future internet

MDPI

Review

Building Trust in Autonomous Aerial Systems: A Review of Hardware-Rooted Trust Mechanisms

Sagir Muhammad Ahmad, Mohammad Samie and Barmak Honarvar Shakibaei Asli *

Faculty of Engineering and Applied Sciences, Cranfield University, Cranfield MK43 0AL, UK; sagir.ahmad@cranfield.ac.uk (S.M.A.); m.samie@cranfield.ac.uk (M.S.)
* Correspondence: barmak@cranfield.ac.uk

Abstract

Unmanned aerial vehicles (UAVs) are redefining both civilian and defense operations, with swarm-based architectures unlocking unprecedented scalability and autonomy. However, these advancements introduce critical security challenges, particularly in location verification and authentication. This review provides a comprehensive synthesis of hardware security primitives (HSPs)—including Physical Unclonable Functions (PUFs), Trusted Platform Modules (TPMs), and blockchain-integrated frameworks—as foundational enablers of trust in UAV ecosystems. We systematically analyze communication architectures, cybersecurity vulnerabilities, and deployment constraints, followed by a comparative evaluation of HSP-based techniques in terms of energy efficiency, scalability, and operational resilience. The review further identifies unresolved research gaps and highlights transformative trends such as AI-augmented environmental PUFs, post-quantum secure primitives, and RISC-V-based secure control systems. By bridging current limitations with emerging innovations, this work underscores the pivotal role of hardware-rooted security in shaping the next generation of autonomous aerial networks.

Keywords: unmanned aerial vehicle UAV; communication; harware security primitives

check for updates

Academic Editor: Christos Kalloniatis

Received: 16 September 2025
Revised: 1 October 2025
Accepted: 7 October 2025
Published: 10 October 2025

Citation: Ahmad, S.M.; Samie, M.; Honarvar Shakibaei Asli, B. Building Trust in Autonomous Aerial Systems: A Review of Hardware-Rooted Trust Mechanisms. *Future Internet* **2025**, *17*, 466. https://doi.org/10.3390/fi17100466

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

UAVs, often referred to as drones, have transitioned from being tactical military tools to essential resources in a variety of civilian fields, such as infrastructure surveillance, precision farming, and emergency response [1–3]. Their capability to operate in dangerous or isolated locations makes them especially valuable for assessing critical infrastructure more effectively than conventional techniques [4,5]. The advent of swarm-based UAV systems represents a notable progress in drone technology [6]. These systems facilitate scalable, fault-tolerant, and cooperative multi-agent operations, providing improved coverage, adaptability, and efficiency for dynamic missions such as inspecting power lines, pipelines, precision agriculture, and bridges [7–9]. As shown in Figure 1, swarms of intelligent, collaborative drones are increasingly utilized in industrial and emergencies situations, where they can sustain real-time communication and data transfer even in regions without ground-based infrastructure [10,11].

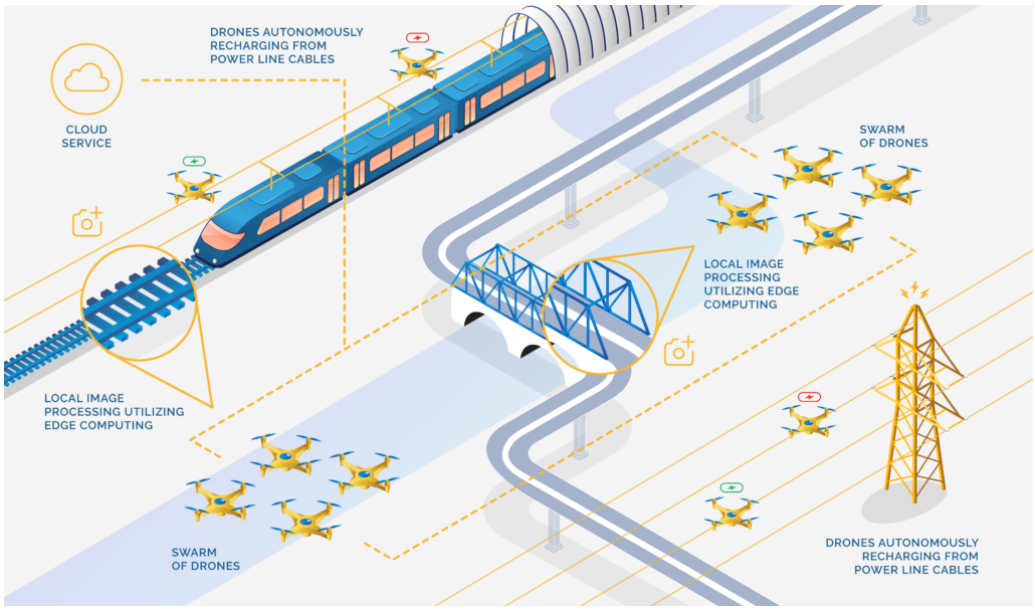

Figure 1. Swarm drones operation [12].

However, these advancements present complex security challenges with the rise in autonomous and interconnected UAV swarms [13]. Ensuring secure communication, strong authentication, and reliable location verification is crucial, particularly in adversarial or resource-limited environments [11]. UAVs are vulnerable to cyber threats, such as data breaches, unauthorized access, and hostile interference, which can jeopardize both the drones and the sensitive information they gather [12,14]. Erroneous or manipulated data can result in misguided evaluations and potentially disastrous failures, especially when assessing safety-critical infrastructure [9,15]. To address these issues, this review emphasizes hardware-based security solutions that provide tamper resistance and energy efficiency, essential requirements for UAV swarm operations [16]. It specifically analyzes three types of HSPs: PUFs, TPMs, and Secure Enclaves, including Blockchain-integrated systems [17–19]. The literature examined spans from 2016 to 2024 and includes peer-reviewed articles from IEEE, Springer, and Elsevier, selected for their relevance to UAV swarm security and their contributions to authentication and location verification at the hardware level.

This review is structured to provide a comprehensive understanding of hardware-based security mechanisms in UAV systems, with a focus on their applicability across diverse operational environments. The paper is organized as follows: Section 2 summarizes related work based on secure communication and data integrity. The broad spectrum of UAV applications, including disaster response, military reconnaissance, urban logistics, infrastructure inspection, and environmental monitoring, are discussed in Section 3 as drone applications. Section 4 describes the typical communication stack in UAV systems, including ground control links, inter-drone communication, flying ad-hoc networks (FANETs), and satellite backhaul. Cybersecurity Challenges in UAVs reviews the main cybersecurity threats facing UAVs, such as GPS spoofing, signal jamming, relay attacks, malware injection, unauthorized access, and the need for hardware-based solutions detailed in Section 5. HSPs Provides an in-depth review of key hardware security primitives, including PUFs, True Random Number Generators (TRNGs), TPMs, and tamper-resistant hardware. Their mechanisms, strengths, and limitations are discussed in Section 6. Section 7 covers emerging methods for enforcing location-aware policies and compliance, including distance-bounding, delay-based decryption, AI-driven PUFs, and blockchain-based attestation. Real-world challenges in securing UAVs across military,

disaster, and urban environments, assessing HSP suitability and current limitations are examined in Section 8. Key findings and open research challenges, such as robust PUF design, scalable distance-bounding, and lightweight blockchain consensus, are discussed along with future directions in post-quantum security and AI-integrated hardware primitives, as summarized in Section 9. The key contributions of this review are summarized as follows:

- Reviews HSPs (PUFs, TPMs, TRNGs, tamper-resistant modules) for UAV swarm security.
- Provides a comparative evaluation of HSP-based techniques in terms of energy efficiency, scalability, and operational resilience.
- Analyzes hardware–software trade-offs and advocates hybrid security architectures.
- Links UAV applications to context-sensitive security needs in urban, rural, and military environments.
- Highlights emerging technologies: AI-augmented PUFs, blockchain-based attestation, and RISC-V secure architectures.
- Summarizes attack surfaces and maps them to hardware/software countermeasures.
- Identifies open research challenges and outlines future directions, including post-quantum security and AI-integrated primitives.

2. Related Work

Drone security is becoming an increasingly vital aspect of drone operations. Many drones were developed without considering security features, functioning in open connections and variable environments [20,21]. Consequently, safeguarding privacy and security is crucial in UAV-assisted networks, as these UAVs are susceptible to attacks and can be easily compromised by intruders [22]. Figure 2 shows a UAV-assisted communication system across space, air, and ground layers. Designed for emergency coordination, it highlights vulnerabilities in data links that are exposed to interception or disruption. The use of low Earth orbit (LEO) satellites, UAVs, and ground stations underscores the need for strong security protocols [23]. These structural features also apply to the broader Internet of Drones (IoD), which faces similar challenges due to the lack of standardized security frameworks [22].

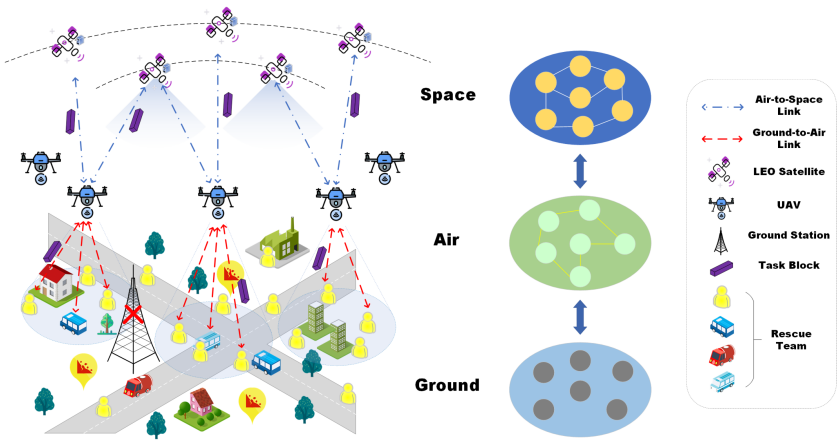

Figure 2. Multi-layered UAV communication system showing interactions between LEO satellites, drones, and ground units. The diagram highlights potential vulnerabilities across air-to-space and ground-to-air links in UAV-assisted networks [23].

Furthermore, the emerging Internet of Drones (IoD) ecosystem lacks established security protocols, resulting in inconsistent practices and difficulties in ensuring robust security measures [24]. The swift advancement of drone technology has led to various security strategies aimed at protecting drones and their operations; drone security encompasses the use of Radio Frequency (RF) signals emitted by drones during their communication with

ground controllers [25]. Nevertheless, there remains considerable ambiguity regarding the relationship between security measures in drone technology, such as encryption, authentication, intrusion detection, and secure communication protocols [26–28]. Bansal et al. discuss the security approach concerning the limited resources of drones, emphasizing that as drones increasingly depend on software and communication networks, cybersecurity becomes critical [29]. Techniques such as intrusion detection systems (IDS) and firewalls are employed to monitor and protect against cyber threats [30]. Drone security is a crucial area in UAV operations, as drones frequently operate in open networks with fluctuating topologies, rendering them susceptible to intrusions and attacks [22]. The IoD ecosystem complicates security initiatives due to the lack of standardized protocols, which results in inconsistent practices and challenges in achieving thorough security [31]. Several strategies have been suggested to mitigate these vulnerabilities, including the application of RF signals for intrusion detection [32], encryption [33,34], authentication schemes [35], and secure communication protocols [36,37]. However, as pointed out by [15], significant uncertainty persists regarding the integration of encryption, authentication, and secure communication protocols. Ref. [30] highlights the necessity of cybersecurity measures such as IDS and algorithms to combat cyber threats. Additionally, optimizing energy consumption is vital for prolonging UAV operational time, as illustrated by [38], who proposed a methodology for calculating UAV energy levels based on path length and operational parameters. As drones become increasingly efficient and prevalent across various applications, including data collection, concerns about privacy and adherence to regulations are gaining importance [39,40]. Ensuring accurate and reliable data collection remains a significant focus in the literature. High-resolution drone cameras, as noted by [41], facilitate precise measurements of pedestrian and bicycle traffic, thereby enhancing data integrity. Gillan et al. further illustrates how innovative drone workflows can markedly boost efficiency, cutting down manual labor by an estimated 111 workdays in rangeland monitoring. These advancements not only streamline large-scale data collection but also illustrate drones' potential to link environmental data with management decisions [42]. However, while these technologies enhance efficiency and accuracy, challenges such as data storage, processing complexity, and regulatory compliance remain areas for further exploration. Beyond data collection, privacy concerns remain a significant challenge in drone-based data collection, particularly regarding the inadvertent capture or disclosour [43]. Tu et al. emphasize the need for clear regulatory guidelines to govern the types of information drones can collect and share, ensuring compliance with privacy and security standards [43]. Similarly, Kim underscores the importance of adhering to local regulations when drones operate in public spaces, as failing to mitigate privacy risks—especially concerning identifiable information—can undermine public trust and ethical integrity [41]. Several surveys have addressed UAV security from a general perspective, often focusing on software-based solutions such as encryption, IDS, and anomaly detection [44]. For instance, some works have reviewed lightweight cryptographic protocols for UAVs, while others have explored secure routing in FANETs [45,46]. However, these approaches often fall short in disconnected or adversarial environments where software defenses can be bypassed or disabled.

Bibliometric Assessment of Secure Drone Communication

To assess evolving research trends in drone security, a bibliometric analysis was performed using Scopus-indexed journal articles. The search included the keywords 'drone', 'security', 'communication', and 'integrity', yielding 578 documents. Keyword co-occurrence mapping was performed using VOSviewer 1.6.20.0, with the resulting visualization shown in Figure 3.

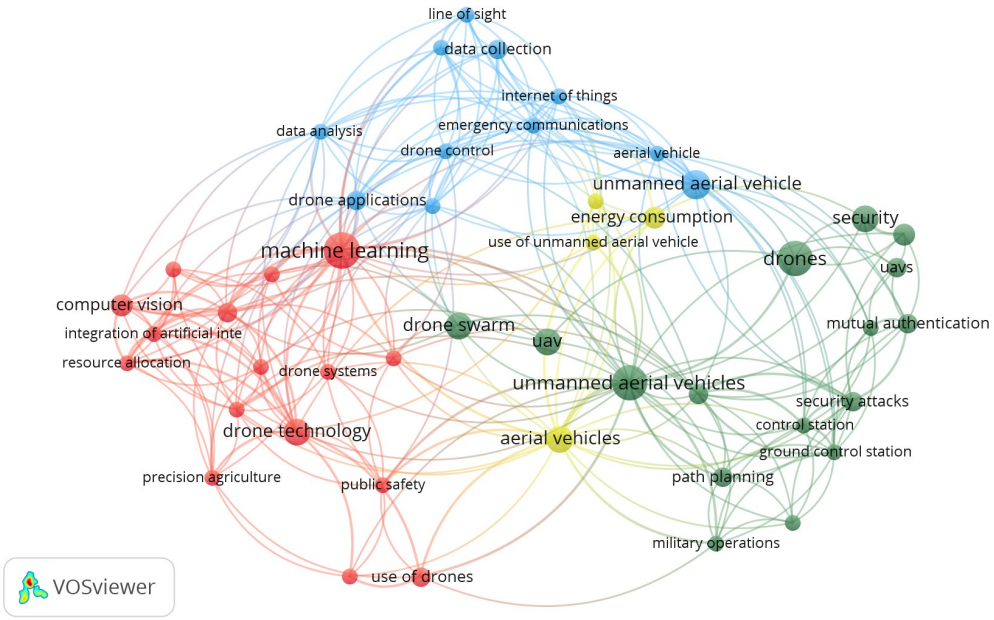

Figure 3. The co-occurrence map reveals four primary clusters representing distinct research trajectories.

The co-occurrence map reveals four primary clusters representing distinct research trajectories as follows:

- The red cluster, centered on terms such as 'machine learning', 'computer vision' and 'drone technology', suggests extensive integration of AI into UAV applications.
- The blue group highlights terms such as 'data collection', 'Internet of Things' and 'emergency communications', indicating a focus on real-time data dissemination and telemetry.
- Green clusters 'mutual authentication', 'security attacks', 'control station' and 'ground control station', pointing toward security-centric research in swarm coordination and secure routing.
- The yellow group, which includes 'energy consumption' and 'use of unmanned aerial vehicles', emphasizes the challenge of balancing computational security overhead with resource constraints in real-world deployments.

Notably, the co-occurrence of "data analysis" with "mutual authentication"—and the relative underrepresentation of "use of drones"—indicates that modern research emphasizes data-centric integrity techniques over basic drone operations. Blockchain-based solutions continue to gain traction due to their tamper-resistance and decentralized ledger characteristics [47]. For instance, the Anonymous Secure Messaging Token Protocol (ASMTP) [48] introduces token-based authentication mechanisms and integrity-preserving communication within UAV swarms, combining formal verification with lightweight encryption. In summary, the literature reflects an increasing convergence between machine learning, energy-efficient cryptographic techniques, and protocol-based authentication, with emerging attention to scalable trust frameworks such as blockchain and PUF-based identity verification [49,50]. In contrast, this review emphasizes hardware-assisted security, which provides stronger guarantees through physical tamper resistance and device-level uniqueness [17]. While a few recent studies have touched on PUFs or TPMs in UAVs, they often do so in isolation or without a comparative framework [16,51–53].

Our contribution is to synthesize these developments, compare their trade-offs, and highlight their applicability to location verification, a critical but underexplored aspect of UAV swarm security.

3. Application of Swarm Drones

The swift advancement of drone technology has considerably broadened the range of UAVs, especially swarm drones, across numerous mission-critical and commercial uses [54–56]. Swarm drones are increasingly utilized in situations such as search and rescue operations, autonomous deliveries, precision farming, and environmental observation [57–59]. UAVs are now embedded in a wide spectrum of applications—including security and surveillance, mapping and farming, filming and inspection, and logistical tasks such as delivery and crop spraying—highlighting their versatility and growing significance across industries [60]. These applications take advantage of swarm intelligence, allowing for distributed decision-making, adaptive control, and collaborative task execution [61,62]. Nevertheless, their use in regulated settings requires strict assurances regarding device authenticity, data origin, and spatial integrity [3].

3.1. Functional Role of the Application Layer

The application layer is vital for the operations of drone swarms, serving as the foundation for reasoning, decision-makingking, and task coordination [5,13]. It encompasses a mission decision component that assigns tasks and formulates collaborative directives to achieve the overarching objectives [18,63]. This layer guarantees that swarm drones can flexibly adjust to mission demands and environmental changes, making them suitable for intricate tasks in real time [30,64].

3.2. Sector-Specific Applications

3.2.1. Agriculture and Environmental Monitoring

In the realm of agriculture, drones have become essential instruments for precision farming [65,66]. They facilitate real-time crop observation, targeted pesticide distribution, and soil health evaluations through multispectral imaging [67,68]. These functionalities not only improve yield optimization, but also encourage sustainable practices by reducing resource waste [65]. In environmental monitoring, sensor-equipped drones are used to evaluate air quality, identify water contamination, and assist in conservation initiatives [69].

3.2.2. Construction and Infrastructure

Drones are extensively utilized in construction and infrastructure for surveying, mapping, and monitoring [70,71]. UAVs equipped with high-resolution cameras and LiDAR sensors offer precise 3D models and real-time updates, boosting safety and operational efficiency [72,73]. Their capability to access difficult or dangerous locations makes them well-suited for inspecting bridges, tunnels, and other vital structures [74].

3.2.3. Logistics and Urban Mobility

In logistics, drones are transforming last-mile deliveries by reaching isolated or congested regions, thereby shortening delivery times and reducing operational costs [43]. This trend is especially prominent in the delivery and logistics sector, which is anticipated to grow at a CAGR of 14.3% from 2025 to 2030 [75]. As the reliability of swarms enhances, drones are expected to be pivotal in urban air mobility and coordinated delivery systems [7].

3.2.4. Disaster Response and Humanitarian Aid

Drones have demonstrated their immense value in humanitarian efforts and disaster relief operations [76,77]. Their ability to quickly assess damage, find survivors, and trans-

port crucial supplies to locations difficult to reach has been evidenced in various emergency situations [78,79]. Throughout the COVID-19 crisis, drones were deployed in more than 18 nations to carry medical supplies and testing samples, underscoring their effectiveness in managing crises [80,81].

3.2.5. Entertainment and Media

The world of entertainment has adopted drones for aerial photography, allowing for the capture of distinctive viewpoints and vibrant visuals [82]. Their nimbleness and accuracy render them perfect for live performances, film production, and engaging media experiences [83].

3.3. Environmental Context and Operational Considerations

The operational environment significantly influences UAV swarm security strategies, with urban, rural, and military settings presenting distinct challenges [84]. Urban airspaces, characterized by dense wireless networks and strict privacy regulations, face risks such as GPS spoofing, WiFi hijacking, and data interception; these can be mitigated through blockchain-based attestation for decentralized trust, AI-driven intrusion detection, and strong encryption for privacy compliance [41,85,86]. In rural and remote areas, where connectivity is sparse and energy efficiency is critical, lightweight primitives like PUF-based authentication and optimized TRNGs enable secure key generation without persistent storage, reducing computational overhead [87–89]. Military and high-assurance contexts demand resilience against jamming, spoofing, and physical tampering, requiring tamper-resistant hardware, TPM-based secure boot and attestation, distance-bounding protocols for location verification, and integration with encrypted channels and anti-jamming techniques to ensure mission continuity under adversarial conditions [90–92].

3.4. Market Trends and Economic Outlook

The international drone market is witnessing swift expansion, propelled by technological advancements and growing business utilization [93]. As per [94], the commercial drone segment is anticipated to reach $51.32 billion by 2030, with a compound annual growth rate (CAGR) of 17.9%. Similarly, refs. [95,96] forecasts an increase in the overall UAV market from $26.12 billion in 2025 to $40.56 billion by 2030. National estimates, such as those from the Indian Ministry of Civil Aviation, predict the domestic drone sector will achieve INR 120–150 billion ($1.5–1.9 billion) by 2026 [97].

3.5. Technological Advancements and Future Directions

The incorporation of artificial intelligence (AI) and machine learning (ML) is further advancing drone functionalities [1,98]. Drones equipped with AI can independently traverse intricate environments, identify irregularities, and process extensive data in real time [99,100]. This evolution is exemplified in Figure 4, which illustrates a UAV mobile edge computing (MEC) network architecture where AI-enabled drones interact with ground users, collaborate with one another, and offload data to edge and cloud infrastructures. Such architectures highlight the growing role of distributed intelligence and real-time analytics in aerial networks [101].

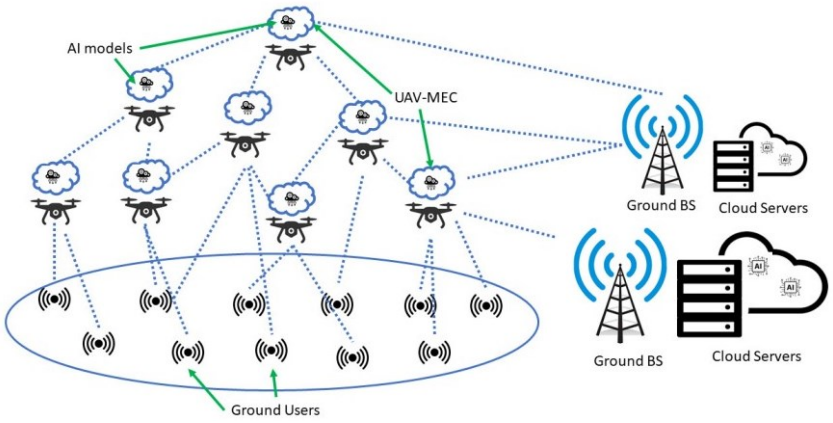

Figure 4. UAV-MEC network architecture showing AI-enabled drones interacting with ground users and offloading data to edge and cloud servers for real-time data collection, processing, and decision-makingking [101].

These developments are paving the way for novel applications in infrastructure assessment, environmental surveillance, and smart city initiatives [102,103]. As the reliability of drone swarms and their mission coordination enhances, their usage is anticipated to broaden into more intricate areas, such as urban air transportation, synchronized delivery systems, and extensive agricultural monitoring [104,105]. For instance, in intelligent seaports, drones assist in reducing fuel usage and decreasing vessel navigation time, leading to significant cost reductions and enhanced sustainability [69]. Beyond the integration of AI and MEC, recent studies demonstrate the practical application of UAV technologies in advanced communication and security frameworks. For example, He et al. illustrates how aerial autonomous vehicles can enhance vehicular platooning in the Internet of Vehicles (IoV) enhanced by non-Orthogonal Multiple Access (NOMA) through optimized resource allocation and low-latency communication, highlighting the role of UAVs in intelligent transportation systems [106]. Similarly, Ahmed et al. explores the use of reconfigurable intelligent surfaces (RIS) to strengthen the security of the physical layer, offering promising directions for secure and energy-efficient UAV communication. These examples underscore the growing convergence of UAVs with next-generation wireless technologies and the need for hardware-based trust mechanisms to complement such innovations [107].

4. Communication Architectures

Communication strategies within drone swarms can be divided into autonomous and managed systems. Autonomous systems depend on local interactions among drones, reducing the necessity for centralized communication [108]. This decentralized model is beneficial in expansive or fluid environments with restricted connectivity [78]. In contrast, managed systems rely on a central unit where a leading drone directs commands to the swarm [109]. Although effective for orchestrated actions, this approach is susceptible to delays and interruptions, especially in large-scale operations [18]. Architectures of drone swarm networks are categorized into infrastructure-supported and FANET frameworks [110]. Figure 5 illustrates a hybrid architecture where clustered UAVs communicate via Bluetooth and relay data to a ground station using WiFi, exemplifying both infrastructure-supported and FANET characteristics [46].

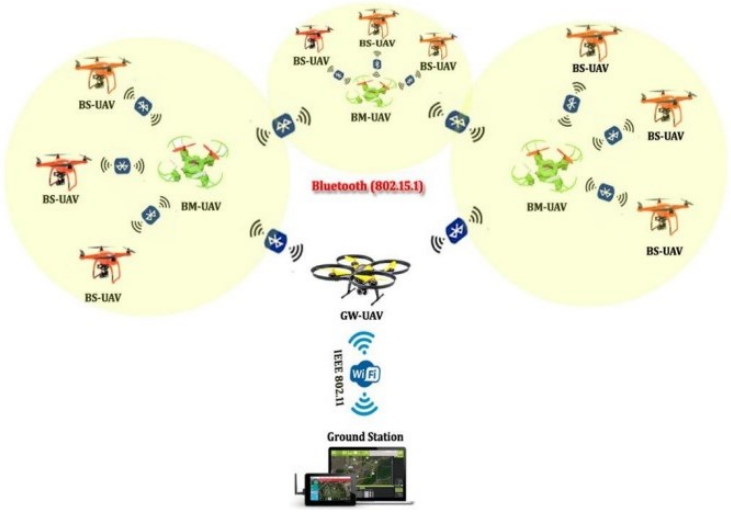

Figure 5. Hierarchical UAV communication network divided into clusters. Each cluster includes a Base Station UAV (BS-UAV), multiple Base Member UAVs (BM-UAVs), and a Gateway UAV (GW-UAV). Bluetooth (802.15.1) is used for intra-cluster communication, while WiFi (IEEE 802.11) connects the GW-UAV to the ground station [46].

As depicted in Figure 6, drones communicated with the ground station and satellites. Infrastructure-based systems rely on a central control unit for communication and task management, making them ideal for inspections and similar tasks [93,111]. However, their scalability is limited by the processing power and bandwidth of the central unit [21]. In contrast, FANETs discard the necessity for a central unit, allowing for direct communication between drones. In contrast, FANETs discard the necessity for a central unit, allowing for direct communication between drones.

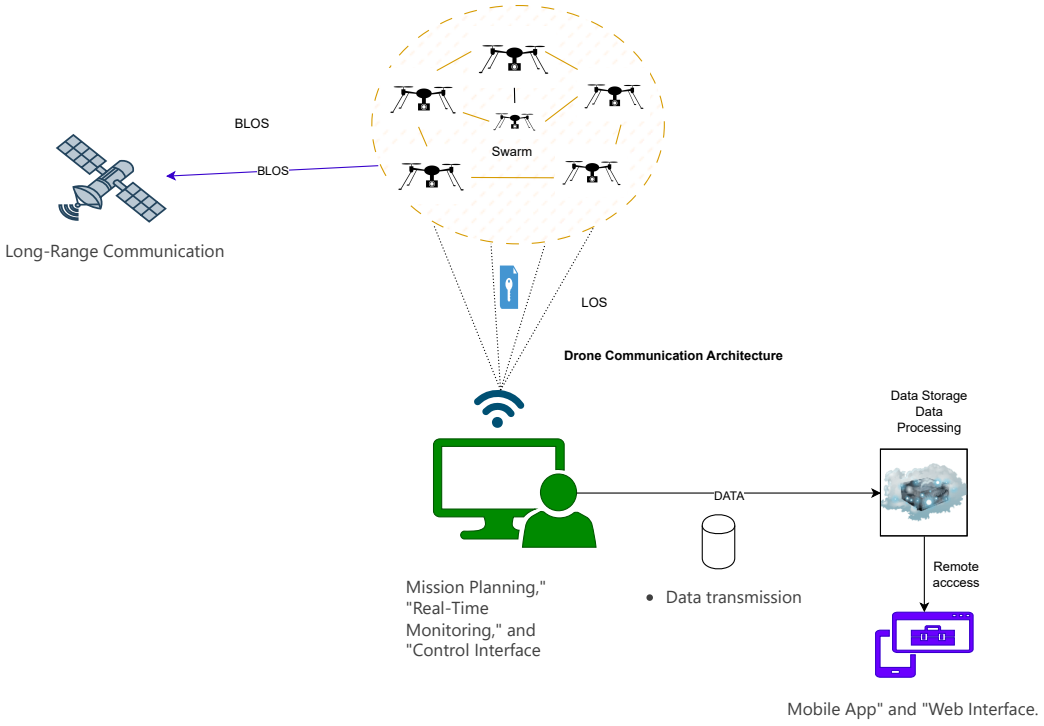

Figure 6. Drone communication architecture.

This decentralized framework provides enhanced scalability and resilience, as the swarm can dynamically adapt to node failures [110]. Nonetheless, FANETs encounter notable obstacles, such as managing dynamic topologies, varying speeds, and

three-dimensional movement, which complicate the design of protocols and network management [13]. Despite the advantages of scalability and resilience in FANETs, ensuring robust connectivity in challenging or dynamic environments remains a considerable hurdle (trust establishment) [108]. Drones are susceptible to failures, and their reliance on wireless communication makes the swarm vulnerable to security threats, such as packet loss attacks and weaknesses in routing protocols [21].

To tackle these challenges, simulation is crucial in the development and evaluation of drone communication systems [112]. Simulation environments offer a controlled space for designing and validating communication protocols, facilitating quick prototyping and minimizing the risk of errors in real-world applications [113,114]. These tools are vital for modeling network behavior, assessing fault tolerance, and optimizing routing methods prior to physical implementation [115–117]. Additionally, the incorporation of AI into drone technology has greatly improved swarm communication capabilities [103]. AI-driven autonomy enables drones to function more efficiently in dangerous or unpredictable situations, while real-time analysis enhances decision-making and coordination within the swarm [104,118]. AI also facilitates adaptive communication methods, such as dynamic routing and load balancing, which are essential in decentralized networks like FANETs [117]. However, the integration of AI brings forth new challenges, including substantial computational requirements and ethical issues surrounding autonomous decision-making [119].

4.1. Communication Protocols

Communication Protocols In drone swarm operations, secure and effective communication is crucial for coordination and resilience against cyber and physical threats [120]. The ever-changing characteristics of FANETs, marked by frequent topology alterations and limited communication range, pose unique challenges [30]. Considering the energy limitations of UAVs—balancing wireless communication, data processing, and flight control—energy-efficient algorithms are essential. For instance, the Resilient UAV Path Optimization Algorithm (RUPOA) reduces energy usage by optimizing communication distances [38]. To facilitate these operations, various communication protocols have been established. Figure 7 presents a secure communication protocol for drone swarm operations, highlighting the interactions among the Certificate Authority (CA), Ground Control Station (GCS), user, master drone, and other drones. It shows how certificates, keys, and mission credentials are exchanged over secure and insecure channels to ensure authentication and mission integrity [90].

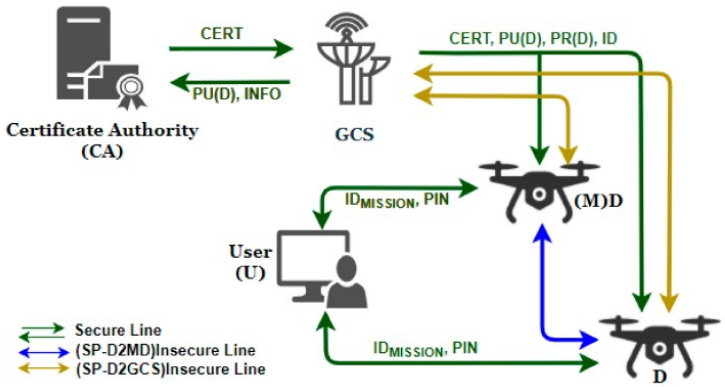

Figure 7. The protocol demonstrates the flow of credentials and keys among the CA, GCS, user, master drone, and other drones. Green arrows indicate secure communication channels, while blue and yellow arrows represent insecure links. Key elements include certificate issuance (CERT), public/private keys (PU(D), PR(D)), and mission credentials (IDMISSION, PIN) [90].

Among the most widely utilized are message queuing telemetry transport (MQTT), constrained application protocol (CoAP), and long range wide area network (LoRaWAN), each presenting specific advantages and drawbacks [100]. For example, the Reputation-based Announcement (RA) scheme improves message reliability but lacks encryption and adaptability [36]. Conversely, the ASMTP improves confidentiality and prevents replay attacks, though it faces scalability and latency challenges [48]. These developments underscore the need for continued innovation in communication protocols that balance security, efficiency, and scalability in UAV swarm environments.

4.1.1. Performance Evaluation of Communication Algorithms

As part of the assessment of communication protocols for UAV networks, execution time acts as a crucial performance metric, especially in latency-sensitive environments where quick reactions are vital [121]. In swarm-based UAV systems, where real-time coordination and data sharing are essential, the computational efficiency of security and communication algorithms greatly affects operational effectiveness [45]. Recent comparative analyses have examined the execution times of various algorithms utilized in UAV networks. Among these, the radio-frequency identification (RFID) with PUF method displayed the highest latency, with execution times nearing 16,000 microseconds [122]. While this technique provides strong security through hardware-based authentication, its considerable computational demands raise concerns regarding its practicality in resource-limited or time-sensitive situations [74]. To provide additional context, these execution times were derived from benchmark studies using embedded platforms such as Raspberry Pi 4 (1.5 GHz CPU, 4 GB RAM) and simulated environments (MATLAB 2018a Simulink and NS-3) for protocols like ASMTP, RFID + PUF, and blockchain-based schemes. The reported values represent average execution times under standard cryptographic libraries and default parameter settings as documented in [122–124]. This clarification ensures transparency regarding the experimental conditions and supports the validity of the performance metrics presented. In contrast to the high-latency RFID with PUF, algorithms such as Salsa, ASMTP, and derived blockchain (DB) showed significantly reduced execution times [33,48]. Their lightweight characteristics and quick processing make them ideal for embedded systems and internet of things (IoT) driven UAV applications, where energy efficiency and real-time reactivity are crucial [102]. These algorithms manage to achieve a favorable balance between security and performance, making them suitable for swarm coordination and dynamic data interchange. Other methods, including identity and aggregate signature (IAS), drone-to-drone (D2D) PUF, grouped authentication (GA), bio-inspired optimized leader election (BOLD), RUPOA, hyperelliptic curve cryptography (HECC) and random oracle model (ROM), and MECC, fall into a moderate execution time range [35,38,87,123–126]. These approaches may serve as effective alternatives for general UAV applications, providing a compromise between computational efficiency and cryptographic strength. For example, RUPOA incorporates routing optimization, while D2D PUF combines device-level authentication with moderate latency. As illustrated in Figure 8, the comparative execution times highlight the necessity of choosing algorithms not solely based on their security capabilities but also on their computational efficiency. In UAV swarm networks, where timing, energy, and processing limitations are crucial, this dual focus ensures that communication protocols are both secure and operationally feasible [10]. These insights guide protocol selection in UAV swarm design, where the need for mission-critical responsiveness must be balanced with secure communication.

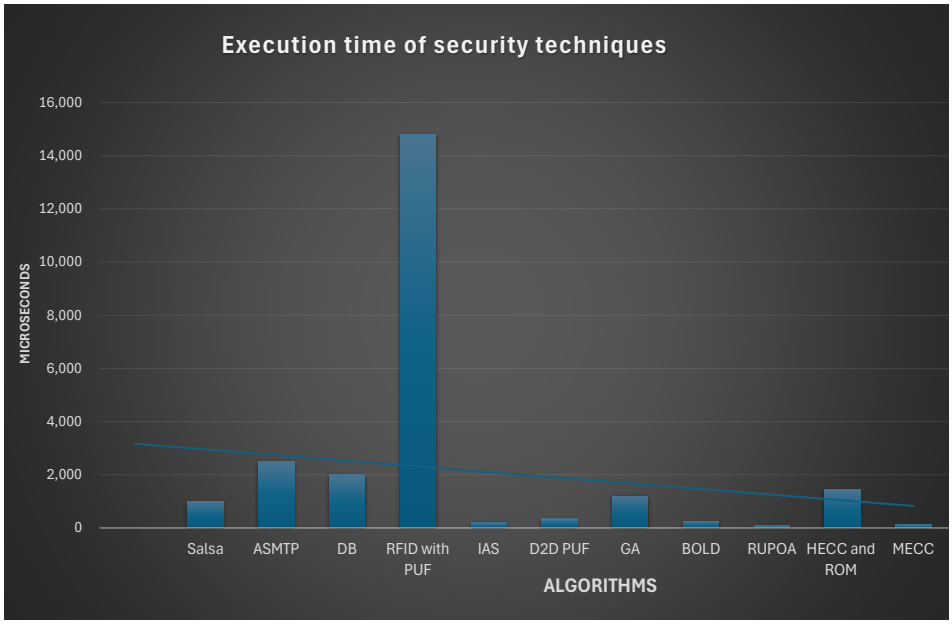

Figure 8. Execution time of communication algorithms.

4.1.2. Authentication and Security Mechanism

As UAV networks continue to grow in complexity and scale, the demand for robust, lightweight, and scalable authentication protocols becomes increasingly important [87]. These protocols safeguard communication between drones and ground stations while facilitating autonomous coordination in swarm- and edge-based scenarios [84]. A variety of authentication methods have been suggested, many of which utilize lightweight cryptographic approaches such as Elliptic Curve Cryptography (ECC) and PUFs [127,128]. These methods are particularly apt for drones with limited computational and energy capabilities, allowing for mutual authentication, session key generation, and data confidentiality with minimal overhead [129]. Blockchain-based systems have also been proposed to provide decentralized trust and integrity in IoD ecosystems, although they may introduce latency and scalability issues as drone density increases [130].

Certain protocols are designed specifically for situations involving post-disaster recovery or compromised infrastructure [93]. Proxy delegation methods enable drones to verify one another within mesh networks without needing centralized oversight, while collective authentication techniques allocate roles (such as guard, network, and operational units) to facilitate scalable, role-based access control [87,131]. Recent protocols in drone detection leveraging RF signal analysis and ML report authentication times in the microsecond range and exhibit high detection accuracy [32]. Despite these promising performance metrics, many approaches have been validated solely through simulations or rely on static parameter configurations, which significantly limit their applicability in dynamic, real-world environments [132,133]. Furthermore, several protocols lack comprehensive threat modeling, leaving critical vulnerabilities unaddressed [114]. Others fail to account for energy consumption and communication overhead, particularly in large-scale or resource-constrained deployments, thereby raising concerns about scalability and operational efficiency [134].

Recent developments feature fog/edge-based mutual authentication protocols that do away with the necessity for ground station involvement. These systems provide efficient key management and automatic key revocation, though they might create single points of failure [135]. An overview of a UAV network architecture emphasizing authentication and security mechanisms, including the role of a Registration Authority (RA), Ground

Station Servers (GSS), and UAVs, as well as the handover process for maintaining secure connectivity during mobility is provided in Figure 9 [26].

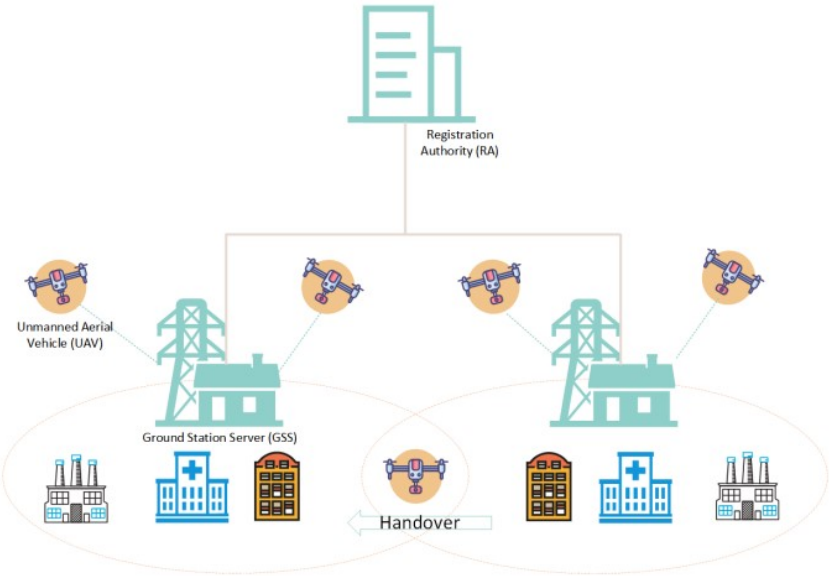

Figure 9. The architecture illustrates interactions among the RA, GSS, and UAVs, highlighting registration, authentication, and secure handover during mobility [26].

Another significant protocol [135], the Lightweight Trustworthy Message Exchange (LTME), facilitates secure communication between drones with minimal overhead and robust resistance to impersonation and replay attacks. However, its simplified version (sLTME) does not include encryption, rendering it susceptible to eavesdropping [36]. Overall, the field of UAV authentication protocols showcases a tension between advancement and ongoing challenges [136]. Future studies should aim at merging these protocols into cohesive, adaptive frameworks that cater to various UAV applications while upholding high standards of security, efficiency, and scalability [90,137]. Table 1 outlines a selection of recent authentication and security protocols for UAV networks, emphasizing their fundamental approaches, advantages, drawbacks, and performance metrics.

Table 1. Record of surveyed papers based on authentication protocols.

Ref.	Approach	Solutions	Limitations	Performance
[34]	Sparse autoencoder + micro-Doppler	5G-based auth in urban setting	Needs LoS & training; costly	99% precision
[33]	Esalsa encryption for military ops	High error sensitivity results	Not integrated; pre-set params	1.0 ms cipher time
[124]	ECC in WSN with UAV sinks	Mutual auth & key agreement	Informal security analysis	Low energy & bandwidth use
[80]	Proxy signature delegation	Post-disaster mesh auth	Unclear threats & timing	Reduced auth time
[122]	RFID + PUF for military auth	Resists MITM & eavesdropping	High exec time	14.58 ms (server), 1.48 ms (UAV)
[35]	ID & aggregate signature (CDHP)	Fast & secure framework	Informal task synergy eval	Enc/Dec: 194/167 ms; Key: 40/35 ms
[123]	PUF-based inter-drone auth	Lightweight & attack-resilient	Single CRP; SRAM variation	340 µs auth time

Table 1. *Cont.*

Ref.	Approach	Solutions	Limitations	Performance
[22]	ID-based auth in HetNets	Confidential & trusted network	Energy use not addressed	Robust & secure
[87]	Grouped auth for new drones	Scalable drone classification	Threshold limits apply	1.2 ms auth; 10 ms data share
[24]	Blockchain for edge IoD	Lightweight & secure ops	Simulated; delay with scale	Low cost & overhead
[125]	Bio-inspired leader election	Efficient cluster formation	No freq/security analysis	Effective multi-drone comms
[138]	LTE-based control system	Real-time GPS & data link	Limited aerial coverage	20 dBm signal; 94 ms latency
[126]	HECC signcryption with ROM	Low cost & privacy-preserving	Threat robustness unclear	3.36 comp cost; 1184-bit comm
[134]	FL-based swarm offloading	Real-time field detection	No collision coordination	0.26–0.28 ms latency; 92–98% fairness
[32]	RF + ML for swarm detection	Unsupervised drone ID	External data; unclear countermeasures	95% accuracy (AWGN)
[27]	Mutual auth between fog and edge drones	Key revocation post-mission	Fog drone is single point of failure	14–20× faster than PKI; may degrade with scale
[36]	Lightweight drone-to-drone comm	Trust-based secure messaging	sLTME lacks encryption; trust mgmt complexity	Low overhead; robust but vulnerable to advanced attacks

5. Cybersecurity in UAV Communication Systems

UAVs are being increasingly utilized in critical mission applications, making them appealing targets for cyber threats [139]. The cybersecurity landscape for UAVs includes both hardware and software vulnerabilities that can be exploited remotely or physically, as shown in Table 2 [140,141].

Table 2. Taxonomy classification of Drone attacks with impacts and their execution tools and mechanisms. Z1: Drones, Z2: Communication Networks, Z3: Base Stations, Z4: Ground Control Stations, and Z5: Certification Authorities, Production and Manufacturing Units, and other involved devices [141].

Drone Attacks	Tools/Mechanisms	Impact	Security Requirements	Attack Surfaces
Traffic Analysis and Network Stalking	SNMP, Packet sniffer, NetFlow	Privacy	Anti-spyware and packet filters	Z2
Interception	Drone Monitoring Equipment, Acoustic Sensors	Privacy	Encryption technique	Z1, Z2, Z3, Z4
Data Capturing and Forensics	Using serial connection, ExtractDJI, Datcon, Prodiscover Basic	Privacy	Encryption technique	Z1, Z2, Z3, Z4
Location Tracing	Drone Monitoring Equipment, Acoustic Sensors, Radar	Integrity	Utilize counter-drone techniques	Z1, Z2
Data/Information Leakage	Substitution and alteration, Modification, Duplication	Integrity	Secure channel switching and encrypted data	Z1, Z2, Z3, Z4, Z5

Table 2. *Cont.*

Drone Attacks	Tools/Mechanisms	Impact	Security Requirements	Attack Surfaces
ACL Modifications	Dronesploit, hacking tools	Integrity	Validate user-controllable input	Z1
Man-In-Middle Attacks	WiFi attack, Remote-AT-Commands, WiFi Pineapple Nano, Raspberry Pi 3, Maldrone, SkyJack	Integrity	Trusted CA-signed public key, encrypted link, mutual authentication, secure key exchange	Z2, Z3
Message Forgery	Dronesploit Remote-AT-Commands	Integrity	Secure channel switching and encrypted data	Z1, Z5
Identity Spoofing and Key Exploitations	Side-channel attacks, weak configuration, vulnerability exploitations	Confidentiality	Robust protocols with strong authentication	Z1, Z2, Z3, Z4, Z5
Unauthorized Access Controls	Drone Monitoring Equipment, Dronesploit, hacking tools, WiFi attack	Confidentiality	Strong passwords	Z1, Z2, Z3, Z4, Z5
Replay Attacks	Protocol manipulation	Confidentiality	Robust protocols, strong authentication, fresh message requests	Z2

5.1. Cybersecurity Threat Landscape in UAV Systems: Infographic-Based Analysis

5.1.1. Data Interception and Malware Injection

UAVs are becoming more susceptible to a variety of cyber threats due to their dependence on unsecured or poorly encrypted communication channels [142]. These vulnerabilities expose them to risks such as eavesdropping, packet manipulation, and malware injection through compromised control pathways, potentially corrupting mission data or hijacking drone operations [29,140,143]. Such threats are especially severe in reconnaissance and delivery missions, where data confidentiality and integrity are crucial [43,90]. As depicted in Figure 10, these threats range from data interception to physical interference, posing substantial risks to operational integrity and safety [144].

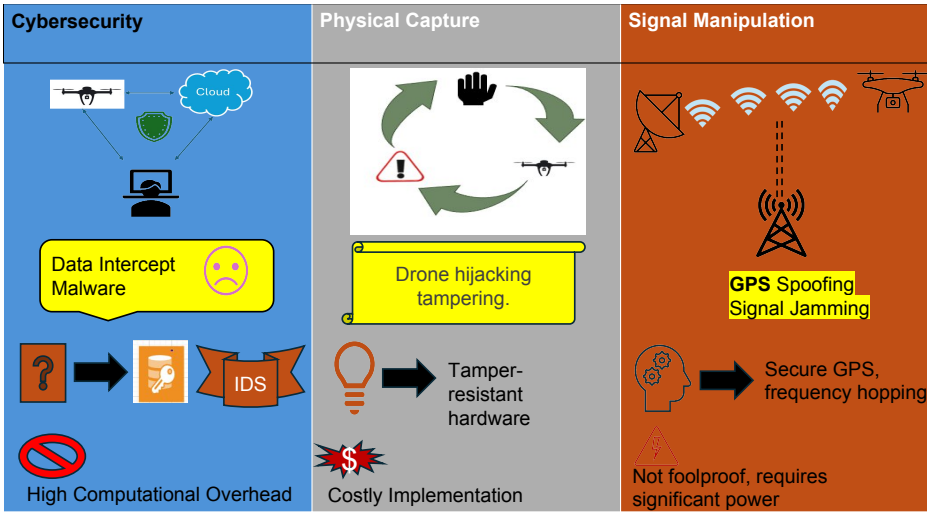

Figure 10. Key threat vectors in UAV swarms [17,22,145–147].

5.1.2. Drone Hijacking and Control Tampering

Beyond data interception, inadequate authentication protocols and open command channels render UAVs vulnerable to hijacking [148]. Attackers can exploit these flaws to take control of drones, redirect missions, or intentionally cause crashes [145]. Recent

incidents, such as the 2022 breach involving an East Coast financial services firm in the US, illustrate how WiFi deauthentication and credential spoofing techniques can be exploited to bypass firmware-level protections and gain unauthorized access to sensitive corporate information [149,150].

5.1.3. GPS Spoofing and Jamming

Navigation systems are also at risk [151]. GPS spoofing and RF jamming represent some of the most disruptive threats to UAV operations [145]. Using low-cost software-defined radios (SDRs) such as HackRF One, attackers can mimic false global navigation satellite system (GNSS) signals, misleading drones to incorrect locations [147]. "A 2023–2024 investigation by Stanford University documented extensive GNSS spoofing activity in regions such as Smolensk and the Black Sea. The study observed multiple aircraft exhibiting anomalous flight behavior, including circular hold patterns and misdirected routes, attributed to spoof navigation signals, underscoring the operational viability of spoofing in uncontrolled environments" [152]. Meanwhile, RF jamming saturates communication frequencies, leading to loss of control or mission failure [114]. Figure 11 depicts a structured representation of spoofing attacks, outlining their operational mechanisms, targeted components.

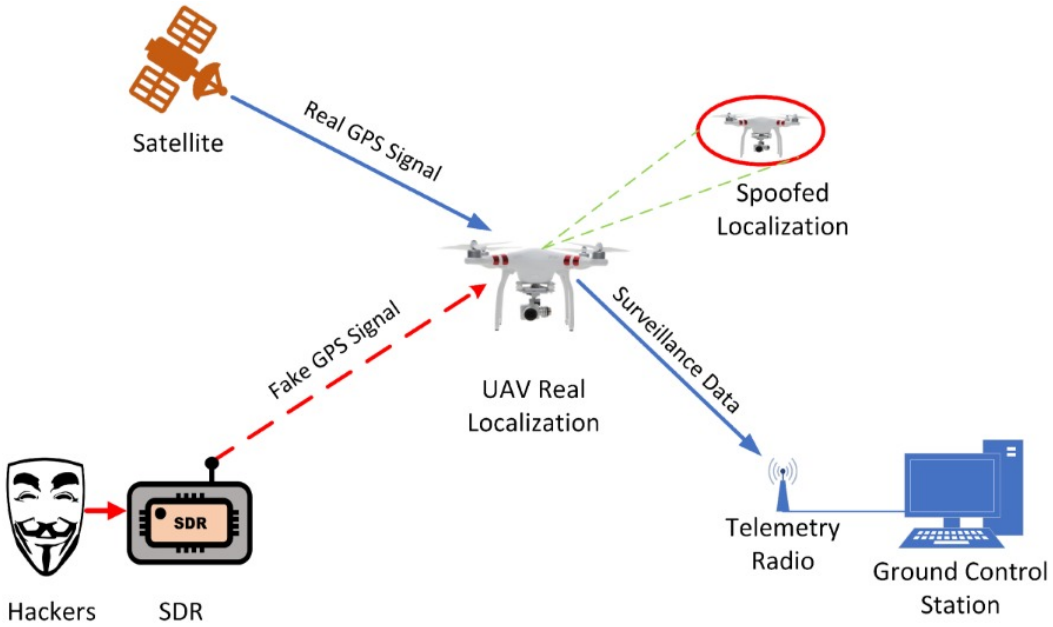

Figure 11. GPS spoofing attack [153].

5.1.4. Firmware Level Manipulation and Physical Tampering

In the hardware stage, alterations to the firmware and physical interference introduce additional risks [154]. Techniques such as laser fault injection (LFI) enable attackers to bypass secure boot processes and cryptographic validations [155]. Tools such as RayV Lite can create temporary faults in microcontrollers, jeopardizing the integrity of drones during operation. Wired Magazine (2024) noted that more than 75% attempts to circumvent embedded controller defenses using local file inclusion (LFI) were successful, highlighting the dangers of non-invasive physical breaches [156].

5.2. Intrusion Detection Systems (IDS) and Firewalls

Given the limited computational and energy resources of UAV platforms, cybersecurity solutions must be lightweight and efficient. Various approaches have been proposed to address these constraints, including the deployment of IDS, lightweight firewalls, and

streamlined cryptographic protocols [154]. As summarized in [30], these methods aim to provide adequate protection without significantly impacting flight time or processing capacity. Furthermore, energy-aware security designs, such as those proposed by Manikandan [38], are essential to maintain erational longevity when security mechanisms introduce computational overhead. One fundamental approach to improving UAV security involves the monitoring of (RF) signals exchanged between drones and Ground Control Stations [32]. These signals can be analyzed for intrusion detection and anomaly recognition, offering a non-invasive method to identify malicious activity [25]. Despite the development of encryption schemes, authentication protocols, and secure communication frameworks, their integration into real-world UAV operations remains inconsistent and often unverified [86].

5.3. Encryption and Authentication Techniques

A major issue in drone communications is safeguarding the confidentiality of transmitted information [86]. Conventional encryption techniques are often unsuitable due to the limited computational power of drones, prompting a preference for lightweight cryptographic methods [15]. ASMTP, which delivers end-to-end encryption and token-based authentication, presents a secure option, yet it depends on trusted servers, creating the risk of a single point of vulnerability [48]. Figure 12 shows a communication workflow for UAV-based IoT systems, where plaintext data is encrypted using a public key before transmission to the cloud. Homomorphic computation enables processing on encrypted data without decryption, and results are returned in encrypted form for local decryption using a private key. This approach enhances confidentiality while supporting advanced analytics in resource-constrained drone environments [157].

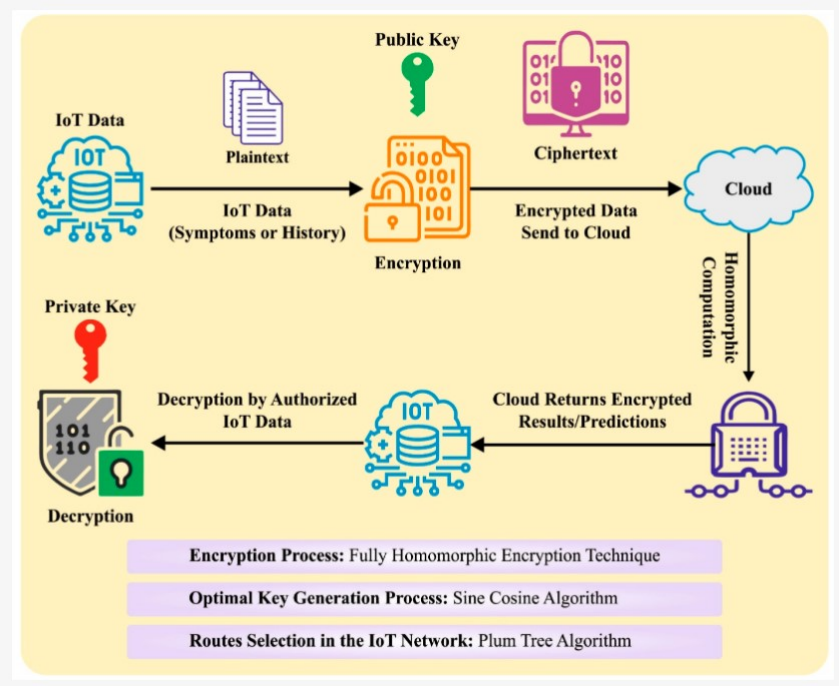

Figure 12. Framework for secure UAV communication using public-key encryption, homomorphic computation in the cloud, and private-key decryption, with key generation and route optimization for confidentiality and efficiency [157].

To reduce unauthorized access, identity-based authentication approaches are gaining popularity, ensuring that only authenticated users can gain network access and thwarting unauthorized interference with communications [22]. Besides secure communication,

data sharing and access control are vital components of the IoD, especially for sensitive applications, where it is crucial to facilitate authorized data sharing while preserving privacy [43]. To further enhance security, the Single-Use Token Methodology has been introduced, providing dynamic token generation for each transmission. This mechanism helps thwart replay attacks and guarantees confidentiality [48].

5.4. Blockchain and Lightweight Cryptography

Blockchain technology has surfaced as a promising approach to strengthening the security and reliability of UAV systems, particularly in infrastructure evaluation and healthcare logistics. Figure 13 demonstrates a blockchain-enabled UAV architecture that combines decentralized ledger technology with UAV control and cloud services. This design ensures secure registration, encrypted communication, and immutable data storage, while enabling auditing and path navigation through blockchain-based verification [158].

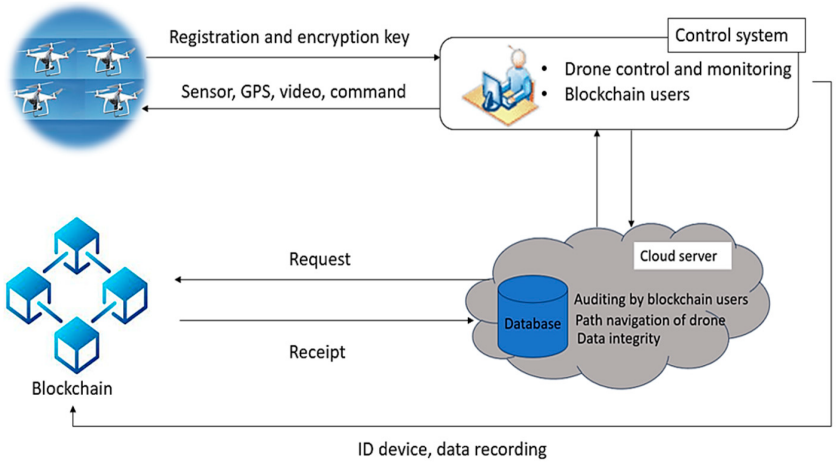

Figure 13. Blockchain-integrated UAV architecture showing UAVs, control systems, cloud servers, and a blockchain network for secure registration, encrypted communication, and decentralized auditing [158].

Its decentralized and immutable characteristics ensure that recorded information cannot be modified without consensus from the network, thus bolstering data integrity and operational trust [143,159]. The cryptographic linking of transaction logs in blockchain enhances transparency across UAV communication networks. When paired with high-speed technologies like 5G, blockchain facilitates secure, low-latency data transmission—essential for real-time tasks such as inspections and emergency responses [20,133]. However, blockchain adoption in UAV systems presents challenges. As the number of transactions increases, the ledger expands, resulting in higher storage demands and slower processing speeds, which can hinder real-time decision-making in drone swarms [47]. Additionally, consensus mechanisms such as Proof of Work (PoW) impose significant energy costs, making them unsuitable for battery-constrained UAVs [160]. Alternatives, such as Proof of Stake (PoS) and Directed Acyclic Graph (DAG)-based models, offer more energy-efficient options. While blockchain enhances data integrity, it does not inherently protect privacy [161]. Public blockchains may expose sensitive information unless supplemented with privacy-preserving technologies such as zero-knowledge proofs. Moreover, vulnerabilities like 51% attacks remain a concern, especially in small-scale deployments [24].

5.5. Privacy Concerns in Data Collection

Beyond cybersecurity, privacy has emerged as a critical concern in UAV-assisted operations [162]. The use of high-resolution cameras and advanced sensors enables precise

data acquisition, but also raises ethical and legal questions regarding the inadvertent capture of personally identifiable or sensitive information [163]. Studies have emphasized the importance of adhering to local data protection regulations and establishing transparent guidelines for data collection, processing, and sharing to maintain public trust and ensure legal compliance [41,43]. The integration of automation and intelligent workflows in UAV operations has led to significant efficiency gains, particularly in applications such as environmental monitoring and infrastructure inspection [42,69]. However, these advancements also introduce new complexities related to data storage, processing, and regulatory oversight. As UAV systems become more autonomous, ensuring secure and responsible data handling becomes increasingly critical [164].

5.6. Limitations of Traditional Security Mechanisms

Software-based anomaly detection and cryptographic safeguards often fail under adversarial conditions [22]. Sybil attacks, where multiple fake identities are injected into a swarm network, can destabilize consensus and authentication protocols [165]. Studies show that injecting Sybil nodes can overwhelm identity-based systems, leading to communication breakdowns and mission failure [166]. UAVs are vulnerable to a wide range of cyber threats, including GPS spoofing, replay attacks, and denial of service intrusions [142,145]. These risks are amplified in swarm-based models, where the attack surface expands and the potential for rogue drone infiltration increases [114]. While software-based defenses—such as anomaly detection and lightweight encryption—offer some protection, they often prove inadequate in disconnected or adversarial environments [22]. This has led to a growing interest in hardware-assisted security solutions, which offer more robust protection against sophisticated attacks [167].

5.7. Emerging Technologies for Secure UAV Networks

To address these vulnerabilities, modern UAV systems are increasingly adopting hardware-rooted security solutions [168]. PUFs and TPMs provide device-specific cryptographic identities and secure attestation [168,169]. PUFs leverage manufacturing variations to generate unique fingerprints without storing keys [123]. Figure 14 summarizes the diverse applications of field programmable gate array (FPGA) based PUFs in UAV security, including IP protection, key sharing, authentication, and random number generation, which collectively enhance hardware-rooted trust in resource-constrained environments [170].

While TPMs enable secure boot and integrity verification before swarm coordination. These mechanisms offer resilience against spoofing, tampering, and identity manipulation [171]. Federated learning offers a privacy-preserving approach to UAV data processing by enabling drones to share model updates rather than raw data. This reduces data exposure while optimizing energy efficiency and maintaining learning performance across distributed networks [134]. Efficient resource management is essential for maintaining data integrity and operational continuity in UAV-assisted networks. Factors such as energy consumption, trajectory planning, and channel modeling directly influence a drone's ability to securely transmit and process data [38]. Optimized resource allocation ensures that computational tasks are assigned to drones with sufficient processing power and battery capacity, minimizing service disruptions and data loss [172]. Advancements in digital twin (DT) technology—such as the TwinPort architecture—have further enhanced real-time monitoring and predictive maintenance, improving both security and operational efficiency in smart infrastructure networks [69].

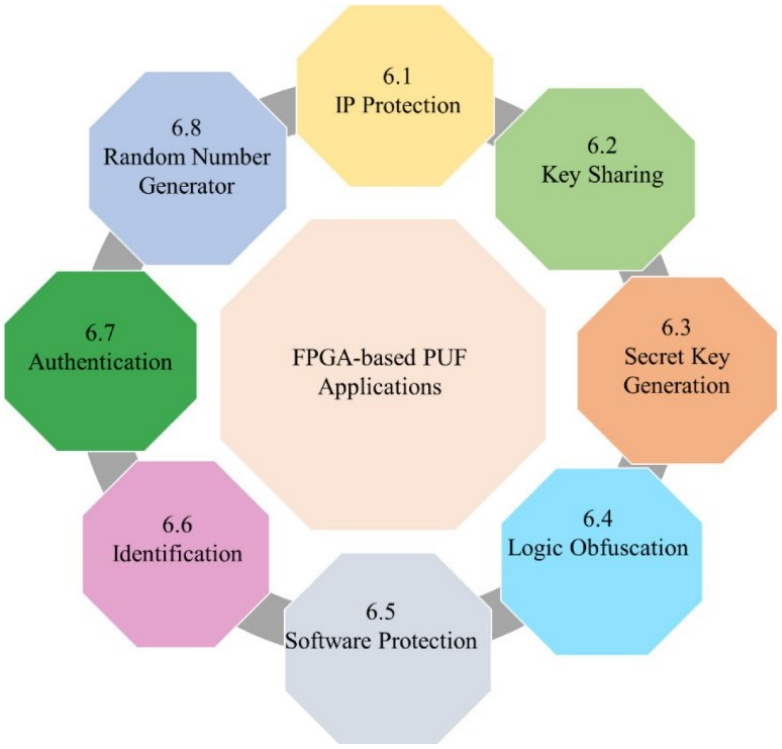

Figure 14. FPGA-based PUF applications, including IP protection, key sharing, secret key generation, logic obfuscation, software protection, identification, authentication, and random number generation [170].

5.8. Swarm Coordination and Optimization Algorithms

Optimizing drone swarm coordination is critical to preventing collisions and ensuring efficient communication. Optimization algorithms such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) are used to identify and protect critical nodes within the swarm's communication topology [30,115]. These algorithms enable effective coordination by optimizing node selection, ensuring that drones can operate without significant interference or risk of disruption [78,125]. Figure 15 represents a hierarchical swarm coordination model, where drones are organized into unit swarms, sub-cluster swarms, and cluster swarms. This structure supports optimization algorithms such as GA and PSO by reducing complexity and improving scalability in large UAV networks [173].

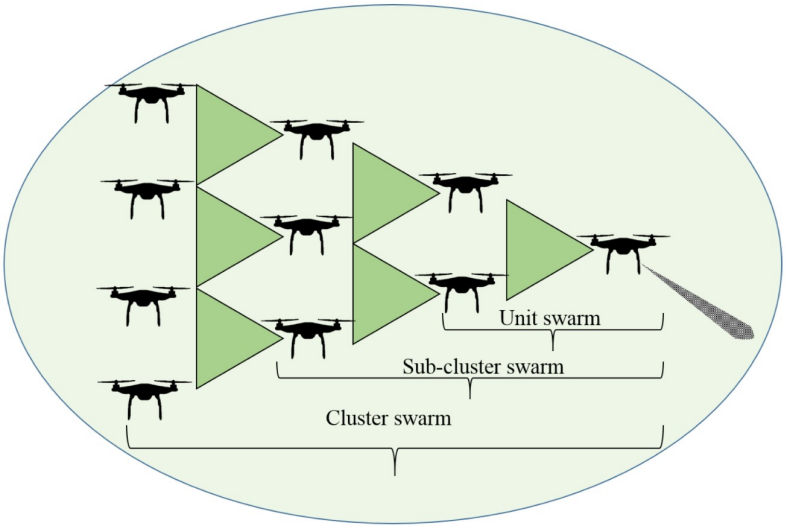

Figure 15. Swarm coordination communication model [173].

Additionally, managing data transmission and controlling response latencies is vital for avoiding collisions, as delays can undermine the effectiveness of collision avoidance strategies [159].

5.9. Case Studies and Real-World Incidents

Incidents from the real world offer concrete proof of the vulnerabilities covered in this section [174]. These examples show how UAV systems are vulnerable to a variety of threats, ranging from coordinated swarm invasions and armed payloads to passive surveillance and infrastructure overflights [29]. By looking at these incidents, we may learn more about how cyber risks affect operations and why proactive, multi-layered security measures are essential [45]. Table 3 documents the security events involving UAVs below, with an emphasis on the various attack methods and operational weaknesses.

Table 3. Documented drone security incidents.

Incident/Source	Description	Attack Mode	Reference
Naval Swarm Overflights (2019)	Coordinated drones circled U.S. naval ships.	Unauthorized presence	[175]
Sofia, Bulgaria (2025)	Air traffic was halted due to an unauthorized drone, leading to delays and an emergency declaration	Disruption	[176]
Langley & UK Airbase Swarm (2023)	Multi-drone incursion into military airspace with unknown controllers	Coordinated swarm intrusion	[175]
Nashville Substation Plot (2024)	Man arrested for planning drone attack with C-4 explosives on power infrastructure	Weaponized payload threat	[177]
Pinyon Plain Uranium Mine (2025)	Drone crashed into safety wires, disrupting operations and leading to arrest	Industrial disruption	[178]

Due to these instances, UAV systems must have strong cybersecurity frameworks in place [99,100]. The range of assault options, from active hijacking demonstrations to passive intrusions over vital infrastructure, highlights the complex nature of UAV vulnerabilities [25]. These real-world examples support the need for hardware, software and regulatory protections in integrated security solutions [177]. The move from software-only defenses to integrated hardware–software security frameworks is required due to the changing threat landscape [166]. Strong defense against identity-based attacks, spoofing, and tampering is provided by hardware security primitives such as PUFs and TPMs [167,169]. In order to further improve UAV resistance in hostile situations, future research should investigate AI-driven threat detection, quantum-resistant cryptography, and decentralized trust models [179].

6. Hardware Security Primitives

In secure drone swarm operations, hardware security primitives are essential to establish trust, verify identities, and protect against physical and cyber threats [180,181].

6.1. Layered Architecture and Embedded Security

Layered Architecture and Embedded Security, Figure 16 presents a multi-layered framework for secure drone collaboration, where the Security Layer integrates essential hardware-based elements like PUFs, TPMs and Distance-Bounding Protocols [19,182,183]. These components facilitate strong authentication and secure communication by utilizing the unique physical characteristics of the devices and their tamper-proof modules [16]. Furthermore, the incorporation of blockchain technology improves decentralized trust and ensures data integrity throughout the swarm [184]. Situated below the Communication Layer, which encompasses both infrastructure networks and FANETs, these security measures guarantee that communication protocols remain not only efficient but also resistant to spoofing, relay attacks, and unauthorized access [123]. This layered strategy highlights the vital importance of hardware security in enabling scalable and reliable drone swarm operations.

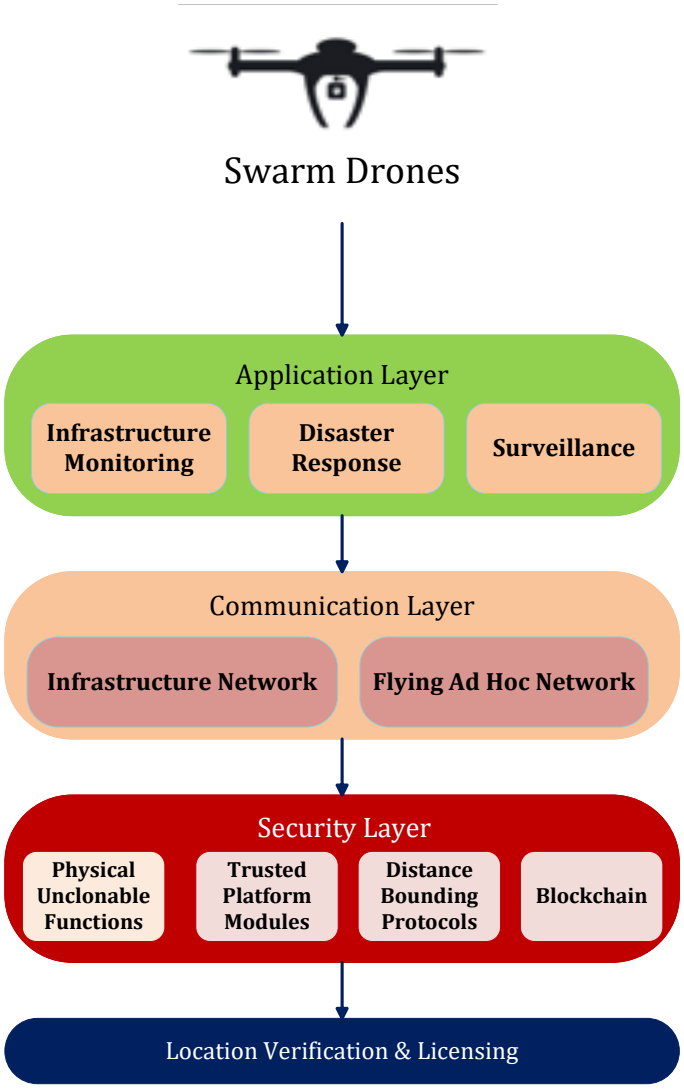

Figure 16. Secure swarm collaboration.

6.2. Core Technologies and Their Roles

HSPs offer tamper-proof security through on-chip features such as PUFs, RNGs, TPMs, and secure enclaves [183]. PUFs are particularly appealing because of their low energy usage and distinctive, nonreplicable response traits [127]. As shown in Figure 17, PUF-based authentication operates on a challenge–response mechanism. A verifier issues a challenge to the device, which uses its intrinsic PUF to generate a unique response.

This response is then compared against pre-stored values in a secure database to confirm authenticity, ensuring lightweight and tamper-resistant verification [185].

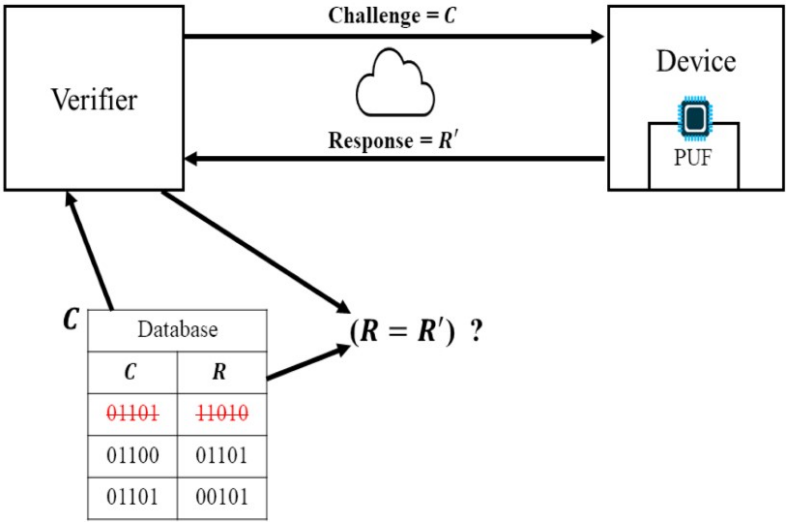

Figure 17. Challenge–response process in a PUF-based authentication system, where a verifier sends a challenge to a device and validates the returned response against stored values [185].

They are increasingly incorporated into blockchain systems to facilitate decentralized identity and licensing structures [184]. TPMs continue to be crucial for secure boot and remote attestation, especially in military-grade UAVs [183]. Secure enclaves, such as ARM TrustZone, provide isolated execution environments, albeit with increased cost and complexity [186]. New designs embed PUFs into RISC-V SoCs to enable low-power hardware-level security and to further elucidate the differences and applications of these primitives [182,187,188]. Figure 18 provides a simplified illustration of the components of hardware security primitives, offering a visual framework to support the classification and understanding of foundational techniques.

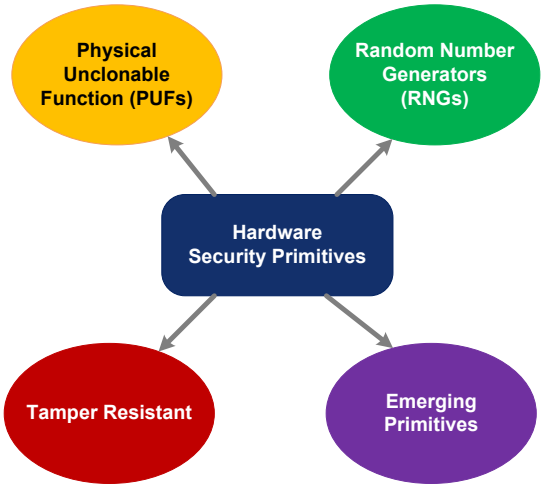

Figure 18. Core components of hardware security primitives.

Table 4 outlines their benefits, drawbacks, real-world applications, and recent research advancements.

Table 4. Condensed summary of hardware security primitives with key metrics.

Refs.	Primitive	Summary	Key Metrics
[51,167,185,189]	**PUFs**	Microscopic manufacturing variations, key-less device identities at very low cost. Environmental drift and modeling attacks limit reliability. Underpin IoT authentication and secure boot.	Entropy: 0.89–0.98; BER: 5–15%; Modeling Resistance: Medium
[19,53,54]	**TRNGs**	High-entropy randomness for cryptographic protocols. Require post-processing, sensitive to environmental conditions. Underpin TLS/SSL session-key negotiation.	Entropy: ≈1.0; NIST SP800-22: Pass; Throughput: 10–100 Mbps
[190–192]	**Logic Locking & Obfuscation**	Protects IP from reverse engineering and overproduction. Area/power overhead, vulnerable to SAT- and side-channel attacks.	Area: 5–15%; Power: 8–12%; SAT Attack: $>10^6$ s
[193–197]	**Tamper-Resistant Hardware**	Detect/respond to physical attacks to safeguard assets. Expensive, high-assurance systems. Smartcards, HSMs use conductive meshes.	FIPS 140-3 Level 3–4; Cost: High
[189,198,199]	**Emerging Primitives**	Novel entropy sources at ultra-low power. Integration challenges, limited standardization. Target next-gen IoT security.	Power: <10 µW; Entropy: 0.95; Standardization: Low

6.3. Comparative Assessment of HSP-Based Security Techniques

A comparative study indicates that PUF-based approaches strike the optimal balance between energy efficiency and security, making them particularly suitable for environments with limited resources [26]. Although blockchain systems ensure robust integrity, they do so at the expense of increased latency and power consumption [20]. TPMs and distance-bounding protocols are preferred in scenarios requiring high assurance or when facing adversarial conditions [52].

6.3.1. Quantitative Comparison

Quantitative Comparison, Table 5 provides a summary of the energy usage, latency, and tamper resistance for each method, supported by evidence from benchmark studies.

Table 5. Quantitative comparison of security techniques.

Technique	Energy (mL/op)	Latency (ms)	Tamper Resistance	References
ECC	∼15.6	∼8–10	No	[116,121]
SRAM/DRAM PUF	∼0.2	∼1–100	Yes	[200–202]
TPM (ECC)	∼15.6	∼8–20	Yes	[194]
Blockchain	≥200	≥1000	Partial (Auditable)	[160,203]

The values are approximate estimates derived from experimental and survey literature. On embedded devices, ECC typically uses tens of millijoules per scalar multiplication, with execution times ranging from 8 to 15 ms for optimized implementations [116,121]. SRAM and DRAM PUFs exhibit very low energy consumption (<1 mJ) and latency, from microseconds for SRAM PUFs to approximately 88 ms for DRAM-latency PUFs, with strong inherent tamper resistance [200–202]. TPMs that implement ECC incur similar computational costs to standalone ECC but add hardware-based tamper resistance and

wake-up energy overhead [52,194]. Blockchain-based mechanisms, particularly PoW and distributed consensus, demand significantly higher energy (≥200 mJ) and latency (≥1 s) per confirmed transaction, providing auditable integrity rather than complete tamper-proofing [160,203].

6.3.2. Radar Chart Analysis

A radar chart comparing five well-known UAV security techniques—ECC, PUFs, TPMs, Blockchain integrated with HSPs, and distance bounding using Ultra-Wideband (UWB)—across five important criteria—scalability, latency, deployment readiness, hardware cost, and energy efficiency—is presented in Figure 19 to summarize the comparative insights covered in this section.

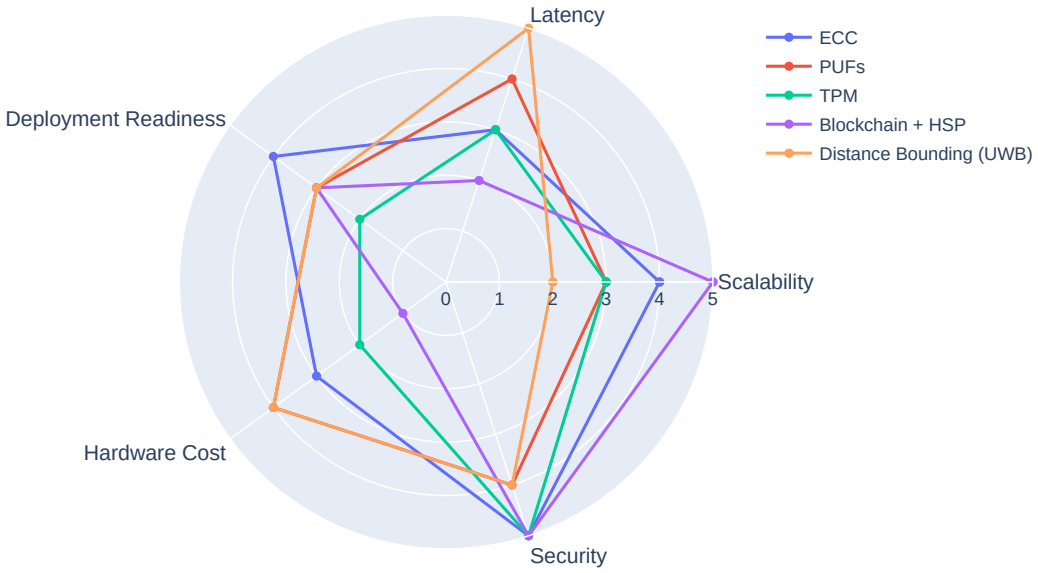

Figure 19. Comparative radar chart OF UAV security techniques.

The chart illustrates the trade-offs inherent in each approach. PUFs demonstrate strong performance in latency, scalability, and cost-effectiveness, making them ideal for lightweight UAV deployments [204]. Blockchain + HSP systems offer decentralized control and auditability but are constrained by high latency and energy demands, limiting their suitability for real-time or energy-sensitive missions [19,49]. TPMs and distance bounding protocols provide robust tamper resistance and proximity assurance, making them well-suited for high-assurance or military-grade operations, albeit with increased hardware complexity [183,196]. ECC, meanwhile, offers a balanced profile across all dimensions, making it a versatile choice for general-purpose swarm cryptography [205]. This visual comparison underscores the importance of context-aware selection of security primitives. No single technique excels across all metrics, and deployment decisions should be guided by mission requirements, operational constraints, and threat models. From an operational feasibility standpoint, emerging methods such as AI-driven PUFs and blockchain-based attestation offer significant advantages over traditional security mechanisms but introduce unique operational considerations [47,204]. AI-augmented PUFs enhance reliability under environmental variations and aging, reducing error rates and improving entropy stability compared to conventional PUFs [206]. However, they require additional computational resources for model training and inference, which may impact energy budgets in UAV swarms [160]. Similarly, blockchain-based attestation provides decentralized trust and immutable audit trails, addressing single points of failure inherent in traditional PKI

systems [143]. Yet, its feasibility in UAV environments is constrained by high latency, bandwidth consumption, and consensus overhead, particularly in large swarms [199]. In contrast, traditional mechanisms such as ECC and TPMs are well-understood, lightweight, and easier to certify but lack adaptability and scalability for dynamic, distributed UAV networks [128]. Therefore, while emerging approaches promise stronger resilience and transparency, their deployment must balance energy efficiency, latency, and interoperability to ensure operational feasibility in real-world UAV scenarios [52].

6.3.3. Why Hardware Is the New Frontier in UAV Swarm Security?

Traditional cybersecurity approaches, such as cryptographic protocols and anomaly detection systems, have been proven to be insufficient in adversarial environments where UAV swarms operate. These software-based methods often lack the resilience needed to counter physical and protocol-level attacks that exploit the inherent vulnerabilities of wireless and distributed systems [183]. For example, low-cost GPS spoofing using (SDRs) such as the HackRF One (priced under $300) has successfully manipulated UAV coordinates in more than 90% of test scenarios, allowing attackers to redirect or force land drones [207]. Similarly, laser fault injection tools such as the RayV Lite (available for less than $500) have demonstrated the ability to bypass firmware integrity checks mid-flight, compromising drone behavior in real time [156]. At the network level, Sybil attacks have overwhelmed swarm coordination protocols by injecting dozens of fake drone identities, effectively paralyzing swarm operations unless mitigated by hardware-based identity verification [129]. These examples underscore the limitations of relying solely on software defenses. In contrast, the hardware roots of trust, including PUFs, TPMs, and secure enclaves, anchor security in the physical properties of the device [195,196]. These primitives offer tamper resistance, device-specific authentication, and secure attestation, which makes them suitable for the constrained and high-risk environments in which UAV swarms operate [168,181]. Moreover, these hardware-level protections are not merely theoretical [19]. Recent research has emphasized the importance of modular subsystem-based architectures that integrate such primitives into broader security frameworks. For instance, a multi-layered defense system developed using MATLAB Simulink demonstrated the effectiveness of integrating hardware-level protections with real-time threat detection and response mechanisms [208]. By embedding security at the hardware level, these mechanisms provide a foundational layer of trust that is difficult to replicate or subvert, even under sophisticated attack scenarios. As such, they represent a critical change in the design of secure UAV systems, allowing more robust protection for both drones and the sensitive data they collect [17,180,182].

6.4. Hardware–Software Trade-Offs and Hybrid Architectures for UAV Swarms

Although HSPs such as TPMs and PUFs provide strong physical roots of trust, their integration with software-based mechanisms is essential for comprehensive UAV swarm security [19]. Hardware solutions offer tamper resistance and unclonable identities, making them highly resilient to physical attacks [168]. However, they introduce cost, weight, and design complexity, and are difficult to update once deployed [181]. Conversely, software-based approaches—such as ECC, blockchain, and federated learning—are flexible, easily upgradable, and cost-effective, but they impose higher computational and energy overhead on resource-constrained UAVs and remain vulnerable to malware and key extraction attacks [128,134,184]. For UAV swarms, these trade-offs are critical: hardware ensures robust identity and secure boot, while software enables adaptive cryptographic agility and distributed trust [183,209]. A hybrid approach that combines hardware anchors such as (PUF-derived keys) with lightweight or post-quantum cryptography and AI-driven

trust scoring offers the best balance between security strength, scalability, and operational efficiency [204]. This integration mitigates single-point weaknesses and aligns with emerging standards for quantum-safe and adaptive security in autonomous aerial systems [185].

6.5. Emerging Trends: AI-Augmented PUFs, Post-Quantum Primitives, and Hybrid Trust Anchors

Recent research leverages ML not only to attack PUFs, but also to enhance their reliability in dynamic environments. Neural network-assisted calibration and error recovery improve stability under voltage and temperature variations, reducing bit error rates without compromising uniqueness, while complementary techniques such as lightweight or reverse fuzzy extractors and multiple-reference enrollment further minimize error correction overheads—an essential property for UAVs operating under rapid environmental changes [210,211]. Conversely, increasingly sophisticated ML/DL modeling attacks against arbiter and composite PUF families (e.g., DNN-based modeling) have motivated adversarial defenses and NN-based challenge–response transformations to increase the complexity of successful attacks. For UAV swarms, where physical capture and CRP harvesting are realistic threats, ML-aided reliability combined with ML-aware anti-modeling countermeasures is becoming best practice [212,213]. Additionally, AI-driven trust scoring and anomaly prediction can be fused with PUF/TPM attestation to detect insider threats during swarm coordination [214]. In parallel, post-quantum cryptography (PQC) is transitioning from research to deployment to counter the "harvest now, decrypt later" threat and accommodate long UAV lifecycles. NIST finalized three PQC standards in August 2024—module lattice KEM (FIPS 203, CRYSTALS-Kyber), module lattice signatures (FIPS 204, CRYSTALS-Dilithium) and stateless hash-based signatures (FIPS 205, SPHINCS+), with a fourth (HQC) announced in 2025 [215–217]. While these primitives provide forward security and quantum resistance, their larger key and signature sizes compared to ECC impact bandwidth and energy in multi-hop swarm networks, prompting hybrid migration strategies and embedded-class optimizations [216]. A practical approach combines PUF-derived identities (for unclonable hardware roots) with PQC credentials (for quantum resilience), anchored by TPM or TEE where available, and couples these anchors with AI-driven trust scoring for continuous, behavior-aware admission control across UAV swarms. This layered architecture aligns with emerging UAV security roadmaps that emphasize adaptive, learning-enhanced defenses while meeting regulatory mandates for quantum-safe cryptography [214,215].

7. Verification, Licensing, and Regulation

In light of the vulnerabilities associated with satellite navigation, alternative strategies such as distance-bounding protocols [218] and delay-based decryption [219] are gaining prominence. These methods enforce location-aware regulations by tying chip functionality to physical presence. AI-enhanced environmental PUFs further bolster this approach by utilizing ambient information for implicit geo-verification [206]. Blockchain-integrated attestation processes support geofencing, licensing, and auditability, thereby reducing reliance on centralized authorities [161].

7.1. Verification

Considering the ongoing susceptibility of GPS-based navigation to spoofing and jamming, both academia and industry have begun to focus on hardware-rooted location verification and decentralized compliance mechanisms within UAV systems [17]. This transition reflects the necessity to enforce spatial limitations, licensing regulations, and operational accountability, especially for swarm drones involved in infrastructure inspection, urban logistics, or cross-border operations [85].

7.1.1. Distance-Bounding Protocols

DB protocols serve as mechanisms for verifying locations by estimating the maximum distance between a verifier and a prover through the analysis of round-trip signal delays [220]. These protocols are formulated to defend against relay (mafia fraud) and wormhole attacks, especially in environments lacking GPS or facing adversarial conditions [92]. DB protocols compatible with UAVs frequently utilize UWB and millimeter-wave (mmWave) technologies to attain precision within sub-meter accuracy [221]. Recent innovations have led to the development of Frequency-Modulated Continuous Wave (FMCW) implementations, which provide enhanced energy efficiency and accuracy for UAV-related applications [92]. Furthermore, multi-point DB protocols have been suggested to improve safety in the airspace and verify trajectories. A system has been introduced that integrates DB with Automatic Dependent Surveillance-Broadcast (ADS-B), capable of accurately identifying spoofed UAVs [222]. Their protocol underwent validation through ArduPilot SITL simulations, affirming its effectiveness for swarm coordination and collision avoidance [223]. Despite their strength, DB protocols encounter obstacles in real-world deployment, including the necessity for precise synchronization, specialized timing hardware, and susceptibility to environmental noise. These limitations hinder scalability in extensive UAV networks [222]. Ongoing studies are investigating low-power DB variations, RFID-based implementations, and alternatives that do not rely on timing to minimize hardware demands and enhance practicality in real-world applications [224].

7.1.2. Delay-Based Cryptographic Decryption

Delay-Based Cryptographic Decryption represents a burgeoning method that imposes geospatial constraints by restricting access to encrypted data or instructions based on latency profiles [225]. These profiles are pre-defined and align with certain physical locations, ensuring that UAVs can only carry out mission-critical operations within authorized areas [219]. This approach proves especially beneficial in environments where GPS is compromised, as traditional geofencing methods may not succeed. By working in conjunction with secure timer modules and Trusted Execution Environments (TEEs), delay-based decryption facilitates real-time enforcement of spatial regulations and mission logic [225]. Figure 20 provides an overview of the workflow for delay-based decryption, where a policy authority provisions latency profiles and a TEE enforces location verification through timing challenges before releasing mission keys [91].

Recent progress has introduced lightweight cryptographic algorithms such as ASCON-128a, which deliver robust security assurances with minimal computational demands, perfect for UAV platforms with limited resources [226]. Additionally, machine learning-based delay-aware detection systems have been proposed to dynamically modify decryption thresholds in response to UAV behavior and environmental factors [227]. These systems bolster resilience against spoofing, unauthorized access, and timing manipulation, particularly in swarm operations where decentralized control is essential [228]. While offering promise, delay-based decryption methods necessitate accurate latency calibration and thorough environmental modeling to guarantee reliability across various operational situations [229].

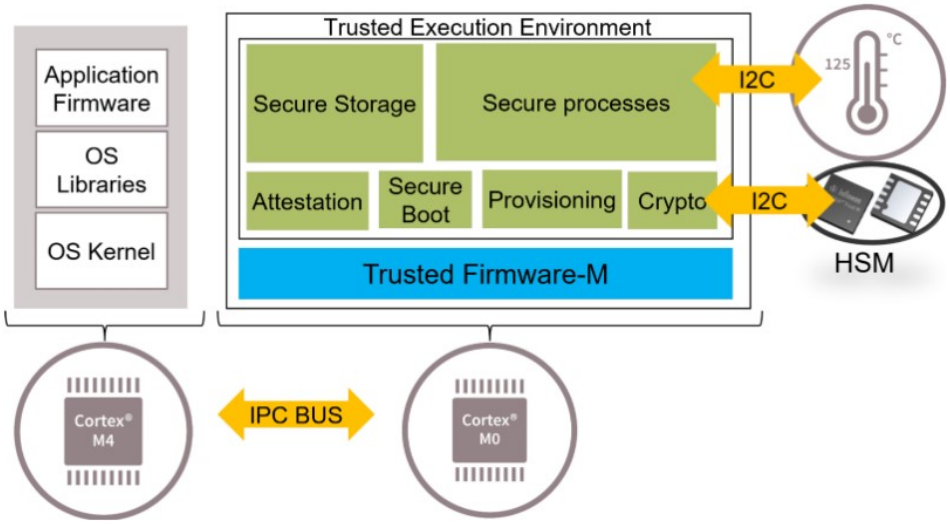

Figure 20. Workflow of delay-based decryption, where a TEE verifies location using timing challenges and releases mission keys only when latency matches authorized profiles [91].

7.1.3. Environmental Physical Unclonable Functions (ePUFs)

Environmental Physical Unclonable Functions (ePUFs) are hardware security constructs that harness variations in the surrounding environment—such as light levels, temperature, magnetic fields, and barometric pressure—to create unique challenge–response pairs [206]. These responses act as implicit geolocation tokens, allowing UAVs to confirm their physical presence without depending on external signals [43]. Recent studies have shown that entropy sourced from environmental noise can yield device-location fingerprints that are resilient to replay and spoofing attempts [197]. For instance, Ref. [198] demonstrated that drones can learn and validate these fingerprints to establish geographic authenticity, enhancing location assurance in environments devoid of GPS. An important application is the PUFloc protocol, created by Nair and Thampi, which merges PUF characteristics with tiered location-based authentication. This protocol utilizes hash functions, XOR operations, and random number generators to facilitate lightweight and secure mutual authentication [230]. FPGA implementations of PUFloc have shown minimal power usage and strong resistance to cloning and interference. ePUFs hold significant importance in safeguarding privacy during location authentication, especially in sensitive or disputed areas [231]. Their combination with AI models enables adaptive learning of environmental signatures, thereby improving robustness and scalability in dynamic UAV operations [199].

7.1.4. Blockchain-Backed Geofencing and Licensing

Blockchain-Enhanced Geofencing and Licensing provides a decentralized structure for UAV mission oversight, licensing, and accountability [20]. By utilizing smart contracts on distributed ledgers, UAVs can independently verify flight permissions, operational regions, and device authenticity, decreasing dependency on centralized entities and increasing transparency [47]. Figure 21 illustrates the system architecture underpinning this approach. It shows how various nodes—Training Nodes, Mining Nodes, and hybrid Training and Mining Nodes—interact with MEC servers via a blockchain network. These nodes collaboratively manage model training and mining tasks, with MEC servers facilitating consensus and blockchain integrity. The use of model upload (solid black arrows) and download (red dashed arrows) pathways highlights the decentralized exchange of operational data, reinforcing the secure and transparent nature of UAV oversight [143].

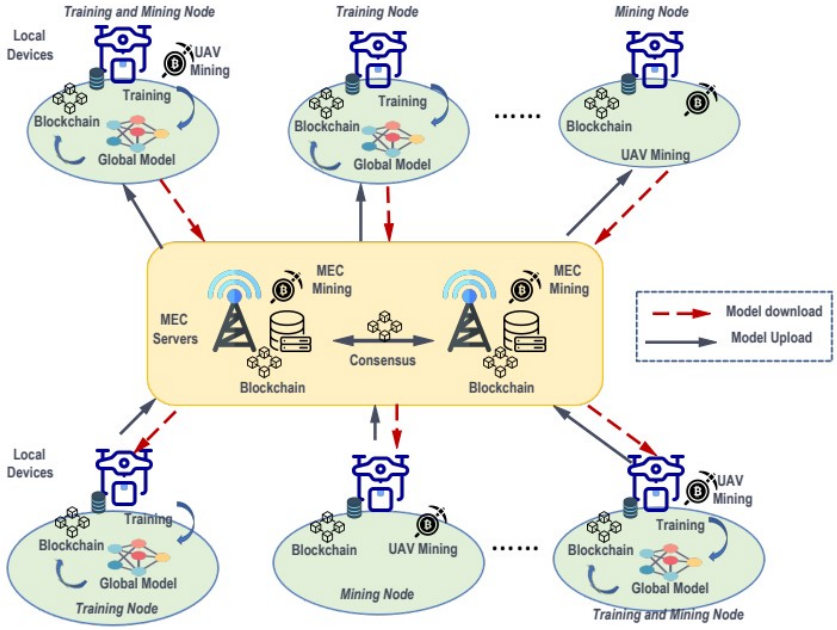

Figure 21. Blockchain-based architecture for UAV geofencing and licensing. The figure shows decentralized interactions between training and mining nodes coordinated by MEC servers, enabling secure model exchange and autonomous UAV operations [143].

Initiatives like those suggested by [199] combine blockchain technology with secure hardware anchors, such as PUF-derived device identities, facilitating trustless verification of mission legitimacy. Smart contracts can actively enforce geofencing rules, triggering alerts or disabling critical flight functions when UAVs stray from designated routes [143]. The Geofences in the Sky initiative expands this concept by merging blockchain with 5G technology, allowing for real-time UAV traffic management across centralized, decentralized, and hybrid modes of operation [184]. This capability enables the dynamic enforcement of no-fly zones and mission parameters, particularly in urban and cross-border settings [20]. Despite its potential, blockchain-based UAV systems encounter challenges related to latency, throughput, and energy usage, particularly in swarm operations and missions with time constraints [130]. Ongoing research into blockchain-supported UAV communication, zero-knowledge proofs, and lightweight consensus protocols seeks to overcome these challenges and enhance scalability [199].

7.2. Regulatory Frameworks for UAV Operations

The transition of drone uses from military to civilian applications has introduced regulatory challenges that must be addressed to fully realize the potential of drone technology [39]. Issues surrounding misuse, privacy violations, and military utilization highlight the necessity for robust regulations [232]. The variability of regulations across different countries significantly influences the acceptance and use of drone technology [233]. Accompanied by a comparative analysis of drone regulations in major regions, highlighting differences in registration processes, altitude restrictions, licensing categories, and limitations on autonomous operations [40]. While regulatory frameworks such as ICAO SARPs and national UAV laws aim to ensure safety and privacy, significant gaps remain. Current policies are fragmented and often lag behind technological progress, resulting in inconsistent altitude limits, BVLOS permissions, and certification standards across jurisdictions [234,235]. This lack of harmonization creates interoperability challenges for UAV swarms operating in multinational contexts. For example, variations in sense-and-avoid requirements, spectrum allocations, and data protection laws complicate cross-border

missions and increase compliance costs [236]. Furthermore, the absence of mutual recognition agreements for UAV certifications and pilot credentials limits scalability for commercial and defense applications. Addressing these gaps requires coordinated international efforts to standardize operational protocols, enable secure data exchange, and align privacy regulations without stifling innovation [237].

Regulations typically encompass pilot licensing, drone registration, restricted operational areas, and insurance requirements, with distinctions based on the drone's weight, population density, altitude, and intended applications [238]. For example, the UK's Air Navigation Order requires human operators to maintain control of drones, limiting fully autonomous operations and restricting drone usage in areas such as underground locations or ventilation shafts without human oversight [39]. Similarly, the Federal Aviation Administration (FAA) in the US prioritizes aerospace safety but lacks guidelines on privacy, leaving a gap in addressing ethical and human rights issues [3]. Several countries are striving to harmonize regulations to promote global consistency [97,239]. The European Union has established categories for drone operations in Figure 22 as open, specific, and certified, each with customized licensing and training requirements [237]. International cooperation and shared best practices are critical to addressing the global nature of drone technology and its applications [40].

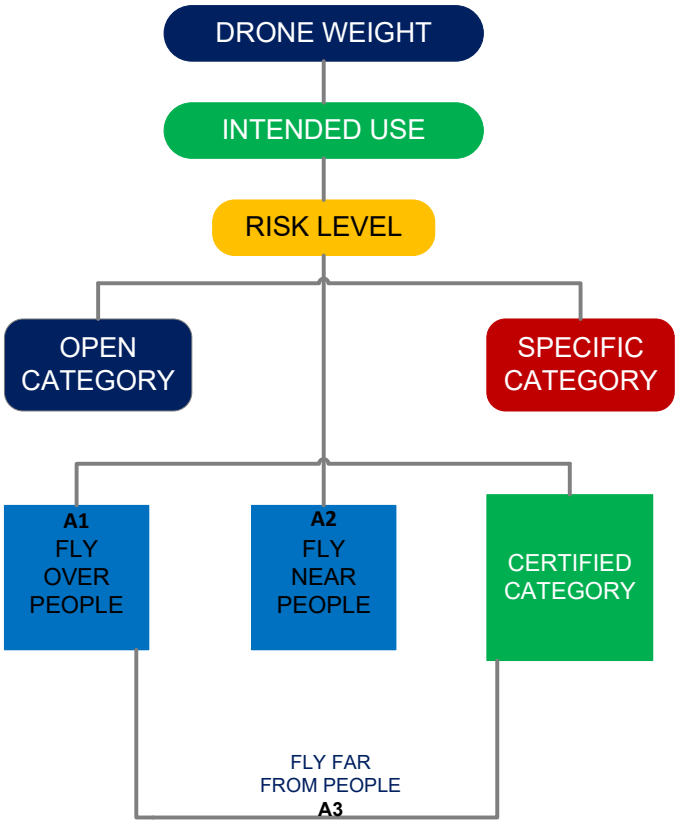

Figure 22. Licensing and regulation of UAV operation in the European context.

7.2.1. Privacy and Data Protection Laws

Privacy and data protection regulations govern the manner in which drones can gather, store, and disseminate information, particularly in public and residential settings [232]. Nonetheless, there are still regulatory shortcomings. For instance, while the FAA ensures airspace safety, it lacks thorough privacy regulations [240]. Laws tailored to specific purposes, such as those overseeing police drone operations in France and the U.S., seek to tackle these issues [240]. Research from [97] indicates that the implementation of Production-

Linked Incentives (PLIs) has eased regulations and offered incentives to boost local drone manufacturing and economic development. However, concerns regarding safety and privacy continue to be significant, requiring ongoing adjustments to laws to keep pace with advancing technologies and emerging threats [241].

7.2.2. Airspace Management and Compliance

Drones are required to adhere to airspace regulations, which often involve registration and obtaining flight permits [242]. Regulatory structures usually outline operational areas, altitude restrictions, and conditions for Beyond Visual Line of Sight (BVLOS) operations. These regulations are vital for preventing conflicts with manned aircraft and ensuring a secure integration into national airspace systems [243].

7.2.3. Ethical Considerations in UAV Deployment

Ethical dilemmas encompass excessive surveillance, data exploitation, and the effects of drones on public confidence [243]. Ref. [239] described drones as "aerial technologies of domination," where local communities experience vulnerabilities due to constant monitoring. Such actions erode sovereignty and perpetuate systemic disparities, particularly evident in African settings. This implies that the public's view of drones, especially in areas where they have been employed for military operations, often entails psychological repercussions, resulting in resistance to their use in civilian applications [88]. Given this context, enhancing capabilities, fostering international collaboration, and educating the public are vital to achieving a balance between innovation and safety, as well as ethical considerations. By tackling these challenges and promoting cooperation, policymakers can ensure that drone technologies develop responsibly and fairly [40,88]. The regulation of UAV systems is a dynamic and complex field influenced by technological progress, public apprehensions, and geopolitical factors [174]. While numerous nations have progressed in outlining operational limits and licensing requirements, there are still deficiencies concerning privacy safeguards, ethical governance, and oversight of autonomous flights [237]. Real-world instances highlight the necessity of purpose-specific legislation and international collaboration [39]. To guarantee the responsible and fair use of drone technologies, ongoing regulatory adjustments, capability enhancement, and public involvement are crucial [40]. By aligning legal structures with emerging threats and societal expectations, policymakers can encourage safe, ethical, and scalable integration of UAVs [174].

7.2.4. Regulatory Integration and Compliance Frameworks

To implement emerging UAV technologies such as distance-bounding, delay-based decryption, and blockchain-supported licensing, regulators are investigating policy-aligned enforcement models. Organizations such as the European Union Aviation Safety Agency (EASA) and the FAA have shown interest in combining remote ID systems and licensing frameworks with secure location verification systems [7,242]. Suggested models encompass the following: Drones ID attestation certificates, location-specific token signing, and real-time revocation lists disseminated via 5G and FANET infrastructure. However, the lack of interoperable standards and inconsistent legal frameworks across jurisdictions remains a significant barrier to global adoption [238]. Harmonizing these approaches will be essential to enable scalable, secure, and internationally compliant UAV operations [97].

8. Deployment Challenges

While hardware security primitives (HSPs) offer promising solutions for securing UAV systems, their practical deployment across diverse operational environments introduces unique challenges [19]. Unlike controlled laboratory settings, real-world scenarios impose constraints related to mobility, connectivity, and environmental unpredictability [114,133].

Factors such as harsh weather conditions, dynamic threat landscapes, and resource limitations amplify the complexity of implementing secure and reliable UAV operations [244]. In addition, mission-specific requirements, ranging from stringent latency demands in military applications to resilience in disaster-stricken areas and compliance with regulatory frameworks in urban airspaces, necessitate context-aware security strategies [245].

8.1. Disaster Zones: Lightweight and Offline-Capable Security

In areas affected by disasters, UAVs frequently function without dependable communication networks or power supplies [246]. These limitations call for lightweight, offline-capable security solutions [81]. PUFs are especially apt for these situations due to their minimal power requirements and their capability to generate cryptographic keys as needed, without the necessity for secure storage [167]. PUFs facilitate secure identity verification and key distribution in the field, aiding autonomous UAV operations during search-and-rescue efforts, infrastructure evaluations, and emergency logistics [50]. Figure 23 presents the PUF-based enrollment process, which enables secure identity verification and key distribution by leveraging unique device-specific responses to challenges. This approach supports autonomous UAV operations in critical missions [185].

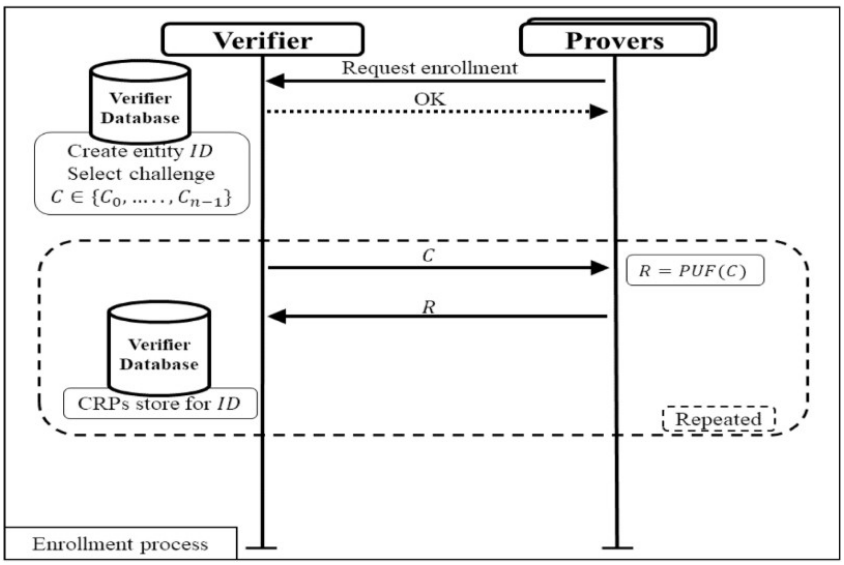

Figure 23. PUF-based enrollment protocol between verifier and UAVs (provers), showing secure challenge–response generation and storage for identity verification [185].

Nevertheless, PUFs can be influenced by environmental changes, and their entropy might diminish over time [230]. Other strategies, such as pre-shared keys or QR-code based authentication, have been utilized in certain deployments, but they do not offer the dynamic and tamper-resistant characteristics of PUFs [219,224]. Additional research is essential to enhance the stability and dependability of PUFs in extreme environmental conditions and to create hybrid systems that merge PUFs with lightweight cryptographic protocols for improved resilience [185].

8.2. Military Deployments: Tamper Resistance and Cryptographic Robustness

Military UAVs function in high-risk environments where adversaries might try to intercept, spoof, or physically compromise devices [90]. In these settings, tamper-resistant hardware and strong cryptographic components are crucial [195]. TPMs and secure elements are routinely employed to safeguard sensitive information and cryptographic keys [196]. Furthermore, distance-bounding protocols are utilized to confirm the proximity of control stations, reducing risks of relay and spoofing attacks [92]. Recent studies have

investigated the incorporation of PUF-based distance bounding to bolster defenses against fraud and man-in-the-middle attacks [206]. However, these protocols typically require precise timing hardware and strict synchronization, which can be challenging to implement across extensive UAV swarms [92]. Alternative strategies like frequency hopping and spread-spectrum communication provide some defense against jamming and interception, but they lack the detailed location verification offered by distance bounding [146]. Future investigations should concentrate on scalable, low-latency distance-bounding solutions and adaptive tamper detection systems that can respond flexibly to physical threats [85].

8.3. Urban Environments: Privacy, Licensing, and Compliance

Urban UAV operations are subject to stringent regulatory frameworks that prioritize privacy safeguarding, airspace management, and adherence to license [85]. To fulfill these criteria, ref. [199] has suggested combining PUF-based device identities with blockchain-supported geofencing and licensing systems. These frameworks utilize smart contracts to enforce operational limits, such as flight areas, time constraints, and payload limitations [143]. For example, a drone equipped with a PUF-derived identity can register its credentials on a blockchain ledger, allowing decentralized validation of its permissions and activities. If the drone strays from its designated route, smart contracts can trigger notifications or disable critical operations [184]. This method improves auditability and trust without the need to rely on centralized authorities [160]. However, blockchain-based systems face issues related to latency, energy demands, and network availability, particularly in real-time or swarm operations [130]. Alternative solutions like centralized remote ID systems or 5G-assisted geofencing provide lower latency, but reintroduce vulnerabilities associated with single points of failure [20]. The utilization of UAVs in disaster areas, military operations, and urban settings requires customized security approaches [247]. Lightweight solutions such as PUFs are ideal for environments with limited infrastructure [51], while TPMs and distance-bounding techniques deliver strong safeguards in hostile situations [196,218]. Deployments in urban areas require compliance-focused solutions that harmonize privacy, auditability, and responsiveness [39]. These differences highlight the need for flexible, context-sensitive security frameworks and an ongoing exploration of scalable, resilient, and interoperable hardware security solutions [183].

9. Conclusions and Future Work

This review has examined the role of HSPs in enabling secure location verification for UAV swarms, analyzing the strengths and limitations of approaches such as PUFs, TPMs, blockchain-integrated systems, and distance-bounding techniques. Among these, PUFs emerge as the most energy-efficient and scalable solution for resource-constrained UAV environments, whereas TPMs and blockchain-based frameworks offer enhanced security for high-assurance and regulated applications. For practical deployment, industry stakeholders are advised to adopt PUF-based authentication for lightweight UAVs, leverage blockchain for decentralized licensing and audit trails, and consider TPMs for secure boot and attestation in mission-critical or military-grade systems. Ultimately, deployment strategies should be tailored to environmental constraints, regulatory requirements, and operational objectives.

Despite these advancements, several challenges persist, creating opportunities for future research. UAVs remain constrained by limited computational and energy resources, which restrict the complexity of current verification mechanisms. Physical vulnerabilities also pose a significant risk, necessitating robust anti-tampering measures. Furthermore, scalability in swarm scenarios, where multiple drones must be verified simultaneously without incurring excessive latency or energy overhead—remains an open problem. Com-

patibility with existing UAV communication protocols is another underexplored area that must be addressed to ensure seamless integration into real-world systems.

To overcome these limitations, future research should prioritize the design of lightweight PUF architectures optimized for UAV platforms to enhance both power efficiency and operational speed. Integrating blockchain-based frameworks with hardware security offers a promising pathway toward decentralized and tamper-proof location verification. In swarm environments, quorum-based consensus mechanisms supported by hardware-secured tokens could provide scalable and reliable verification solutions. Additionally, the fusion of ML techniques with hardware roots of trust holds significant potential for real-time anomaly detection and spoofing prevention. Beyond these directions, emerging areas such as post-quantum secure primitives, AI-augmented PUFs, and RISC-V-based secure architectures represent transformative opportunities for UAV security. Post-quantum cryptography will be essential to counter "harvest now, decrypt later" threats, ensuring long-term confidentiality for mission-critical data in swarms with extended lifecycles. AI-augmented PUFs can significantly improve reliability under environmental variations while enabling adaptive trust scoring and anomaly detection, which are crucial for dynamic swarm coordination. Similarly, RISC-V-based secure control systems offer open, customizable hardware platforms that integrate hardware roots of trust with lightweight cryptographic accelerators, reducing energy overhead while maintaining strong security guaranties. Together, these innovations pave the way for scalable, quantum-safe, and context-aware security frameworks that align with regulatory requirements and operational constraints. Future research should focus on integrating these technologies into hybrid architectures, validating their performance in real-world swarm deployments, and developing interoperability standards to ensure seamless adoption across heterogeneous UAV ecosystems.

Author Contributions: Conceptualization, S.M.A., M.S. and B.H.S.A.; methodology, S.M.A. and B.H.S.A.; resources, S.M.A., M.S. and B.H.S.A.; writing—original draft preparation, B.H.S.A. and S.M.A.; writing—review and editing, S.M.A., B.H.S.A. and M.S.; visualization, B.H.S.A. and S.M.A. Supervision, B.H.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Alqudsi, Y.; Makaraci, M. UAV swarms: Research, challenges, and future directions. *J. Eng. Appl. Sci.* **2025**, *72*, 12. [CrossRef]
2. Tahir, A.; Böling, J.; Haghbayan, M.H.; Toivonen, H.T.; Plosila, J. Swarms of unmanned aerial vehicles—A survey. *J. Ind. Inf. Integr.* **2019**, *16*, 100106. [CrossRef]
3. Federal Aviation Administration. What to Know About Drones. 2025. Available online: https://www.faa.gov/newsroom/what-know-about-drones (accessed on 18 August 2025).
4. Guan, H.; Sun, X.; Su, Y.; Hu, T.; Wang, H.; Wang, H.; Peng, C.; Guo, Q. UAV-lidar aids automatic intelligent powerline inspection. *Int. J. Electr. Power Energy Syst.* **2021**, *130*, 106987. [CrossRef]
5. Shi, L.; Marcano, N.J.H.; Jacobsen, R.H. A review on communication protocols for autonomous unmanned aerial vehicles for inspection application. *Microprocess. Microsyst.* **2021**, *86*, 104340. [CrossRef]
6. U.S. Government Accountability Office. *Science & Tech Spotlight: Drone Swarm Technologies*; Technical Report GAO-23-106930; U.S. Government Accountability Office: Washington, DC, USA, 2023.
7. Zaitseva, E.; Levashenko, V.; Mukhamediev, R.; Brinzei, N.; Kovalenko, A.; Symagulov, A. Review of reliability assessment methods of drone swarm (fleet) and a new importance evaluation based method of drone swarm structure analysis. *Mathematics* **2023**, *11*, 2551. [CrossRef]
8. Doggalli, G.; Santhoshinii, E.; Manojkumar, H.; Srivastava, M.; Ganesh, H.; Barigal, A.; Anithaa, V.; Ameen, A.; Kundu, R. Drone technology for crop disease resistance: Innovations and challenges. *J. Sci. Res. Rep.* **2024**, *30*, 174–180. [CrossRef]

9. Humpe, A. Bridge inspection with an off-the-shelf 360 camera drone. *Drones* **2020**, *4*, 67. [CrossRef]
10. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
11. Constantinescu, N.; Ticleanu, O.A.; Hunyadi, I.D. Securing Authentication and Detecting Malicious Entities in Drone Missions. *Drones* **2024**, *8*, 767. [CrossRef]
12. Jacobsen, R.H.; Matlekovic, L.; Shi, L.; Malle, N.; Ayoub, N.; Hageman, K.; Hansen, S.; Nyboe, F.F.; Ebeid, E. Design of an autonomous cooperative drone swarm for inspections of safety critical infrastructure. *Appl. Sci.* **2023**, *13*, 1256. [CrossRef]
13. Zhou, Y.; Rao, B.; Wang, W. UAV swarm intelligence: Recent advances and future trends. *IEEE Access* **2020**, *8*, 183856–183878. [CrossRef]
14. Zhai, X.; Shao, M.; Cang, M.; Cheng, X.; Wu, S.; Wang, J. Application of drone technology in power grid engineering. *J. Phys. Conf. Ser.* **2024**, *2798*, 012007. [CrossRef]
15. Lin, C.; He, D.; Kumar, N.; Choo, K.K.R.; Vinel, A.; Huang, X. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [CrossRef]
16. Bhunia, S.; Tehranipoor, M. Hardware security primitives. In *Hardware Security*; Morgan Kaufmann: San Mateo, CA, USA, 2019; pp. 311–345.
17. Vidaković, M.; Vinko, D. Hardware-based methods for electronic device protection against invasive and non-invasive attacks. *Electronics* **2023**, *12*, 4507. [CrossRef]
18. Chen, W.; Zhu, J.; Liu, J.; Guo, H. A fast coordination approach for large-scale drone swarm. *J. Netw. Comput. Appl.* **2024**, *221*, 103769. [CrossRef]
19. Tehranipoor, M.; Pundir, N.; Vashistha, N.; Farahmandi, F. *Hardware Security Primitives*; Springer: Berlin/Heidelberg, Germany, 2023.
20. Jagatheesaperumal, S.K.; Rahouti, M.; Chehri, A.; Xiong, K.; Bieniek, J. Blockchain-based security architecture for unmanned aerial vehicles in b5g/6g services and beyond: A comprehensive approach. *IEEE Open J. Commun. Soc.* **2025**, *6*, 1042–1069. [CrossRef]
21. Chen, X.; Tang, J.; Lao, S. Review of unmanned aerial vehicle swarm communication architectures and routing protocols. *Appl. Sci.* **2020**, *10*, 3661. [CrossRef]
22. Wani, A.R.; Gupta, S.K.; Khanam, Z.; Rashid, M.; Alshamrani, S.S.; Baz, M. A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. *IET Intell. Transp. Syst.* **2023**, *17*, 2171–2189. [CrossRef]
23. Zhang, H.; Xi, S.; Jiang, H.; Shen, Q.; Shang, B.; Wang, J. Resource allocation and offloading strategy for UAV-assisted LEO satellite edge computing. *Drones* **2023**, *7*, 383. [CrossRef]
24. Singh, M.; Aujla, G.S.; Bali, R.S. Derived blockchain architecture for security-conscious data dissemination in edge-envisioned Internet of Drones ecosystem. *Clust. Comput.* **2022**, *25*, 2281–2302. [CrossRef]
25. Lv, H.; Liu, F.; Yuan, N. Drone presence detection by the drone's RF communication. *J. Phys. Conf. Ser.* **2021**, *1738*, 012044. [CrossRef]
26. Wen, K.; Wang, S.; Wu, Y.; Wang, J.; Han, L.; Xie, Q. A secure authentication protocol supporting efficient handover for UAV. *Mathematics* **2024**, *12*, 716. [CrossRef]
27. Han, K.; Al Nuaimi, E.; Al Blooshi, S.; Psiakis, R.; Yeun, C.Y. Scalable authenticated communication in drone swarm environment. *J. Internet Technol.* **2024**, *25*, 255–265.
28. Kumar, A.; Yadav, A.S.; Gill, S.S.; Pervaiz, H.; Ni, Q.; Buyya, R. A secure drone-to-drone communication and software defined drone network-enabled traffic monitoring system. *Simul. Model. Pract. Theory* **2022**, *120*, 102621. [CrossRef]
29. Bansal, G.; Sikdar, B. S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12088–12100. [CrossRef]
30. Chen, W.; Meng, X.; Liu, J.; Guo, H.; Mao, B. Countering large-scale drone swarm attack by efficient splitting. *IEEE Trans. Veh. Technol.* **2022**, *71*, 9967–9979. [CrossRef]
31. Kim, S.K. Advanced drone swarm security by using blockchain governance game. *Mathematics* **2022**, *10*, 3338. [CrossRef]
32. Ashush, N.; Greenberg, S.; Manor, E.; Ben-Shimol, Y. Unsupervised drones swarm characterization using rf signals analysis and machine learning methods. *Sensors* **2023**, *23*, 1589. [CrossRef]
33. Jomaa, I.; Saleh, W.; Rokan, R.; Hussien, S. Secured drone communication based on esalsa20 algorithm. *Int. J. Circuits Syst. Signal Process* **2023**, *17*, 67–75. [CrossRef]
34. Senigagliesi, L.; Ciattaglia, G.; Gambi, E. Autoencoder based physical layer authentication for UAV communications. In Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023; pp. 1–6.
35. Jan, S.U.; Khan, H.U. Identity and aggregate signature-based authentication protocol for IoD deployment military drone. *IEEE Access* **2021**, *9*, 130247–130263. [CrossRef]

36. Liu, Z.; Guo, J.; Huang, F.; Cai, D.; Wu, Y.; Chen, X.; Igorevich, K.K. Lightweight trustworthy message exchange in unmanned aerial vehicle networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2144–2157. [CrossRef]
37. Gopi, S.P.; Magarini, M.; Alsamhi, S.H.; Shvetsov, A.V. Machine learning-assisted adaptive modulation for optimized drone-user communication in b5g. *Drones* **2021**, *5*, 128. [CrossRef]
38. Manikandan, K.; Sriramulu, R. Optimized path planning strategy to enhance security under swarm of unmanned aerial vehicles. *Drones* **2022**, *6*, 336. [CrossRef]
39. Krook, J.; Bossens, D.; Winter, P.; Araujo-Estrada, S.; Downer, J.; Windsor, S. Mapping the complexity of legal challenges for trustworthy drones on construction sites in the United Kingdom. *ACM J. Responsible Comput.* **2024**, *1*, 1–26. [CrossRef]
40. Kutynska, A.; Dei, M. Legal regulation of the use of drones: Human rights and privacy challenges. *J. Int'l Leg. Commc'n* **2023**, *8*, 39. [CrossRef]
41. Kim, D. Pedestrian and bicycle volume data collection using drone technology. *J. Urban Technol.* **2020**, *27*, 45–60. [CrossRef]
42. Gillan, J.K.; Ponce-Campos, G.E.; Swetnam, T.L.; Gorlier, A.; Heilman, P.; McClaran, M.P. Innovations to expand drone data collection and analysis for rangeland monitoring. *Ecosphere* **2021**, *12*, e03649. [CrossRef]
43. Tu, Y.J.; Piramuthu, S. Security and privacy risks in drone-based last mile delivery. *Eur. J. Inf. Syst.* **2024**, *33*, 617–630. [CrossRef]
44. Telli, K.; Kraa, O.; Himeur, Y.; Ouamane, A.; Boumehraz, M.; Atalla, S.; Mansoor, W. A comprehensive review of recent research trends on unmanned aerial vehicles (uavs). *Systems* **2023**, *11*, 400. [CrossRef]
45. Patel, A.; Cherukuri, A.K. Analysis of Light-Weight Cryptography Algorithms for UAV-Networks. *arXiv* **2025**, arXiv:2504.04063. [CrossRef]
46. Khan, M.A.; Qureshi, I.M.; Khanzada, F. A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET). *Drones* **2019**, *3*, 16. [CrossRef]
47. Alsamhi, S.H.; Shvetsov, A.V.; Shvetsova, S.V.; Hawbani, A.; Guizani, M.; Alhartomi, M.A.; Ma, O. Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. *IEEE Trans. Green Commun. Netw.* **2022**, *7*, 328–338. [CrossRef]
48. Manikandan, K.; Sriramulu, R. ASMTP: Anonymous secure messaging token-based protocol assisted data security in swarm of unmanned aerial vehicles. *Int. J. Netw. Manag.* **2024**, *34*, e2271. [CrossRef]
49. Kumar, R.; Aljuhani, A.; Kumar, P.; Kumar, A.; Franklin, A.; Jolfaei, A. Blockchain-enabled secure communication for unmanned aerial vehicle (UAV) networks. In Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, Sydney, Australia, 17 October 2022; pp. 37–42.
50. Xie, Q.; Wang, H. PUF-Based Secure and Efficient Anonymous Authentication Protocol for UAV Towards Cross-Domain Environments. *Drones* **2025**, *9*, 260. [CrossRef]
51. Boke, A.K.; Nakhate, S.; Rajawat, A. FPGA implementation of PUF based key generator for secure communication in IoT. *Integration* **2023**, *89*, 241–247. [CrossRef]
52. Bathalapalli, V.K.; Mohanty, S.P.; Kougianos, E.; Iyer, V.; Rout, B. PUFchain 4.0: Integrating PUF-based TPM in distributed ledger for security-by-design of IoT. In Proceedings of the Great Lakes Symposium on VLSI 2023, Knoxville, TN, USA, 5–7 June 2023; pp. 231–236.
53. Gao, B.; Lin, B.; Li, X.; Tang, J.; Qian, H.; Wu, H. A unified PUF and TRNG design based on 40-nm RRAM with high entropy and robustness for IoT security. *IEEE Trans. Electron. Devices* **2022**, *69*, 536–542. [CrossRef]
54. Emimi, M.; Khaleel, M.; Alkrash, A. The current opportunities and challenges in drone technology. *Int. J. Electr. Eng. Sustain.* **2023**, *1*, 74–89.
55. Vergouw, B.; Nagel, H.; Bondt, G.; Custers, B. Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. In *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 21–45.
56. Tuğrul, K.M. Drone technologies and applications. In *Drones-Various Applications*; IntechOpen: London, UK, 2023.
57. Dutta, G.; Goswami, P. Application of drone in agriculture: A review. *Int. J. Chem. Stud.* **2020**, *8*, 181–187. [CrossRef]
58. Shahmoradi, J.; Talebi, E.; Roghanchi, P.; Hassanalian, M. A comprehensive review of applications of drone technology in the mining industry. *Drones* **2020**, *4*, 34. [CrossRef]
59. Ayamga, M.; Akaba, S.; Nyaaba, A.A. Multifaceted applicability of drones: A review. *Technol. Forecast. Soc. Change* **2021**, *167*, 120677. [CrossRef]
60. Mohsan, S.A.H.; Khan, M.A.; Ghadi, Y.Y. Editorial on the advances, innovations and applications of UAV Technology for Remote Sensing. *Remote Sens.* **2023**, *15*, 5087. [CrossRef]
61. Mandloi, D.; Arya, R.; Verma, A.K. Internet of drones. In *Recent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 353–373.
62. Home. Skybound Intelligence: AIS Impact on Drone Technology. Whitepaper/Report. 2024. Available online: https://ijsrem.com/download/skybound-intelligence-ais-impact-on-drone-technology/ (accessed on 11 August 2025).

63. Marek, D.; Paszkuta, M.; Szyguła, J.; Biernacki, P.; Domański, A.; Szczygieł, M.; Król, M.; Wojciechowski, K. Swarm of drones in a simulation environment—Efficiency and adaptation. *Appl. Sci.* **2024**, *14*, 3703. [CrossRef]
64. Bakirci, M. A Novel Swarm Unmanned Aerial Vehicle System: Incorporating Autonomous Flight, Real-Time Object Detection, and Coordinated Intelligence for Enhanced Performance. *Trait. Du Signal* **2023**, *40*, 2063. [CrossRef]
65. Ahirwar, S.; Swarnkar, R.; Bhukya, S.; Namwade, G. Application of drone in agriculture. *Int. J. Curr. Microbiol. Appl. Sci.* **2019**, *8*, 2500–2505. [CrossRef]
66. Pathak, H.; Kumar, G.; Mohapatra, S.; Gaikwad, B.; Rane, J. Use of drones in agriculture: Potentials, Problems and Policy Needs. *ICAR-Natl. Inst. Abiotic Stress Manag.* **2020**, *300*, 4–15.
67. Rejeb, A.; Abdollahi, A.; Rejeb, K.; Treiblmaier, H. Drones in agriculture: A review and bibliometric analysis. *Comput. Electron. Agric.* **2022**, *198*, 107017. [CrossRef]
68. Spoorthi, S.; Shadaksharappa, B.; Suraj, S.; Manasa, V. Freyr drone: Pesticide/fertilizers spraying drone-an agricultural approach. In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 23–24 February 2017; pp. 252–255.
69. Yigit, Y.; Nguyen, L.D.; Ozdem, M.; Kinaci, O.K.; Hoang, T.; Canberk, B.; Duong, T.Q. TwinPort: 5G drone-assisted data collection with digital twin for smart seaports. *Sci. Rep.* **2023**, *13*, 12310. [CrossRef] [PubMed]
70. Adegboye, M.A.; Fung, W.K.; Karnik, A. Recent advances in pipeline monitoring and oil leakage detection technologies: Principles and approaches. *Sensors* **2019**, *19*, 2548. [CrossRef]
71. Altshuler, Y.; Pentland, A.; Bruckstein, A. Defending Large-Scale Critical Infrastructures Using a Swarm of Drones. In *Applied Swarm Intelligence*; CRC Press: Boca Raton, FL, USA, 2024; pp. 180–218.
72. Day, D. Drones for transmission infrastructure inspection and mapping improve efficiency. *Nat. Gas Electr.* **2017**, *33*, 7–11. [CrossRef]
73. Yang, L.; Fan, J.; Liu, Y.; Li, E.; Peng, J.; Liang, Z. A review on state-of-the-art power line inspection techniques. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 9350–9365. [CrossRef]
74. Nooralishahi, P.; Ibarra-Castanedo, C.; Deane, S.; López, F.; Pant, S.; Genest, M.; Avdelidis, N.P.; Maldague, X.P. Drone-based non-destructive inspection of industrial sites: A review and case studies. *Drones* **2021**, *5*, 106. [CrossRef]
75. Grand View Research. Drone Market Size, Share & Trends Report. 2025. Available online: https://www.grandviewresearch.com/press-release/global-drone-market (accessed on 18 August 2025).
76. Erdelj, M.; Król, M.; Natalizio, E. Wireless sensor networks and multi-UAV systems for natural disaster management. *Comput. Netw.* **2017**, *124*, 72–86. [CrossRef]
77. Erdelj, M.; Natalizio, E.; Chowdhury, K.R.; Akyildiz, I.F. Help from the sky: Leveraging UAVs for disaster management. *IEEE Pervasive Comput.* **2017**, *16*, 24–32. [CrossRef]
78. Innocente, M.S.; Grasso, P. Self-organising swarms of firefighting drones: Harnessing the power of collective intelligence in decentralised multi-robot systems. *J. Comput. Sci.* **2019**, *34*, 80–101. [CrossRef]
79. Mao, J.; Jia, Z.; Gu, H.; Shi, C.; Shi, H.; He, L.; Wu, Q. Robust UAV Path Planning with Obstacle Avoidance for Emergency Rescue. In Proceedings of the 2025 IEEE Wireless Communications and Networking Conference (WCNC), Milan, Italy, 24–27 March 2025; pp. 1–6.
80. Abdel-Malek, M.A.; Akkaya, K.; Saputro, N.; Ibrahim, A.S. Efficient authentication of drones to mmWave wireless mesh networks in post-disaster scenarios. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
81. Bushnaq, O.M.; Mishra, D.; Natalizio, E.; Akyildiz, I.F. Unmanned aerial vehicles (UAVs) for disaster management. In *Nanotechnology-Based Smart Remote Sensing Networks for Disaster Prevention*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 159–188.
82. Hu, M.; Liu, W.; Lu, J.; Fu, R.; Peng, K.; Ma, X.; Liu, J. On the joint design of routing and scheduling for vehicle-assisted multi-UAV inspection. *Future Gener. Comput. Syst.* **2019**, *94*, 214–223. [CrossRef]
83. Ghandeharizadeh, S. Holodeck: Immersive 3D Displays Using Swarms of Flying Light Specks. In Proceedings of the 3rd ACM International Conference on Multimedia in Asia, Gold Coast, Australia, 1–3 December 2021; pp. 1–7.
84. Ahmed, G.; Sheltami, T.; Mahmoud, A.; Imam, M. Performance Evaluation of Three Routing Protocols for Drone Communication Networks. *Arab. J. Sci. Eng.* **2024**, *49*, 13149–13161. [CrossRef]
85. Feng, O.; Zhang, H.; Tang, W.; Wang, F.; Feng, D.; Zhong, G. Digital Low-Altitude Airspace Unmanned Aerial Vehicle Path Planning and Operational Capacity Assessment in Urban Risk Environments. *Drones* **2025**, *9*, 320. [CrossRef]
86. Feng, C.; Yu, K.; Bashir, A.K.; Al-Otaibi, Y.D.; Lu, Y.; Chen, S.; Zhang, D. Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach. *IEEE Netw.* **2021**, *35*, 130–137. [CrossRef]
87. Aydin, Y.; Kurt, G.K.; Ozdemir, E.; Yanikomeroglu, H. Authentication and handover challenges and methods for drone swarms. *IEEE J. Radio Freq. Identif.* **2022**, *6*, 220–228. [CrossRef]

88. Nyaaba, A.A.; Ayamga, M. Intricacies of medical drones in healthcare delivery: Implications for Africa. *Technol. Soc.* **2021**, *66*, 101624. [CrossRef]
89. Baturone, I.; Román, R.; Corbacho, Á. A unified multibit PUF and TRNG based on ring oscillators for secure IoT devices. *IEEE Internet Things J.* **2022**, *10*, 6182–6192. [CrossRef]
90. Ko, Y.; Kim, J.; Duguma, D.G.; Astillo, P.V.; You, I.; Pau, G. Drone secure communication protocol for future sensitive applications in military zone. *Sensors* **2021**, *21*, 2057. [CrossRef] [PubMed]
91. Cabrera-Gutiérrez, A.J.; Castillo, E.; Escobar-Molero, A.; Cruz-Cozar, J.; Morales, D.P.; Parrilla, L. Secure sensor prototype using hardware security modules and trusted execution environments in a blockchain application: Wine logistic use case. *Electronics* **2023**, *12*, 2987. [CrossRef]
92. Khalil, F.M.; Fazil, A.; Hussain, M.J.; Masood, A. Cross-Layer RF Distance Bounding Scheme for Passive and Semi-passive Ubiquitous Computing Systems. *Comput. Secur.* **2024**, *137*, 103633. [CrossRef]
93. Kumar, P.; Darshi, S.; Shailendra, S. Drone assisted device to device cooperative communication for critical environments. *IET Commun.* **2021**, *15*, 957–972. [CrossRef]
94. Grand View Research. AI in Drone Market Size, Share & Trends Analysis Report by Type (Station Based, Cloud Based), by Component (Hardware, Software, Services), by Application, by End Use, by Region, And Segment Forecasts, 2025–2033. Report ID: GVR-4-68040-645-7; Historical Range: 2021–2023; Forecast Period: 2025–2033. Market Size Was Estimated at USD 12,292.6 million in 2024 and Projected to Reach USD 51,328.7 Million by 2033 (CAGR 17.9%). 2023. Available online: https://www.grandviewresearch.com/industry-analysis/ai-drone-market-report (accessed on 11 August 2025).
95. MarketsandMarkets™. UAV (Drone) Industry Worth $40.56 billion by 2030. Press Release: UAV (Drone) Market (OEM+Aftermarket) Estimated at USD 26.12 Billion in 2025, Projected to Reach USD 40.56 Billion by 2030 (CAGR 9.2% from 2025–2030). 2025. Available online: https://www.marketsandmarkets.com/PressReleases/unmanned-aerial-vehicles-uav.asp (accessed on 18 August 2025).
96. MarketsandMarkets™. UAV (Drone) Market by Type (Fixed Wing, Rotary Wing, Hybrid); Platform (Civil & Commercial, Defense & Government); Point of Sale; Systems; Function; Industry; Application; Mode of Operation; MTOW; Range; Region—Global Forecast to 2030. Estimated UAV (Drone) Market (OEM + Aftermarket) Value: USD 26.12 Billion in 2025; Projected to Reach USD 40.56 Billion by 2030 (CAGR: 9.2% from 2025–2030). 2025. Available online: https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html (accessed on 18 August 2025).
97. Edulakanti, S.R.; Ganguly, S. The emerging drone technology and the advancement of the Indian drone business industry. *J. High Technol. Manag. Res.* **2023**, *34*, 100464. [CrossRef]
98. Anandhi, D.; Keerthana, B.; Velmurugan, D. Skybound Intelligence: AI's Impact on Drone Technology. *Int. J. Sci. Res. Eng. Manag. (IJSREM)* **2024**, *8*, 1–7. [CrossRef]
99. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D.; Alsewari, A.A. A comprehensive collection and analysis model for the drone forensics field. *Sensors* **2022**, *22*, 6486. [CrossRef]
100. Al-Fuwaiers, A.; Mishra, S. ML-based Intrusion Detection for Drone IoT Security. *J. Cybersecur. Inf. Manag.* **2024**, *14*, 64.
101. Yazid, Y.; Ez-Zazi, I.; Guerrero-González, A.; El Oualkadi, A.; Arioua, M. UAV-enabled mobile edge-computing for IoT based on AI: A comprehensive review. *Drones* **2021**, *5*, 148. [CrossRef]
102. Alotaibi, A.; Chatwin, C.; Birch, P. A secure communication framework for drone swarms in autonomous surveillance operations. *J. Comput. Commun.* **2024**, *12*, 1–25. [CrossRef]
103. Javed, S.; Hassan, A.; Ahmad, R.; Ahmed, W.; Ahmed, R.; Saadat, A.; Guizani, M. State-of-the-art and future research challenges in uav swarms. *IEEE Internet Things J.* **2024**, *11*, 19023–19045. [CrossRef]
104. Tang, R.; Tang, J.; Talip, M.S.A.; Aridas, N.K.; Xu, X. Enhanced multi agent coordination algorithm for drone swarm patrolling in durian orchards. *Sci. Rep.* **2025**, *15*, 9139. [CrossRef] [PubMed]
105. Spanaki, K.; Karafili, E.; Sivarajah, U.; Despoudi, S.; Irani, Z. Artificial intelligence and food security: Swarm intelligence of AgriTech drones for smart AgriFood operations. *Prod. Plan. Control* **2022**, *33*, 1498–1516. [CrossRef]
106. He, Y.; Huang, F.; Wang, D.; Chen, B.; Li, T.; Zhang, R. Performance analysis and optimization design of AAV-assisted vehicle platooning in NOMA-enhanced Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 8810–8819. [CrossRef]
107. Ahmed, M.; Soofi, A.A.; Raza, S.; Li, Y.; Khan, F.; Khan, W.U.; Asif, M.; Han, Z. A Comprehensive Survey on RIS-Enhanced Physical Layer Security in UAV-Assisted Networks. *IEEE Internet Things J.* **2025**, *12*, 32538–32562. [CrossRef]
108. Teng, M.; Gao, C.; Wang, Z.; Li, X. A communication-based identification of critical drones in malicious drone swarm networks. *Complex Intell. Syst.* **2024**, *10*, 3197–3211. [CrossRef]
109. Girma, A.; Brown, K. Security Analysis of Drone Communication Methods. In Proceedings of the International Conference on Information Technology-New Generations, Las Vegas, NV, USA, 14–18 April 2024; pp. 125–131.
110. Srivastava, A.; Prakash, J. Future FANET with application and enabling techniques: Anatomization and sustainability issues. *Comput. Sci. Rev.* **2021**, *39*, 100359. [CrossRef]

111. Campion, M.; Ranganathan, P.; Faruque, S. A review and future directions of UAV swarm communication architectures. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 0903–0908.
112. Yue, K. Application of EEUC-based inter aircraft ultraviolet communication network algorithm in energy consumption optimization of drone swarm. *Energy Inform.* **2024**, *7*, 27. [CrossRef]
113. Soria, E.; Schiano, F.; Floreano, D. SwarmLab: A MATLAB drone swarm simulator. In Proceedings of the 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Las Vegas, NV, USA, 24 October 2020–24 January 2021; pp. 8005–8011.
114. Svaigen, A.R.; Boukerche, A.; Ruiz, L.B.; Loureiro, A.A. Trajectory matters: Impact of jamming attacks over the drone path planning on the Internet of Drones. *Ad Hoc Netw.* **2023**, *146*, 103179. [CrossRef]
115. Liu, C.; Huang, L.; Dong, Z. A two-stage approach of joint route planning and resource allocation for multiple UAVs in unmanned logistics distribution. *IEEE Access* **2022**, *10*, 113888–113901. [CrossRef]
116. Lara-Nino, C.A.; Diaz-Perez, A.; Morales-Sandoval, M. Energy/area-efficient scalar multiplication with binary Edwards curves for the IoT. *Sensors* **2019**, *19*, 720. [CrossRef]
117. Yesodha, K.; Krishnamurthy, M.; Thangaramya, K.; Kannan, A. Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. *J. Supercomput.* **2024**, *80*, 18866–18899. [CrossRef]
118. Covaciu, F.; Iordan, A.E. Control of a drone in virtual reality using MEMS sensor technology and machine learning. *Micromachines* **2022**, *13*, 521. [CrossRef]
119. Li, H.; Zhan, Z.; Wang, Z. Energy-consumption model for rotary-wing drones. *J. Field Robot.* **2024**, *41*, 1940–1959. [CrossRef]
120. Tosato, P.; Facinelli, D.; Prada, M.; Gemma, L.; Rossi, M.; Brunelli, D. An autonomous swarm of drones for industrial gas sensing applications. In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–6.
121. Saare, M.A.; Jawad, M.N.; Al-Shareeda, M.A.; Almaiah, M.A.; Obeidat, M. Evaluating elliptic curve cryptography in constrained environments: A Raspberry Pi-based approach. *Int. J. Innov. Res. Sci. Stud.* **2025**, *8*, 3966–3976. [CrossRef]
122. Gope, P.; Millwood, O.; Saxena, N. A provably secure authentication scheme for RFID-enabled UAV applications. *Comput. Commun.* **2021**, *166*, 19–25. [CrossRef]
123. Lounis, K.; Ding, S.H.; Zulkernine, M. D2D-MAP: A drone to drone authentication protocol using physical unclonable functions. *IEEE Trans. Veh. Technol.* **2022**, *72*, 5079–5093. [CrossRef]
124. Ever, Y.K. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* **2020**, *155*, 143–149. [CrossRef]
125. Ganesan, R.; Raajini, X.M.; Nayyar, A.; Sanjeevikumar, P.; Hossain, E.; Ertas, A.H. Bold: Bio-inspired optimized leader election for multiple drones. *Sensors* **2020**, *20*, 3134. [CrossRef] [PubMed]
126. Khan, M.A.; Ullah, I.; Abdullah, A.M.; Mohsan, S.A.H.; Noor, F. An efficient and conditional privacy-preserving heterogeneous signcryption scheme for the Internet of drones. *Sensors* **2023**, *23*, 1063. [CrossRef]
127. Ning, H.; Farha, F.; Ullah, A.; Mao, L. Physical unclonable function: Architectures, applications and challenges for dependable security. *IET Circuits Devices Syst.* **2020**, *14*, 407–424. [CrossRef]
128. Awaludin, A.M.; Park, J.; Wardhani, R.W.; Kim, H. A high-performance ECC processor over Curve448 based on a novel variant of the Karatsuba formula for asymmetric digit multiplier. *IEEE Access* **2022**, *10*, 67470–67481. [CrossRef]
129. Pu, C.; Choo, K.K.R. Lightweight Sybil attack detection in IoT based on bloom filter and physical unclonable function. *Comput. Secur.* **2022**, *113*, 102541. [CrossRef]
130. Alaya, H.; Ben Letaifa, A.; Rachedi, A. State of the art and taxonomy survey on federated learning and blockchain integration in UAV applications. *J. Supercomput.* **2025**, *81*, 655. [CrossRef]
131. Khan, M.A.; Shah, H.; Rehman, S.U.; Kumar, N.; Ghazali, R.; Shehzad, D.; Ullah, I. Securing internet of drones with identity-based proxy signcryption. *IEEE Access* **2021**, *9*, 89133–89142. [CrossRef]
132. Shelare, S.; Belkhode, P.; Nikam, K.C.; Yelamasetti, B.; Gajbhiye, T. A payload based detail study on design and simulation of hexacopter drone. *Int. J. Interact. Des. Manuf. (IJIDeM)* **2024**, *18*, 2675–2692. [CrossRef]
133. Sabuncu, Ö.; Bilgehan, B. Revolutionizing healthcare 5.0: Blockchain-driven optimization of drone-to-everything communication using 5G network for enhanced medical services. *Technol. Soc.* **2024**, *77*, 102552. [CrossRef]
134. Rahbari, D.; Alam, M.M.; Le Moullec, Y.; Jenihhin, M. Fast and fair computation offloading management in a swarm of drones using a rating-based federated learning approach. *IEEE Access* **2021**, *9*, 113832–113849. [CrossRef]
135. Gope, P.; Sikdar, B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13621–13630. [CrossRef]
136. Mohsan, S.A.H.; Othman, N.Q.H.; Li, Y.; Alsharif, M.H.; Khan, M.A. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot.* **2023**, *16*, 109–137. [CrossRef] [PubMed]

137. Banafaa, M.K.; Pepeoğlu, Ö.; Shayea, I.; Alhammadi, A.; Shamsan, Z.A.; Razaz, M.A.; Alsagabi, M.; Al-Sowayan, S. A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges. *IEEE Access* **2024**, *12*, 7786–7826. [CrossRef]
138. Zulkifley, M.A.; Behjati, M.; Nordin, R.; Zakaria, M.S. Mobile network performance and technical feasibility of LTE-powered unmanned aerial vehicle. *Sensors* **2021**, *21*, 2848. [CrossRef] [PubMed]
139. Kolios, A. Assessing risks for the use of drones for wind turbine inspections. *J. Phys. Conf. Ser.* **2024**, *2767*, 032030. [CrossRef]
140. Liu, X.; Ahmad, S.F.; Anser, M.K.; Ke, J.; Irshad, M.; Ul-Haq, J.; Abbas, S. Cyber security threats: A never-ending challenge for e-commerce. *Front. Psychol.* **2022**, *13*, 927398. [CrossRef]
141. Sihag, V.; Choudhary, G.; Choudhary, P.; Dragoni, N. Cyber4drone: A systematic review of cyber security and forensics in next-generation drones. *Drones* **2023**, *7*, 430. [CrossRef]
142. Alsariera, Y.A.; Awwad, W.F.; Algarni, A.D.; Elmannai, H.; Gamarra, M.; Escorcia-Gutierrez, J. Enhanced Dwarf Mongoose optimization algorithm with deep learning-based attack detection for drones. *Alex. Eng. J.* **2024**, *93*, 59–66. [CrossRef]
143. Zhu, C.; Zhu, X.; Qin, T. An efficient privacy protection mechanism for blockchain-based federated learning system in UAV-MEC Networks. *Sensors* **2024**, *24*, 1364. [CrossRef]
144. Ezuma, M.; Erden, F.; Anjinappa, C.K.; Ozdemir, O.; Guvenc, I. Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference. *IEEE Open J. Commun. Soc.* **2019**, *1*, 60–76. [CrossRef]
145. Mykytyn, P.; Brzozowski, M.; Dyka, Z.; Langendoerfer, P. GPS-spoofing attack detection mechanism for UAV swarms. *arXiv* **2023**, arXiv:2301.12766. [CrossRef]
146. Atheeq, C.; Gulzar, Z.; Al Reshan, M.S.; Alshahrani, H.; Sulaiman, A.; Shaikh, A. Securing uav networks: A lightweight chaotic-frequency hopping approach to counter jamming attacks. *IEEE Access* **2024**, *12*, 38685–38699. [CrossRef]
147. Mekdad, Y.; Acar, A.; Aris, A.; El Fergougui, A.; Conti, M.; Lazzeretti, R.; Uluagac, S. Exploring jamming and hijacking attacks for micro aerial drones. In Proceedings of the ICC 2024-IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024; pp. 1939–1944.
148. Omolara, A.E.; Alawida, M.; Abiodun, O.I. Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey. *Neural Comput. Appl.* **2023**, *35*, 23063–23101. [CrossRef]
149. Thubron, R. Drones Helped Hackers Penetrate Financial Firm Network Remotely. 2022. Available online: https://www.techspot.com/news/96321-drones-helped-hackers-penetrate-financial-firm-network-remotely.html (accessed on 25 August 2025).
150. Wadhwani, S. U.S. Financial Services Company Targeted by Hackers Using DJI Drones. 2022. Available online: https://www.spiceworks.com/it-security/network-security/news/wifi-cyberattack-using-drones/ (accessed on 25 August 2025).
151. Pardhasaradhi, B.; Cenkeramaddi, L.R. GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion. *IEEE Sens. J.* **2022**, *22*, 11122–11134. [CrossRef]
152. Lo, S.; Liu, Z.; Ibrahim, L.; Chen, Y.H.; Walter, T. Observations of GNSS Spoofing in Russia in 2023–2024. In Proceedings of the 2025 International Technical Meeting of The Institute of Navigation, Anaheim, CA, USA, 26–29 January 2025; pp. 425–442.
153. Ren, Y.; Restivo, R.D.; Tan, W.; Wang, J.; Liu, Y.; Jiang, B.; Wang, H.; Song, H. Knowledge distillation-based gps spoofing detection for small uav. *Future Internet* **2023**, *15*, 389. [CrossRef]
154. Richter-Brockmann, J.; Sasdrich, P.; Güneysu, T. Revisiting fault adversary models–hardware faults in theory and practice. *IEEE Trans. Comput.* **2022**, *72*, 572–585. [CrossRef]
155. Grandamme, P.; Tissot, P.A.; Bossuet, L.; Dutertre, J.M.; Colombier, B.; Grosso, V. Switching off your device does not protect against fault attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2024**, *2024*, 425–450. [CrossRef]
156. Greenberg, A. A $500 Open-Source Tool Lets Anyone Hack Computer Chips with Lasers. Wired. RayV Lite by NetSPI Enables Laser Fault Injection and Laser Logic State Imaging Using Low-Cost, Open-Source Components to Democratize Hardware-Level Chip Hacking. 2024. Available online: https://www.wired.com/story/rayv-lite-laser-chip-hacking-tool/ (accessed on 13 August 2025).
157. Albakri, A.; Alshahrani, R.; Alharbi, F.; Ahamed, S.B. Fully homomorphic encryption with optimal key generation secure group communication in Internet of Things environment. *Appl. Sci.* **2023**, *13*, 6055. [CrossRef]
158. Tychola, K.A.; Voulgaridis, K.; Lagkas, T. Beyond flight: Enhancing the Internet of Drones with blockchain technologies. *Drones* **2024**, *8*, 219. [CrossRef]
159. Raivi, A.M.; Huda, S.A.; Alam, M.M.; Moh, S. Drone routing for drone-based delivery systems: A review of trajectory planning, charging, and security. *Sensors* **2023**, *23*, 1463. [CrossRef] [PubMed]
160. Alshahrani, H.; Islam, N.; Syed, D.; Sulaiman, A.; Al Reshan, M.S.; Rajab, K.; Shaikh, A.; Shuja-Uddin, J.; Soomro, A. Sustainability in blockchain: A systematic literature review on scalability and power consumption issues. *Energies* **2023**, *16*, 1510. [CrossRef]
161. Ilakkiya, N.; Rajaram, A. A secured trusted routing using the structure of a novel directed acyclic graph-blockchain in mobile ad hoc network internet of things environment. *Multimed. Tools Appl.* **2024**, *83*, 87903–87928. [CrossRef]
162. Fang, J.; Li, Y.; Ji, P.N.; Wang, T. Drone detection and localization using enhanced fiber-optic acoustic sensor and distributed acoustic sensing technology. *J. Light. Technol.* **2022**, *41*, 822–831. [CrossRef]

163. Shan, L.; Miura, R.; Kagawa, T.; Ono, F.; Li, H.B.; Kojima, F. Machine learning-based field data analysis and modeling for drone communications. *IEEE Access* **2019**, *7*, 79127–79135. [CrossRef]
164. Da Silva, R.I.; Rezende, J.D.C.V.; Souza, M.J.F. Collecting large volume data from wireless sensor network by drone. *Ad Hoc Netw.* **2023**, *138*, 103017. [CrossRef]
165. Dehkordi, A.S.; Zehmakan, A.N. More Efficient Sybil Detection Mechanisms Leveraging Resistance of Users to Attack Requests. *arXiv* **2025**, arXiv:2501.16624. [CrossRef]
166. Airlangga, G.; Liu, A. A study of the data security attack and defense pattern in a centralized UAV–cloud architecture. *Drones* **2023**, *7*, 289. [CrossRef]
167. Al-Meer, A.; Al-Kuwari, S. Physical unclonable functions (PUF) for IoT devices. *ACM Comput. Surv.* **2023**, *55*, 1–31. [CrossRef]
168. Demigha, O.; Larguet, R. Hardware-based solutions for trusted cloud computing. *Comput. Secur.* **2021**, *103*, 102117. [CrossRef]
169. McGrath, T.; Bagci, I.E.; Wang, Z.M.; Roedig, U.; Young, R.J. A puf taxonomy. *Appl. Phys. Rev.* **2019**, *6*, 011303. [CrossRef]
170. Lata, K.; Cenkeramaddi, L.R. Fpga-based puf designs: A comprehensive review and comparative analysis. *Cryptography* **2023**, *7*, 55. [CrossRef]
171. Verri, F.A.N.; Marcondes, C.A.; Loubach, D.S.; Sbruzzi, E.F.; Marques, J.C.; Júnior, L.A.P.; Maximo, M.R.O.D.A.; Curtis, V.V. An analysis on tradable permit models for last-mile delivery drones. *IEEE Access* **2020**, *8*, 186279–186290. [CrossRef]
172. Kang, W.; Jeong, E.; Shim, S.; Ha, S. Optimization of Task Allocation for Resource-Constrained Swarm Robots. *IEEE Trans. Autom. Sci. Eng.* **2024**, *22*, 3068–3085. [CrossRef]
173. Khalil, H.; Rahman, S.U.; Ullah, I.; Khan, I.; Alghadhban, A.J.; Al-Adhaileh, M.H.; Ali, G.; ElAffendi, M. A UAV-swarm-communication model using a machine-learning approach for search-and-rescue applications. *Drones* **2022**, *6*, 372. [CrossRef]
174. Shafik, W. Cyber security perspectives in public spaces: Irone case study. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems*; IGI Global: Hershey, PA, USA, 2023; pp. 79–97.
175. Kehoe, A. Navy Ships Swarmed by Drones, Not UFOs, Defense Officials Confirm. The War Zone 2022. DoD Officials Confirmed During a Congressional Hearing That Mysterious Swarms of Objects Around U.S. Navy Ships Off Southern California in July 2019 Were Drones—Not UFOs—Prompting Defensive Measures Including Onboard Security and Radio-Frequency Counter-Drone Responses. Available online: https://www.twz.com/navy-ships-swarmed-by-drones-not-ufos-defense-officials-confirm (accessed on 20 August 2025).
176. Fox News. Unknown Drone Fleet Breached US Military Base Airspace in Virginia for 17 Straight Days. 2025. Available online: https://www.foxnews.com/politics/unknown-drone-fleet-breached-us-military-base-airspace-virginia-17-straight-days-report (accessed on 18 August 2025).
177. U.S. Attorney's Office, Middle District of Tennessee. Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville. Press Release: Skyler Philippi, 24, Was Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and Destroy an Energy Facility in Nashville, Allegedly Motivated by White Supremacist Ideology. Threat Includes Drone-Based Sabotage of the Power Grid. 2024. Available online: https://www.justice.gov/usao-mdtn/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy (accessed on 15 August 2025).
178. Marizco, M. Man Arrested for Using Drones to Smuggle Meth Across Border. *Border Report*, 18 August 2025.
179. Obiuto, N.C.; Festus-Ikhuoria, I.C.; Olajiga, O.K.; Adebayo, R.A. Reviewing the role of ai in drone technology and applications. *Comput. Sci. IT Res. J.* **2024**, *5*, 741–756. [CrossRef]
180. Alioto, M. Trends in hardware security: From basics to ASICs. *IEEE Solid-State Circuits Mag.* **2019**, *11*, 56–74. [CrossRef]
181. Wali, A.; Das, S. Hardware and information security primitives based on 2D materials and devices. *Adv. Mater.* **2023**, *35*, 2205365. [CrossRef]
182. De, A.; Basu, A.; Ghosh, S.; Jaeger, T. Hardware assisted buffer protection mechanisms for embedded RISC-V. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 4453–4465. [CrossRef]
183. Michailidis, E.T.; Vouyioukas, D. A review on software-based and hardware-based authentication mechanisms for the internet of drones. *Drones* **2022**, *6*, 41. [CrossRef]
184. Wang, Y.; Su, Z.; Ni, J.; Zhang, N.; Shen, X. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. *IEEE Commun. Surv. Tutor.* **2021**, *24*, 160–209. [CrossRef]
185. Tun, N.W.; Mambo, M. Secure PUF-based authentication systems. *Sensors* **2024**, *24*, 5295. [CrossRef]
186. Pinto, S.; Santos, N. Demystifying arm trustzone: A comprehensive survey. *ACM Comput. Surv. (CSUR)* **2019**, *51*, 1–36. [CrossRef]
187. Haj-Yahya, J.; Wong, M.M.; Pudi, V.; Bhasin, S.; Chattopadhyay, A. Lightweight secure-boot architecture for risc-v system-on-chip. In Proceedings of the 20th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 6–7 March 2019; pp. 216–223.
188. Valente, L.; Nadalini, A.; Veeran, A.H.C.; Sinigaglia, M.; Sá, B.; Wistoff, N.; Tortorella, Y.; Benatti, S.; Psiakis, R.; Kulmala, A.; et al. A heterogeneous risc-v based soc for secure nano-uav navigation. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2024**, *71*, 2266–2279. [CrossRef]

189. Taneja, S. Energy-efficient and low-cost hardware security primitives for secure ubiquitous computing. In Proceedings of the 65th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2022), Fukuoka, Japan, 7–10 August 2022.
190. Kamali, H.M.; Azar, K.Z.; Farahmandi, F.; Tehranipoor, M. Advances in logic locking: Past, present, and prospects. *Cryptol. Eprint Arch.* **2022**.
191. Bernard, C.; Bryant, W.; Becker, R.; Di, J. Design of asynchronous polymorphic logic gates for hardware security. In Proceedings of the 2021 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 20–24 September 2021; pp. 1–5.
192. Azar, K.Z.; Kamali, H.M.; Farahmandi, F.; Tehranipoor, M. *Understanding Logic Locking*; Springer: Berlin/Heidelberg, Germany, 2024.
193. Garb, K.; Obermaier, J.; Ferres, E.; Künig, M. Fortress: FORtified tamper-resistant envelope with embedded security sensor. In Proceedings of the 2021 18th International Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 13–15 December 2021; pp. 1–12.
194. Trusted Platform Module. 2018. Available online: https://researchedsolution.wordpress.com/2013/09/14/trusted-platform-module/ (accessed on 25 July 2025).
195. Lu, D.; Han, R.; Shen, Y.; Dong, X.; Ma, J.; Du, X.; Guizani, M. xTSeH: A trusted platform module sharing scheme towards smart IoT-eHealth devices. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 370–383. [CrossRef]
196. Sharma, G.; Joshi, A.M.; Mohanty, S.P. Fortified-grid: Fortifying smart grids through the integration of the trusted platform module in internet of things devices. *Information* **2023**, *14*, 491. [CrossRef]
197. Al-Hazbi, S.; Hussain, A.; Sciancalepore, S.; Oligeri, G.; Papadimitratos, P. Radio frequency fingerprinting via deep learning: Challenges and opportunities. In Proceedings of the 2024 International Wireless Communications and Mobile Computing (IWCMC) Ayia Napa, Cyprus, 27–31 May 2024; pp. 0824–0829.
198. Wei, J.; Yu, L.; Zhu, L.; Zhou, X. RF fingerprint extraction method based on CEEMDAN and multidomain joint entropy. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5326892. [CrossRef]
199. Al-Ghuraybi, H.A.; AlZain, M.A.; Soh, B. Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. *Multimed. Tools Appl.* **2024**, *83*, 35629–35672. [CrossRef]
200. Mars, A.; Ghandour, H.; Adi, W. SRAM-SUC: Ultra-Low Latency Robust Digital PUF. *arXiv* **2021**, arXiv:2106.07105.
201. Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comput. Netw.* **2020**, *183*, 107593. [CrossRef]
202. Kim, J.S.; Patel, M.; Hassan, H.; Mutlu, O. The DRAM latency PUF: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity DRAM devices. In Proceedings of the 2018 IEEE International Symposium on High Performance Computer Architecture (HPCA), Vienna, Austria, 24–28 February 2018; pp. 194–207.
203. Papageorgiou, O.; Sedlmeir, J.; Fridgen, G.; Vlachos, I.; Kostopoulos, N.; Damvakeraki, T.; Noszek, Z.; Papoutsoglou, I.; Anania, A.; Belotti, M.; et al. Energy efficiency of blockchain technologies. In *Energy Efficiency of Blockchain Technologies*; European Union Blockchain Observatory & Forum: Brussels, Belgium, 2021.
204. Choi, J.; Son, S.; Kwon, D.; Park, Y. A puf-based secure authentication and key agreement scheme for the internet of drones. *Sensors* **2025**, *25*, 982. [CrossRef]
205. Choe, H.; Kang, D. ECC based Authentication Protocol for Military Internet of Drone (IoD): A Holistic Security Framework. *IEEE Access* **2025**, *13*, 21503–21519. [CrossRef]
206. Zhou, Z.; Li, G.; Zhang, Y.; Zheng, Z.; Yuan, T.; Wang, P. A Strong PUF Based Security Protocol to Protect AI Model Parameters against Privacy Information Leakage. *IEEE Internet Things J.* **2025**, *12*, 20815–20827. [CrossRef]
207. Basan, E.; Makarevich, O.; Lapina, M.; Mecella, M. Analysis of the Impact of a GPS Spoofing Attack on a UAV. In Proceedings of the CEUR Workshop Proceedings, Ljubljana, Slovenia, 29 November 2022; Volume 3094, pp. 6–16.
208. Torba, E.; Jahankhani, H. Securing Systems from Aerial Threats: Cybersecurity in the Drone Era. In *Autonomous Revolution: Strategies, Threats and Challenges*; Springer: Berlin/Heidelberg, Germany, 2025; pp. 261–306.
209. Wang, W.; Chen, Q.; Yin, Z.; Srivastava, G.; Gadekallu, T.R.; Alsolami, F.; Su, C. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet Things J.* **2021**, *9*, 8883–8891. [CrossRef]
210. Gao, Y.; Su, Y.; Xu, L.; Ranasinghe, D.C. Lightweight (reverse) fuzzy extractor with multiple reference PUF responses. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1887–1901. [CrossRef]
211. Ayub, M.F.; Saleem, M.A.; Altaf, I.; Mahmood, K.; Kumari, S. Fuzzy extraction and PUF based three party authentication protocol using USB as mass storage device. *J. Inf. Secur. Appl.* **2020**, *55*, 102585. [CrossRef]
212. Wang, H.; Hao, W.; Tang, Y.; Zhu, B.; Dong, W.; Liu, W. Deep neural network modeling attacks on arbiter-PUF-based designs. *Cybersecurity* **2025**, *8*, 11. [CrossRef]
213. Ebrahimabadi, M.; Lalouani, W.; Younis, M.; Karimi, N. Countering PUF modeling attacks through adversarial machine learning. In Proceedings of the 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Tampa, FL, USA, 7–9 July 2021; pp. 356–361.

214. Yang, Z.; Zhang, Y.; Zeng, J.; Yang, Y.; Jia, Y.; Song, H.; Lv, T.; Sun, Q.; An, J. AI-Driven safety and security for UAVs: From machine learning to large language models. *Drones* **2025**, *9*, 392. [CrossRef]
215. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography. 2024. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed on 29 September 2025).
216. Khan, M.A.; Javaid, S.; Mohsan, S.A.H.; Tanveer, M.; Ullah, I. Future-proofing security for UAVs with post-quantum cryptography: A review. *IEEE Open J. Commun. Soc.* **2024**, *5*, 6849–6871. [CrossRef]
217. Alagic, G.; Bros, M.; Ciadoux, P.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.K.; Miller, C.; et al. *Status Report on the Fourth Round of the Nist Post-Quantum Cryptography Standardization Process*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025.
218. Mauw, S.; Smith, Z.; Toro-Pozo, J.; Trujillo-Rasua, R. Distance-bounding protocols: Verification without time and location. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 549–566.
219. Medley, L.; Loe, A.F.; Quaglia, E.A. Sok: Delay-based cryptography. In Proceedings of the 2023 IEEE 36th Computer Security Foundations Symposium (CSF), Dubrovnik, Croatia, 10–14 July 2023; pp. 169–183.
220. Languell, Z.P.; Gu, Q. Securing ADS-B with multi-point distance-bounding for UAV collision avoidance. In Proceedings of the 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Monterey, CA, USA, 4–7 November 2019; pp. 145–153.
221. Wang, B.; Song, H.; Rhee, W.; Wang, Z. Overview of ultra-wideband transceivers—System architectures and applications. *Tsinghua Sci. Technol.* **2021**, *27*, 481–494. [CrossRef]
222. Khan, S.; Thorn, J.; Wahlgren, A.; Gurtov, A. Intrusion detection in automatic dependent surveillance-broadcast (ADS-B) with machine learning. In Proceedings of the 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 3–7 October 2021; pp. 1–10.
223. Lin, Z.; Castano, L.; Mortimer, E.; Xu, H. Fast 3D collision avoidance algorithm for fixed wing UAS. *J. Intell. Robot. Syst.* **2020**, *97*, 577–604. [CrossRef]
224. Li, S.; Meng, Q.; Bai, Y.; Zhang, C.; Song, Y.; Li, S.; Lu, L. Go beyond rfid: Rethinking the design of rfid sensor tags for versatile applications. In Proceedings of the 29th Annual International Conference on Mobile Computing and Networking, Madrid, Spain, 2–6 October 2023; pp. 1–16.
225. Kanagala, P. Implementing cryptographic-based DH approach for enterprise network. *Optik* **2023**, *272*, 170252. [CrossRef]
226. Wei, X.; El-Hadedy, M.; Mosanu, S.; Zhu, Z.; Hwu, W.M.; Guo, X. RECO-HCON: A high-throughput reconfigurable compact ascon processor for trusted iot. In Proceedings of the 2022 IEEE 35th International System-on-Chip Conference (SOCC), Belfast, UK, 5–8 September 2022; pp. 1–6.
227. Hwang, J.; Kale, G.; Patel, P.P.; Vishwakarma, R.; Aliasgari, M.; Hedayatipour, A.; Rezaei, A.; Sayadi, H. Machine learning in chaos-based encryption: Theory, implementations, and applications. *IEEE Access* **2023**, *11*, 125749–125767. [CrossRef]
228. Kalutharage, C.S.; Mohan, S.; Liu, X.; Chrysoulas, C. Enhancing Automotive Intrusion Detection Systems with Capability Hardware Enhanced RISC Instructions-Based Memory Protection. *Electronics* **2025**, *14*, 474. [CrossRef]
229. Loe, A.F.; Medley, L.; O'Connell, C.; Quaglia, E.A. TIDE: A novel approach to constructing timed-release encryption. In Proceedings of the Australasian Conference on Information Security and Privacy, Wollongong, Australia, 28–30 November 2022; pp. 244–264.
230. Nair, A.S.; Thampi, S.M. A location-aware physical unclonable function and Chebyshev map-based mutual authentication mechanism for internet of surveillance drones. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7564. [CrossRef]
231. Nair, A.S.; Thampi, S.M. PUFloc: PUF and location based hierarchical mutual authentication protocol for surveillance drone networks. In Proceedings of the Inernational Conference on Ubiquitous Security, Guangzhou, China, 28–31 December 2021; pp. 66–89.
232. Sindiramutty, S.R.; Jhanjhi, N.Z.; Tan, C.E.; Yun, K.J.; Manchuri, A.R.; Ashraf, H.; Murugesan, R.K.; Tee, W.J.; Hussain, M. Data security and privacy concerns in drone operations. In *Cybersecurity Issues and Challenges in the Drone Industry*; IGI Global Scientific Publishing: Hershey, PA, USA, 2024; pp. 236–290.
233. Jones, T. *International Commercial Drone Regulation and Drone Delivery Services*; Technical Report; RAND: Santa Monica, CA, USA, 2017.
234. Stöcker, C.; Bennett, R.; Nex, F.; Gerke, M.; Zevenbergen, J. Review of the current state of UAV regulations. *Remote Sens.* **2017**, *9*, 459.
235. International Civil Aviation Organization. *Unmanned Aircraft Systems (UAS): Report on the Global Regulatory & Standards Situation—2022*; Technical Report; International Civil Aviation Organization: Montreal, QC, Canada, 2022.
236. Sipos, A. ICAO Standards and Recommended Practices (SARPs). In *International Aviation Law: Regulations in Three Dimensions*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 203–231.
237. Janke, C.; de Haag, M.U. Implementation of European drone regulations-status quo and assessment. *J. Intell. Robot. Syst.* **2022**, *106*, 33. [CrossRef]

238. Rauhala, A.; Tuomela, A.; Leviäkangas, P. An overview of unmanned aircraft systems (UAS) governance and regulatory frameworks in the European Union (EU). In *Unmanned Aerial Systems in Agriculture*; Academic Press: Cambridge, MA, USA, 2023; pp. 269–285.
239. Olumba, E.E. The necropolitics of drone bases and use in the African context. *Crit. Stud. Terror.* **2025**, *18*, 139–161. [CrossRef]
240. Watney, M. Ethical and Legal Aspects Pertaining to law Enforcement use of Drones. In Proceedings of the International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022; Volume 17, pp. 358–365.
241. AL-Dosari, K.; Hunaiti, Z.; Balachandran, W. Systematic review on civilian drones in safety and security applications. *Drones* **2023**, *7*, 210. [CrossRef]
242. Bassi, E. European drones regulation: Today's legal challenges. In Proceedings of the 2019 International Conference on Unmanned Aircraft Systems (ICUAS), Atlanta, GA, USA, 11–14 June 2019; pp. 443–450.
243. van der Sluijs, J.; Saiet, E.; Bakelaar, C.N.; Wentworth, A.; Fraser, R.H.; Kokelj, S.V. Beyond visual-line-of-sight (BVLOS) drone operations for environmental and infrastructure monitoring: A case study in northwestern Canada. *Drone Syst. Appl.* **2023**, *11*, 1–15. [CrossRef]
244. Phadke, A.; Medrano, F.A. Towards resilient UAV swarms—A breakdown of resiliency requirements in UAV swarms. *Drones* **2022**, *6*, 340. [CrossRef]
245. Ariante, G.; Del Core, G. Unmanned aircraft systems (UASs): Current state, emerging technologies, and future trends. *Drones* **2025**, *9*, 59. [CrossRef]
246. Kucharczyk, M.; Hugenholtz, C.H. Remote sensing of natural hazard-related disasters with small drones: Global trends, biases, and research opportunities. *Remote Sens. Environ.* **2021**, *264*, 112577. [CrossRef]
247. Pu, C.; Wall, A.; Choo, K.K.R.; Ahmed, I.; Lim, S. A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment. *IEEE Internet Things J.* **2022**, *9*, 9918–9933. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

https://dspace.org/

Building trust in autonomous aerial systems: a review of hardware-rooted trust mechanisms

Ahmad, Sagir Muhammad; Samie, Mohammad; Honarvar Shakibaei Asli, Barmak

2025-10-01
MDPI
https://doi.org/10.3390/fi17100466
Ahmad SM, Samie M, Honarvar Shakibaei Asli B. (2025) Building trust in autonomous aerial systems: a review of hardware-rooted trust mechanisms. Future Internet, Volume 17, Issue 10, October 2025, Article number 466

Downloaded from a DSpace repository. https://dspace.org/