survey on Security, Privacy and Intelligence for UAV-Enabled 6G Networks

mehru, Asjad Amin
Information and Communication Engineering / Islamia University of Bahawalpur
Bahawalpur, Pakistan
Email: mmehruuni@gmail.com

***Abstract*—Unmanned aerial vehicles (UAVs) are anticipated to be a key element of sixth generation (6G) networks, serving as aerial base stations, relays, sensing platforms, edge nodes, and autonomous swarms. Such capabilities enable services such as emergency coverage, disaster response, smart cities, intelligent transportation, precision agriculture, surveillance, and Internet of Drones applications [18], [41], [51], [58]. However, UAV enabled 6G systems are exposed to a large attack surface because they operate on open wireless channels, collect sensitive data, and rely increasingly on artificial intelligence (AI), blockchain, edge computing, software defined networking (SDN), and integrated sensing and communication (ISAC). This survey gives a holistic view of UAV enabled 6G architectures, systematic selection of studies, security threats, privacy leakage, intelligent countermeasures, comparative complexity, practical deployment constraints, and open research challenges. .**

***Index Terms*—UAV, 6G, security, privacy, federated learning, blockchain, edge intelligence, Internet of Drones, ISAC.**

I. Introduction

The 6G networks will combine terrestrial, aerial, satellite, and edge cloud infrastructures. This vision can be achieved with mobile, rapidly deployable UAVs that support line of sight communication, sensing, relaying, and local computation. UAVs can provide connectivity for emergency response when terrestrial infrastructure is damaged [58]. They can assist smart cities by monitoring traffic, maintaining public safety, and inspecting infrastructure. In precision agriculture, UAVs can acquire multispectral images for intelligent crop monitoring [38], [41]. UAVs can also be exploited as aerial relays or edge nodes for data aggregation and computation offloading in vehicular and IoT environments [2], [42], [52], [55].

However, there are serious security and privacy challenges for UAV enabled 6G. UAVs are vulnerable to physical capture, jamming, spoofing, eavesdropping, malware, fake data injection, AI poisoning, and swarm manipulation [7], [16], [18], [45]. The sensing payloads they carry may raise privacy concerns such as location tracking, surveillance, identity linking, and model-update leakage in federated learning [8]–[10]. These risks are further magnified by 6G functionalities such as terahertz links, semantic communication, network slicing, ISAC, reconfigurable intelligent surfaces (RIS), edge AI, and autonomous resource orchestration.

PUF authentication, federated learning, and blockchain audit procedures are known concepts unless they are experimentally modified and validated. In this article, we present a comprehensive review of security, privacy, and intelligence aspects of UAV-enabled 6G. The article covers: (i) a systematic study-selection workflow, (ii) a layered architecture, (iii) a taxonomy of security, privacy, and intelligence, (iv) a comparative study of authentication, blockchain, federated learning, AI detection, physical-layer security, and post-quantum security, and (v) practical deployment challenges and future directions.

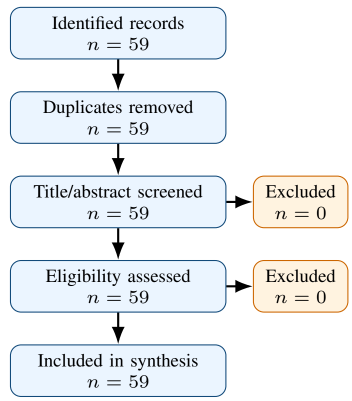

Fig. 1. PRISMA-style study-selection workflow for the curated 59-paper evidence base.

II. Prior Work and Techniques

The evidence base includes 59 studies on UAV security, Internet of Drones (IoD), blockchain, authentication, federated learning, edge computing, GPS spoofing, post quantum security, and 6G/ISAC. The flow is shown in Fig. 1 using a PRISMA style diagram. A fully systematic version should also include database names, search strings, rules for detecting duplicates, independent screening, explicit reasons for exclusion, quality scoring, and inter rater agreement.

The eight-page document is organized around four research questions. RQ1 asks: What is the common attack surface of UAV-enabled 6G? RQ2 asks: What are the privacy threats for aerial sensing and distributed learning? RQ3 asks: How can AI, blockchain, and edge intelligence help protection? RQ4 asks: What are the practical limitations of real world deployments? The five evaluation criteria are clarity of threat model, relevance to UAV and 6G, presence of evaluation, discussion of overhead, and reproducibility of assumptions. Bias risk includes recency bias, database selection bias, citation bias, simulation-only evaluation, and subjective taxonomy mapping.

DOI: https://doi.org/10.67535/tsp.000003.029
Published under the ICACNC 2026 Proceedings

TABLE I
SURVEY FOCUS AND QUALITY ASSESSMENT CRITERIA

Item	Description
Contribution type	Survey paper; no new unsupported algorithms
Novelty focus	Security, privacy, and intelligence of UAV-assisted 6G networks
Quality criteria	Relevance, threat model, UAV/6G applicability, evaluation, overhead, reproducibility
Risk of bias	Recency, database bias, citation bias, simulation-only evaluation, taxonomy bias
Topics of interest	Authentication, federated learning, blockchain, physical-layer security, edge AI, post-quantum security, ISAC

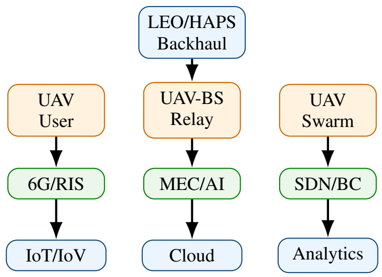

Fig. 2. Layered architecture of UAV-enabled 6G networks. BC: blockchain.

Prior work has covered UAV communication and routing [44], [51], IoD security and privacy [18], drone cybersecurity [45], AI for UAVs [50], blockchain-assisted UAV communication [48], UAV edge computing [52], [53], and federated learning privacy [8]. However, the work in this paper is different because it focuses on a narrower but deeper aspect. Instead of treating them as separate topics, it considers lightweight authentication, federated intelligence, blockchain trust, physical layer security, post-quantum authentication, and secure ISAC as integrated parts of a comprehensive UAV-enabled 6G framework.

III. ENABLERS: TECHNOLOGY AND ARCHITECTURE

The architecture is shown in Fig. 2. UAV-enabled 6G is comprised of device, aerial, terrestrial edge, cloud, and satellite HAPS layers. The device layer has IoT sensors, mobile users, vehicles, robots, and industrial machines. The aerial layer consists of UAV users, UAV base stations, sensing UAVs, relays, and cooperative swarms. The terrestrial edge layer provides 6G base stations, RIS, MEC, SDN control, and blockchain services. The cloud and satellite/HAPS layers provide worldwide backhaul, mission management, large scale analytics, and training of AI models.

The enabling technologies are FSO/THz links, NOMA relaying, semantic command and control, RIS, ISAC, MEC, SDN, blockchain, and AI-native resource management [1], [2], [4], [5], [25], [35], [42], [52], [53], [56]. FSO/THz links can achieve high data rates but require accurate alignment and are susceptible to blockage. NOMA and short-packet communications can support low-latency relay scenarios [5]. Semantic-aware command and control reduces transmission overhead by transmitting only information relevant to the task [4]. RIS can improve coverage and reduce interference, but it also introduces additional requirements for control and channel estimation. Edge computing reduces latency but increases offloading and trust risks. Blockchain provides auditability and distributed trust, but may introduce communication, storage, and consensus overheads.

TABLE II
MAIN SECURITY CHALLENGES OF 6G UAVS

UAV Role	Function	Main Security Challenge
Airborne user	Command/control telemetry	Tracking and takeover
UAV base station	Coverage on demand	Jamming and rogue base station
UAV relay	Forwarding data	Selective forwarding and eavesdropping
Edge UAV	Edge computing	Data loss and malware
Sensing UAV	Imaging and monitoring	Privacy and surveillance exposure
Swarm UAV	Cooperative missions	Byzantine and Sybil behavior

IV. SECURITY PROBLEMS

Security threats include hardware tampering, key extraction, GPS spoofing, jamming, eavesdropping, replay, rogue UAVs, routing attacks, DoS, malware, poisoning, adversarial examples, and Sybil/Byzantine swarm attacks [19], [26], [27], [36], [44]. UAVs are required to operate in open environments, and physical capture is a real threat. An attacker could steal keys, swap sensors, change firmware, or inject malicious payloads. Thus, secure boot, trusted execution, tamper evidence, and hardware roots of trust are crucial for mission-critical UAVs [3], [12], [14].

Wireless attacks are another important aspect. UAVs usually enjoy high-quality line-of-sight links, which can facilitate eavesdropping. Command and control links can be jammed. GPS spoofing has the potential to mislead navigation, produce unsafe landings, and cause missions to fail. Deep learning and 3D radio maps have been used to study GPS spoofing detection and mitigation [26], [27]. If an SDN controller is compromised, it can result in large scale disruption. Flying ad hoc networks are affected by routing attacks such as blackhole, wormhole, and selective forwarding. Swarm attacks are very dangerous because a compromised UAV can affect formation, consensus, or collaborative sensing.

Channel aware beamforming, physical layer security, covert communication, and hybrid FSO/THz design techniques can improve confidentiality, but they need accurate channel information and mobility control [1], [21], [23]. In practice, they are meant to augment, not replace, cryptographic authentication and access control mechanisms.

V. SENSITIVITY AND PRIVACY

The classification is illustrated in Fig. 3. Privacy threats include trajectory leakage, aerial surveillance, sensitive image/video exposure, data leakage from edge cloud systems, and inference from model updates [7]–[9], [18]. UAVs can take photos of faces, license plates, private property, and mobility patterns. Although payload data may be encrypted, metadata such as timing, handover events, beam direction, and radio fingerprints can be exploited to disclose sensitive location information. Smart city deployments need to enforce data minimization, purpose limitation, access auditing, and privacy filtering at or near the sensor/edge [10].

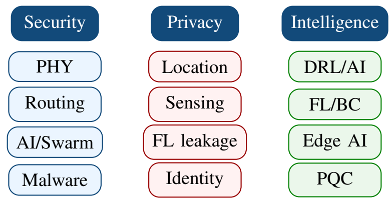

Fig. 3. Taxonomy of security, privacy, and intelligence issues in UAV enabled 6G.

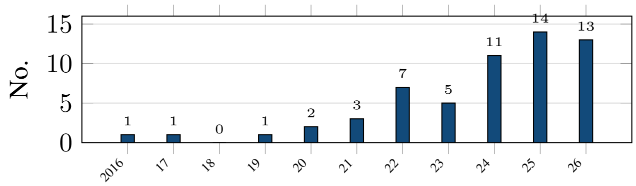

Fig. 4. Publication-year trend of the dated references.

Federated learning avoids sharing raw data but is vulnerable to poisoning, non-IID data, membership inference, and model-inversion attacks [8], [9], [21], [22], [24]. These can be alleviated by secure aggregation, differential privacy, anomaly filtering, and robust aggregation, but such mechanisms may degrade accuracy or increase communication overhead. Blockchain is useful for logging, provenance, identity, and isolation of malicious nodes [31], [40], [46]–[48], [57]. However, consensus latency and storage overhead restrict the application of blockchain in swarms. Lightweight authentication, PUF/ECC, anonymous credentials, and post quantum remote identification are needed for long-lived deployments [11]–[15], [20], [29], [32], [33].

VI. Study Comparison

The main methods are given in Table III. No algorithms are presented here because this is a survey. Authentication costs $O(1)$–$O(k)$ per session. Federated learning training is $O(E|D|P)$, and aggregation is $O(NP)$. Permissioned blockchain usually requires $O(N^2)$ consensus messages. Deep inference is $O(P)$ on average per forward pass, where P is the number of model parameters. These are only rough indicators; actual costs depend on key size, model depth, number of UAVs, radio bandwidth, consensus method, and hardware accelerator availability.

Fig. 4 shows the post-2024 surge, mainly driven by blockchain secured UAVs, federated learning, post quantum authentication, 6G edge intelligence, and ISAC privacy. The trend indicates movement of UAV security research from classical cryptography and routing toward AI native, privacy-preserving, and quantum-resilient designs.

VII. Deployment Considerations

Simulation is not the same as real deployment. UAV battery limits cryptographic computation, model inference, radio transmission, and blockchain participation. Payload size limits trusted hardware, multi sensor fusion, and edge accelerators. Weather, obstacles, and urban canyons can affect air-to-ground links and GPS availability. System design must also consider regulatory requirements such as remote identification, flight authorization, spectrum rules, and privacy law. Interoperability among UAV vendors, mobile operators, edge providers, and public safety agencies remains unresolved. Current works are mostly based on synthetic datasets, while field-test datasets with real mobility, attacks, radio maps, and energy traces remain limited.

Deployment decisions are mission driven. Emergency response UAVs need reliable command links and fast authentication. Smart city drones need privacy filtering and access auditing. Industrial UAVs need secure firmware updates and deterministic latency. Defense UAVs need anti jamming, covert communications, and post quantum ready capability. Such practical issues make purely cloud based or computation intensive defense impractical for many UAV enabled 6G scenarios.

VIII. Problems and Trends Ahead

The main open challenges are as follows. First, adaptive and lightweight security is needed for battery constrained UAVs. Heavy encryption, blockchain consensus, and deep learning are unlikely to become practical unless they are tailored to hardware capability and mission risk. Second, trustworthy AI is needed because UAVs can be attacked with poisoned data, adversarial examples, or malicious model updates. Third, privacy preserving sensing should be done close to the UAV or edge before sending sensitive data. Fourth, secure integration of sensing, communication, computing, and control is required, as an attack on one function may affect the others. Fifth, there is a lack of realistic datasets and field testbeds to evaluate defenses under realistic mobility, weather, interference, and adversarial conditions. Sixth, regulation-aware deployment should cover remote identification, spectrum rules, privacy law, firmware updates, and accountability.

Future directions include experimentally validated lightweight authentication, robust federated learning, low latency blockchain, UAV specific post quantum schemes, and secure ISAC testbeds. Researchers need to design digital twins and hardware in the loop platforms for repeatable evaluation. Finally, future surveys should follow a fully systematic search protocol, include quality scoring, and perform quantitative meta-analysis when comparable metrics are available.

IX. Conclusion

UAV-enabled 6G networks can provide flexible aerial communication, sensing, and computation, but they also suffer from multi layer security and privacy risks. This survey gives an overview of the architecture, study selection methodology, taxonomy, comparative methods, research trends, practical deployment, and open challenges. The core message is that secure UAV-enabled 6G requires the joint design of lightweight authentication, privacy-preserving intelligence, blockchain assisted trust, physical layer security, edge AI, secure ISAC, and post-quantum readiness.

TABLE III
ADVANTAGES AND DISADVANTAGES OF TECHNIQUE FAMILIES

Technique	Advantage	Disadvantage	Typical Overhead
PUF/ECC authentication [12], [14], [29]	Lightweight and robust identity/access management	Cross-domain trust and revocation	Low to medium computation; few messages
Blockchain [31], [48]	Audit, provenance, malicious-node isolation	Latency, scalability, storage	Medium to high communication and consensus cost
Federated learning [8], [9], [24]	Data remain on the device	Poisoning and information leakage	High training cost; repeated model exchange
AI/DRL detection [26], [27], [35]	Adaptive anomaly/spoofing detection	Dataset dependence and adversarial vulnerability	High training; low/moderate inference
Physical-layer security [1], [23]	Supports confidentiality and extends encryption	Mobility and CSI dependence	Beamforming, CSI acquisition, and power cost
Post-quantum security [6], [20], [32]	Long-term security	Larger keys and signatures	Above-ECC memory and bandwidth overhead

TABLE IV
DEPLOYMENT SCENARIOS AND TOP PRIORITY NEEDS

Scenario	Priority	Security/Privacy Need
Emergency coverage	Speed and reliability	Rapid authentication, anti-jamming
Smart city	Sensing and monitoring	Audit logging, privacy filtering
Industrial inspection	Deterministic operation	Secure updates, low latency
Agriculture	Large-area sensing	Data integrity, lightweight AI
Defense	Mission resilience	PQC, covert links, swarm trust

REFERENCES

[1] T. H. Do, T. V. Nguyen, H. D. Le, and N. T. Dang, "DRL-based power optimization for hybrid FSO/THz-enabled UAV systems using IR-HARQ," *IEICE Communications Express*, 2026.

[2] Z. A. Haider, I. Ullah, A. Abdusalomov, M. Shah, M. Z. Khan, and B. A. Zneid, "Edge-intelligent semantic aggregation in blockchain-secured 6G UAV-assisted Internet of vehicles," *Journal of Electronic Science and Technology*, p. 100350, 2026.

[3] Y. Han, Z. Jia, J. Zhao, L. He, Y. Wu, and Q. Wu, "SDN-Blockchain Based Security Routing for UAV Communication via Reinforcement Learning," *arXiv preprint arXiv:2601.12774*, 2026.

[4] B. Li, X. Liu, D. Liu, D. Niyato, and Z. Han, "Semantic-Aware Command and Control Transmission for Multi-UAVs," *arXiv preprint arXiv:2602.00142*, 2026.

[5] T. M. Hoang, B. C. Nguyen, X. N. Tran, G. T. Luu et al., "Analysis of multiantenna UAV-aided NOMA relay systems for short-packet communications between multiuser pairs," *IEEE Trans. Aerospace and Electronic Systems*, vol. 60, no. 3, pp. 3237–3254, 2024.

[6] M. Aljamal et al., "A Novel Dual-Layer Quantum-Resilient Encryption Strategy for UAV–Cloud Communication Using Adaptive Lightweight Ciphers and Hybrid ECC–PQC," *Computers*, vol. 15, no. 2, p. 101, 2026.

[7] B. Cordill, D. Fang, and S. Xu, "A comprehensive survey of security and privacy in UAV systems," *IEEE Access*, 2025.

[8] A. S. S. Al Farsi, A. Khan, M. R. Mughal, and M. M. Bait-Suwailam, "Privacy and security challenges in federated learning for uav systems: A systematic review," *IEEE Access*, vol. 13, pp. 86599–86615, 2025.

[9] A. Yao et al., "FedShufde: A privacy preserving framework of federated learning for edge-based smart UAV delivery system," *Future Generation Computer Systems*, vol. 166, p. 107706, 2025.

[10] A. Abu-Khadrah et al., "Drone-assisted adaptive object detection and privacy-preserving surveillance in smart cities using whale-optimized deep reinforcement learning techniques," *Scientific Reports*, vol. 15, no. 1, p. 9931, 2025.

[11] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[12] V. O. Nyangaresi, M. Ahmad, L. A. Maghrabi, and T. Althaqafi, "Cost-effective PUF and ECC based authentication protocol for secure internet of drones communication," *IEEE Internet of Things Journal*, 2025.

[13] M. A. Sen, S. Al-Rubaye, and A. Tsourdos, "Securing uav flying ad hoc wireless networks: Authentication development for robust communications," *Sensors*, vol. 25, no. 4, p. 1194, 2025.

[14] Q. Xie and H. Wang, "PUF-based secure and efficient anonymous authentication protocol for UAV towards cross-domain environments," *Drones*, vol. 9, no. 4, p. 260, 2025.

[15] A. Aljumah, "UAV-based secure data communication: multilevel authentication perspective," *Sensors*, vol. 24, no. 3, p. 996, 2024.

[16] G. E. M. Abro et al., "Comprehensive review of UAV detection, security, and communication advancements to prevent threats," *Drones*, vol. 6, no. 10, p. 284, 2022.

[17] A. F. S. Akhter, M. Ahmed, A. F. S. Shah, A. Anwar, and A. Zengin, "A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, 2021.

[18] M. Yahuza et al., "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[19] R. N. Akram et al., "Security, privacy and safety evaluation of dynamic and static fleets of drones," in *2017 IEEE/AIAA DASC*, 2017, pp. 1–12.

[20] P. D. Roodsari, S. B. Sarmadi, and H. M. Boorani, "Post-Quantum Authentication and Communication Security for Drone Networks," *IEEE Trans. Dependable and Secure Computing*, 2025.

[21] M. Wu et al., "Federated Learning Driven Covert Communication in Satellite Terrestrial Integrated Networks: A Privacy-Preserving Framework," *IEEE JSAC*, 2025.

[22] A. A. Alshdadi et al., "Federated deep learning for scalable and privacy-preserving distributed denial-of-service attack detection in internet of things networks," *Future Internet*, vol. 17, no. 2, p. 88, 2025.

[23] Y. Qu, Y. Zhang, Y. Wang, and Y. Yang, "Secure and privacy-preserving issues in integrated sensing and communication-enabled wireless networks: a survey," *EURASIP J. Adv. Signal Process.*, vol. 2026, no. 1, p. 4, 2026.

[24] S. Shao et al., "Empowering AI-native 6G wireless networks with quantum federated learning," *IEEE Wireless Communications*, 2025.

[25] C. Balaji et al., "A unified AI-driven framework for quantum-secured 6G THz networks with intelligent reflecting surfaces and federated edge learning," *Scientific Reports*, vol. 15, no. 1, p. 42510, 2025.

[26] R. A. Agyapong et al., "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," in *IEEE SSCI*, 2021, pp. 01–08.

[27] Y. Dang, A. Karakoc, S. Norshahida, and R. Jäntti, "3D radio map-based GPS spoofing detection and mitigation for cellular-connected UAVs," *IEEE Trans. Machine Learning in Communications and Networking*, vol. 1, pp. 313–327, 2023.

[28] G. S. Rawat, K. Singh, N. I. Arshad, K. Hadidi, and A. Ahmadian, "A lightweight authentication scheme with privacy preservation for vehicular networks," *Computers and Electrical Engineering*, vol. 100, p. 108016, 2022.

[29] X. Chen, C. Hu, H. Xia, P. Hu, and J. Yu, "Lightweight and Efficient Authentication Scheme for Secure Intra/Inter-Domain Communications in the Internet of Drones," *IEEE Trans. Network Science and Engineering*, vol. 13, pp. 3810–3827, 2025.

[30] J. Subramani et al., "Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones," *Security and Privacy*, vol. 7, no. 3, p. e364, 2024.

[31] S. Fugkeaw et al., "ChainDrone: Lightweight Group Authentication and Audited Data Transfer for Drone Swarms with Blockchain Integration," *IEEE Open J. Commun. Soc.*, 2026.

[32] J. Kim, Y. Lee, J.-H. Kang, and S.-H. Seo, "pqRID: Compact, Anonymous Remote Identification and Post-Quantum Authentication for Drones," *IEEE Internet of Things Journal*, 2026.

[33] C. Fu and Y. Guan, "LQSCPPA: Lightweight and Quantum-Secure Lattice-Based Conditional Privacy-Preserving Authentication Scheme for VANET," *IEEE Internet of Things Journal*, 2026.

[34] R. Latif et al., "BBAS: A blockchain-based authentication system for e-health with multi-factor authentication, access control, and post-quantum security," *Scientific Reports*, 2026.

[35] V. H. Nam, G. Jeon, A. Chehri, B. T. Thanh, and V. K. Quy, "An Improved Reinforcement Learning Approach for Sustainable 6G UAV Communications," *Expert Systems*, vol. 43, no. 2, p. e70192, 2026.

[36] Y. Yao, P. Dash, and K. Pattabiraman, "Poster: May the swarm be with you: Sensor spoofing attacks against drone swarms," in *ACM CCS*, 2022, pp. 3511–3513.

[37] G. Zhao et al., "Passive User Authentication Utilizing Screen-Touch Trajectory for Unmanned Aerial Vehicle Systems," unpublished.

[38] P. Wang et al., "PWD-MFS: a lightweight multispectral fusion network for detection of pine wilt disease with UAV imagery," *J. King Saud Univ. Computer and Information Sciences*, 2026.

[39] H. Yu et al., "YOLO-LIRTU: a lightweight infrared real-time UAV detection framework," *Pattern Analysis and Applications*, vol. 29, no. 1, p. 29, 2026.

[40] K. A. Tychola, K. Voulgaridis, and T. Lagkas, "Beyond flight: Enhancing the Internet of Drones with blockchain technologies," *Drones*, vol. 8, no. 6, p. 219, 2024.

[41] F. Toscano et al., "Unmanned aerial vehicle for precision agriculture: A review," *IEEE Access*, vol. 12, pp. 69188–69205, 2024.

[42] A. Koubaa et al., "Deepbrain: Experimental evaluation of cloud-based computation offloading and edge computing in the internet-of-drones for deep learning applications," *Sensors*, vol. 20, no. 18, p. 5240, 2020.

[43] N. H. Qasim and A. M. Jawad, "5G-enabled UAVs for energy-efficient opportunistic networking," *Heliyon*, vol. 10, no. 12, 2024.

[44] M. Y. Arafat and S. Moh, "Routing protocols for unmanned aerial vehicle networks: A survey," *IEEE Access*, vol. 7, pp. 99694–99720, 2019.

[45] A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey," *Neural Computing and Applications*, vol. 35, no. 31, pp. 23063–23101, 2023.

[46] K. N. Qureshi et al., "Blockchain-based trust and authentication model for detecting and isolating malicious nodes in flying ad hoc networks," *IEEE Access*, vol. 12, pp. 95390–95401, 2024.

[47] K. Huang, H. Hu, and C. Lin, "Bakas-uav: A secure blockchain-assisted authentication and key agreement scheme for unmanned aerial vehicles networks," *IEEE Internet of Things Journal*, vol. 11, no. 22, pp. 36858–36883, 2024.

[48] S. Hafeez et al., "Blockchain-assisted UAV communication systems: A comprehensive survey," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 558–580, 2023.

[49] S. H. Alsamhi et al., "Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration," *IEEE Trans. Green Communications and Networking*, vol. 7, no. 1, pp. 328–338, 2022.

[50] S. Sai, A. Garg, K. Jhawar, V. Chamola, and B. Sikdar, "A comprehensive survey on artificial intelligence for unmanned aerial vehicles," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 713–738, 2023.

[51] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 4, pp. 2624–2661, 2016.

[52] N. Fatima, P. Saxena, and M. Gupta, "Integration of multi access edge computing with unmanned aerial vehicles: Current techniques, open issues and research directions," *Physical Communication*, vol. 52, p. 101641, 2022.

[53] S. A. Huda and S. Moh, "Survey on computation offloading in UAV-Enabled mobile edge computing," *J. Network and Computer Applications*, vol. 201, p. 103341, 2022.

[54] M. A. Qadir, S. Sharif, S. Zeadally, and W. Ejaz, "Digital twin-enabled unmanned aerial vehicles network for disaster management," *IEEE Internet Computing*, 2025.

[55] H. Sikarwar et al., "Secure: Secure and efficient protocol using randomness and edge-computing for drone-assisted internet of vehicles," *IEEE Trans. Network and Service Management*, vol. 21, no. 6, pp. 6974–6988, 2024.

[56] T. Wang, X. Ouyang, D. Sun, Y. Chen, and H. Li, "Offloading strategy based on graph neural reinforcement learning in mobile edge computing," *Electronics*, vol. 13, no. 12, p. 2387, 2024.

[57] R. Alkadi, N. Alnuaimi, C. Y. Yeun, and A. Shoufan, "Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues," *IEEE Access*, vol. 10, pp. 14463–14479, 2022.

[58] T. R. Pijnappel, J. van den Berg, S. C. Borst, and R. Litjens, "Online positioning of a drone-mounted base station in emergency scenarios," *IEEE Trans. Vehicular Technology*, vol. 73, no. 4, pp. 5572–5586, 2023.

[59] F. B. Sorbelli, P. Chatterjee, F. Corò, S. Ghobadi, L. Palazzetti, and C. M. Pinotti, "A novel graph-based multi-layer framework for managing drone bvlos operations," *IEEE Trans. Network and Service Management*, vol. 21, no. 5, pp. 5091–5105, 2024.