobility, delayed threat verification, and high operator workload. Addressing these limitations requires architectural integration rather than incremental upgrades to individual technologies. This review develops an evidence-based five-layer IoT–AI–UAV swarm reference architecture that integrates sensing, coordinated autonomy, edge intelligence, human-supervised decision-making, and cross-layer cybersecurity within a unified airport-security ecosystem. The proposed framework is examined through three representative airport-security use cases—perimeter intrusion detection, wildlife hazard monitoring, and rapid-response surveillance using evidence from the reviewed literature. Cross-study synthesis indicates that multi-sensor fusion is essential for reliable detection of low-slow-small targets under heterogeneous operating conditions, onboard edge intelligence is necessary for time-critical response, and hybrid swarm coordination provides the most effective balance between centralized mission optimization and decentralized resilience under degraded communications. Human supervision forms a core architectural layer, supporting alert prioritization, workload management, trust calibration, and escalation control. The study identifies five key deployment barriers—battery endurance, communication resilience, airspace regulation, AI explainability, and human factors and proposes a phased research roadmap toward field-validated and certifiable airport-security systems. The principal contribution is a unified, operationally grounded IoT–AI–UAV swarm architecture tailored to the threat environment, regulatory constraints, and human-factors requirements of modern airport security.

Corresponding Author: Rexcharles Enyinna Donatus (e-mail: rexcharles.donatus@gmail.com)

1. INTRODUCTION

Airports are among the most security-sensitive infrastructures in modern transportation systems, requiring continuous surveillance across runways, taxiways, perimeter boundaries, cargo facilities, terminal approaches, and restricted operational zones. Growing passenger volumes, expanding airport footprints, increasing low-altitude aerial threats, and the operational consequences of security failures have exposed limitations in traditional surveillance architectures [1][2]. The central challenge is no longer the availability of surveillance technologies but their ability to provide timely, integrated, and actionable situational awareness across complex airport environments [3].

Current airport surveillance relies primarily on fixed CCTV networks, radar systems, access-control infrastructure, and human patrols. Although these technologies remain indispensable, each has distinct limitations. CCTV systems generate large volumes of video data and are vulnerable to false alarms, human patrols are resource-intensive and constrained by operator workload, and radar systems struggle to identify small, slow-moving, low-altitude targets such as unauthorized drones and wildlife. Evidence from counter-

UAS research further demonstrates that no single sensing modality can provide reliable airport-wide coverage, making sensor fusion a practical necessity rather than an optional enhancement [4][5][6].

Unmanned aerial vehicles (UAVs) extend surveillance capability through mobility and rapid deployment; however, single-UAV systems remain limited by flight endurance, payload capacity, communication vulnerabilities, and single-point failure risk [7][8]. UAV swarms address these constraints by distributing sensing, computation, and response functions across multiple cooperating platforms. Comparative studies indicate that coordinated swarms provide greater coverage, fault tolerance, and mission adaptability than either single UAVs or independently operating multi-UAV systems because resources can be dynamically reallocated as operational conditions change [9][10][11].

The effectiveness of swarm-based surveillance depends on integration with supporting digital infrastructure. IoT technologies provide connectivity between airborne assets, ground sensors, edge nodes, and command systems, while AI transforms large volumes of heterogeneous sensor data into actionable intelligence through anomaly detection, target classification, adaptive mission planning, and multi-agent coordination [10]. Together, IoT, AI, and UAV swarms provide the basis for adaptive airport-security operations capable of detecting, interpreting, and responding to evolving threats in near real time.

Despite rapid advances in these fields, the literature remains fragmented. Existing airport-security studies typically focus on isolated applications such as perimeter monitoring, wildlife management, or counter-drone operations. Similarly, swarm research emphasizes coordination algorithms and communication architectures, while IoT and AI studies focus primarily on sensing or analytics[12]. Evidence from intelligent transportation systems, critical infrastructure protection, and low-altitude airspace management demonstrates the value of integrated architectures; however, airport-specific frameworks that combine IoT sensing, AI decision-making, UAV swarm coordination, and human supervision remain limited [13].

Human factors represent a second major research gap. Increased automation changes the role of security personnel from direct monitoring to supervisory control. While AI can reduce workload and improve situational awareness, poorly designed automation can generate alert fatigue, automation bias, and reduced operator trust [14][15]. Consequently, human supervision should be considered a core system requirement rather than a secondary interface consideration.

Despite substantial advances in IoT, artificial intelligence, UAV swarms, edge computing, and airport-surveillance technologies, existing research remains fragmented across these domains. Most studies focus on individual components—such as sensing technologies, swarm coordination, AI-enabled analytics, or cybersecurity without explaining how they can be integrated into a unified operational architecture for intelligent airport security. Consequently, limited guidance exists on how distributed sensing, cooperative UAV operations, intelligent decision-making, cybersecurity, and human supervision should interact to support resilient and accountable airport-security operations.

This limitation is increasingly significant as modern airports face evolving threats that demand coordinated responses across physical and cyber domains. Although advances in individual technologies have improved specific capabilities, optimizing isolated components alone is unlikely to address the broader system-level challenges of scalability, interoperability, resilience, and regulatory compliance. There is therefore a need for an integrated architectural perspective that synthesizes current knowledge into a coherent operational framework suitable for intelligent autonomous airport-security systems.

Accordingly, this review develops a unified five-layer IoT–AI–UAV swarm architecture that integrates multi-modal sensing, cooperative UAV swarm coordination, edge–cloud intelligence, human-supervised command and control, and cybersecurity resilience within a single operational framework. The review pursues four objectives: (1) to synthesize recent advances in airport-security, IoT, AI, and UAV swarm research; (2) to develop and position the proposed five-layer architecture; (3) to evaluate enabling technologies and swarm coordination paradigms for airport-security applications; and (4) to identify the principal technical, operational, regulatory, cybersecurity, and human-factor challenges that must be addressed for practical deployment.

Figure 1 presents the proposed integrated five-layer IoT–AI–UAV swarm architecture for airport security. The figure summarizes the principal architectural components and the information flow that underpin the unified operational framework discussed throughout this review.

The remainder of this paper is organized as follows. Section 2 reviews airport-security requirements and UAV swarm foundations. Section 3 examines IoT architectures and communication infrastructures. Section 4 discusses AI techniques for anomaly detection and swarm coordination. Section 5 presents the integrated architecture. Section 6 evaluates representative use cases. Section 7 discusses deployment challenges and open research issues. Section 8 presents future research directions, and Section 9 concludes the paper.

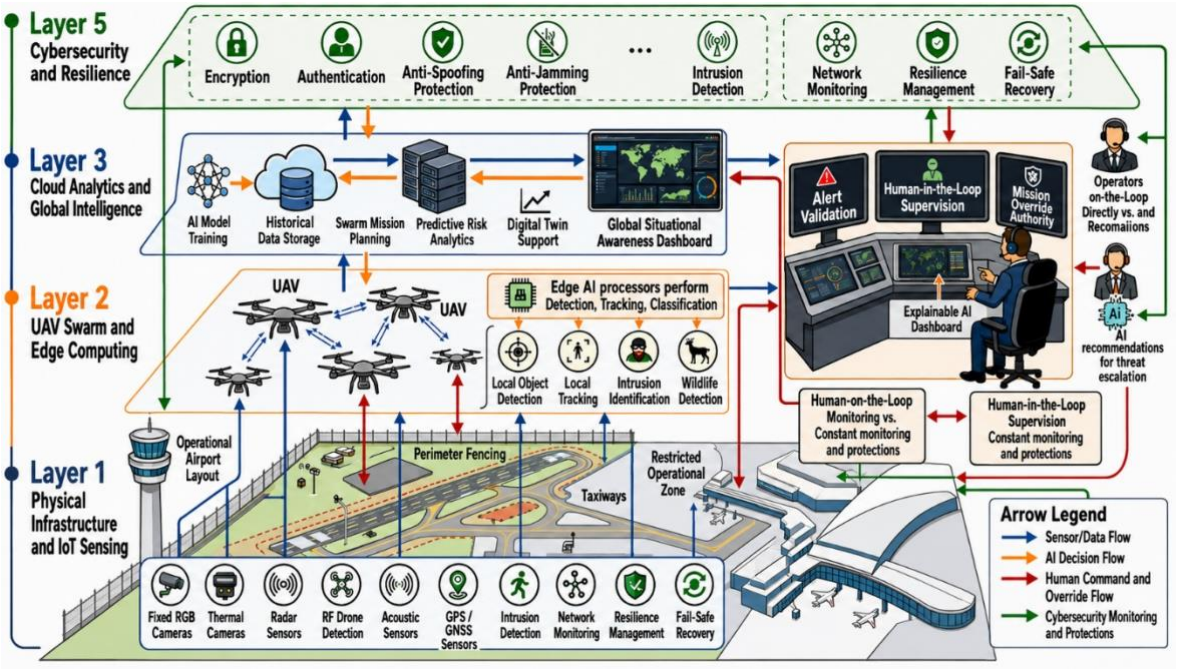

Figure 1. Integrated Five-Layer IoT-AI-UAV Swarm Architecture for Airport Security

2. AIRPORT SECURITY REQUIREMENTS AND UAV SWARM FOUNDATIONS

2.1. Airport Threat Landscape and Surveillance Requirements

Airport security environments are characterized by three operational challenges: spatial dispersion, heterogeneous threat types, and time-critical response requirements. Surveillance systems must simultaneously monitor extensive perimeter boundaries, runways, taxiways, restricted zones, cargo facilities, and terminal approaches while responding to both physical and cyber-physical threats. These requirements exceed the capabilities of any single sensing modality, making multi-modal integration essential [6][13].

Unauthorized drone activity illustrates this challenge. Small UAVs operating at low altitude possess flight characteristics that reduce radar detectability, requiring complementary Radio Frequency (RF), electro-optical, and infrared sensing for reliable identification and classification [16]. Similarly, wildlife monitoring depends on thermal, optical, and Light Detection and Ranging (LiDAR) sensing because no single sensor can provide consistent performance across varying environmental conditions [13]. Beyond physical threats, airports increasingly face cyber-physical risks including spoofing, eavesdropping, unauthorized access, and location manipulation across interconnected IoT and UAV systems [17]. Together, these threats require layered sensing, resilient communications, rapid analytics, and coordinated response mechanisms.

2.2. Limitations of Existing Surveillance Approaches

Conventional airport surveillance relies on CCTV systems, radar installations, access-control infrastructure, and human patrols. While each contributes valuable capability, none independently satisfies modern airport-security requirements.

CCTV systems provide broad visual coverage but generate large volumes of data that increase operator workload and false-alarm rates. Human patrols offer contextual judgment and intervention capability but are constrained by staffing requirements, limited coverage capacity, and delayed response across large operational areas [5]. Radar systems provide long-range detection but perform poorly against small, slow-moving, low-signature targets and therefore require complementary sensing technologies for reliable identification [6].

Single-UAV platforms partially address mobility limitations by providing aerial surveillance and rapid deployment. However, endurance constraints, payload limitations, communication vulnerabilities, and single-point failure risks restrict their suitability for persistent airport-security missions [7][8]. Comparative evidence therefore suggests that the primary challenge is architectural rather than technological: isolated surveillance assets generate fragmented situational awareness, whereas airport operations require integrated sensing, analysis, and response capabilities.

Table 1 compares the principal surveillance approaches currently used or proposed for airport-security operations. The comparison is based on six operational criteria identified throughout the literature:

coverage continuity, nighttime effectiveness, response latency, scalability, operator workload, and breadth of threat coverage. The comparison highlights the limitations of single-modality systems and the potential of integrated IoT–AI–UAV architectures to improve performance across heterogeneous airport-security scenarios.

Table 1. Comparative Performance of Existing Airport Surveillance Approaches

Surveillance Approach	Coverage Continuity	Nighttime Performance	Response Latency	Scalability	Operator Burden	Threat Coverage	Overall Assessment
Fixed CCTV Systems	Moderate	Moderate	Moderate	Low	High	Low	Effective for localized monitoring but limited by fixed viewpoints and operator workload.
Human Patrols	Low	Low	Low	Low	Very High	Moderate	Valuable for on-site verification but unsuitable for continuous wide-area surveillance.
Radar Surveillance	High	High	High	Moderate	Moderate	Moderate	Provides persistent wide-area detection but requires complementary sensors for identification and low-signature targets.
Ground Sensor Networks	High	High	High	High	Moderate	High	Improves situational awareness through distributed sensing but benefits from multi-sensor fusion.
Single UAV Platforms	Moderate	High	High	Moderate	Moderate	High	Enhances mobility and inspection capability but remains constrained by endurance and single-platform limitations.
UAV Swarms	High	High	Very High	High	Moderate	High	Enables adaptive, coordinated surveillance with improved coverage and resilience.
Proposed IoT–AI–UAV Swarm Framework	Very High	Very High	Very High	Very High	Moderate	Very High	Integrates sensing, analytics, and swarm coordination to provide the most comprehensive airport-security capability.

Key Finding: Integrated IoT–AI–UAV architectures offer the broadest operational capability by combining complementary sensing, real-time analytics, coordinated aerial mobility, and human-supervised decision-making within a unified framework.

The limitations of fixed surveillance assets and single-platform UAV deployments have motivated increasing interest in cooperative UAV swarms. By distributing sensing, communication, and response tasks across multiple aerial agents, swarm architectures offer a promising pathway toward scalable and resilient airport-security operations. Section 2.3 examines the foundations and operational advantages of UAV swarms.

2.3. UAV Swarm Foundations and Operational Advantages

UAV swarms extend surveillance capability beyond the simple multiplication of individual platforms. Their principal advantage arises from coordinated behavior, whereby multiple agents share sensing information, distribute tasks, and adapt collectively to changing operational conditions.

Compared with single-UAV deployments, swarm architectures improve coverage continuity, fault tolerance, and mission resilience because sensing and response tasks can be dynamically redistributed when individual platforms fail or return for battery replacement [11]. This capability is particularly important in airport environments where surveillance requirements span large areas, and threats can emerge simultaneously at multiple locations. Coordinated swarms also enable persistent tracking of moving targets and support parallel mission execution, capabilities that exceed the operational capacity of individual UAVs [18]. The value of swarms therefore derives not from increased platform numbers alone, but from coordination mechanisms that transform multiple UAVs into a cooperative sensing and response system.

2.4. Swarm Coordination Paradigms: Comparative Analysis

The effectiveness of swarm operations depends largely on the coordination paradigm employed. Three approaches dominate the literature: centralized, decentralized, and hybrid coordination. Centralized coordination relies on a single controller with global system awareness. This approach generally achieves superior mission optimization because task allocation decisions are based on complete operational information. However, performance degrades significantly when communication links fail or become congested, creating a potential single point of failure [9][18].

Decentralized coordination distributes decision-making among individual UAVs using local sensing and peer-to-peer communication. The resulting architecture is highly resilient to node loss and communication disruption because no single component governs overall system behavior. The trade-off is reduced global optimization, as locally efficient decisions may not produce the best system-wide outcomes [11].

Hybrid coordination combines centralized strategic planning with decentralized local execution. Under normal operating conditions, centralized oversight supports efficient resource allocation and mission planning, while decentralized behaviors preserve operational continuity when communications degrade or unexpected events occur. The reviewed literature generally identifies hybrid architectures as offering a favorable balance among optimization efficiency, scalability, resilience, and supervisory control requirements, making them particularly suitable for airport-security applications [10].

Table 2 compares the three principal UAV swarm coordination paradigms discussed in the literature: centralized, decentralized, and hybrid coordination. The comparison focuses on operational criteria most relevant to airport-security applications, including latency, scalability, resilience, mission optimization, and compatibility with human supervision. The analysis demonstrates that hybrid coordination provides the most balanced solution for airport environments, where both centralized oversight and local autonomy are required.

Key Finding: Hybrid coordination offers the most suitable balance for airport-security operations by combining centralized mission management with decentralized resilience and local autonomy.

Figure 2 summarizes the trade-offs among centralized, decentralized, and hybrid coordination approaches and illustrates the suitability of hybrid coordination for airport-security missions.

Table 3 compares centralized, decentralized, and hybrid UAV swarm coordination paradigms using operational criteria relevant to airport-security applications. The comparison focuses on latency, scalability, resilience to node loss, communication dependency, global optimization capability, and compatibility with human supervision, providing a basis for positioning the coordination approach adopted in the proposed framework

Table 2. Comparative Analysis of UAV Swarm Coordination Paradigms

Evaluation Criterion	Centralized	Decentralized	Hybrid	Airport Security Implication
Response Latency	Moderate	High	Very High	Hybrid supports rapid response while retaining mission oversight.
Robustness to Node Failure	Low	High	Very High	Hybrid maintains operations despite UAV losses.
Robustness to Communication Loss	Low	High	Very High	Local autonomy improves continuity during link degradation.
Scalability	Moderate	High	Very High	Hybrid supports large airport-wide deployments.
Global Mission Optimization	Very High	Moderate	High	Central planning remains important for strategic task allocation.
Local Adaptability	Low	Very High	High	Hybrid balances adaptation and coordination.
Fault Tolerance	Low	High	Very High	Essential for safety-critical airport missions.
Communication Overhead	Moderate	High	Moderate	Hybrid reduces unnecessary network traffic.
Computational Distribution	Low	Very High	High	Supports edge-based swarm intelligence.
Human Supervisory Compatibility	Very High	Moderate	High	Hybrid aligns with human-supervised autonomy.
Regulatory Suitability	High	Moderate	High	Better supports accountability and traceability.
Operational Complexity	Moderate	Moderate	High	Greater complexity but improved performance.
Routine Patrol Suitability	High	Moderate	Very High	Supports persistent perimeter monitoring.
Emergency Response Suitability	Moderate	High	Very High	Enables rapid retasking during incidents.
Overall Deployment Suitability	Moderate	High	Very High	Best balance of resilience, scalability, and oversight.

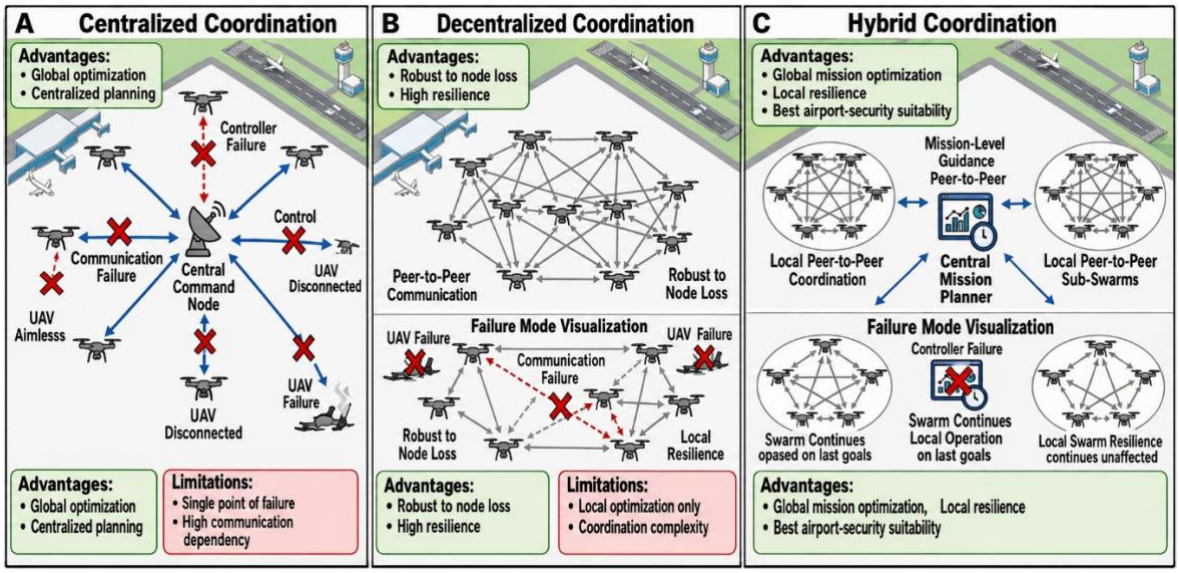

Figure 2. Comparison of UAV Swarm Coordination Paradigms for Airport Security

Table 3. Comparison of UAV Swarm Coordination Paradigms for Airport-Security Applications

Criteria	Centralized	Decentralized	Hybrid
Latency	✓	✓	✓
Scalability	✓	✓	✓
Node-Loss Robustness	✓	✗	✓
Communication Dependency	✗	✗	✓
Global Optimization	✓	✓	✓
Human Supervisory Compatibility	✓	✗	✓

2.5. Human Factors and Supervisory Control

The introduction of AI-enabled UAV swarms changes the role of airport-security personnel from direct monitoring to supervisory control. While automation can reduce workload and improve situational awareness, excessive alert volumes and poor automation design can generate alert fatigue, automation bias, and reduced trust in system outputs [5].

Two complementary supervisory models emerge from the literature. Human-on-the-loop supervision allows AI systems to perform routine detection, prioritization, and task assignment while operators monitor performance and intervene when necessary. This approach is suitable for routine patrol and surveillance operations. Human-in-the-loop supervision requires explicit human authorization before high-consequence actions are executed, including security escalation, regulatory reporting, or mission re-tasking involving operational risk [15].

Effective airport-security architectures should therefore combine both approaches through structured escalation workflows that preserve accountability while minimizing operator burden. Equally important is trust calibration, whereby operator confidence remains aligned with actual system performance through transparency, feedback mechanisms, and training [14].

2.6. Cross-Study Synthesis and Architectural Positioning

Research has advanced considerably in airport surveillance, UAV swarm coordination, edge–cloud intelligence, and cybersecurity. However, these research streams have largely evolved independently. Airport-security studies predominantly focus on threat detection and counter-UAS sensing, whereas UAV swarm research emphasizes coordination, path planning, coverage optimization, and communication efficiency. Similarly, edge–cloud intelligence studies focus on latency reduction and distributed inference, while cybersecurity research primarily addresses isolated threats such as jamming, spoofing, intrusion, and denial-of-service (DoS) attacks.

A consistent finding across these domains is that no individual technology can simultaneously satisfy the operational requirements of modern airport security, including persistent surveillance, low-latency response, scalable coordination, cyber resilience, and regulatory accountability. Fixed sensing infrastructures provide continuous monitoring but suffer from coverage limitations and restricted adaptability. UAV-based sensing improves mobility and situational awareness but remains constrained by endurance, communication reliability, and autonomy-related challenges. Consequently, recent studies increasingly advocate multimodal sensing and integrated edge–cloud processing to improve operational effectiveness.

Despite these advances, three major research gaps remain. First, most airport-security studies concentrate on sensing performance without defining how sensing outputs should be integrated with UAV operations and command decision processes. Second, existing UAV swarm frameworks rarely address airport-specific governance, operator supervision, and cybersecurity requirements. Third, current AI-enabled surveillance architectures often treat autonomy, resilience, and human oversight as separate design problems rather than interconnected components of a unified operational system.

The proposed framework responds to these limitations through a five-layer architecture that integrates IoT sensing, UAV swarm coordination, edge–cloud intelligence, cybersecurity and resilience mechanisms, and human-supervised command and control. Unlike approaches that optimize individual subsystems, the framework explicitly defines information flow, decision pathways, and operational dependencies across the five layers. It therefore provides an airport-security reference architecture that combines detection, coordination, resilience, and governance within a single operational framework. Table 4 summarizes the principal limitations identified in existing literature and the corresponding contributions of the proposed framework.

Table 4. Research Gaps in Existing Literature and Contributions of the Proposed Framework

Literature Area	Main Limitation	Proposed Framework Contribution
Airport surveillance and counter-UAS systems	Focus on sensing and detection technologies	Integrates sensing with coordinated UAV response and decision support
UAV swarm coordination	Emphasis on coverage and autonomy	Links swarm operations to airport-security workflows and governance
Edge–cloud analytics	Optimizes latency and inference performance	Provides multi-layer fusion and airport-wide situational awareness
AI-enabled IoT surveillance	Technology-centric architectures	Develops an airport-security-specific operational architecture
UAV/IoT cybersecurity	Addresses isolated attack vectors	Introduces cross-layer cybersecurity and resilience mechanisms
Existing airport-security frameworks	Limited integration across sensing, autonomy, and governance	Provides unified five-layer architecture with human supervision

To clarify the novelty of the proposed five-layer architecture, a comparative analysis was conducted against representative frameworks reported in the literature. Rather than comparing individual technologies in isolation, the comparison considers the extent to which existing approaches integrate IoT-based sensing, AI-enabled analytics, UAV or swarm capabilities, edge/cloud intelligence, human supervision, cybersecurity, and airport-specific operational requirements within a unified architecture. This comparison is important because recent studies demonstrate progress in individual components of intelligent airport security, but the literature remains fragmented across detection, surveillance, counter-UAS, cybersecurity, and operational decision-support functions. For example, recent airport-security research has proposed multimodal integration of X-ray detection, video anomaly detection, IoT sensing, and secure event logging, while other work has developed AI-enabled counter-UAS frameworks incorporating multimodal sensing, risk assessment, intervention, and human-in-the-loop decision support [19].

Table 5 therefore contrasts representative existing approaches with the proposed framework across the principal architectural dimensions. The purpose is not to claim that existing systems lack these capabilities entirely, but to identify differences in their degree of integration and airport-security orientation. The proposed five-layer architecture is distinguished by its explicit integration of IoT sensing, AI analytics, UAV swarm coordination, distributed edge/cloud intelligence, human supervision, cybersecurity, and airport-specific operational integration within a single conceptual framework.

Table 5. Comparative Analysis of Representative Airport-Security and UAV-Swarm Security Frameworks

Study	IoT Sensing	AI Analytics	UAV / Swarm Integration	Edge / Cloud Intelligence	Human Supervision	Cybersecurity	Airport-Specific Focus	Integrated Architecture
[20]	✓	✓	–	✓	✓	–	✓	Partial
[19]	✓	✓	–	–	–	✓	✓	Partial
[21]	✓	✓	✓	✓	✓	✓	✓	Partial
[22]	–	✓	✓	–	–	✓	–	Partial
[23]	–	–	✓	–	–	✓	–	Partial
Proposed	✓	✓	✓	✓	✓	✓	✓	✓

The comparison demonstrates that existing research has addressed important components of intelligent airport and UAV security, but these capabilities remain distributed across different architectural and operational contexts. Basem et al. [20], for example, integrate IoT sensing and deep learning for airport-security monitoring and intelligent resource recommendation, whereas Shobha et al. [19] combine X-ray detection, video anomaly analysis, IoT sensing, and blockchain-based logging within a multi-layer airport-security framework. Zieliński [21] extends the integration toward UAS threats in smart airports through

sensor fusion, AI-based risk assessment, and defense-in-depth mechanisms. In contrast, UAV-swarm security studies have primarily concentrated on swarm communication, cybersecurity, key agreement, and resilience rather than airport-specific security integration [22][23].

The proposed five-layer architecture builds on these developments by bringing sensing, intelligent analytics, UAV swarm coordination, distributed computing, cybersecurity, and human supervision into a unified airport-security architecture. The novelty therefore does not arise from claiming individual technologies as new; rather, it lies in their systematic integration and functional organization for autonomous airport-security operations. This distinction is important because the comparative evidence indicates that existing studies generally emphasize particular technological or operational components, whereas the proposed framework provides an integrated systems-level structure connecting these components within a common airport-security context

2.7. Positioning of the Present Study

The preceding analysis reveals a common limitation in airport-security research: although substantial progress has been achieved in sensing technologies, UAV swarm coordination, AI-enabled analytics, and cybersecurity, these capabilities are rarely integrated within a single operational architecture. Existing studies typically address specific technical challenges in isolation, leaving important questions regarding interoperability, governance, resilience, and human supervision insufficiently explored.

Accordingly, this study proposes a five-layer IoT–AI–UAV swarm framework combining multimodal sensing, coordinated aerial surveillance, distributed intelligence, cybersecurity resilience, and human-supervised decision-making within an airport-security architecture. The following section presents the proposed framework and describes the functional relationships among its constituent layers.

Figure 3 summarizes the principal research gaps identified in the literature and shows how the proposed five-layer architecture addresses them through integrated sensing, coordinated autonomy, intelligent analytics, human supervision, and cross-layer resilience. Identifies the principal limitations in current airport-security research, highlighting the fragmented treatment of sensing, UAV operations, AI, cybersecurity, and human supervision. Illustrates the proposed five-layer architecture, demonstrating how these limitations are addressed through integrated sensing, coordinated autonomy, edge–cloud intelligence, human-supervised decision-making, and cross-layer cybersecurity resilience.

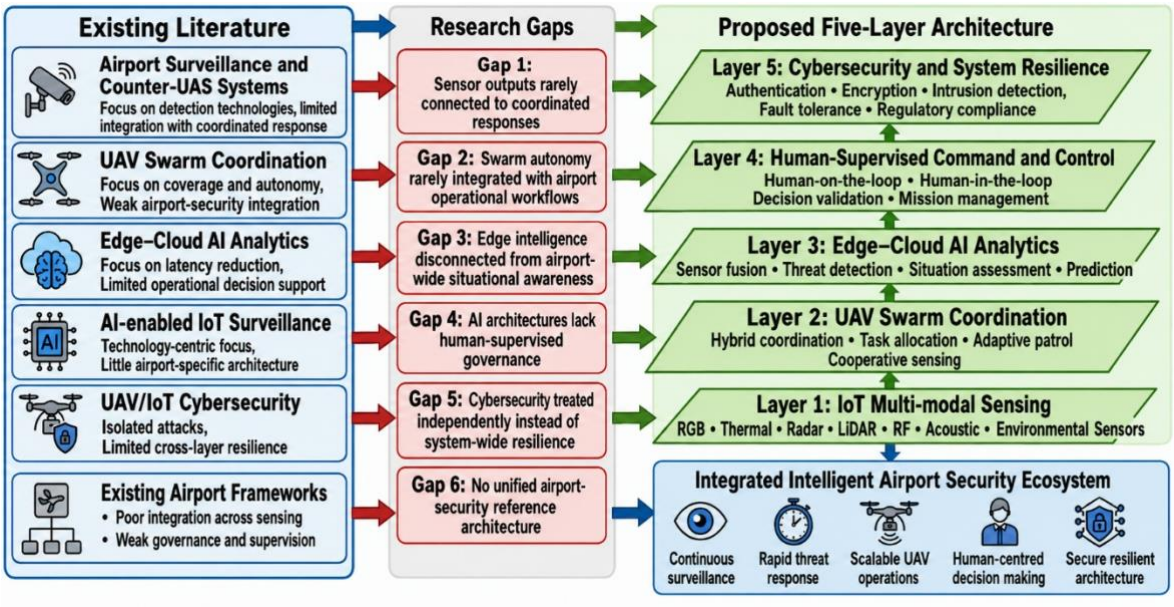

Figure 3. Research gaps identified across existing airport-security literature and the proposed five-layer IoT–AI–UAV swarm architecture developed to address them.

3. IOT SENSING ARCHITECTURE FOR AIRPORT SECURITY

3.1. Multi-Modal Sensing and Fusion Strategy

Airport-security sensing must operate under highly variable environmental conditions, including darkness, fog, precipitation, electromagnetic interference, and dynamic target behavior. Under such

conditions, individual sensing modalities tend to fail under different circumstances, making multi-modal fusion more robust than reliance on a single sensor.

Evidence from autonomous perception systems demonstrates that radar maintains environmental robustness when camera and LiDAR performance degrade in fog, while thermal sensing improves detection under low illumination and adverse weather conditions [24][25]. Although much of this evidence originates from autonomous driving and intelligent transportation systems, the underlying principle is transferable: heterogeneous sensors provide complementary information that improves detection reliability when individual modalities become unreliable[26].

For airport security, optical cameras support object detection, classification, and tracking under normal visibility conditions [27]. Thermal sensors enhance nighttime and wildlife monitoring by detecting heat signatures that are difficult to observe using visible-light imagery. Radar provides all-weather detection capability, while RF sensors improve identification of unauthorized drones with small radar cross-sections [16]. Acoustic and motion sensors offer additional ground-level intrusion detection but require careful calibration because environmental noise can increase false alarms. Global Positioning System (GPS) infrastructure supports navigation and swarm coordination but remains vulnerable to spoofing, necessitating integration with inertial navigation systems (INS) and visual odometry for resilient positioning [17].

These findings suggest that airport-security systems should not rely on any single sensor as a primary source of truth. Instead, sensing layers should be designed around cross-validation, where one modality confirms, supplements, or compensates for another under degraded operating conditions.

Most evidence supporting multi-modal sensor fusion originates from autonomous vehicle perception and intelligent transportation systems. Although these findings provide a strong technical foundation, airport-specific validation remains necessary because operational environments, threat characteristics, and performance requirements differ substantially.

Table 6 summarizes the sensing modalities commonly employed in airport-security monitoring and highlights their complementary strengths and limitations. The comparison shows that no single sensor can reliably address all airport threats and environmental conditions, supporting the use of multi-modal sensor fusion within the proposed architecture.

Table 6. Airport IoT Sensor Modalities and Their Operational Roles

Sensor Modality	Detection Capability	Environmental Robustness	Threats Addressed	Key Limitation	Recommended Role
(Red–Green–Blue) RGB Camera	High	Moderate	Intrusions, vehicles, wildlife, drones	Poor low-light performance	Visual identification and verification
Thermal Camera	High	High	Wildlife, intrusions, drones	Limited object detail	Night and adverse-weather monitoring
Radar	High	Very High	Drones, vehicles, intrusions	Limited target classification	Wide-area detection and tracking
LiDAR	High	Moderate	Intrusions, vehicles, infrastructure	Weather sensitivity	Precision localization and mapping
RF Detector	Moderate	High	Unauthorized drones	Cannot detect silent drones	Early drone detection
Acoustic Sensor	Moderate	Moderate	Drones, intrusions	Noise sensitivity	Passive cueing and warning
Motion Sensor	Moderate	Moderate	Human and vehicle intrusions	Limited classification ability	Perimeter triggering
GPS/Global Navigation Satellite System (GNSS)	Moderate	High	Cooperative assets	Vulnerable to spoofing	Navigation and fleet coordination
Environmental Sensor	Low	High	Environmental anomalies	No direct threat detection	Context-aware adaptation
Multi-Modal Fusion	Very High	Very High	All threat categories	Integration complexity	Primary airport-security sensing architecture

Key Finding: Multi-modal fusion improves detection reliability by compensating for the limitations of individual sensing modalities.

3.2. Edge–Cloud Processing Architecture

Airport-security operations impose strict latency requirements that cannot be satisfied by cloud-only processing architectures. Time-critical events such as perimeter intrusions, wildlife incursions, and unauthorized drone activity require immediate local analysis and response, whereas strategic analytics and long-term optimization can tolerate higher processing delays.

Studies consistently show that edge AI is better suited than cloud-only approaches for UAV applications because inference occurs near the sensing source, reducing communication delays and dependence on continuous network connectivity [28]. Reported implementations have achieved near-real-time performance with end-to-end latencies below three seconds and onboard processing rates exceeding 15 (Frames per Second) FPS on embedded platforms [29][30].

The proposed architecture adopts a tiered processing model. Edge nodes perform real-time detection, target tracking, anomaly identification, and preliminary classification, while cloud infrastructure supports computationally intensive tasks such as model retraining, historical analysis, mission optimization, and fleet-level coordination. This partition balances latency, bandwidth consumption, scalability, and computational efficiency.

To support low-latency airport-security operations while maintaining global situational awareness, intelligent processing must be distributed across sensing devices, edge computing platforms, and cloud infrastructure. Figure 4 illustrates the proposed tiered IoT processing architecture and the interaction among sensing, edge intelligence, cloud analytics, and supervisory control for airport-security operations.

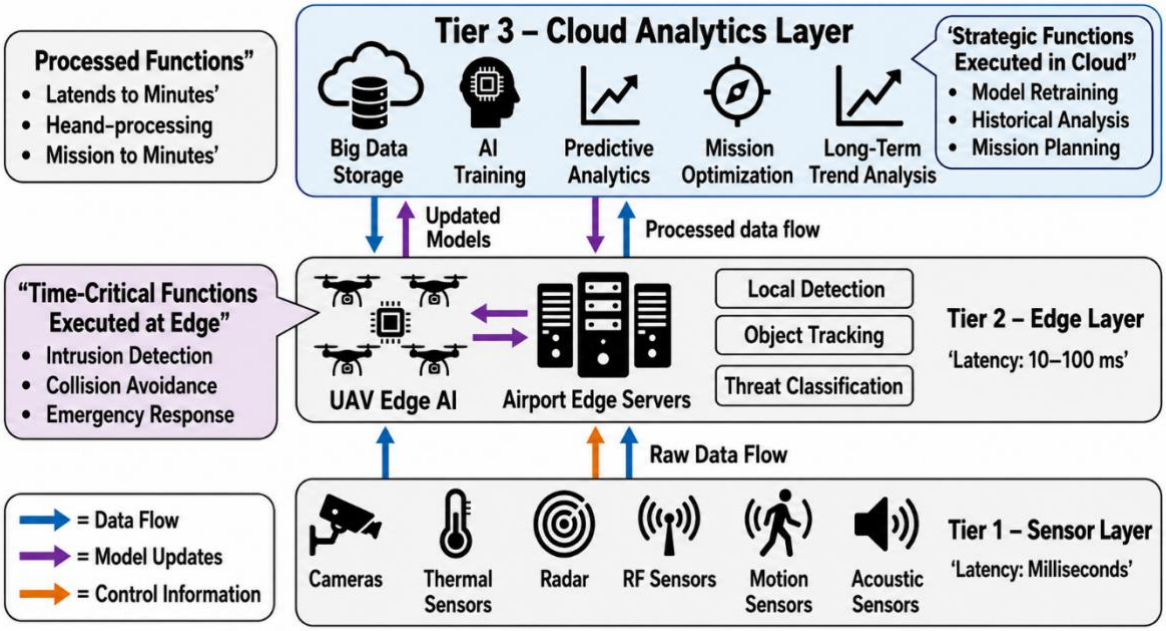

Figure 4. Tiered IoT Processing Architecture for Airport Security

3.3. Communication Infrastructure and Resilience

Communication architecture directly influences surveillance continuity, swarm coordination effectiveness, and operational resilience. No single communication technology satisfies all airport-security requirements; consequently, protocol selection should be mission-dependent.

5G networks provide low latency, high bandwidth, and support for dense IoT deployments, making them suitable for AI-intensive surveillance applications. However, their effectiveness depends on infrastructure availability and resilience against cyber-physical attacks. Long-Term Evolution (LTE)/4G networks remain valuable for broad-area connectivity and operational backhaul, whereas Wi-Fi is more appropriate for short-range local communications between UAVs and nearby infrastructure [29].

Counter-UAV research further demonstrates that command, control, positioning, and video links can all be disrupted through jamming or spoofing attacks [31]. Consequently, communication resilience should be achieved through redundancy rather than reliance on a single technology. Hybrid communication

architectures combining dedicated control links, cellular networks, and local mesh networking provide greater continuity under degraded conditions than any individual solution.

Table 7 compares the communication technologies available for IoT-enabled UAV swarm operations in airport environments. Since communication requirements vary across surveillance, coordination, and command functions, no single technology is sufficient. The architecture adopts a redundant, heterogeneous communication strategy to improve resilience and operational continuity.

Table 7. Communication Technologies for Airport IoT–AI–UAV Swarm Systems

Technology	Latency	Bandwidth	Range	Infrastructure Dependency	Interference Resilience	Recommended Role
Wi-Fi	Low	Moderate	Low	Moderate	Low	Local UAV and sensor connectivity
Long-Term Evolution (LTE)/4G	Moderate	Moderate	High	High	Moderate	Wide-area backup connectivity
5G	Low	High	High	Very High	Moderate	Primary AI-enabled surveillance backbone
Satellite	Very High	Moderate	Very High	High	High	Long-range backup communications
Radio Frequency (RF) Mesh Network	Low–Moderate	Low–Moderate	Moderate	Low	Moderate	Inter-UAV coordination and failover
Dedicated Command-and-Control (C2) Links	Low	Low	Moderate–High	Moderate	High	Safety-critical command and control
Hybrid Architecture	Low	High	Very High	Moderate	High	Resilient multi-layer communications

Key Finding**:** Hybrid communication architectures provide a practical balance between the low latency of terrestrial networks and the resilience of mesh and backup communication links.

3.4. Cybersecurity-by-Design

The integration of IoT devices, AI systems, communication networks, and UAV swarms substantially expands the airport-security attack surface. Cybersecurity must therefore be treated as an architectural requirement rather than a post-deployment enhancement.

A Zero Trust approach provides an appropriate security model for this distributed architecture because IoT sensors, UAVs, edge nodes, cloud services, and operator interfaces should not be assumed to operate within a trusted network boundary. Zero Trust principles require continuous authentication, authorization, device identity verification, least-privilege access, and continuous monitoring of participating devices and services. In the proposed architecture, these mechanisms can be applied across the sensing, UAV, edge, cloud, and command layers to reduce the risk of compromised devices gaining unrestricted access to mission-critical resources [32][33]. Accordingly, Zero Trust should be implemented as a cross-layer security principle rather than as a standalone network-security mechanism, with device identity, least-privilege access, continuous authentication, secure communications, anomaly detection, and AI-model integrity jointly enforced across the proposed five-layer architecture.

Experimental studies demonstrate that GPS spoofing can alter UAV navigation behavior, while software-defined radio (SDR)-based attacks can simultaneously disrupt positioning, control, and video transmission. Reviews consistently identify spoofing, jamming, eavesdropping, denial-of-service attacks, and unauthorized access as primary threats to UAV-enabled systems [34] .

The integration of AI introduces an additional class of adversarial threats that extends beyond conventional network attacks. AI-enabled surveillance and distributed learning systems may be exposed to adversarial examples, data poisoning, model manipulation, malicious client updates, and evasion attacks that

can degrade detection or influence automated decisions [35]. These risks are particularly important in UAV swarm environments because compromised nodes may contribute corrupted observations or model updates to distributed intelligence processes. Accordingly, adversarially resilient learning, anomaly detection, trust-weighted aggregation, and Byzantine-resilient mechanisms should be considered where collaborative or federated AI is employed [36].

Mitigation requires layered security mechanisms including encryption, authentication, secure key management, lightweight cryptography, anomaly detection, and adaptive trust management. Secure communications are particularly important because the proposed architecture depends on continuous information exchange among sensors, UAVs, edge nodes, cloud services, and command infrastructure. Communication protection should therefore include authenticated links, confidentiality and integrity mechanisms, key-management procedures, anti-jamming measures, and resilient routing or failover mechanisms. For UAV operations, navigation and communication resilience should also address GNSS spoofing, radio-frequency interference, and compromised communication links because disruption at these levels can propagate across sensing, coordination, and command functions[19][37].

However, these protections introduce computational, communication, and energy overhead and may affect inference latency, bandwidth consumption, and UAV endurance, creating a measurable trade-off between security and operational responsiveness. These parameters should therefore form part of future quantitative evaluation of the proposed architecture.

Despite these advances, integrated validation of IoT–AI–UAV swarm architectures against coordinated cyber-physical and AI-specific attacks under realistic airport operating conditions remains limited. Existing studies generally evaluate individual security mechanisms or subsystem-level threats rather than the interaction of sensing, communications, distributed intelligence, and human-supervised command under simultaneous attacks. Consequently, future validation should assess the architecture using measurable indicators such as detection degradation under attack, communication delay, packet loss, recovery time, energy overhead, and resilience to compromised nodes. Demonstrating acceptable performance across these dimensions will be important for establishing operational assurance and supporting future regulatory and deployment assessments.

4. AI SYSTEMS FOR ANOMALY DETECTION AND SWARM COORDINATION

4.1. Detection Intelligence: Rule-Based Versus Learning-Based Approaches

The effectiveness of airport-security AI depends not only on detection accuracy but also on robustness across changing environmental conditions. Rule-based systems perform adequately when threats are well defined, and operating conditions remain predictable; however, their effectiveness deteriorates when lighting, weather, scale, and target appearance vary substantially.

Learning-based approaches generally outperform rule-based methods because they can learn complex spatial and contextual representations from large datasets [38][39]. Recent UAV-detection systems employing Convolutional Neural Network (CNN)–transformer and vision-transformer architectures have demonstrated strong detection performance while maintaining real-time processing capability on embedded platforms [40]. Similarly, deep-learning models incorporating image restoration and weather-adaptation mechanisms outperform conventional pipelines under degraded visibility conditions [41].

Nevertheless, model performance can decline significantly when environmental conditions differ from those represented during training. Studies report substantial reductions in detection accuracy under severe rain, noise, and motion blur, although weather-aware data augmentation partially mitigates these effects [42]. These findings support the use of learning-based approaches for operational deployment, complemented by rule-based safeguards, confidence monitoring, and escalation mechanisms when model uncertainty becomes excessive. For airport-security applications, the optimal strategy is therefore not AI replacement of deterministic logic, but a layered approach in which learning-based systems perform primary detection and rule-based mechanisms provide verification, safety constraints, and fallback behavior.

4.2. Distributed Inference and the Latency–Accuracy Trade-off

Inference location is a critical architectural decision because it determines response latency, bandwidth consumption, and operational resilience. Cloud-only processing introduces communication delays that can limit responsiveness during time-critical incidents, whereas onboard inference enables immediate detection and local decision-making even under degraded connectivity. Empirical evidence demonstrates that embedded AI platforms can achieve real-time detection and tracking performance while maintaining acceptable accuracy levels [29].

However, onboard deployment constrains model complexity because UAV platforms possess limited computational and energy resources. Hybrid architectures address this constraint by distributing workloads across onboard processors, edge infrastructure, and cloud resources. Frameworks such as AERO

and eCoEI demonstrate that distributing intelligence across UAV, swarm, and cloud layers improves scalability, fault tolerance, and operational continuity under communication disruptions [43].

Accordingly, the proposed architecture adopts distributed inference, where latency-sensitive tasks execute onboard or at nearby edge nodes, while computationally intensive analytics are performed at higher processing layers.

4.3. Reinforcement Learning for Swarm Coordination and Task Allocation

Reinforcement learning (RL) is increasingly used for dynamic swarm management because it enables agents to adapt decisions to changing environmental conditions. Recent studies demonstrate that RL can improve trajectory planning, UAV–device association, anti-jamming behavior, coverage optimization, and energy efficiency in multi-UAV systems [3][44]. These capabilities are particularly relevant for airport-security operations, where surveillance priorities may change rapidly in response to evolving incidents, communication disruptions, or emerging threats.

However, RL should be viewed as a coordination mechanism rather than a complete decision-making solution. Airport environments impose strict safety, explainability, and regulatory requirements that limit acceptance of fully autonomous decision policies. Consequently, RL is most appropriate for adaptive task allocation and resource optimization operating within constraints established by human supervisors and mission-level rules.

The most relevant performance indicators for airport deployment extend beyond detection accuracy and include latency, energy consumption, communication efficiency, false-alarm rates, and robustness under environmental and operational uncertainty [45]. Available evidence provides representative quantitative benchmarks for these performance dimensions, although airport-specific integrated benchmarks remain limited. For example, edge-based multimodal sensing has demonstrated an F1-score of 0.94, AUC of 0.96, and inference latency of 23 ms on resource-constrained hardware [46]. UAV-edge studies further evaluate latency, energy consumption, offloading cost, communication delay, and task-execution efficiency as key indicators of distributed intelligence performance [47][48]. These results support the use of latency, energy consumption, communication overhead, scalability, and detection performance as core evaluation metrics for the proposed architecture. However, such values should be interpreted as subsystem-level evidence rather than as direct performance claims for the proposed airport-security architecture.

4.4. Explainable AI as a Deployment Requirement

Detection accuracy alone is insufficient for operational deployment in safety-critical airport environments. Security personnel, regulators, and certification authorities must understand why AI systems generated specific alerts and recommendations.

Aviation anomaly detection often requires interpretation of complex event sequences rather than isolated observations, making explainability particularly important [49][50]. Furthermore, aviation datasets frequently suffer from limited labeled data because expert annotation is costly and time-consuming, constraining the applicability of purely supervised approaches.

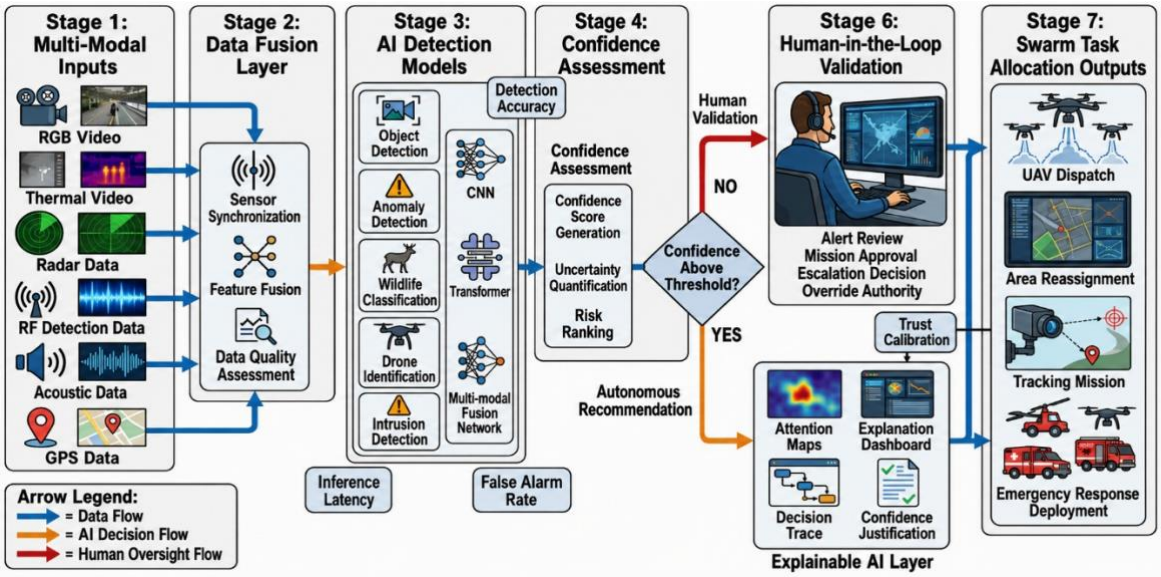

Figure 5. AI Decision Pipeline for Airport Security and UAV Swarm Coordination

Research in explainable AI (XAI) increasingly recognizes interpretability as necessary for trust, verification, validation, and certification, rather than merely as a visualization feature [38][51]. For airport-security systems, explanations should support three stakeholder groups: operators who must evaluate alerts, supervisors who must authorize responses, and regulators who must assess system compliance and safety.

Certification-grade benchmarks for real-time explainability under uncertain, evolving, and previously unseen threat conditions remain unavailable. Addressing this gap will be essential before highly autonomous airport-security systems can achieve widespread operational acceptance. Effective airport-security decision-making requires more than threat detection; it requires structured processing that transforms raw sensor observations into validated operational actions. Figure 5 presents the AI decision pipeline proposed in this review, from multi-modal data acquisition and edge inference to cloud-based threat assessment, human supervision, and coordinated UAV swarm response.

4.5. Research Gaps and Architectural Novelty

Existing airport-security research remains divided across sensing, UAV autonomy, AI analytics, and cybersecurity, with limited integration among these domains. Counter-Unmanned Aircraft System (Counter-UAS) studies primarily focus on detection and mitigation technologies, UAV swarm research emphasizes coordination and path planning, while AI and edge-cloud studies concentrate on analytics performance and computational efficiency. Although these streams provide valuable advances, they are typically developed as independent solutions rather than components of an integrated airport-security system.

The literature also lacks computational continuity between physical sensing and operational decision-making. Existing studies often optimize individual layers such as sensing, swarm control, edge computing, cloud analytics, or cybersecurity, but rarely define how these layers interact within an operational architecture for airport-security missions under real-world constraints [52][53].

Autonomy and resilience also remain largely separate concerns in the existing literature. UAV swarm studies frequently prioritize coverage efficiency, task allocation, and communication performance, whereas cybersecurity studies focus on intrusion detection, anti-jamming, and adversarial defense[54]. Consequently, little attention has been devoted to architectures that jointly integrate sensing, autonomous coordination, cybersecurity, and human supervision within a single airport-security framework.

The contribution of this paper lies not in introducing new sensing technologies or swarm algorithms, but in integrating physical sensing, UAV swarm coordination, edge intelligence, cloud analytics, human-supervised command and control, and cybersecurity resilience within a five-layer operational framework for airport security. The reviewed literature identifies gaps in the integration of IoT, AI, UAV, and cybersecurity capabilities for airport security. Table 8 summarizes these gaps and shows how the proposed five-layer architecture addresses them at the architectural level.

Table 8. Research Gaps Identified in Existing Literature and Corresponding Contributions of the Proposed Five-Layer Airport-Security Architecture

Existing Research Area	Key Limitation	Consequence for Airport Security	Proposed Framework Contribution
Counter-UAS and Airport Sensing	Primarily focuses on detection technologies	Detection alone does not guarantee coordinated response	Integrates sensing with UAV, AI, and command layers
UAV Swarm Coordination	Often coverage-focused and platform-centric	Limited integration with airport operations	Links swarm coordination with sensing and decision layers
Edge-Cloud Analytics	Primarily optimizes latency and inference	Potentially fragmented situational awareness	Provides edge-cloud intelligence for local and global decision support
AI-enabled IoT Systems	Often technology-centric	Limited airport-specific architectural integration	Reframes connected technologies within airport-security operations
UAV/IoT Cybersecurity	Frequently addresses individual system layers	Cross-layer vulnerabilities may remain	Treats cybersecurity as a cross-cutting architectural requirement

5. INTEGRATED IOT–AI–UAV SWARM ARCHITECTURE

5.1. Positioning and Novelty of the Proposed Framework

The proposed framework is positioned as a systems-level architectural contribution that brings together capabilities identified separately across the reviewed literature. Rather than introducing a new sensing algorithm, UAV coordination algorithm, or cybersecurity mechanism, the framework organizes established capabilities into five functionally interconnected architectural layers: IoT-based multimodal sensing, UAV swarm coordination and edge intelligence, cloud-based analytics and mission intelligence, human-supervised command and control, and cross-layer cybersecurity and resilience.

The novelty therefore lies primarily in the integration and operational organization of these capabilities for airport-security applications. The architecture explicitly links distributed sensing to edge and cloud intelligence, coordinated UAV operations, human decision-making, and cross-layer resilience. This arrangement provides a continuous operational pathway from threat detection and data processing to mission coordination, human supervision, and response, while recognizing that cybersecurity and resilience must operate across the entire architecture rather than as an isolated subsystem.

In contrast to many existing frameworks that address cybersecurity and human supervision as supporting considerations rather than explicit architectural dimensions, the proposed framework incorporates both as integral components of the overall system design. This positioning reflects the operational requirements of modern airport environments, where autonomous surveillance capabilities must simultaneously address safety, accountability, communication resilience, and regulatory expectations. By consolidating capabilities supported across the reviewed literature into a coherent operational model, the framework provides a basis for future implementation, field evaluation, and certification-oriented assessment of intelligent airport-security systems.

To further establish its position relative to existing work, Table 9. Comparative Positioning of Existing Studies and the Proposed Airport-Security Architecture compares representative airport-security and IoT–AI–UAV studies with the proposed framework across the principal functional capabilities identified in this review. The comparison is intended to demonstrate differences in architectural scope rather than to imply that existing studies lack the individual capabilities they investigate.

Table 9. Comparative Positioning of Existing Studies and the Proposed Airport-Security Architecture

Framework/Study	IoT Sensing	AI Analytics	UAV Swarms	Human Supervision	Cybersecurity	Integrated Airport-Security Architecture
[6]	✓	Limited	✗	Limited	✓	✗
[7]	Limited	✓	✓	✗	✓	✗
[12]	✓	✓	✗	✗	Limited	✗
[13]	✓	Limited	Limited	✗	Limited	✗
Proposed Framework	✓	✓	✓	✓	✓	✓

Note: ✓ indicates explicit and substantive treatment of the capability within the framework or system architecture; Limited indicates partial or secondary treatment; and ✗ indicates that the capability is not substantively addressed as an architectural component. The assessment is based on the primary focus of each reviewed study.

The comparison with existing studies indicates that the principal contribution of this review is architectural integration rather than algorithmic innovation. While previous studies have significantly advanced sensing technologies, UAV coordination, AI analytics, edge computing, and cybersecurity, these capabilities are generally investigated independently or within specific application contexts. By synthesizing evidence across these research domains, the proposed framework organizes established technological capabilities into a coherent airport-security reference architecture that integrates sensing, coordination, intelligence, cybersecurity, and human supervision within a single operational ecosystem.

5.2. Unified Five-Layer Architecture

The preceding analysis shows that airport-security challenges cannot be addressed through isolated improvements in sensing, analytics, or UAV deployment. Effective surveillance requires an integrated

architecture capable of transforming distributed sensor observations into coordinated operational responses while maintaining human oversight and regulatory compliance. This paper proposes a five-layer IoT–AI–UAV swarm architecture that links sensing, communication, intelligence, coordination, and supervision into a single operational ecosystem.

The proposed five-layer architecture was derived from recurring functional requirements consistently identified across the reviewed literature, namely multi-modal sensing, coordinated autonomy, intelligent analytics, human supervision, and system resilience. These functional domains recur across airport-security, UAV swarm, IoT, and AI studies and collectively represent the core operational capabilities required for intelligent airport-security systems. Organizing the framework into these five interoperable layers provides a structured decomposition of system functions and facilitates information flow, coordinated decision-making, scalability, and regulatory accountability.

Layer 1: Physical Infrastructure and IoT Sensing forms the perception foundation of the system. Distributed optical, thermal, radar, RF, acoustic, motion, positioning, and environmental sensors provide complementary observations across airport perimeters, runways, restricted zones, and critical infrastructure. Consistent with the fusion logic developed in Section 3, no sensor operates as an independent decision source; instead, heterogeneous sensing streams are fused to improve robustness under adverse weather, low visibility, and target ambiguity.

Layer 2: UAV Swarm Operations and Edge Intelligence provides mobile sensing and rapid-response capability. UAVs perform localized detection, tracking, and target verification using onboard AI inference, while nearby edge nodes support collaborative processing and swarm-level coordination. Hybrid coordination enables centralized mission planning during routine operations and decentralized adaptation during communication degradation or dynamic incidents.

Layer 3: Cloud Analytics and Mission Intelligence supports computational resources for long-term analytics, model retraining, historical pattern analysis, and strategic mission optimization. Rather than transmitting raw sensor streams, edge nodes forward processed alerts and metadata, reducing bandwidth consumption while preserving operational relevance.

Layer 4: Command, Control, and Human Supervision enables operators to oversee missions, validate alerts, authorize interventions, and coordinate with airport security personnel and air traffic management systems. Human operators remain responsible for consequential decisions, ensuring accountability and regulatory compatibility.

Layer 5: Cybersecurity and Resilience operates across all architectural layers. Security mechanisms include authenticated communications, encrypted data exchange, spoofing-resistant navigation, network anomaly detection, and failsafe behaviors that maintain safe operation during cyber or communication disruptions. Together, these layers create a closed-loop security architecture in which sensing, interpretation, coordination, and response operate continuously while preserving human authority and operational transparency.

5.3. Architectural Validation through Threat-to-Response Mapping

The proposed architecture was evaluated conceptually against the principal airport-security challenges identified in Section 2, yielding three main observations.

First, no individual sensing modality consistently provides adequate performance across perimeter intrusion, wildlife monitoring, and unauthorized drone detection. Multi-modal sensing therefore functions as a structural requirement rather than a performance enhancement.

Second, operational response times are largely determined by inference location. Architectures dependent on cloud-only processing introduce communication delays that are incompatible with time-critical incidents. Edge-enabled processing provides the most practical balance between responsiveness and computational capability.

Third, coordination architecture directly influences operational resilience. Centralized control performs well under normal conditions but is vulnerable to communication failures, whereas decentralized systems improve robustness but may sacrifice global optimization. Hybrid coordination is well suited to airport operations

These findings collectively support the proposed architecture as a practical and evidence-informed framework integrating the IoT sensing, AI analytics, swarm coordination, and human supervision capabilities identified in the current literature.

5.4. Design Principles for Airport Deployment

Four design principles emerge from the synthesis.

Principle 1: Multi-modal sensing is a core requirement. Sensor selection should be driven by threat characteristics and environmental conditions rather than technology availability.

Principle 2: Time-critical intelligence must execute at the edge. Detection, tracking, and alert generation should occur as close as possible to the sensing source.

Principle 3: Communication resilience must be engineered through redundancy**.** Hybrid communication architectures are preferable to single-network solutions in safety-critical environments.

Principle 4: Human factors should be incorporated as architectural constraints. Alert generation, interface design, trust calibration, and escalation workflows directly influence operational effectiveness and cannot be addressed after deployment.

5.5. Architecture Validation through Cross-Literature Evidence

Because the proposed architecture is conceptual rather than experimentally implemented, its validation is based on cross-literature synthesis. This approach is appropriate because each architectural layer is supported by substantial evidence from prior studies in airport surveillance, UAV swarms, edge intelligence, cloud analytics, human-supervised AI, and cybersecurity.

Table 7 summarizes the evidence supporting each layer of the proposed framework. Multi-modal sensing is supported by evidence that no single sensor can provide reliable all-weather, all-condition surveillance, whereas sensor fusion improves detection robustness and reduces perception gaps. UAV swarm research consistently shows that coordinated multi-agent systems provide superior coverage, adaptability, and resilience compared with individual UAV deployments. Edge-computing studies further demonstrate that latency-sensitive surveillance tasks benefit from local processing, while cloud-based analytics support large-scale data integration, historical analysis, and strategic decision-making.

Human-supervised decision-making is also strongly supported in the literature because safety-critical security operations require explainable and accountable AI outputs. Cybersecurity cannot be treated as a standalone component; research consistently highlights the need for cross-layer protection spanning sensing devices, communication links, AI services, and command systems.

Taken together, these findings indicate that the proposed five-layer architecture is grounded in established technological capabilities rather than speculative assumptions. The contribution of this work is the integration of validated sensing, communication, and AI subsystems into a coherent airport-security architecture that links sensing, autonomous coordination, intelligence, human oversight, and resilience within a single operational framework.

Nevertheless, this validation should be interpreted as evidence-based architectural plausibility rather than operational proof. Most supporting studies originate from simulations, laboratory environments, or adjacent application domains. Airport-specific field trials are therefore still needed to evaluate interoperability, false-alarm behaviour, human workload, regulatory compliance, and end-to-end system resilience under realistic operational conditions. Table 10 maps the functional requirements identified from the reviewed literature to the five architectural layers. This evidence-based mapping shows how the literature supports the role and placement of each layer without implying experimental validation of the complete architecture.

Table 10. Evidence-Based Mapping of Literature-Derived Requirements to the Proposed Five-Layer Airport-Security Architecture

Architectural Layer	Functional Requirement Identified from Literature	Evidence Synthesized from the Reviewed Literature	Implication for the Proposed Architecture
Layer 1: Physical Infrastructure and IoT Sensing	Reliable all-weather detection requires complementary sensing modalities rather than reliance on individual sensors.	Reviewed airport-security and surveillance studies indicate that complementary thermal, RGB, radar, RF, acoustic, and LiDAR modalities can address different limitations associated with occlusion, illumination, target characteristics, and environmental variability.	Supports a dedicated multimodal sensing layer as the perception foundation of the architecture.
Layer 2: UAV Swarm Operations and Edge Intelligence	Large airport environments require persistent surveillance, distributed coverage, adaptive task allocation, and rapid local response.	Reviewed UAV-swarm literature reports advantages in coverage, adaptability, resilience, and mission flexibility, while edge computing supports low-latency local inference.	Supports integrating coordinated UAV swarms with edge intelligence for scalable real-time surveillance and

			incident verification.
Layer 3: Cloud Analytics and Mission Intelligence	Airport-wide situational awareness requires centralized data fusion, historical analysis, model updating, and strategic mission optimization.	Reviewed edge-cloud studies indicate that cloud resources complement edge processing through large-scale analytics, long-term learning, and decision support.	Supports retaining a cloud-intelligence layer for global situational awareness and longer-term operational optimization.
Layer 4: Command, Control and Human Supervision	Safety-critical airport operations require explainable AI, operator oversight, accountability, and regulated intervention.	Reviewed human-supervised AI and human-in-the-loop studies emphasize the importance of trust calibration, decision accountability, and supervisory authority in autonomous systems.	Supports maintaining human supervision as a core architectural layer rather than treating operators as external users.
Layer 5: Cybersecurity and Resilience	Security threats can affect sensing devices, communication links, AI services, navigation systems, and command infrastructure simultaneously.	Reviewed cybersecurity literature recommends cross-layer protection through secure communications, intrusion detection, resilient networking, spoofing mitigation, and anomaly detection.	Supports cybersecurity as a cross-cutting architectural layer spanning system components.

Having established the architectural rationale and literature-based validation of the proposed framework, the subsequent section examines its applicability across representative airport-security scenarios. By mapping the five-layer architecture onto perimeter intrusion detection, wildlife hazard monitoring, and rapid-response surveillance, the discussion illustrates how the integrated IoT–AI–UAV framework addresses diverse operational requirements while highlighting the differing sensing, coordination, communication, and decision-support demands associated with each application.

6. AIRPORT-SECURITY USE CASES

The proposed architecture is examined through three representative airport-security scenarios. These scenarios show how integrated IoT sensing, AI analytics, UAV swarms, and human supervision contribute to detection, situational awareness, and response.

6.1. Perimeter Intrusion Detection

Perimeter security requires rapid detection, verification, tracking, and interception of unauthorized persons, vehicles, or drones across large and often sparsely monitored areas. Evidence from airport-security research indicates that radar-only approaches are insufficient and that layered Radio Frequency (RF), optical, thermal, and radar sensing is required for reliable detection and identification.

Cross-domain studies generally report better performance from thermal–visual fusion than from single-modality approaches under variable illumination and adverse weather conditions. Reported performance includes recall values exceeding 98% and detection accuracies above 94% in multispectral surveillance settings [55]. Although these results originate primarily from industrial and urban-security applications, they suggest that heterogeneous sensing may reduce missed detections and false alarms in airport environments[56].

Within the architecture, fixed sensors provide continuous monitoring while UAV swarms perform rapid verification and target tracking beyond the field of view of stationary infrastructure. This combination addresses the principal limitation of conventional CCTV systems: the inability to maintain persistent situational awareness during mobile intrusion events. Multi-modal sensing improves detection reliability by combining complementary sensor observations before initiating coordinated UAV response. Figure 6 illustrates the proposed intrusion-detection workflow, showing how heterogeneous sensing, AI-based threat classification, swarm coordination, and human validation operate together within the proposed airport-security framework.

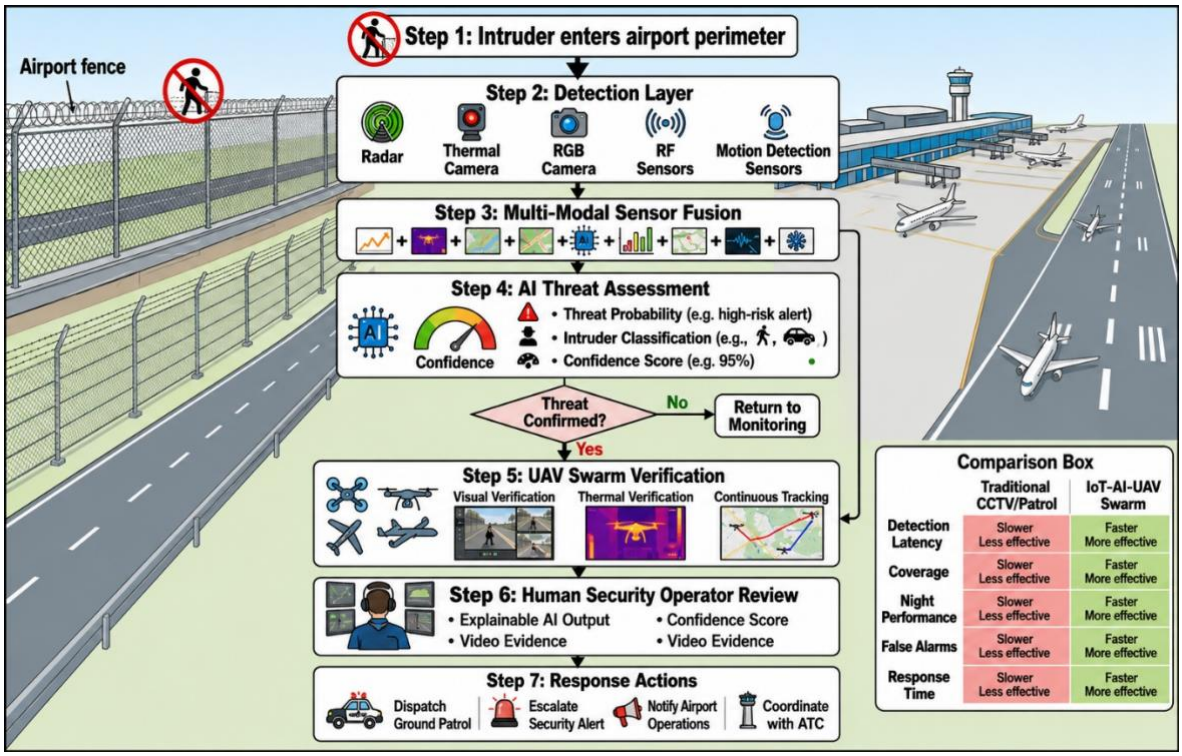

Figure 6. Multi-Modal UAV Swarm Intrusion Detection Workflow

6.2. Wildlife Hazard Monitoring

Wildlife strikes remain a persistent aviation-safety risk because animals often enter operational areas with limited warning time and under poor visibility conditions.

Among the three use cases examined, wildlife monitoring possesses the strongest airport-specific evidence base. Operational deployments have reported detection efficiencies of approximately 92% for large animals and near-perfect bird-identification performance under thermal-vision fusion architectures [57]. Additional studies demonstrate that thermal-visible fusion substantially improves wildlife detection relative to individual sensing modalities because thermal imagery highlights biological targets while visible imagery provides species-level detail [58][59].

The proposed architecture applies this principle through continuous runway monitoring using fixed sensors and UAV-assisted verification when elevated risk is detected. Thermal sensors identify potential hazards, AI models classify targets, and UAVs provide close-range confirmation when required. The combination improves coverage and intervention lead time while reducing unnecessary wildlife-response deployments.

6.3. Rapid-Response Surveillance

Rapid-response incidents, including perimeter breaches, suspicious vehicles, emergency landings, and coordinated security threats, require simultaneous surveillance of multiple locations under severe time constraints.

Evidence from multi-UAV coordination research indicates that cooperative swarms can outperform single-UAV deployments in tracking accuracy, coverage continuity, and mission completion time [60][61]. Additional studies demonstrate significant improvements in sensing efficiency and communication-resource utilization through coordinated swarm behavior [62].

In airport-security operations, these capabilities support faster deployment, broader incident coverage, and greater operational resilience. Hybrid coordination is particularly valuable because centralized mission control maintains strategic oversight while decentralized execution enables continued operation during communication degradation. UAV assets can therefore be dynamically redistributed according to incident severity, target movement, and communication availability while operators retain mission-level authority.

Table 11 compares the three principal airport-security use cases discussed in this review: perimeter intrusion detection, wildlife hazard monitoring, and rapid-response surveillance. The comparison highlights differences in sensing requirements, AI processing demands, swarm coordination needs, operational

constraints, and deployment value. Although all three applications benefit from integrated IoT–AI–UAV architectures, they impose different performance priorities and operational trade-offs.

Table 11. Comparative Assessment of Representative Airport Security Use Cases

Evaluation Dimension	Perimeter Intrusion Detection	Wildlife Hazard Monitoring	Rapid-Response Surveillance
Primary Objective	Detect and localize unauthorized perimeter breaches	Detect and track wildlife near operational areas	Provide immediate situational awareness during security incidents
Typical Threats	Human intruders, vehicles, unauthorized drones	Birds, mammals, runway wildlife	Dynamic aerial or ground threats
Critical Sensors	RGB, Thermal, LiDAR, Motion Sensors	Thermal, RGB, Radar, LiDAR	Multi-modal sensor fusion
AI Requirements	Intruder detection and classification	Small-object detection and species discrimination	Real-time fusion and threat prioritization
UAV Swarm Function	Persistent perimeter patrol and verification	Distributed wildlife monitoring	Rapid deployment and cooperative tracking
Response Time Requirement	Seconds–minutes	Continuous monitoring	Immediate
Environmental Sensitivity	Illumination, terrain, occlusion	Weather, visibility, target size	Network quality and scene dynamics
Communication Dependency	High	Moderate–High	Very High
Human Supervision	Moderate	Moderate–High	High
Key Operational Challenge	Coverage continuity and false alarms	Reliable small-target detection	Low-latency coordination and secure communications
Overall Deployment Value	High	High	Very High

Key Insight: Rapid-response surveillance places the greatest demands on communication resilience, latency, and swarm coordination, whereas wildlife monitoring presents the primary sensing challenge because of the small and highly variable nature of its targets.

6.4. Cross-Use-Case Synthesis

Across the three use cases, the benefits do not arise primarily from UAV deployment, AI analytics, or IoT sensing in isolation. Instead, benefits arise from the interaction of all three components.

IoT expands sensing coverage, AI transforms observations into actionable intelligence, and UAV swarms provide adaptive mobility and verification capability. Human supervision integrates these outputs into accountable operational decisions. The evidence therefore supports the central argument of this paper: airport-security effectiveness depends on architectural integration rather than isolated technology adoption.

6.5. Synthesis of the Study Objectives

The findings of this review address the four main objectives of the study. First, the analysis establishes the role of integrated IoT-enabled sensing and communication infrastructure in supporting distributed airport surveillance and situational awareness. Second, the reviewed evidence demonstrates how AI-enabled analytics can support threat detection, anomaly identification, risk assessment, and intelligent decision-making across edge, cloud, and UAV platforms. Third, the comparative analysis of UAV coordination approaches identifies the importance of coverage, latency, robustness, scalability, and communication resilience in selecting suitable swarm-coordination strategies for airport-security operations.

Fourth, the analysis identifies the principal technical, cybersecurity, regulatory, and human-factor barriers that must be addressed before practical deployment of the proposed architecture.

Taken together, these findings support the four study objectives and provide an evidence-grounded basis for the proposed five-layer IoT–AI–UAV swarm architecture. The framework should be understood as a conceptual reference architecture derived from the reviewed evidence, rather than as an experimentally validated operational system.

7. CHALLENGES AND OPEN RESEARCH ISSUES

Despite substantial technological progress, several barriers continue to limit operational deployment of integrated IoT–AI–UAV swarm systems in airport environments.

7.1. Energy Constraints and Coverage Continuity

Battery endurance remains one of the most significant operational limitations. Current multirotor platforms experience inherent trade-offs among endurance, payload capacity, sensing capability, and onboard computing resources [7].

The limitation extends beyond individual flight duration. Because airport-security operations require persistent surveillance, endurance constraints directly affect coverage continuity, handover reliability, and mission availability. Although experimental battery-management approaches demonstrate promising improvements, their operational suitability for routine airport deployment remains unproven [63]. Priority areas include endurance-aware mission planning, automated battery-rotation strategies, charging infrastructure integration, and hybrid aerial-ground coverage models.

7.2. Communication Resilience

Reliable communication is fundamental to swarm coordination, situational awareness, and human supervision. However, airport environments present challenging RF conditions characterized by congestion, interference, and potential cyber-physical attacks.

Communication failures can degrade coordination quality, interrupt video transmission, and reduce operator visibility during critical incidents [64][65]. Beyond conventional link failures, cybersecurity must account for intentional attacks against distributed communication and AI infrastructure. Zero-Trust principles provide a relevant security model for such environments by requiring continuous authentication, authorization, and verification rather than assuming that devices, UAVs, or network nodes are inherently trusted. In addition, adversarial AI threats, including data poisoning, malicious model updates, evasion attacks, and compromised swarm participants, may undermine distributed inference and coordinated decision-making. Secure and resilient communications should therefore be considered jointly with AI robustness, incorporating authenticated communication, dynamic trust assessment, anomaly detection, anti-spoofing mechanisms, and resilient multi-link communication strategies. However, evidence for integrated Zero-Trust and adversarial-AI protection specifically in airport UAV-swarm environments remains limited. Existing studies provide limited airport-specific evidence regarding acceptable communication-degradation thresholds before operational performance becomes unacceptable.

Future work should establish quantitative resilience benchmarks covering packet loss, latency, bandwidth availability, GNSS degradation, and communication-recovery performance. Available literature provides representative quantitative benchmarks for some of these performance dimensions, although airport-specific integrated benchmarks remain limited. Latif et al. [46] reported an F1-score of 0.94, an AUC of 0.96, and an inference latency of 23 ms for multimodal cybersecurity threat detection deployed on resource-constrained edge hardware. In UAV-enabled edge computing, Huda and Moh [48] evaluated offloading cost, energy consumption, and task-execution delay in UAV-swarm surveillance, while Zhang et al. [47] investigated distributed UAV–edge inference under latency constraints and varying computational and communication resources. These results support the use of latency, energy consumption, communication/offloading overhead, scalability, and detection performance as core evaluation metrics for future validation of the proposed architecture. However, these values represent subsystem-level evidence rather than direct performance claims for the proposed airport-security architecture.

7.3. Regulatory Integration and Airspace Governance

Regulatory approval may represent one of the most significant long-term deployment challenges. Unlike many civilian UAV applications, airport-security systems operate within controlled airspace where safety, accountability, and coordination with air traffic management are mandatory requirements.

Current regulations remain fragmented across jurisdictions, and fully autonomous swarm operations lack mature certification pathways [66][67]. A realistic deployment pathway is likely to be incremental: controlled pilot programs, supervised Beyond Visual Line of Sight (BVLOS) operations, UAS Traffic

Management (UTM)-integrated deployments, and eventually higher levels of autonomy subject to demonstrated safety performance.

Research must therefore address not only technical feasibility but also regulatory compliance, certification evidence generation, and Air Traffic Control (ATC) integration protocols.

7.4. Explainability, Verification, and Certification

AI systems cannot be deployed in airport-security environments solely on the basis of detection accuracy. Regulatory authorities require evidence that decisions are explainable, auditable, and predictable under operational conditions.

Current XAI approaches improve interpretability, but certification-grade methodologies for validating real-time AI decisions remain immature [68]. This gap becomes particularly significant when systems encounter previously unseen threats or operate under limited labeled-data conditions. Establishing explainability standards linked directly to certification requirements represents a critical research priority.

Beyond model interpretability, explainability is increasingly regarded as an enabling requirement for the assurance of AI-enabled safety-critical systems. Contemporary XAI research emphasizes that explanations should support not only developer understanding but also operational decision-making, post-incident analysis, and regulatory auditing [69][70]. In airport-security applications, explainable outputs can improve operator trust, facilitate verification of AI-assisted threat assessments, and provide transparent justification for security decisions under uncertain conditions. Consequently, future airport-security architectures should integrate explainability with verification, traceability, and human supervision as complementary components of trustworthy AI rather than treating XAI as an isolated visualization technique.

7.5. Human Factors and Human–AI Teaming

The transition from manual surveillance to supervisory control fundamentally changes the role of airport-security personnel. Operators must manage larger information volumes, oversee autonomous assets, and make decisions based on AI-generated recommendations.

The principal challenge is maintaining effective trust calibration. Excessive trust may encourage automation bias, whereas insufficient trust may lead operators to ignore valuable system recommendations [71]. Alert fatigue represents an additional concern because high false-alarm rates can degrade operator performance and increase the likelihood of missed threats.

Research remains limited regarding acceptable alert volumes, workload thresholds, and interface designs for swarm-supervision environments. Longitudinal studies are therefore needed to examine operator trust, workload evolution, and human–AI collaboration under realistic airport conditions.

7.6. Open Research Roadmap

Across these deployment barriers, the central issue is that technological capability is advancing faster than validation, certification, and operational integration. Future research should prioritize:

1. Airport-scale field trials under realistic operational conditions.
2. Adversarial testing of communication and cybersecurity resilience.
3. Certification-oriented explainable AI methodologies.
4. Human-factors studies focused on trust calibration and workload management.
5. Formal Air Traffic Control (ATC) and Unmanned Aircraft System Traffic Management (UTM) integration frameworks for autonomous swarm operations.

Table 12 presents the major barriers preventing large-scale deployment of integrated IoT–AI–UAV swarm systems in airport-security environments. The barriers are grouped into technical, operational, regulatory, AI-assurance, and human-factors categories, with each entry linked to its operational consequence, evidence maturity, and priority research direction.

Table 12. Deployment Barriers and Priority Research Directions for Airport IoT–AI–UAV Swarm Systems

Barrier Category	Major Challenge	Operational Consequence	Evidence Maturity	Priority Research Direction	Priority
Energy & Endurance	Battery limitations	Reduced patrol persistence and loiter time	High	Energy-aware scheduling and charging strategies	Critical
Coverage Continuity	UAV failures and rotation cycles	Surveillance gaps during operations	Moderate	Autonomous handoff and redundancy	Critical

				mechanisms	
Communications	Link loss and bandwidth constraints	Degraded coordination and delayed alerts	High	Multi-link failover and adaptive networking	Critical
Navigation Integrity	GNSS spoofing and jamming	Loss of positioning accuracy	Moderate	Multi-source resilient localization	Critical
Cybersecurity	Attacks on communication and data layers	Reduced trust, availability, and mission assurance	High	Secure-by-design swarm architectures	Critical
Regulatory Integration	Airport authorization and Air Traffic Management (ATM) /UTM integration	Delayed operational deployment	Moderate	Airport-specific regulatory frameworks	High
AI Assurance	Explainability and certification	Reduced trust and approval readiness	Low	Certification-oriented XAI and validation frameworks	Critical
Human Factors	Trust calibration, workload, alert fatigue	Reduced supervisory effectiveness	Low–Moderate	Human-in-the-loop performance studies	High
Scalability	Large-scale swarm orchestration	Increased coordination complexity	Moderate	Hierarchical and cluster-based control methods	High
Operational Validation	Lack of airport-scale field trials	Limited deployment evidence	Low	End-to-end airport demonstrations	Critical

Key Insight: The principal deployment obstacles extend beyond sensing and detection accuracy. The dominant deployment barriers are certification, communication resilience, human supervision, cybersecurity, and airport-specific operational validation.

The central challenge is therefore no longer whether IoT, AI, and UAV swarms can support airport security, but whether they can be validated, certified, and integrated into operational aviation environments while preserving safety, accountability, and human control.

8. FUTURE RESEARCH ROADMAP

Moving from conceptual IoT–AI–UAV swarm architectures to operational airport-security systems requires a research agenda addressing technical validation, regulatory integration, human factors, and certification. Existing studies demonstrate the feasibility of individual technologies, but the main challenge is generating the evidence necessary for deployment in safety-critical airport environments.

8.1. Near-Term Priorities (1–3 Years)

The most immediate requirement is field validation under operational airport conditions. Current evidence remains dominated by simulations, laboratory experiments, and non-airport case studies, limiting confidence in real-world performance. Controlled airport trials should evaluate detection accuracy, false-alarm rates, response latency, swarm coordination reliability, and operator workload across daytime, nighttime, adverse-weather, and low-visibility conditions [2][72].

A second priority is the development of formal ATC–UTM coordination procedures. Although UAV traffic-management concepts have matured, airport-security operations require explicit protocols governing authorization, contingency handling, geofencing, communication handoff, and emergency intervention. Current reviews identify interoperability between UAV operations and existing air-traffic-management systems as a major unresolved challenge [2][73].

A third priority is adversarial robustness testing of AI detection systems. Airport-security architectures depend heavily on AI-based threat identification, yet AI–IoT reviews continue to identify

susceptibility to spoofing, adversarial manipulation, and data-poisoning attacks [74][75]. Systematic red-team evaluations should form part of airport-security validation programs.

8.2. Medium-Term Priorities (3–5 Years)

In the medium term, research should move beyond performance validation towards operational standardization and certification. Regulatory authorities currently lack mature frameworks for certifying autonomous and semi-autonomous UAV swarm systems, particularly when AI contributes to safety-relevant decisions. Emerging evidence suggests that formal verification, automated traceability, and compliance-driven software engineering can support certification readiness [76][77].

A parallel requirement is cross-airport deployment standardization. Current regulatory approaches vary substantially across jurisdictions, creating barriers to large-scale adoption. Harmonized standards covering communication protocols, cybersecurity requirements, swarm coordination behaviors, and operational procedures would improve interoperability and accelerate deployment [73][78].

Human-factors research also requires further development. Although human-centered AI is widely advocated, airport-security operations lack longitudinal evidence regarding operator trust calibration, override behavior, workload adaptation, and alert-compliance trends. Such studies are needed to establish how supervisory performance evolves as operators transition from direct surveillance to AI-assisted swarm management.

8.3. Long-Term Priorities (5–10 Years)

The long-term goal is to develop human-supervised autonomous airport-security ecosystems capable of persistent monitoring, adaptive response, and resilient operation across large airport infrastructures. Achieving this vision requires advances in swarm autonomy, scalable coordination, communication resilience, and explainable decision-making [10][79].

Future systems should support coordination among multiple concurrent swarms operating across airports and connected through broader smart-airport infrastructures. However, challenges related to high-density UAV traffic management, secure inter-swarm communication, conflict resolution, and large-scale autonomy remain unresolved [72]. Integrated airport-security ecosystems will depend on secure AI-driven network management, adaptive cybersecurity architectures, and seamless interoperability between IoT infrastructure, UAV swarms, airport operations, and regulatory oversight systems [80]. Despite continued progress in the enabling technologies, large-scale deployment still depends on resolving several technical and operational challenges. Figure 7 summarizes the proposed research roadmap, identifying the key research priorities required to transition from prototype architectures toward certifiable, human-supervised autonomous airport-security systems.

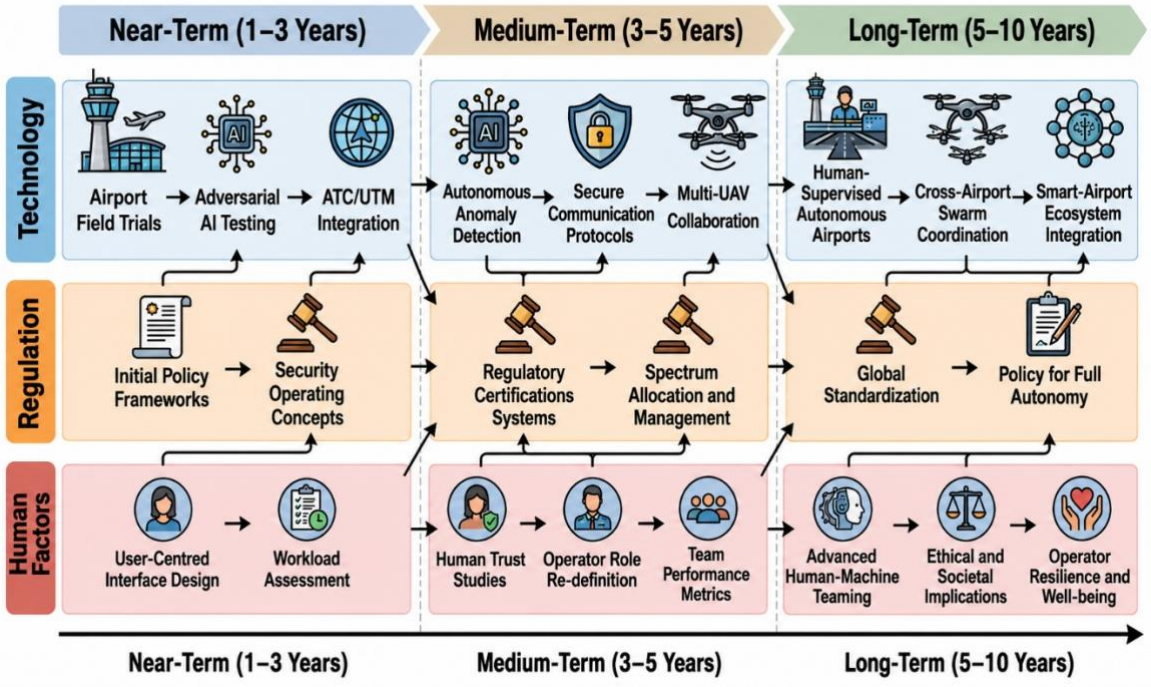

Figure 7. Future Research Roadmap toward Human-Supervised Autonomous Airport-Security Systems

9. CONCLUSION

This review's principal contribution is not a new sensing algorithm, coordination protocol, or cybersecurity mechanism, but the architectural integration of capabilities previously investigated largely as separate components into a single, evidence-grounded reference architecture for airport security. The proposed five-layer framework explicitly links multimodal sensing, UAV swarm coordination, edge and cloud intelligence, human supervision, and cross-layer cybersecurity within a unified operational model. The comparative analysis indicates that existing studies have made substantial progress in individual areas of intelligent airport and UAV security, but these capabilities are often addressed within different technical or operational contexts. The contribution of this study therefore lies in synthesizing these capabilities into a coherent systems-level architecture in which autonomy, resilience, cybersecurity, and human oversight are treated as interconnected design requirements.

Practically, the architecture provides airport operators, systems engineers, and regulators with a reference model for future implementation, interoperability planning, certification-oriented evaluation, and regulatory assessment. It should not be interpreted as a deployment-ready system because the proposed architecture has not yet been validated through airport-scale field trials. Its practical value must therefore be established through quantitative performance benchmarking, simulation, expert evaluation, airport-specific testing, and assessment against applicable aviation and cybersecurity requirements. Future research should focus on these validation activities, with particular emphasis on communication resilience, energy efficiency, scalability, explainable AI, human supervision, cybersecurity, and integration with existing air traffic management and UAS traffic management infrastructures.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article, as no datasets were generated or analyzed during the current study

CONFLICTS OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] Z. Xia *et al.*, "A systematic review on human-AI hybrid systems and human factors in air traffic management," *J. Eng. Des.*, vol. 37, no. 3, pp. 871–919, 2026, doi: 10.1080/09544828.2025.2509056.

[2] J. Samu and Y. Chuyang, "Airport Ground-Based Aerial Object Surveillance Technologies for Enhanced Safety: A Systematic Review," *Drones*, vol. 10, no. 1, p. 22, 2026, doi: 10.3390/drones10010022.

[3] R. Donatus, K. Ter, O. Ajayi, D. Udekwe, and L. G. Aug, "Multi-Agent Reinforcement Learning in Intelligent Transportation Systems : A Comprehensive Survey," *arxiv.org*, pp. 1–21, 2025, doi: 10.48550/arXiv.2508.20315.

[4] A. M. Varghese, J. Biju, N. J. Manasrayil, L. Shaji, and R. Thomas, "Human exclusive alerts in CCTV surveillance using computer vision," in *2025 Emerging Technologies for Intelligent Systems (ETIS)*, IEEE, 2025, pp. 1–6. doi: 10.1109/etis64005.2025.10961654.

[5] F. Jalalvand, M. Baruwal Chhetri, S. Nepal, and C. Paris, "Alert prioritisation in security operations centres: A systematic survey on criteria and methods," *ACM Comput. Surv.*, vol. 57, no. 2, pp. 1–36, 2024, doi: 10.1145/3695462.

[6] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies," *Sensors*, vol. 20, no. 12, p. 3537, 2020, doi: 10.3390/s20123537.

[7] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intell. Serv. Robot.*, vol. 16, no. 1, pp. 109–137, 2023, doi: 10.1007/s11370-022-00452-4.

[8] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the unmanned aerial vehicles (UAVs): A comprehensive review," *Drones*, vol. 6, no. 6, p. 147, 2022, doi: 10.3390/drones6060147.

[9] S. Javaid *et al.*, "Communication and control in collaborative UAVs: Recent advances and future trends," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 6, pp. 5719–5739, 2023, doi: 10.1109/tits.2023.3248841.

[10] Y. Alqudsi and M. Makaraci, "UAV swarms: research, challenges, and future directions," *J. Eng. Appl. Sci.*, vol. 72, no. 1, p. 12, 2025, doi: 10.1186/s44147-025-00582-3.

[11] B. Xia, I. Mantegh, and W. Xie, "Decentralized UAV swarm control: A multi-layered architecture for integrated flight mode management and dynamic target interception," *Drones*, vol. 8, no. 8, p. 350, 2024, doi: 10.3390/drones8080350.

[12] R. Arranz, D. Carramiñana, G. de Miguel, J. A. Besada, and A. M. Bernardos, "Application of deep reinforcement learning to UAV swarming for ground surveillance," *Sensors*, vol. 23, no. 21, p. 8766, 2023, doi: 10.3390/s23218766.

[13] B. Kovács, F. Vörös, T. Vas, K. Károly, M. Gajdos, and Z. Varga, "Safety and security-specific application of multiple drone sensors at movement areas of an aerodrome," *Drones*, vol. 8, no. 6, p. 231, 2024, doi: 10.3390/drones8060231.

[14] K. van de Merwe, S. Mallam, and S. Nazir, "Agent transparency, situation awareness, mental workload, and

operator performance: A systematic literature review," *Hum. Factors*, vol. 66, no. 1, pp. 180–208, 2024, doi: 10.1177/00187208221077804.

[15] D. Huegli, A. Chavaillaz, J. Sauer, and A. Schwaninger, "Effects of false alarms and miscues of decision support systems on human–machine system performance: A study with airport security screeners," *Ergonomics*, vol. 68, no. 12, pp. 2088–2103, 2025, doi: 10.1080/00140139.2025.2453546.

[16] R. E. Donatus, M. D. Dere, I. H. Donatus, U. O. Chiedu, M. B. Abdulrazaq, and M. F. Ohemu, "Development of an Optimised Neural Network Model for RF Based UAV Detection and Identification," *Dutse J. Pure Appl. Sci.*, vol. 8, no. 4b, pp. 82–91, 2023, doi: 10.4314/dujopas.v8i4b.10.

[17] E. Ntizikira, W. Lei, F. Alblehai, K. Saleem, and M. A. Lodhi, "Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles," *Sensors*, vol. 23, no. 19, p. 8077, 2023, doi: 10.3390/s23198077.

[18] M. Bakirci, "A novel swarm unmanned aerial vehicle system: Incorporating autonomous flight, real-time object detection, and coordinated intelligence for enhanced performance," *Trait. du Signal*, vol. 40, no. 5, pp. 2063–2078, 2023, doi: 10.18280/ts.400524.

[19] T. Shobha, R. Rashmi, L. R. Chaitanya, C. V Medhini, R. J. Chandana, and S. P. Gowda, "A multi-layer airport security framework using YOLO-based X-ray detection, video anomaly analysis, IoT sensor monitoring and blockchain logging," *Sci. Rep.*, 2026, doi: 10.1038/s41598-026-52894-w.

[20] M. Basem, J. Zaki, M. S. Saraya, and F. M. Talaat, "Improving airport security with IoT-powered deep learning methods for threat detection and intelligent recommendation systems," *Sci. Rep.*, vol. 16, no. 1, p. 16591, 2026, doi: 10.1038/s41598-026-54104-z.

[21] T. Zieliński, "Ai-Enabled Defense-in-Depth: A Multi-Layered Framework for Countering Uas Threats in Smart Airports," *Sci. J. Silesian Univ. Technol. Ser. Transp.*, 2026, doi: 10.20858/sjsutst.2026.130.17.

[22] X. Wang *et al.*, "A survey on security of UAV swarm networks: Attacks and countermeasures," *ACM Comput. Surv.*, vol. 57, no. 3, pp. 1–37, 2024, doi: 10.1145/3703625.

[23] G. Kou *et al.*, "Intelligent UAV swarm key agreement survey: Systematic taxonomy, cryptographic automaton and quantum resistance," *Internet of Things*, p. 101720, 2025, doi: 10.1016/j.iot.2025.101720.

[24] C. Zhang, H. Wang, Y. Cai, L. Chen, and Y. Li, "TransFusion: multi-modal robust fusion for 3D object detection in foggy weather based on spatial vision transformer," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 9, pp. 10652–10666, 2024, doi: 10.1109/TITS.2024.3420432.

[25] M. Bijelic *et al.*, "Seeing through fog without seeing fog: Deep multimodal sensor fusion in unseen adverse weather," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 11682–11692.

[26] M. Nawaz *et al.*, "Improving autonomous vehicle cognitive robustness in extreme weather with deep learning and thermal camera fusion," *IEEE Open J. Veh. Technol.*, vol. 6, pp. 426–441, 2025, doi: 10.1109/OJVT.2025.3529495.

[27] R. E. Donatus, O. C. Ubadike, M. U. Bonet, and S. D. Iyaghiba, "Automated Aircraft Structural Defect Detection Using Deep Learning and Computer Vision," *Mekatronika J. Mechatronics Intell. Manuf.*, vol. 7, no. 2, pp. 108–123, 2025, doi: 10.15282/mekatronika.v7i2.11787.

[28] P. McEnroe, S. Wang, and M. Liyanage, "A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15435–15459, 2022, doi: 10.1109/JIOT.2022.3176400.

[29] A. Koubaa, A. Ammar, M. Abdelkader, Y. Alhabashi, and L. Ghouti, "AERO: AI-enabled remote sensing observation with onboard edge computing in UAVs," *Remote Sens.*, vol. 15, no. 7, p. 1873, 2023, doi: 10.3390/rs15071873.

[30] W. Zhu and K. Chen, "Real-time object detection for unmanned aerial vehicles based on vision transformer and edge computing," *Sci. Rep.*, 2026, doi: 10.1038/s41598-026-37938-5.

[31] Y. Zidane, J. S. Silva, and G. Tavares, "Jamming and spoofing techniques for drone neutralization: An experimental study," *Drones*, vol. 8, no. 12, p. 743, 2024, doi: 10.3390/drones8120743.

[32] A. A. Hossain, P. M. Kumar, F. Amsaad, and D. Ahner, "Secure and privacy-preserving ai: A zero trust architecture for federated machine learning," in *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*, IEEE, 2025, pp. 1–7. doi: 10.1109/SATC65530.2025.11137026.

[33] Z. Abbas, S. F. Ahmad, A. Anjum, M. H. Syed, S. U. R. Malik, and S. Rehman, "Ensuring zero trust in gdpr-compliant deep federated learning architecture," *Computers*, vol. 14, no. 8, p. 317, 2025, doi: 10.3390/computers14080317.

[34] M. Moustahcine and T. Mazri, "Securing UAV Communication Systems: Architectures, Attacks and Solutions," in *2025 8th International Conference on Networking, Intelligent Systems & Security (NISS)*, IEEE, 2025, pp. 70–76. doi: 10.1109/NISS66502.2025.00019.

[35] Y. Ding, Z. Yang, Q.-V. Pham, Y. Hu, Z. Zhang, and M. Shikh-Bahaei, "Distributed machine learning for UAV swarms: Computing, sensing, and semantics," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7447–7473, 2023, doi: 10.1109/JIOT.2023.3341307.

[36] R. Aljohani, A. Bushnag, and A. Alessa, "Ai-based intrusion detection for a secure internet of things (iot)," *J. Netw. Syst. Manag.*, vol. 32, no. 3, p. 56, 2024, doi: 10.1007/s10922-024-09829-5.

[37] A. A. Laghari *et al.*, "A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture," *Sci. Rep.*, vol. 15, no. 1, p. 26843, 2025, doi: 10.1038/s41598-025-11738-9.

[38] R. E. Donatus, L. O. Uhiah, and C. O. Njoku, "Afropolitan Journals Artificial Intelligence for Aircraft Fault Detection : From Accuracy to Airworthiness through Modality-Aware Analysis , Validation , and Certification

Perspectives Afropolitan Journals," *Afropolitan Journals*, vol. 22, no. 1, pp. 138–171, 2026, doi: 10.62154/ajastr.2026.022.01019.

[39] R. E. Donatus, "Comprehensive Review of Artificial Intelligence for Image- and Signal-Based Nondestructive Testing in Aerospace Structures," *J. Comput. Mech. Manag.*, vol. 4, no. 6, pp. 1–14, 2025, doi: 10.57159/jcmm.4.6.25230.1.

[40] X. Ye, F. Song, Z. Zhang, and Q. Zeng, "A review of small UAV navigation system based on multisource sensor fusion," *IEEE Sens. J.*, vol. 23, no. 17, pp. 18926–18948, 2023, doi: 10.1109/JSEN.2023.3292427.

[41] W. Fang, G. Zhang, Y. Zheng, and Y. Chen, "Multi-task learning for uav aerial object detection in foggy weather condition," *Remote Sens.*, vol. 15, no. 18, p. 4617, 2023, doi: 10.3390/rs15184617.

[42] A. Munir, A. J. Siddiqui, S. Anwar, A. El-Maleh, A. H. Khan, and A. Rehman, "Impact of adverse weather and image distortions on vision-based UAV detection: A performance evaluation of deep learning models," *Drones*, vol. 8, no. 11, p. 638, 2024, doi: 10.3390/drones8110638.

[43] Y. Qu *et al.*, "Elastic collaborative edge intelligence for UAV swarm: Architecture, challenges, and opportunities," *IEEE Commun. Mag.*, vol. 62, no. 1, pp. 62–68, 2023, doi: 10.1109/MCOM.002.2300129.

[44] Z. U. A. Tariq, E. Baccour, A. Erbad, M. Hamdi, and M. Guizani, "RL-based adaptive UAV swarm formation and clustering for secure 6G wireless communications in dynamic dense environments," *IEEE Access*, vol. 12, pp. 125609–125628, 2024, doi: 10.1109/ACCESS.2024.3455250.

[45] Z. Cao, L. Kooistra, W. Wang, L. Guo, and J. Valente, "Real-time object detection based on uav remote sensing: A systematic literature review," *Drones*, vol. 7, no. 10, p. 620, 2023, doi: 10.3390/drones7100620.

[46] M. Latif *et al.*, "AI-based intelligent sensing detection of cybersecurity threats using multimodal sensor data in smart devices," *Sci. Rep.*, vol. 16, no. 1, p. 11091, 2026, doi: 10.1038/s41598-026-40614-3.

[47] P. Zhang, H. Tian, H. Luo, X. Li, and G. Nie, "A hybrid fast inference approach with distributed neural networks for edge computing enabled UAV swarm," *Phys. Commun.*, vol. 60, p. 102129, 2023, doi: 10.1016/j.phycom.2023.102129.

[48] S. M. A. Huda and S. Moh, "Deep reinforcement learning-based computation offloading in UAV swarm-enabled edge computing for surveillance applications," *IEEE Access*, vol. 11, pp. 68269–68285, 2023, doi: 10.1109/ACCESS.2023.3292938.

[49] M. Memarzadeh, A. Akbari Asanjan, and B. Matthews, "Robust and explainable semi-supervised deep learning model for anomaly detection in aviation," *Aerospace*, vol. 9, no. 8, p. 437, 2022, doi: 10.3390/aerospace90804377.

[50] R. E. Donatus and L. O. Uhiah, "Certification And Trustworthy Deployment Of Explainable And Physics-Informed Artificial Intelligence For Aerospace Non-Destructive Testing," *Int. J. Eng. Process. Saf. Res.*, vol. 11, no. 5, pp. 1–30, 2026, doi: 10.70382/caijepsr.v11i5.010.

[51] A. P. Saraf, K. Chan, M. Popish, J. Browder, and J. Schade, "Explainable artificial intelligence for aviation safety applications," in *AIAA Aviation 2020 Forum*, 2020, p. 2881. doi: 10.2514/6.2020-2881.

[52] Y. Wang *et al.*, "Toward realization of low-altitude economy networks: Core architecture, integrated technologies, and future directions," *IEEE Trans. Cogn. Commun. Netw.*, vol. 11, no. 5, pp. 2788–2820, 2025, doi: 10.1109/TCCN.2025.3601015.

[53] J. Chen, X. Li, L. Pan, and S. Liu, "A lyapunov optimization-based online algorithm for scheduling cloud-edge collaborative real-time video stream analytics tasks," *IEEE Internet Things J.*, vol. 12, no. 14, pp. 27713–27727, 2025, doi: 10.1109/JIOT.2025.3563576.

[54] S. N. Ashraf *et al.*, "IoT empowered smart cybersecurity framework for intrusion detection in internet of drones," *Sci. Rep.*, vol. 13, no. 1, p. 18422, 2023, doi: 10.1038/s41598-023-45065-8.

[55] K. Li *et al.*, "FCAT: Frequency-Domain Cross-Attention for All-Weather Multispectral Object Detection in Low-Altitude UAV Security Inspection of Urban and Industrial Areas," *Remote Sens.*, vol. 18, no. 5, p. 826, 2026, doi: 10.3390/rs18050826.

[56] I. Jahan *et al.*, "Alignment-Aware and Reliability-Gated Multimodal Fusion for Unmanned Aerial Vehicle Detection Across Heterogeneous Thermal-Visual Sensors," *arXiv Prepr. arXiv2603.08208*, 2026, doi: 10.48550/arXiv.2603.08208.

[57] D. Dziak *et al.*, "Airport wildlife hazard management system-a sensor fusion approach," *Elektron. ir Elektrotechnika*, vol. 28, no. 3, pp. 45–53, 2022, doi: 10.5755/j02.eie.31418.

[58] S. Lee, Y. Song, and S.-H. Kil, "Feasibility analyses of real-time detection of wildlife using UAV-derived thermal and RGB images," *Remote Sens.*, vol. 13, no. 11, p. 2169, 2021, doi: 10.3390/rs13112169.

[59] B. S. Krishnan *et al.*, "Fusion of visible and thermal images improves automated detection and classification of animals for drone surveys," *Sci. Rep.*, vol. 13, no. 1, p. 10385, 2023, doi: 10.1038/s41598-023-37295-7.

[60] A. Phadke and F. A. Medrano, "Towards resilient UAV swarms—A breakdown of resiliency requirements in UAV swarms," *Drones*, vol. 6, no. 11, p. 340, 2022, doi: 10.3390/drones6110340.

[61] L. Zhou, S. Leng, Q. Liu, and Q. Wang, "Intelligent UAV swarm cooperation for multiple targets tracking," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 743–754, 2021, doi: 10.1109/jiot.2021.3085673.

[62] L. Zhou, S. Leng, Q. Wang, and Q. Liu, "Integrated sensing and communication in UAV swarms for cooperative multiple targets tracking," *IEEE Trans. Mob. Comput.*, vol. 22, no. 11, pp. 6526–6542, 2022, doi: 10.1109/tmc.2022.3193499.

[63] H. Kim and C. Son, "Research on Multi-Stage Battery Detachment Multirotor UAV to Improve Endurance," *Drones*, vol. 9, no. 9, p. 616, 2025, doi: 10.3390/drones9090616.

[64] A. Hamissi and A. Dhraief, "A survey on the unmanned aircraft system traffic management," *ACM Comput. Surv.*, vol. 56, no. 3, pp. 1–37, 2023, doi: 10.1145/3617992.

[65] Z. Liu and Y. Jiang, "Design and implementation for a UAV-based streaming media system," *Ad Hoc Networks*, vol. 156, p. 103443, 2024, doi: 10.1016/j.adhoc.2024.103443.
[66] S. J. McTegg, F. Tarsha Kurdi, S. Simmons, and Z. Gharineiat, "Comparative approach of unmanned aerial vehicle restrictions in controlled airspaces," *Remote Sens.*, vol. 14, no. 4, p. 822, 2022, doi: 10.3390/rs14040822.
[67] V. De Luca, C. Pascarelli, M. Colucci, P. Afrune, A. Corallo, and G. Avanzini, "A platform for safe operations of unmanned aircraft systems in critical areas," *Engineering*, vol. 49, pp. 314–331, 2025, doi: 10.1016/j.eng.2025.02.004.
[68] Q. U. Ain, A. A. A. Jilani, N. A. Butt, S. Ur Rehman, and H. A. Alhulayyil, "Anomaly Detection for Aviation Cyber-Physical System: Opportunities and Challenges," *IEEE Access*, vol. 12, pp. 175905–175925, 2024, doi: 10.1109/ACCESS.2024.3495519.
[69] S. Suseelan, "Explainable AI (XAI) for FAA Certifiable Aviation Systems," *SAMRIDDHI A J. Phys. Sci. Eng. Technol.*, vol. 15, no. 04, pp. 441–451, 2023, doi: 10.18090/samriddhi.v15i04.09.
[70] S. Kargarnovin, C. I. Hernandez, D. Reiners, C. Cruz-Neira, G. Bochenek, and W. Karwowski, "From testbeds to high-stakes work: a review of Human-AI teaming domains and teaming factors," *Front. Robot. AI*, vol. 13, p. 1733942, 2026, doi: 10.3389/frobt.2026.1733942.
[71] A. Mohsin, H. Janicke, A. Ibrahim, I. H. Sarker, and S. Camtepe, "A unified framework for human ai collaboration in security operations centers with trusted autonomy," *arXiv Prepr.*, 2025, doi: 10.48550/arxiv.2505.23397.
[72] H. Shakhatreh, A. H. Sawalmeh, A. L. A. Al-fuqaha, S. Member, and Z. Dou, "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019, doi: 10.1109/ACCESS.2019.2909530.
[73] P. Aposporis, "A review of global and regional frameworks for the integration of an unmanned aircraft system in air traffic management," *Transp. Res. Interdiscip. Perspect.*, vol. 24, p. 101064, 2024, doi: 10.1016/j.trip.2024.101064.
[74] M. A. Bonsu and P. Akekudaga, "Enhancing Critical Infrastructure Security: Addressing Cybersecurity Risks and Regulatory Gaps in AI-Enabled IoT Systems," in *2025 IEEE 16th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, 2025, pp. 627–633. doi: 10.1109/UEMCON67449.2025.11267559.
[75] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the internet of things in artificial intelligence era: A comprehensive survey," *IEEE access*, vol. 12, pp. 25469–25490, 2024, doi: 10.1109/ACCESS.2024.3365634.
[76] M. Fisher, V. Mascardi, K. Y. Rozier, B.-H. Schlingloff, M. Winikoff, and N. Yorke-Smith, "Towards a framework for certification of reliable autonomous systems," *Auton. Agent. Multi. Agent. Syst.*, vol. 35, no. 1, p. 8, 2021, doi: 10.1007/s10458-020-09487-2.
[77] R. Zrelli *et al.*, "Integrating formal methods and automated tools for DO-178C compliance in UAV software," *Inf. Softw. Technol.*, vol. 194, p. 108068, 2026, doi: 10.1016/j.infsof.2026.108068.
[78] G. R. Bhat *et al.*, "Autonomous drones and their influence on standardization of rules and regulations for operating–A brief overview," *Results Control Optim.*, vol. 14, p. 100401, 2024, doi: 10.1016/j.rico.2024.100401.
[79] S. Javed *et al.*, "State-of-the-art and future research challenges in UAV swarms," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19023–19045, 2024, doi: 10.1109/JIOT.2024.3364230.
[80] M. Almutairi and F. T. Sheldon, "IoT–cloud integration security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, 2025, doi: 10.3390/electronics14071394.

BIOGRAPHIES OF AUTHORS

Rexcharles Enyinna Donatus holds dual master's degrees in aerospace Vehicle Design from the Air Force Institute of Technology (AFIT), Nigeria, and Information Technology from the National Open University of Nigeria (NOUN). He is currently a PhD candidate in Artificial Intelligence at the Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, with research focused on multimodal deep learning and affective computing. Since 2020, he has served as a Lecturer in the Department of Aerospace Engineering at AFIT, where he leads research at the intersection of artificial intelligence and aerospace applications. His scholarly contributions span over 10 peer-reviewed journal and conference publications, with research interests covering deep learning, computer vision, multimodal fusion systems, UAV detection, and intelligent control for autonomous aerospace operations. He can be contacted at rexcharles.donatus@gmail.com.