Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

Privacy Issues and Solutions for UAVs in B5G Networks: A Survey

Mahnoor Arshad[1*], Irshad Ahmed Sumra[2], Abdul Sattar[2], and Muhammad Sharjeel[1]

[1]Department of Data Science, Lahore Garrison University, Lahore, Pakistan.
[2]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan.
[*]Corresponding Author: Mahnoor Arshad. Email: mahnoorarshad8@gmail.com

Received: August 21, 2024 **Accepted:** December 01, 2024

Abstract: Unmanned aerial vehicles (UAVs) within the context of beyond 5G (B5G) technology are pivotal in transforming a range of sectors, including surveillance, agriculture, and logistics, by facilitating high-speed data transmission, ultra-low latency communication, and highly reliable connectivity. Nevertheless, the incorporation of UAVs into B5G networks raises significant privacy challenges. These challenges include the potential for unauthorized access, data breaches, and cyber-physical attacks, all of which threaten the integrity, confidentiality and availability of UAV operations. Furthermore, UAVs operating within B5G networks are particularly vulnerable to machine learning (ML)-based attacks that exploit weaknesses in ML models, resulting in adversarial manipulation, data poisoning, and model evasion techniques. Such vulnerabilities can undermine the integrity of UAV operations, cause navigation inaccuracies, and compromise sensitive data collected by these vehicles. In light of these privacy issues, this review article aims to present emerging solutions tailored for UAVs in B5G networks. Initially, we provide a foundational overview of the integration of UAVs into B5G networks, highlighting both the benefits and the security challenges associated with this novel integrated network architecture. Subsequently, we analyze the privacy landscape by identifying the threats and requirements pertinent to UAVs in B5G environments. Based on this analysis, we discuss and elaborate on potential solutions, including federated learning (FL), and post-quantum cryptography (PQC).

Keywords: B5G Networks; Unmanned Aerial Vehicles (UAVs); Federated Learning (FL); Post-Quantum Cryptography (PQC).

1. Introduction

Unmanned aerial vehicles (UAVs) are poised to assume a significant role in networks beyond 5G (B5G), owing to their growing prevalence and utility across various civilian and military domains [1-2]. B5G networks are expected to emulate the advancements of 5G networks by offering UAVs comprehensive coverage, enhanced intelligence, automation, and extensive connectivity, accompanied by diverse quality-of-service (QoS) provisions [3]. Despite the existing regulatory frameworks governing the use of UAVs in civilian and commercial contexts, which impose certain limitations on their expansion and integration, the potential for UAVs to operate autonomously could lead to a scenario where the skies are populated with swarms of UAVs, akin to flocks of birds executing their respective tasks across multiple sectors [4]. To achieve this ambitious vision for UAVs, B5G networks have catalyzed the development of several enabling technologies, including network function virtualization (NFV), multi-access edge computing (MEC), network slicing (NS), and software-defined networking (SDN) [5–19]. NFV facilitates the rapid deployment of new services and offers flexibility by decoupling network operations from the underlying hardware, thereby enhancing the scalability and operational capabilities of UAVs for mission-critical tasks. Conversely, SDN enables the dynamic and programmable configuration and monitoring of networks, which is instrumental in the comprehensive and global management of UAV networks [20]. Through the implementation of Multi-access Edge Computing (MEC), Unmanned Aerial Vehicles (UAVs) with constrained computational and storage capabilities can leverage cloud computing services to execute complex computations and manage extensive storage tasks [21]. Network Slicing (NS) facilitates the customization of services and the segregation of resources by establishing multiple logical networks on a single physical infrastructure [22].

On one hand, the integration of UAVs with Beyond 5G (B5G) networks can enhance the automation and intelligence of these aerial systems [23– 28]. Conversely, the deployment of UAVs for extensive commercial and civilian purposes within national airspace raises significant security and privacy concerns [29]. The incorporation of UAVs into national airspace poses risks to individual privacy and the security of critical infrastructure, such as nuclear power facilities and research institutions [30]. The onboard sensors and modules commonly integrated into Unmanned Aerial Vehicles (UAVs), such as cameras, GPS, gyroscopes, inertial measurement units (IMUs), storage systems, and wireless communication modules, possess the capability to record, store, locate, and transmit data that could potentially be utilized for incriminating individuals [31]. Several factors contribute to security vulnerabilities in UAVs, including the lack of security measures like intrusion detection systems (IDS), inadequate onboard computational resources for executing complex cryptographic algorithms, reliance on insecure wireless communication channels, and the inherent high mobility of these systems [32]. These vulnerabilities are particularly pertinent to UAVs and must be addressed when developing security protocols. One proposed solution involves the implementation of physical layer security (PLS) mechanisms, which aim to protect UAV communication channels from unauthorized access, eavesdropping, and interception, thereby safeguarding sensitive information.

Given that Beyond 5G (B5G) networks integrate artificial intelligence and machine learning (AI/ML) as well as edge AI/ML models and techniques within unmanned aerial vehicles (UAVs), it is imperative that these systems incorporate robust security measures to mitigate the risk of AI/ML-related attacks [33]. Failure to address privacy concerns associated with AI/ML could significantly restrict their utilization in the management of next-generation networks. Recent research has identified model inversion and model extraction as two prevalent forms of attacks within the framework of machine learning as a service. In model inversion attacks, adversaries exploit model parameters to reconstruct training data and retrieve sensitive information. Conversely, model extraction attacks involve the acquisition of model parameters through querying the model. Various malicious activities targeting both the training and evaluation phases, such as poisoning attacks, pose significant threats to machine learning methodologies, including evasion attacks [34]. To address the vulnerabilities associated with ML-based attacks, federated learning (FL) offers a privacy-preserving and secure framework for training ML models in UAVs. This approach decentralizes the training process, reduces data exposure, and enhances the resilience of ML models against adversarial threats. The increasing prevalence of quantum computers poses a significant threat to the privacy and security of Unmanned Aerial Vehicles (UAVs) operating within Beyond 5G (B5G) networks. Traditional symmetric and asymmetric encryption methods are vulnerable to quantum attacks, which raises concerns regarding the potential interception of UAV communication links, unauthorized access to data, and data tampering. Such vulnerabilities jeopardize mission-critical operations and sensitive information. In response to this challenge, post-quantum cryptography (PQC) has emerged as a promising solution to safeguard UAVs against quantum threats in both B5G and forthcoming 6G networks.

In summary, Physical Layer Security (PLS) will enhance security at the signal transmission level by utilizing the unique physical characteristics of the 6G environment. Federated Learning (FL) will support distributed artificial intelligence model training on edge devices, thereby preserving data privacy and minimizing latency. PQC will provide robust encryption to secure communications against the anticipated threats posed by quantum computing, ensuring resilience in the highly interconnected landscape of 6G. Collectively, these technologies will establish a comprehensive, multi-layered security framework for 6G networks.

This review analyzes privacy challenges in UAV-enabled B5G networks and evaluates emerging solutions like Federated Learning and Post-Quantum Cryptography

The rest of the paper is organized as follows: Section 2 reviews the existing literature and highlights its limitations, focusing on studies related to security and privacy challenges in UAV-enabled B5G networks. Section 3 provides a comparative analysis of state-of-the-art approaches addressing these challenges. Section 4 outlines the overview of UAV integration in B5G Networks. Section 5 and 6 proposes potential solutions for privacy utilizing Federated Learning (FL), and Post-Quantum Cryptography (PQC) methods. Section 7 presents a comparative evaluation of security solutions for UAV networks. Finally, Section 8 concludes the study.

2. Existing Literature and Their Limitations

In recent years, a substantial body of literature, including reviews, tutorials, and survey articles, has been dedicated to examining various dimensions of privacy concerning Unmanned Aerial Vehicles (UAVs). Notably, Fotouhi et al. [35] published a survey that comprehensively addresses the factors that facilitate the seamless integration of UAVs with 5G technology within cellular networks. The authors emphasized the role of regulatory bodies in the formulation and implementation of new regulations pertaining to public safety and personal privacy. Furthermore, they investigated emerging cyber-physical security challenges and delineated potential avenues for future research. The authors posited that forthcoming networks, such as 5G, possess the capability to mitigate issues arising from UAV operations. In a related study, Nassi et al. [36] conducted an extensive literature review focusing on security and privacy concerns associated with commercial drones. They examined both academic and industry strategies for the detection and neutralization of drones, ultimately proposing future research directions and evaluating the risks associated with permitting drone operations in densely populated areas.

Wuet et al. [37] examined various concepts and strategies aimed at ensuring secure communications between unmanned aerial vehicles (UAVs) and ground stations, particularly in the context of potential malicious eavesdropping and jamming attacks targeting UAVs. The authors addressed identification methods and proposed innovative solutions to effectively tackle physical layer (PHY) security challenges. Their numerical findings substantiate the efficacy of these solutions, and the study also identifies promising avenues for future research.

Wang et al. [38] provided a comprehensive review of UAV networks through the lens of cyber-physical systems (CPS). They analyzed the foundational principles and advancements related to the three core components of CPS within UAV networks. Furthermore, the study explicitly illustrates the interdependencies among these components, which may offer valuable insights for resolving issues pertinent to each individual element. The authors conclude by discussing new research trajectories and unresolved challenges in the field.

Noor et al. [39] conducted a review focusing on the communication aspects of aerial ad-hoc networks, specifically those involving UAVs. They evaluated a range of wireless technologies applicable to UAV networks and advocated for the adoption of 5G and 6G technologies to meet extensive coverage and high throughput demands. This study also addresses critical issues related to the security, privacy, and open research questions surrounding UAV networks.

Yaacoub et al. [40] conducted an investigation into the rise of cyber-attacks and the associated challenges faced by commercial drones. They presented a practical attack scenario, detailing the simulation of an attack on a specific drone following the hacking cycle. Additionally, they introduced novel approaches and technologies aimed at improving the detection and prevention of attacks on unmanned aerial vehicles (UAVs). The authors also addressed the privacy and security concerns related to UAV networks, identifying their limitations and offering recommendations for improvement.

In a separate study, Wang et al. [41] examined critical issues pertaining to UAV communications from the perspective of physical layer security (PLS) within beyond fifth-generation (B5G) networks. They reviewed contemporary research advancements in UAV-PLS, categorizing them into two scenarios: UAVs deployed in static positions and those in motion along predetermined trajectories during communication. Furthermore, they summarized the prevalent methodologies employed in the analysis and design for each scenario and provided a detailed discussion of significant literature in the field. Finally, they underscored several promising avenues for future research.

Shafique et al. [42] conducted a review of the vulnerabilities associated with security measures in unmanned aerial vehicles (UAVs). Their findings led to the formulation of guidelines aimed at enhancing security and identifying future research avenues. Wang et al. [43] investigated prevalent threats to UAV communications in order to establish security requirements. They conducted a thorough assessment of existing security countermeasures designed to bolster UAV communication security at both the physical and network levels. The article concluded with a discussion of unresolved challenges and future prospects for UAV security.

Yang et al. [44] performed an extensive review of security issues and solutions related to drones, delineating security requirements and emphasizing recent advancements in security and privacy research. This review also explored various critical security technologies, with particular attention to authentication methods and blockchain-powered schemes. The authors underscored the limitations of current approaches and proposed future research directions based on a comprehensive analysis. Their research indicates that drone security challenges can be effectively addressed through appropriate security measures, and that new security solutions should prioritize a balance between security and computational costs.

McEnroe et al. [45] provided a thorough review of the influence of edge artificial intelligence (AI) on fundamental technical aspects of UAVs, including security, privacy, AI, and blockchain. The study also addressed the challenges associated with the implementation of UAV-based edge AI, shared lessons learned, and outlined directions for future research.

Sandeepa et al. [46] conducted a comprehensive survey addressing privacy-related issues within B5G/6G networks, which included a taxonomy of various privacy perspectives. They articulated privacy objectives alongside the associated barriers and potential solutions. Furthermore, the authors examined standardization initiatives pertinent to these topics and concluded with a proposed roadmap for future research directions in privacy. Khan et al. [47] presented a review article that focused on the operational dynamics of swarms of Unmanned Aerial Vehicles (UAVs) within 6G mobile networks. This review addressed multiple challenges related to privacy, security, intelligence, and energy efficiency faced by UAV swarms. The authors discussed the integration of Blockchain (BC) and Artificial Intelligence/Machine Learning (AI/ML) technologies within UAV networks, concluding with an outline of research challenges and prospective avenues for future inquiry in the evolving domain of UAV networks in the 6G ecosystem.

Mekdad et al. [48] provided an extensive survey on the privacy and security challenges associated with UAVs, systematically classifying these issues across four levels: hardware, software, communication, and sensor. They identified common vulnerabilities that threaten the civilian applications of UAVs and examined potential active and passive attacks. The authors summarized key insights regarding UAV security and privacy, concluding with suggestions for future research directions.

Hadi et al. [49] explored UAV privacy and security concerns from the perspectives of software, hardware, and communication domains. They thoroughly discussed emerging technologies such as Blockchain, Machine Learning, and Intrusion Detection Systems (IDSs) as solutions to the security challenges faced by UAVs, concluding with a discussion of significant research directions.

In 2024, Banafaa et al. [50] conducted a comprehensive survey on UAVs, addressing deployment scenarios, applications, future technologies, and regulatory considerations within B5G networks. Their examination of regulatory considerations included detailed discussions on privacy, safety, flight guidelines, and spectrum allocation, as well as the identification of key challenges and promising future research directions. In the same year, Javed et al. [51] reviewed critical aspects of UAV swarms, including swarm formation control, security, autonomy, coordination, communication, and swarm path planning. This article also explored recent advancements in UAV swarm algorithms, applications in civilian, commercial, and military contexts, and ethical considerations. The review concluded by identifying potential topics for future research.

3. Comparison of Existing Studies

Table 1. A Comparative Analysis of Existing Studies Addressing Privacy Issues in Unmanned Aerial Vehicles (UAVs) within Beyond 5G (B5G) Networks.

Study	Focus	Proposed Method	Working of Method	Limitations
Fotouhi et al. [35]	Integration of UAVs with 5G networks and regulatory aspects.	Highlighted regulatory body roles; proposed 5G as a solution for UAV issues.	Explored 5G technology integration for addressing UAV challenges and improving network reliability.	Lack of detailed implementation for regulatory frameworks; limited focus on deployment scenarios.
Nassi et al. [36]	Security and privacy in commercial drones; detection and neutralization.	Proposed future research directions; reviewed academic and industry approaches for detection/neutralization.	Evaluated existing detection strategies and suggested better protocols for managing drone risks.	Limited emphasis on real-world deployment in densely populated areas.
Wuet et al. [37]	Secure communication between UAVs and ground stations.	Proposed innovative PHY solutions for eavesdropping and jamming prevention.	Numerical simulations validated proposed solutions for tackling physical layer security issues.	Narrow focus on physical layer (PHY) security; limited coverage of broader attack scenarios.
Wang et al. [38]	UAV networks through the lens of Cyber-Physical Systems (CPS).	Analyzed interdependencies in CPS components to enhance UAV system performance.	Established connections among CPS components and identified unresolved	Lack of practical implementation insights; primarily theoretical.

			research issues for UAV networks.	
Noor et al. [39]	Communication technologies in aerial ad-hoc networks.	Advocated for 5G/6G adoption; addressed security, privacy, and open research questions.	Explored wireless technologies with future networks for extended coverage and high throughput.	Limited emphasis on physical security and implementation challenges of 6G.
Yaacoub et al. [40]	Cyber-attacks and challenges in UAV networks.	Practical attack scenario simulation; proposed detection and prevention approaches.	Simulated drone attacks and recommended advanced detection mechanisms for UAVs.	Simulation-focused with limited real-world testing.
Wang et al. [41]	Physical Layer Security (PLS) in B5G UAV communications.	Reviewed UAV-PLS advancements and categorized static/dynamic trajectory communication scenarios.	Provided a classification of UAV-PLS scenarios and recommended future directions in PLS research.	Limited focus on dynamic trajectory scenarios in PLS.
Shafique et al. [42]	UAV security vulnerabilities.	Guidelines for improving UAV security; identified research gaps.	Highlighted common vulnerabilities and provided recommendations for enhanced UAV security.	Generalized recommendations without specific deployment examples.
Wang et al. [43]	Threat assessment and countermeasures for UAV communications.	Proposed multi-layered security countermeasures.	Assessed existing approaches and suggested layered security models.	Limited focus on hybrid attacks combining physical and network-level vulnerabilities.
Yang et al. [44]	Security issues and solutions, with a focus on authentication and blockchain.	Proposed lightweight authentication mechanisms and blockchain schemes.	Demonstrated blockchain schemes to improve UAV security while minimizing computational costs.	High computational cost of blockchain-based solutions.
McEnroe et al. [45]	Influence of Edge AI on UAVs, addressing security, privacy, and blockchain.	Introduced edge AI with blockchain integration.	Explored lessons from edge AI in UAVs and provided future directions for implementation.	Lack of scalability insights for edge AI implementation.
Sandeepa et al. [46]	Privacy-related issues in B5G/6G networks.	Proposed privacy taxonomy and objectives;	Categorized privacy concerns and suggested solutions tailored	Limited focus on practical applications of

		recommended privacy roadmaps.	for B5G/6G UAV networks.	proposed privacy solutions.
Khan et al. [47]	UAV swarm operations in 6G networks, addressing security and intelligence.	Integrated Blockchain and AI/ML for secure and intelligent UAV swarms.	Combined blockchain with AI/ML techniques to enhance swarm security and coordination.	Limited operational details for UAV swarm management.
Mekdad et al. [48]	UAV security and privacy challenges across four levels (hardware, software, etc.).	Classified challenges and suggested active/passive attack mitigation strategies.	Explored UAV vulnerabilities and offered targeted solutions based on attack type.	Limited focus on real-time attack detection in practical scenarios.
Hadi et al. [49]	Emerging security technologies for UAVs, including IDS and blockchain.	Proposed blockchain and IDS-based security systems.	Discussed resource-efficient IDS and blockchain technologies for UAV security enhancement.	High resource demand for advanced security technologies.
Banafaa et al. [50]	UAV deployment, regulations, and future technologies in B5G networks.	Proposed privacy and spectrum allocation frameworks.	Examined regulations and deployment scenarios for UAVs in emerging networks.	Limited focus on cross-border regulatory challenges.

As presented in Table 1, the surveys, reviews, and tutorials cited address various privacy and security issues pertinent to Unmanned Aerial Vehicle (UAV) networks. However, the existing literature fails to provide a comprehensive examination of all privacy aspects relevant to UAVs within Beyond 5G (B5G) networks. Notably, critical topics such as Post-Quantum Cryptography (PQC), which is essential in contemporary security discourse, are notably absent from the reviewed articles. Additionally, while Federated Learning (FL) shows significant potential for UAV networks, it has only been partially addressed, with limited insights available in references [39] and [45], and more extensive discussions found in [50]. Furthermore, emerging issues such as energy efficiency, intrusion detection systems (IDSs), and cross-layer security strategies receive minimal attention. These observations reveal the fragmented nature of current research and emphasize the urgent need for a comprehensive and systematically organized review that thoroughly investigates all privacy dimensions associated with UAVs in B5G networks. This necessity is further underscored by the growing significance of UAVs and their integration into the B5G ecosystem, rendering privacy challenges a critical focus for future research endeavors.

4. An Overview of UAV Integration in B5G Networks

The integration of UAVs into 5G and B5G networks has opened up exciting possibilities for real-time applications. B5G networks provide advanced technologies and services for UAVs, transforming their connectivity, sensing, and intelligence in the digital era [51–55]. By utilizing UAVs within B5G networks, they can function as aerial base stations (ABSs), delivering reliable, widespread, cost-effective, and easily accessible wireless communication services to targeted areas [56]. Additionally, this integration allows UAVs to act as aerial user equipment (UE) alongside ground users for tasks such as delivery or surveillance.

Furthermore, the increasing demand for data-heavy services can be addressed through physical layering techniques like beamforming, mmWaves, intelligent reflecting surfaces (IRS), cognitive radios, and massive MIMO, which support UAVs operating as both ABS and UE [57]. Moreover, given the limited computing and storage capabilities of UAVs, this integration helps to mitigate these challenges by enabling resource-constrained UAVs to offload computation and storage-heavy tasks to cloud computing servers facilitated by B5G networks.

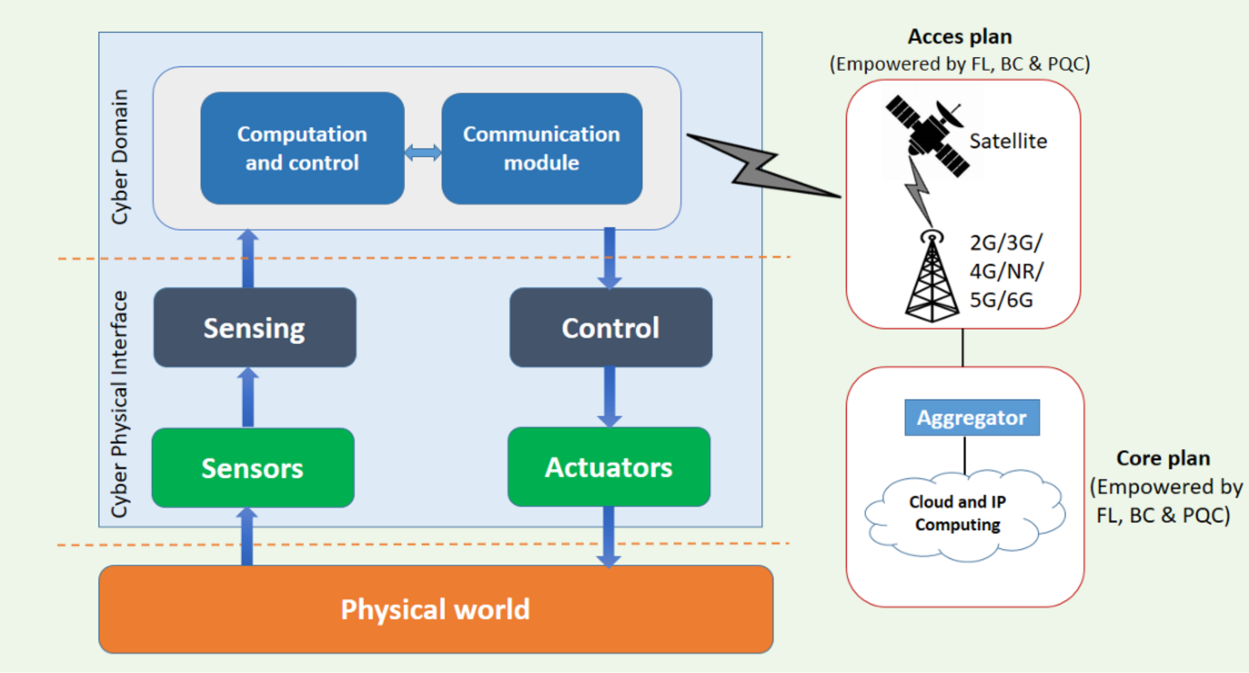

Figure. 1. The interaction among different modules of a typical UAV system in networks B5G [19].

UAVs enhance the unique capabilities and features of B5G's KPIs, including mMTC, uMUB, uHSLLC, and uHDD [58–60]. For instance, UAVs can act as a platform for uMUB, providing high mobility services to access remote and difficult-to-reach areas during disasters or in challenging environments [61]. Likewise, the use of UAVs in uHSLLC can support edge computing, network slicing, and AI technologies, leading to improved network performance and energy efficiency, along with enhanced communication security and privacy [62]. In terms of massive connectivity for devices and sensors, UAVs can play a vital role in mMTC by functioning as ABSs in areas lacking adequate terrestrial communication infrastructure [63]. Additionally, uHDD support can fulfill the needs of UAVs for high data transfer rates, substantial storage, and real-time information processing by leveraging advanced technologies like NFV, SDN, and AI [64-65].

The integration of satellites is a key advancement in B5G networks, enabling UAVs to function worldwide while offering centimeter-level positioning accuracy and diverse quality of service (QoS) options [66]. Furthermore, satellites within B5G networks can accommodate mobility needs of up to 1000 km/h in crowded urban areas, achieving a maximum data transfer rate of 1 TBPS per UAV. Figure 1 depicts how UAVs are incorporated into B5G networks alongside advanced technologies and their associated security aspects.

B5G networks provide numerous benefits for UAVs, but they also introduce specific security challenges. One challenge is the potential use of quantum cryptography in B5G networks. Although it offers exceptional security, UAV operators need to implement quantum-safe encryption algorithms to protect their communications from future quantum attacks [67]. Furthermore, the integration of AI in B5G networks brings its own security issues. UAV operators must utilize AI-based security solutions that can detect and respond to threats in real-time to defend against evolving cyber risks. Additionally, the use of advanced technologies such as holographic beamforming [68] and THz communication requires strong authentication and encryption methods to prevent unauthorized access and tampering. Similarly, Meta surface-based communication n [69-70], a key element of B5G networks, demands strict security protocols to guard against signal interception and manipulation.

In order to tackle the privacy challenges associated with Unmanned Aerial Vehicles (UAVs), it is imperative to adopt sophisticated privacy-preserving strategies within UAV networks. Federated Learning (FL) facilitates collaborative model training among UAVs and ground stations while maintaining the confidentiality of raw data, thus significantly improving data privacy. Furthermore, Post-Quantum Cryptography (PQC) offers resilient encryption methodologies designed to safeguard sensitive UAV communications from potential future threats posed by quantum computing. The incorporation of these privacy-centric solutions into UAV operations within Beyond 5G (B5G) networks not only enhances data confidentiality but also ensures secure information exchange, thereby reducing privacy-related risks.

This section explored how UAVs can be integrated into B5G networks, enhancing their capabilities with cloud computing services, improved scalability, increased mobility, and better availability. Figure 1 shows a sample architecture for this integration. UAVs contribute to key performance indicators (KPIs) of B5G, such as massive Machine Type Communications (mMTC), ultra-reliable Low Latency Communications (uHSLLC), and ultra-high Data Density (uHDD), facilitating tasks like high-level computation, storage, and processing. We also examined the role of satellite integration in UAV communication within B5G networks, which provides UAVs with centimeter-level positioning accuracy, widespread connectivity, global coverage, and diverse Quality of Service (QoS) options. This satellite can achieve a maximum data throughput of 1 TBPS per device and support autonomous mobility at speeds of up to 1,000 km/h in remote areas. While B5G networks offer numerous benefits for UAVs, they also introduce various privacy challenges, including traditional threats as well as those arising from machine learning, artificial intelligence, and quantum computing. Finally, we proposed potential solutions utilizing Federated Learning (FL), and Post-Quantum Cryptography (PQC) methods.

5. Federated Learning

Federated Learning (FL) is a machine learning approach that enables devices or entities to collaboratively train a common model locally without disclosing their individual data to a central server [71-72]. This method is particularly advantageous for Unmanned Aerial Vehicles (UAVs) due to their unique characteristics and challenges [73]. UAVs often collect sensitive information, such as images, videos, or sensor data, during their operations. In these cases, they can independently train machine learning models without transmitting raw data to a central server; instead, they only send model updates, which helps maintain the confidentiality of sensitive information [74].

Decentralized computation involves utilizing UAVs located in remote or dispersed areas with limited access to centralized computing resources. FL allows UAVs to perform local model training using their onboard computational power, which distributes the workload and reduces reliance on central servers [75]. The integration of FL within UAVs in Beyond 5G (B5G) networks represents a significant technological advancement that can greatly enhance communication, computation, and data analysis [76] in aerial systems.

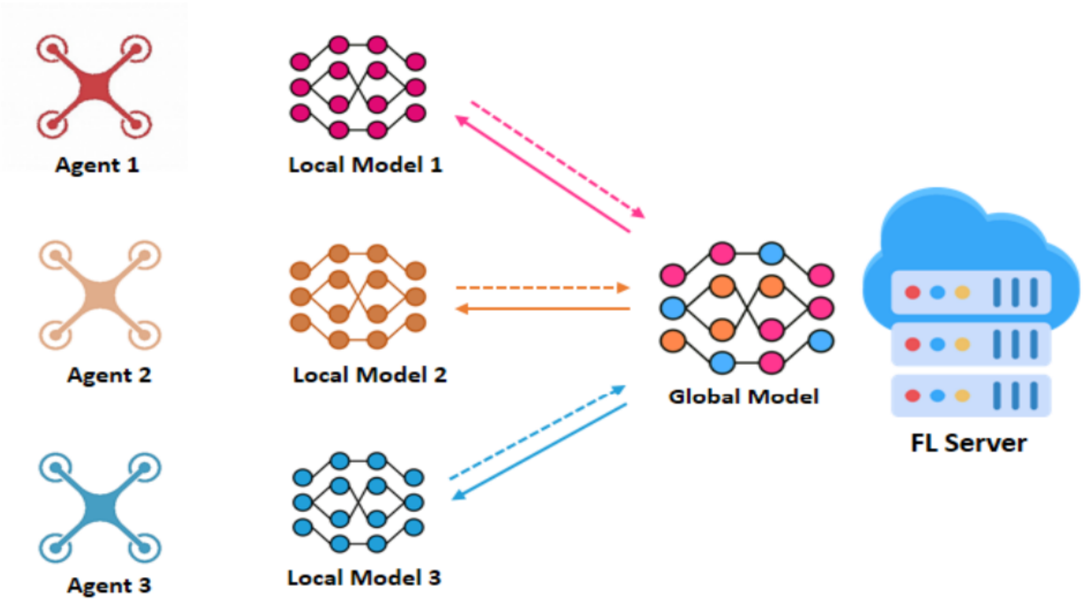

Figure 2. Illustration of FL concept considering N number of UAVs in B5G networks [19]

An illustration of the FL concept with N UAVs in B5G networks shows how the server collects local model updates from UAVs, aggregates them, and disseminates the global model until the desired performance is reached [77]. FL effectively addresses privacy and security issues while utilizing the computational strengths of distributed UAV nodes [78-79]. For instance, it ensures that sensitive data, such as surveillance videos or sensor data, remains on the device and is not externally shared [80]. In B5G networks, FL facilitates dynamic model fusion, allowing UAVs to collaboratively adjust their machine learning models in response to changing environmental conditions or mission needs. This process enables continuous performance improvement without compromising data privacy. Additionally, FL can incorporate adversarial training techniques to protect against malicious attacks on UAV networks [81-84]. By training models with adversarial examples created by potential attackers, UAVs can bolster their defenses against security threats while preserving data privacy.

Federated Learning (FL) provides a strong framework for improving the security and privacy of Unmanned Aerial Vehicles (UAVs) operating in Beyond 5G (B5G) networks. By implementing decentralized data processing, privacy-preserving model updates, secure aggregation methods, and the ability to adapt dynamically to threats, FL enables UAVs to take advantage of collaborative machine learning while effectively reducing privacy and security risks. This allows UAVs to function securely and protect data privacy in the ever-changing and distributed environments of B5G. However, some aspects require further exploration. For instance, the high mobility, flexible deployment, and increased likelihood of line-of-sight connections associated with UAVs can raise significant security and threat issues. If UAVs are intentionally used for malicious purposes, they could potentially disrupt or intercept model updates between users and the targeted UAVs. Therefore, it is crucial to develop secure UAVs within B5G networks using the FL approach, which warrants further research. This research could leverage the flexible deployment and high mobility of UAVs to create secure FL-based solutions. Additionally, Blockchain (BC) is an emerging technology with distinctive characteristics such as immutability, transparency, persistence, decentralization, and auditability, which can be integrated with FL to address UAV security and privacy challenges in B5G networks [85].

The previous section explored the use of Federated Learning (FL) for Unmanned Aerial Vehicles (UAVs) within Beyond 5G (B5G) networks, addressing security and privacy concerns in detail. FL utilizes the processing capabilities of UAVs while safeguarding data privacy, allowing them to collaboratively train machine learning models without sharing raw data. Furthermore, FL enhances resilience, scalability, and adaptability to changing conditions, facilitating collaborative and privacy-conscious machine learning on a large scale in B5G networked UAV operations. However, the rapid movement, flexible deployment, and high potential for Line of Sight (LoS) connections in UAVs may introduce significant security vulnerabilities. Creating prototypes and implementing them in real-world scenarios pose considerable challenges that require further research. Additionally, developing emulation tools that accurately reflect the characteristics of aerial FL systems—such as aerial dynamics, diverse datasets, and varying learning needs—could serve as a solution to bridge existing gaps. The research community should have access to these emulation tools to innovate new modules and enhance existing ones.

6. Post-Quantum Cryptography

Quantum computers have the capability to compromise both symmetric and asymmetric cryptographic systems using Grover's and Shor's algorithms. Grover's search algorithm reduces the time needed to find a key in symmetric systems like AES and 3DES to a square root of the original time. On the other hand, Shor's factoring algorithm can solve problems in polynomial time, threatening asymmetric cryptographic systems such as RSA and ECC. Consequently, traditional cryptographic algorithms may need to be adapted to be resistant to quantum attacks or replaced with new algorithms designed to withstand such threats. This has led to the emergence of Post-Quantum Cryptography (PQC), [86-89] which focuses on developing quantum-resistant algorithms. PQC aims to identify and create cryptographic primitives that can withstand attacks from advanced quantum computers, ensuring the long-term security of data communication and storage [90]. While classical cryptography is based on the difficulty of problems like factoring large integers or calculating discrete logarithms, PQC utilizes different mathematical foundations for security. Promising approaches for developing post-quantum cryptographic primitives include lattice-based cryptography [91], code-based cryptography [92-93], hash-based cryptography [94], multivariate polynomial cryptography [95], isogeny-based cryptography, non-commutative cryptography [96], and other emerging methods.

David Deutsch's creation of the first universal quantum computing model, grounded in physical principles and the Church-Turing hypothesis [97], laid the theoretical groundwork for assessing the security of post-quantum cryptography (PQC) primitives. Quantum computing fundamentally relies on quantum bits, or qubits [98], which, unlike classical bits, can exist in multiple states simultaneously—both 0 and 1—due to the principle of superposition [99–102]. This characteristic allows quantum computers to process numerous potential inputs at once, leading to an exponential increase in computational power [103]. A prominent illustration of this power is Shor's algorithm, introduced by mathematician Peter Shor in 1994, which efficiently factors large integers and addresses the discrete logarithm problem, both of which are crucial for many asymmetric cryptographic systems like RSA and ECC [104–106]. Additionally, Grover's algorithm, proposed by Lov Grover in 1996, showcases another aspect of quantum computing's influence on classical cryptography, particularly in symmetric schemes such as AES and 3DES [107–109]. Grover's algorithm offers a quadratic speedup over classical methods when searching through unsorted databases, effectively reducing the security strength of symmetric encryption and hash functions by halving their effective key lengths.

PQC, or Post-Quantum Cryptography, is defined by the premise that potential attackers have access to sophisticated quantum computers, necessitating cryptographic techniques that can resist quantum threats [110]. The primary goal of PQC is to maintain cryptographic effectiveness and flexibility by creating algorithms and protocols that can endure quantum challenges [111-112]. This involves the need for classical cryptography, including both symmetric and asymmetric systems, to innovate new algorithms that do not solely depend on the difficulty of problems like integer factorization and discrete logarithms, but instead utilize problems that can withstand quantum attacks from advanced quantum computers [113]. Consequently, there is a push for the Internet to enhance classical cryptographic methods against quantum threats [114-115] and transition towards PQC, even though large-scale quantum computers capable of launching such attacks are not yet widely accessible. The rationale for this shift includes the need to securely store and later decrypt sensitive information using PQC, as well as to integrate pre-quantum public-key cryptography into existing protocols and applications [116]. Following these principles, various PQC algorithms have been developed to satisfy the requirements of PQC, with each proposed algorithm categorized into one of the PQC families based on its mathematical foundation.

Unmanned Aerial Vehicles (UAVs) have become essential elements of contemporary communication networks, enabling a variety of applications such as surveillance, monitoring, disaster response, and delivery services. However, the rise of quantum computing poses a serious threat to UAV security, as conventional cryptographic methods like RSA and ECC are susceptible to quantum attacks. This vulnerability puts UAV communication links at risk of interception, data manipulation, and unauthorized access, jeopardizing critical operations and sensitive data. To address this issue, Post-Quantum Cryptography (PQC) has emerged as a viable solution to protect UAVs within Beyond 5G (B5G) networks. Additionally, the limited resources of UAV platforms create further challenges in deploying computationally demanding PQC algorithms while ensuring efficient performance and low latency. Despite these obstacles, the implementation of PQC presents significant opportunities to improve UAV communication security in B5G networks. PQC algorithms that utilize lattice-based, hash-based, code-based, and multivariate polynomial-based cryptography have demonstrated resilience against quantum attacks while remaining practical and efficient for UAV use. Lattice-based methods like NTRUEncrypt and Kyber offer strong security and compact key sizes suitable for UAVs. Likewise, code-based algorithms such as McEliece and BIKE provide long-term security with minimal computational demands, making them ideal for resource-limited settings. Hash-based and multivariate polynomial-based approaches enable rapid signature generation and verification, making them particularly suitable for real-time UAV communication.

Assessing PQC algorithms for UAVs in B5G networks requires an evaluation of their security, performance, scalability, and compatibility with existing communication protocols and standards. However, research should also prioritize the creation of lightweight PQC implementations specifically designed for UAV platforms, taking into account energy efficiency, memory usage, and real-time functionality. Future research could investigate hybrid cryptographic methods, combine PQC with new technologies such as blockchain and artificial intelligence, and tackle practical challenges in deploying these solutions within UAV communication networks. These avenues could significantly improve the security of UAV communications in B5G networks.

PQC has significant potential to enhance the security of UAVs in B5G networks against threats from quantum computing. By implementing PQC techniques, stakeholders can guarantee the confidentiality, integrity, and authenticity of communication links, which is essential for the reliable operation of UAVs in challenging and dynamic environments. However, this also necessitates collaboration across various fields, including researchers, industry professionals, and regulatory agencies, to effectively tackle the technical, operational, and regulatory challenges. With dedicated efforts and progress in PQC technology, UAVs can continue to perform their critical functions in B5G networks while protecting against new security risks associated with quantum computing.

7. Comparative Analysis of Privacy Solutions for UAV Networks

The privacy challenges in UAV networks within B5G environments necessitate robust solutions to address evolving threats and meet stringent QoS requirements. Table 2 provides a detailed analysis of two prominent privacy solutions—Federated Learning (FL), and Post-Quantum Cryptography (PQC)—highlighting their strengths, weaknesses, and ideal application scenarios.

Table 2. Comparative Analysis of Privacy Solutions for UAV Networks, Highlighting Strengths and Weaknesses

Security Solution	Advantages	Limitations	Ideal use case
FL (Federated Learning)	Protects user privacy by keeping data on local devices, reducing risks of centralized data leaks.	Vulnerable to certain indirect attacks, like model inversion, if differential privacy is inadequately implemented.	Best for sensitive data applications like healthcare UAVs or surveillance systems where data privacy is crucial.
PQC (Post-Quantum Cryptography)	Offers resilience against future quantum computing threats, ensuring robust encryption.	Computationally intensive, leading to higher resource consumption compared to traditional encryption.	Critical for highly sensitive operations like military drone communications or critical infrastructure monitoring.

8. Conclusion

In today's interconnected world, privacy have become increasingly crucial. The integration of UAVs into B5G mobile connectivity will enhance their reliability and availability. However, as technology advances, new privacy threats and vulnerabilities arise. It is essential to adopt and develop new privacy focused measures in response to emerging threats from AI/ML and quantum computing. This paper offers an overview of the privacy challenges and solutions for UAVs within B5G networks, stressing the importance of creating security measures to protect UAVs from cyber-physical and AI/ML-driven attacks, especially in the context of quantum computing. We thoroughly examined emerging privacy solutions, including Federated Learning (FL) and Post-Quantum Cryptography (PQC).

References

1. B. P. S. Sahoo, D. Puthal, and P. K. Sharma, "Toward Advanced UAV Communications: Properties, Research Challenges, and Future Potential", IEEE Internet of Things Magazine, vol. 5, no. 1, pp. 154–159, 2022.
2. B. Alzahrani, O. S. Oubbati, A. Barnawi, M. Atiquzzaman, and D. Alghazzawi, "UAV assistance paradigm: State-of-the-art in applications and challenges", Journal of Network and Computer Applications, vol. 166, p. 102706, 2020.
3. M. Z. Islam, R. Ali, A. Haider, and H. S. Kim, "QoS Provisioning: Key Drivers and Enablers Towards the Tactile Internet in Beyond 5G Era", IEEE Access, pp. 1–1, 2022.
4. M. A. Khan, H. Menouar, A. Eldeeb, A. Abu-Dayya, and F. D. Salim, "On the Detection of Unauthorized Drones—Techniques and Future Perspectives: A Review", IEEE Sensors Journal, vol. 22, no. 12, pp. 11439–11455, 2022.
5. A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies", IEEE Access, vol. 9, pp. 67512–67547, 2020.
6. W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey", IEEE Open Journal of the Communications Society, vol. 2, pp. 334–366, 2021.
7. I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems", IEEE access, vol. 8, pp. 133995–134030, 2020.
8. H. Viswanathan and P. E. Mogensen, "Communications in the 6G era", IEEE Access, vol. 8, pp. 57063–57074, 2020.
9. M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research direction", IEEE Open Journal of the Communications Society, vol. 1, pp. 957–975, 2020.
10. L. Bariah et al., "A prospective look: Key enabling technologies, applications and open research topics in 6G networks", IEEE access, vol. 8, pp. 174792–174820, 2020.
11. S. Nayak and R. Patgiri, "6G communication: Envisioning the key issues and challenges", arXiv preprint arXiv:2004. 04024, 2020.
12. L. Bariah, L. Mohjazi, S. Muhaidat, P. C. Sofotasios, G. K. Kurt, H. Yanikomeroglu, and O. A. Dobre, "A prospective look: Key enabling technologies, applications and open research topics in 6G networks," IEEE Access, vol. 8, pp. 174792–174820, 2020.
13. Z. Lv, L. Qiao, and I. You, "6G-enabled network in box for internet of connected vehicles", IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5275–5282, 2020.
14. P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques", IEEE network, vol. 33, no. 4, pp. 70–75, 2019.
15. K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?", IEEE vehicular technology magazine, vol. 13, no. 3, pp. 72–80, 2018.
16. T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies", IEEE access, vol. 7, pp. 175758–175768, 2019.
17. W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems", IEEE network, vol. 34, no. 3, pp. 134–142, 2019.
18. F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G", IEEE Wireless Communications, vol. 27, no. 4, pp. 118–125, 2020.
19. Y. Lu and X. Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues", Journal of Industrial Information Integration, vol. 19, p. 100158, 2020.

20. I. Alam, M. A. Rahman, M. S. Hossain, M. Alrubaian, M. Atiquzzaman, and A. Alelaiwi, "A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV", vol. 53, no. 2, 2020.
21. Q.-V. Pham, F. Fang, V. N. Q. Bao, R. Piran, M. Le, Z. Ding, and W.-J. Hwang, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," IEEE Access, vol. 8, pp. 116974–117017, 2020.
22. C. D. Alwis, Q.-V. Pham, K. Dev, P. J. E. Jesudoss, D. B. da Costa, W.-J. Hwang, M. Liyanage, and M. Gupta, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research", IEEE Open Journal of the Communications Society, vol. 2, pp. 836–886, 2021.
23. S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?", Nature Electronics, vol. 3, no. 1, pp. 20–29, 2020.
24. E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication", IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 42–50, 2019.
25. W. Guo, "Explainable artificial intelligence for 6G: Improving trust between human and machine", IEEE Communications Magazine, vol. 58, no. 6, pp. 39–45, 2020.
26. C. Li, W. Guo, S. C. Sun, S. Al-Rubaye, and A. Tsourdos, "Trustworthy deep learning in 6G-enabled mass autonomy: From concept to quality-of-trust key performance indicators", IEEE Vehicular Technology Magazine, vol. 15, no. 4, pp. 112–121, 2020.
27. J. Du, C. Jiang, J. Wang, Y. Ren, and M. Debbah, "Machine learning for 6G wireless networks: Carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service", IEEE Vehicular Technology Magazine, vol. 15, no. 4, pp. 122–134, 2020.
28. H.J. Hadi, Y. Cao, S. Li, L. Xu, Y. Hu, and M. Li, "Real-time fusion multi-tier DNN-based collaborative IDPS with complementary features for secure UAV-enabled 6G networks," Expert Systems with Applications, vol. 252, pp. 124215–124215, Oct. 2024.
29. Z. Lv, "The security of Internet of drones", Computer Communications, vol. 148, pp. 208–214, 2019.
30. C. St¨ocker, R. Bennett, F. Nex, M. Gerke, and J. Zevenbergen, "Review of the Current State of UAV Regulations", Remote Sensing, vol. 9, no. 5, 2017.
31. S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review", Drones, vol. 6, no. 6, 2022.
32. M. A. Khan, M. S. Farash, M. S. Hossain, G. Srivastava, and M. Alazab, "Securing Internet of Drones with Identity-Based Proxy Signcryption", IEEE Access, vol. 9, pp. 89133–89142, 2021.
33. D. C. Le, N. Zincir-Heywood, and M. I. Heywood, "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning", IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 30–44, 2020.
34. J. Chen, X. Lin, Z. Shi, and Y. Liu, "Link Prediction Adversarial Attack Via Iterative Gradient Attack", IEEE Transactions on Computational Social Systems, vol. 7, no. 4, pp. 1081–1094, 2020.
35. A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges", IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3417–3442, 2019.
36. B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "SoK- Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps", ArXiv, vol. abs/1903.05155, 2019.

37. Q. Wu, W. Mei, and R. Zhang, "Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective", IEEE Wireless Communications, vol. 26, no. 5, pp. 12–18, 2019.
38. H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective", IEEE Communications Surveys and Tutorials, vol. 22, no. 2, pp. 1027–1070, 2020.
39. F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying AD-HOC networks: Key enabling wireless technologies, applications, challenges and open research topics", Drones, vol. 4, no. 4, p. 65, 2020.
40. J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations", Internet of Things, vol. 11, p. 100218, 2020.
41. J. Wang, C. Jiang, K. Ma, J. Jin, and Y. Ren, "Physical layer security for UAV communications in 5G and beyond networks," 2021, arXiv:2105.11332.
42. A. Shafique, A. Mehmood, and M. Elhadef, "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles", IEEE Access, vol. 9, pp. 46927–46948, 2021.
43. L. Wang, Y. Chen, P. Wang, and Z. Yan, "Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications", IEEE Communications Standards Magazine, vol. 5, no. 4, pp. 41–47, 2021.
44. W. Yang, S. Wang, X. Yin, X. Wang, and J. Hu, "A Review on Security Issues and Solutions of the Internet of Drones", IEEE Open Journal of the Computer Society, vol. 3, pp. 96–110, 2022.
45. P. McEnroe, S. Wang, and M. Liyanage, "A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges", IEEE Internet of Things Journal, pp. 1–1, 2022.
46. C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, and M. Liyanage, "A Survey on Privacy for B5G/6G: New Privacy Goals, Challenges, and Research Directions", ArXiv, vol. abs/2203.04264, 2022.
47. M. A. Khan, M. R. Khandaker, A. Jamalipour, M. Shakir, and A. Imran, "Swarm of UAVs for Network Management in 6G: A Technical Review," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 741-761, March 2023.
48. Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A Survey on Security and Privacy Issues of UAVs", Computer Networks, vol. 224, p. 109626,2023.
49. H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil and Q. Ni, "A comprehensive survey on security privacy issues and emerging defence technologies for UAVs", J. Netw. Comput. Appl., vol. 213, Apr. 2023.
50. M. K. Banafaa, A. Chaoub, A. E. Samhat, M. Guizani, and H. Otrok, "A Comprehensive Survey on 5G-and-Beyond Networks with UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges," in IEEE Access, vol. 12, pp. 7786-7826, 2024.
51. S. Javed, M. A. Khan, A. Ahmad, M. Z. Khan, and C. S. Hong, "State-of-the-Art and Future Research Challenges in UAV Swarms," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3364230.
52. M. A. B. Siddiki Abir, M. Z. Chowdhury and Y. M. Jang, "Software-Defined UAV Networks for 6G Systems: Requirements, Opportunities, Emerging Techniques, Challenges, and Research Directions," in IEEE Open Journal of the Communications Society, vol. 4, pp. 2487-2547, 2023.
53. P. McEnroe, S. Wang and M. Liyanage, "A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges," in IEEE Internet of Things Journal, vol. 9, no. 17, pp. 15435-15459, 1 Sept.1, 2022.

54. N. Hossein Motlagh, T. Taleb and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 899-922, Dec. 2016.
55. A. N. Wilson, A. Kumar, A. Jha and L. R. Cenkeramaddi, "Embedded Sensors, Communication Technologies, Computing Platforms and Machine Learning for UAVs: A Review," in IEEE Sensors Journal, vol. 22, no. 3, pp. 1807-1826, 1 Feb.1, 2022.
56. M. Riedel, G. Cavallaro and J. A. Benediktsson, "Practice and Experience in Using Parallel and Scalable Machine Learning in Remote Sensing from HPC Over Cloud to Quantum Computing," 2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS, Brussels, Belgium, 2021, pp. 1571-1574.
57. H. Wang, H. Zhao, W. Wu, J. Xiong, D. Ma, and J. Wei, "Deployment algorithms of flying base stations: 5G and beyond with UAVs," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10 009–10 027, Aug. 2019.
58. N. M. Nasir, S. Hassan and K. M. Zaini, "Evolution Towards 6G Intelligent Wireless Networks: The Motivations and Challenges on the Enabling Technologies," 2021 IEEE 19th Student Conference on Research and Development (SCOReD), Kota Kinabalu, Malaysia, 2021, pp. 305-310.
59. S. K. A. Yaklaf, K. S. Tarmissi and N. A. A. Shashoa, "6G Mobile Communications Systems: Requirements, Specifications, Challenges, Applications, and Technologies," 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, Tripoli, Libya, 2021, pp. 679-683.
60. M. Alsabah, R. M. Shubair, J. M. Sampe, A. Alkhateeb, M. Albreem, S. K. Goudos, and F. H. Juwair, "6G Wireless Communications Networks: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 148191-148243, 2021, doi: 10.1109/ACCESS.2021.3124812.
61. A. Verma, P. Bhattacharya, D. Saraswat, S. Tanwar, N. Kumar, and R. Sharma, "SanJeeVni: Secure UAV-envisioned massive vaccine distribution for COVID-19 underlying 6G network," IEEE Sensors J., vol. 23, no. 2, pp. 955–968, Jun. 2023.
62. K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A taxonomy of AI techniques for 6G communication networks," Comput. Commun., vol. 161, pp. 279–303, Sep. 2020.
63. X. Liu and N. Ansari, "Resource allocation in UAV-assisted M2M communications for disaster rescue," IEEE Wireless Commun. Lett., vol. 8, no. 2, pp. 580–583, Apr. 2019.
64. W. Wang, Y. Wang, F. Zhou, Q. Wu, and R. Q. Hu, "Robust 3D-trajectory and time switching optimization for dual-UAV-enabled secure communications," IEEE J. Sel. Areas Commun., vol. 39, no. 11, pp. 3334–3347, Nov. 2021.
65. M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," IEEE Open J. Commun. Soc., vol. 1, pp. 957–975, 2020.
66. S. Chen, S. Sun and S. Kang, "System integration of terrestrial mobile communication and satellite communication —the trends, challenges and key technologies in B5G and 6G," in China Communications, vol. 17, no. 12, pp. 156-171, Dec. 2020.
67. J. Mulholland, M. Mosca and J. Braun, "The Day the Cryptography Dies," in IEEE Security and Privacy, vol. 15, no. 4, pp. 14-21, 2017.

68. R. Deng, B. Di, H. Zhang, Y. Tan and L. Song, "Reconfigurable Holographic Surface: Holographic Beamforming for Metasurface-Aided Wireless Communications," in IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 6255-6259, June 2021.
69. W. Tang, M. Chen, X. Chen, J. Y. Dai, Y. Han, M. Di Renzo, and S. Jin, "Wireless Communications with Programmable Metasurface: New Paradigms, Opportunities, and Challenges on Transceiver Design," in IEEE Wireless Communications, vol. 27, no. 2, pp. 180-187, April 2020.
70. Y. Guo, X. Liu, Z. Wang, H. Zhang, and Q. Chen, "A Security Protection Technology Based on Multi-factor Authentication," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5.
71. A. Imteaj, U. Thakker, S. Wang, J. Li and M. H. Amini, "A Survey on Federated Learning for Resource-Constrained IoT Devices," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 1-24, 1 Jan.1, 2022.
72. M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Bakas, T. P. Andriole, and S. Ruppert, "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data," Scientific Reports, vol. 10, no. 1, p. 12598, 2020.
73. Q.-V. Pham, M. Zeng, R. Ruby, T. Huynh-The, and W.-J. Hwang, "UAV Communications for Sustainable Federated Learning," IEEE Transactions on Vehicular Technology, vol. 70, no. 4, pp. 3944–3948, 2021.
74. B. Brik, A. Ksentini, and M. Bouaziz, "Federated Learning for UAVs-Enabled Wireless Networks: Use Cases, Challenges, and Open Problems," IEEE Access, vol. 8, pp. 53841–53849, 2020.
75. Y. Qu, J. Yu, W. Zhang, Z. Zhao, X. Chen, and Y. Zhang, "Decentralized Federated Learning for UAV Networks: Architecture, Challenges, and Opportunities," IEEE Network, vol. 35, no. 6, pp. 156–162, 2021.
76. S. H. Alsamhi, O. Ma, M. S. Ansari, and B. Almalki, "Drones' Edge Intelligence Over Smart Environments in B5G: Blockchain and Federated Learning Synergy," IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 295–312, 2022.
77. Q.-V. Pham, M. Zeng, T. Huynh-The, Z. Han and W.-J. Hwang, "Aerial Access Networks for Federated Learning: Applications and Challenges," in IEEE Network, vol. 36, no. 3, pp. 159-166, May/June 2022.
78. Y. Liu, J. Nie, X. Li, S. H. Ahmed, W. Y. B. Lim, and C. Miao, "Federated learning in the sky: Aerial-ground air quality sensing framework with UAV swarms," IEEE Internet Things J., vol. 8, no. 12, pp. 9827–9837, Jun. 2021.
79. S. Tang, W. Zhou, L. Chen, L. Lai, J. Xia, and L. Fan, "Batteryconstrained federated edge learning in UAV-enabled IoT for B5G/6G networks," 2021. [Online]. Available: arXiv:2101.12472.
80. N. I. Mowla, N. H. Tran, I. Doh, and K. Chae, "Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network," IEEE Access, vol. 8, pp. 4338–4350, 2020.
81. W. Y. B. Lim, N. C. Luong, D. T. Hoang, S. Kar, C. S. Hong, and D. Niyato, "Towards Federated Learning in UAV-Enabled Internet of Vehicles: A Multi-Dimensional Contract-Matching Approach," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5140–5154, 2021.
82. A. V. Shvetsov, I. Y. Im, M. S. Safaei, A. M. Kharitonov, and V. D. Lyakhov, "Federated Learning Meets Intelligence Reflection Surface in Drones for Enabling 6G Networks: Challenges and Opportunities," IEEE Access, vol. 11, pp. 130860–130887, 2023,
83. C. Zhu, X. Zhu, J. Ren, and T. Qin, "Blockchain-Enabled Federated Learning for UAV Edge Computing Network: Issues and Solutions," IEEE Access, vol. 10, pp. 56591–56610, 2022.

84. C. Huang, S. Wang, Y. Chen, Q. Wu, and R. Zhang, "Federated Learning for RIS-Assisted UAV-Enabled Wireless Networks: Learning-Based Optimization for UAV Trajectory, RIS Phase Shifts and Weighted Aggregation," in 2023.
85. Z. Du, X. Wang, H. Zhang, Y. Li, and L. Wang, "Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues," IEEE Open J. Comp. Soc., vol. 1, May 2020, pp. 45–61.
86. D. J. Bernstein, "Introduction to post-quantum cryptography," in Post-quantum cryptography. Springer, 2009, pp. 1–14.
87. D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, 2017.
88. P. S. Barreto, F. Piazza Biasi, R. Dahab, J. C. Lopez-Hern ´ andez, E. M. ´ de Morais, A. D. S. de Oliveira, G. C. Pereira, and J. E. Ricardini, "A panorama of post-quantum cryptography," Open Problems in Mathematics and Computational Science, pp. 387–439, 2014.
89. D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," Nature, vol. 605, no. 7909, pp. 237–243, 2022.
90. T. R. N. G. S. Or and A. Q. Adversaries, "Certifiable quantum dice," 2012. [16] X. Wang, G. Xu, and Y. Yu, "Lattice-based cryptography: A survey," Chinese Annals of Mathematics, Series B, vol. 44, no. 6, pp. 945–960, 2023.
91. R. Overbeck and N. Sendrier, "Code-based cryptography. post-quantum cryptography/ed. bernstein dj, buchmann j., dahmen e," 2009.
92. V. Weger, N. Gassner, and J. Rosenthal, "A survey on code-based cryptography," arXiv preprint arXiv:2201.07119, 2022.
93. M. D. Noel, V. O. Waziri, S. M. Abdulhamid, and J. A. Ojeniyi, "Review and analysis of classical algorithms and hash-based post-quantum algorithm," Journal of Reliable Intelligent Environments, pp. 1–18, 2021.
94. J. Ding and A. Petzoldt, "Current state of multivariate cryptography," IEEE Security Privacy, vol. 15, no. 4, pp. 28–36, 2017.
95. C. Peng, J. Chen, S. Zeadally, and D. He, "Isogeny-based cryptography: a promising post-quantum technique," IT Professional, vol. 21, no. 6, pp. 27–32, 2019.
96. S. Kanwal and R. Ali, "A cryptosystem with noncommutative platform groups," Neural Computing and Applications, vol. 29, pp. 1273–1278, 2018.
97. D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," in Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 100, no. 1818, 1985, pp. 97–117.
98. J. Clarke and F. K. Wilhelm, "Superconducting quantum bits," Nature, vol. 453, no. 7198, pp. 1031–1042, 2008.
99. S. T. Marella and H. S. K. Parisa, "Introduction to quantum computing," Quantum Computing and Communications, 2020.
100. H. Riel, "Quantum computing technology," in 2021 IEEE International Electron Devices Meeting (IEDM). IEEE, 2021, pp. 1–3. IEEE, VOL. XX, NO. XX, XXX 2022 11.
101. M. Moller and C. Vuik, "On the impact of quantum computing¨ technology on future developments in high-performance scientific computing," Ethics and information technology, vol. 19, pp. 253–269, 2017.
102. A. Y. Kitaev, A. Shen, and M. N. Vyalyi, Classical and quantum computation. American Mathematical Soc., 2002, no. 47.
103. M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," Phys. Today, vol. 54, no. 2, p. 60, 2001.

104. S. Aaronson, "The limits of quantum," Scientific American, vol. 298, no. 3, pp. 62–69, 2008.

105. V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," arXiv preprint arXiv:1804.00200, 2018.

106. M. D. Noel, V. O. Waziri, S. M. Abdulhamid, and J. A. Ojeniyi, "Review and analysis of classical algorithms and hash-based post-quantum algorithm," Journal of Reliable Intelligent Environments, pp. 1–18, 2021.

107. W. Y. Seo, "Comparing rsa ecc and post quantum cryptography," J. Math. Anal. Appl, vol. 10, pp. 19–33, 2018.

108. S. Gajbhiye, S. Karmakar, M. Sharma, and S. Sharma, "Paradigm shift from classical cryptography to quantum cryptography," in 2017 International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2017, pp. 548–555.

109. A. Ahilan and A. Jeyam, "Breaking barriers in conventional cryptography by integrating with quantum key distribution," Wireless Personal Communications, vol. 129, no. 1, pp. 549–567, 2023.

110. H.-J. Shiu, C.-T. Yang, Y.-R. Tsai, W.-C. Lin, and C.-M. Lai, "Maintaining secure level on symmetric encryption under quantum attack," Applied Sciences, vol. 13, no. 11, p. 6734, 2023.

111. P. Shrivastava, K. K. Soni, and A. Rasool, "Evolution of quantum computing based on grover's search algorithm," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2019, pp. 1–6.

112. N. Farrugia, D. Bonanno, N. Frendo, and A. Xuereb, "Pqc and qkd are both required to enable a quantum-safe future," in Toward a Quantum-Safe Communication Infrastructure. IOS Press, 2024, pp. 24–36.

113. A. Nilsson and A. Advenica, Decryption Failure Attacks on Post-Quantum Cryptography. Department of electrical and information technology, faculty of engineering . . . , 2023.

114. S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing," The Journal of Supercomputing, vol. 80, no. 3, pp. 3738–3816, 2024.

115. J. Suo, L. Wang, S. Yang, W. Zheng, and J. Zhang, "Quantum algorithms for typical hard problems: a perspective of cryptanalysis," Quantum Information Processing, vol. 19, pp. 1–26, 2020.

116. S. Joshi, A. K. Bairwa, A. P. Pljonkin, P. Garg, and K. Agrawal, "From pre-quantum to post-quantum rsa," in Proceedings of the 6th International Conference on Networking, Intelligent Systems and Security, 2023, pp. 1–8.