IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 August 2022, accepted 12 August 2022, date of publication 17 August 2022, date of current version 23 August 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3199408*

TOPICAL REVIEW

# Secure UAV-Aided Mobile Edge Computing for IoT: A Review

**EMMANOUEL T. MICHAILIDIS[1,2], (Member, IEEE), KONSTANTINOS MALIATSOS[2], DIMITRIOS N. SKOUTAS[2], (Senior Member, IEEE), DEMOSTHENES VOUYIOUKAS[2], (Senior Member, IEEE), AND CHARALABOS SKIANIS[2], (Senior Member, IEEE)**

[1]Department of Electrical and Electronics Engineering, University of West Attica, 12241 Egaleo, Greece
[2]Department of Information and Communication Systems Engineering, School of Engineering, University of the Aegean, 83200 Samos, Greece

Corresponding author: Emmanouel T. Michailidis (emichail@uniwa.gr)

This work was funded by the Research e-Infrastructure [e-Aegean R&D Network] (Code Number MIS 5046494), which is implemented within the framework of the ''Regional Excellence'' Action of the Operational Program ''Competitiveness, Entrepreneurship and Innovation''. This action was co-funded by the European Regional Development Fund (ERDF) and the Greek State [Partnership and Cooperation Agreement 2014-2020].

**ABSTRACT** As the Internet of Things (IoT) ecosystem evolves, innovative applications with stringent demands with respect to latency will emerge. To handle computation-intensive tasks in a timely manner, data offloading to Mobile Edge Computing (MEC) servers has been suggested. On the other hand, prospective IoT networks are expected to include Unmanned Aerial Vehicles (UAVs) to enhance coverage and connectivity, while retaining reliable communication links with ground nodes in urban, suburban, and rural terrain. Nevertheless, the evolution of UAV-aided MEC-enabled IoT presupposes the mitigation of security threats through the implementation of efficient and robust countermeasures. As UAVs inherently have certain limitations in terms of energy, computational, and memory resources, designing lightweight security solutions is required. This paper provides an overview of the UAV-aided MEC-enabled IoT and a detailed presentation of use cases and application scenarios, where security is of utmost importance. Subsequently, up-to-date research works on security solutions for the UAV-aided MEC-enabled IoT are comprehensively presented. To this end, the adoption of information-theoretic techniques that ensure adequate Physical-Layer Security (PLS) is discussed along with sophisticated security approaches based on emerging technologies, such as Blockchain and Machine Learning (ML). In addition, research studies on software- and hardware-based methods for the identification and authentication of network nodes are presented. Finally, this paper provides future perspectives in this research domain, stimulating further work.

**INDEX TERMS** Blockchain, Internet of Things (IoT), machine learning (ML), mobile edge computing (MEC), physical-layer security (PLS), unmanned aerial vehicle (UAV).

## ACRONYMS

| Acronym | Description |
|---|---|
| 3-D | Three-Dimensional |
| 5G | Fifth-Generation |
| AGMEN | Air-Ground Integrated Mobile Edge Network |
| ANN | Artificial Neural Networks |
| AP | Access Point |
| AR | Augmented Reality |
| AVISPA | Automated Validation for Internet Security Validation and Application |
| B5G | Beyond Fifth-Generation |
| BCD | Block Coordinate Descent |
| BF | Bloom Filter |
| BS | Base Station |
| C-RAN | Cloud Radio Access Network |
| CA | Certification Authority |
| CAP | Computational Access Point |
| CK | Canetti–Krawczyk |
| CL-BS | Certificateless Blind Signature |
| CNN | Convolutional Neural Network |

The associate editor coordinating the review of this manuscript and approving it for publication was Vyasa Sai.

| | |
|---|---|
| CPU | Central Processing Unit |
| CSI | Channel State Information |
| CSMA/CA | Carrier Sense Multiple Access Protocol with Collision Avoidance |
| DDPG | Deep Deterministic Policy Gradient |
| DF | Decode-and-Forward |
| DL | Deep Learning |
| DNN | Deep Neural Network |
| DoS | Denial of Service |
| DP | Differential Privacy |
| DQL | Deep Q-Learning |
| DQN | Deep Q-Network |
| DRL | Deep Reinforcement Learning |
| DY | Dolev and Yao |
| ECS | Edge Computing Stations |
| ECC | Elliptic-Curve Cryptography |
| eMBB | enhanced Mobile Broadband |
| ETSI | European Telecommunications Standards Institute |
| FAA | Federal Aviation Administration |
| FANET | Flying Ad-hoc Network |
| FEEL | Federated Edge Learning |
| FL | Federated Learning |
| FLIR | Forward-looking infrared |
| FM-JSFP | Fading Memory Joint Strategy Fictitious Play |
| GCS | Ground Control Station |
| GPS | Global Positioning System |
| GS | Ground Station |
| GU | Ground User |
| HECC | Hyperelliptic Curve Cryptography |
| HSM | Hardware Security Module |
| IC | Integrated Circuit |
| IMU | Inertial Measurement Unit |
| IoD | Internet of Drones |
| IoFT | Internet of Flying Things |
| IOS | Intelligent Omni Surface |
| IoT | Internet of Things |
| ISG | Industry Specification Group |
| ITS | Intelligent Transportation System |
| LAP | Low-Altitude Platform |
| LDP | Local Differential Privacy |
| LoS | Line-of-Sight |
| M-UAV | Monitoring UAV |
| M2M | Machine-to-Machine |
| MCS | Mobile Crowdsensing |
| MDP | Markov Decision Process |
| ML | Machine Learning |
| MEC | Mobile Edge Computing |
| MEMS | Micro Electromechanical Systems |
| MIMO | Multiple-Input Multiple-Output |
| mMTC | massive Machine Type Communications |
| MTD | Machine-Type Device |
| NASA | National Aeronautics and Space Administration |
| NOMA | Non-Orthogonal Multiple Access |
| PER | Prioritized Experience Replay |
| PKI | Public Key Infrastructure |
| PLS | Physical-Layer Security |
| PUF | Physically Unclonable Function |
| OAI | OpenAirInterface |
| QoE | Quality of Experience |
| QoLM | Quality of Local Model Update |
| QoS | Quality of Service |
| RA | Radio Access |
| RF | Radio Frequency |
| RL | Reinforcement Learning |
| RMEC | Raspberry Pi-Based Multi-Access Edge Computing |
| RTCA | Radio Technical Commission for Aeronautics |
| RIS | Reconfigurable Intelligent Surface |
| RSU | Road-Side Units |
| SCA | Successive Convex Approximation |
| SDN | Software-Defined Networking |
| SEE | Secrecy Energy Efficiency |
| SHA | Secure Hash Algorithm |
| SI | Self-Interference |
| SIC | Successive Interference Cancellation |
| SLPAKA | Secure Lightweight Proven Authenticated Key Agreement |
| TA | Trusted Authority |
| TAC | Trusted Authority Center |
| TDMA | Time-Division Multiple Access |
| TON | Task Offloading Notices |
| TPM | Trusted Platform Module |
| U2U | UAV-to-UAV |
| UAS | Unmanned Aerial System |
| UAV | Unmanned Aerial Vehicle |
| UHD | Ultra-High Definition |
| URLLC | Ultra-Reliable Low Latency Communications |
| V2X | Vehicle-to-Everything |
| VANET | Vehicular Ad hoc Network |
| VR | Virtual Reality |
| WPT | Wireless Power Transfer |
| WSN | Wireless Sensor Network |
| YOLO | You only look once |

## I. INTRODUCTION

As the Internet of Things (IoT) and big data era emerge in next-generation communication networks, a vast number of interconnected nodes equipped with computation and communication units will pave the way for novel services. Apart from the ground terminals, aerial nodes based on Unmanned Aerial Vehicles (UAVs) flying in three-dimensional (3-D) space are expected to act as moving radio access (RA) nodes [1] and provide flexibility, ubiquitous connectivity, and sufficient radio coverage in the Internet of Drones (IoD) paradigm [2]. However, the next wave of applications, including Augmented/Virtual Reality (AR/VR), Ultra-High Definition

(UHD) video streaming, and Tactile Internet, will reach the limits of current technologies and pose strict requirements in terms of computation, storage, latency, and throughput. For locally processed computation tasks, a large amount of energy is consumed, which in turn reduces the endurance of energy-limited IoT nodes. In addition, it is often infeasible for resource-constrained nodes to handle computation-intensive tasks in a timely manner, whereas a massive number of these nodes in large-scale IoT deployments usually makes the core network congested.

To meet the critical latency requirements of modern data-intensive applications, satisfy the demands of real-time data processing, and provide exceptional Quality of Experience (QoE), task offloading to Mobile Edge Computing (MEC) servers has been suggested as an extension of centralized cloud computing [3], [4]. The MEC servers are generally located in close proximity to resource-limited nodes and have powerful storage and processing capabilities. In [5], the implementation challenges of UAV-aided MEC-enabled networks were described, whereas an Air-Ground Integrated Mobile Edge Network (AGMEN) with multiple flexibly deployed drone cells was proposed in [6]. Based on AGMEN, IoT application scenarios were envisioned with drones acting either as edge network controllers or fog computing platforms for IoT services. In [7], single- and multi-UAV aerial computing architectures were proposed with UAVs acting as MEC servers, users, or relays. Moreover, case study simulations were performed to depict the benefits of MEC-enabled networks with joint computation and communication design over conventional infrastructure-based MEC-enabled networks. Most recent relevant research work has emphasized on energy-aware techniques [8], optimization of resource allocation [9], latency [10], and computation efficiency [11]. Furthermore, emerging communication and network technologies are envisioned to enhance the performance of Fifth Generation (5G) IoT networks and the Quality of Service (QoS), such as Wireless Power Transfer (WPT) [12], Non-Orthogonal Multiple Access (NOMA) [12], Software-Defined Networking (SDN) [13], Reconfigurable Intelligent Surface (RIS) [14], massive Multiple-Input Multiple-Output (MIMO) [15], and Machine Learning (ML) [16].

Nevertheless, there exist various challenges and barriers to secure IoT network operation and task offloading [17], due to the wide distribution of nodes in open and remote environments, highly dynamic network topology, high possibility of short-distance Line-of-Sight (LoS) connections, and unencrypted wireless links [18]. As node authentication is a prevalent requirement for security, efficient authentication mechanisms should be also implemented. More importantly, several security attacks [19] should be mitigated to avoid potential economic, societal, and environmental impact. However, UAVs have intrinsic constraints in terms of energy, computational, and memory resources. Thus, the design of robust security solutions is a non-trivial and complicated process, whereas the application of upper-layer cryptography-based schemes may be infeasible in practice. In this respect, Physical-Layer Security (PLS) can be used to obtain secure information-theoretic transmissions, while maintaining low computational complexity [20]. In addition, ML [21] and Blockchain [22] have been recently recognized as key enabling technologies for precisely handling the decision-making process and safeguarding security, respectively.

### *A. CONTRIBUTION*

Motivated by the aforementioned observations, this review paper intends to shed light on a broad set of up-to-date, state-of-the-art mechanisms for successfully realizing secure UAV-aided MEC-enabled IoT. Recently, a plethora of review and survey works focusing on IoT architectures, the deployment of UAVs as network nodes, the use of MEC technology, and the development of security methods for next-generation networks has been published. To the best of the authors' knowledge, there are no review papers on secure UAV-aided MEC-enabled IoT and the intersection of IoT, UAVs, MEC, and security has not yet been adequately investigated. Towards this end, the main contributions of this paper can be summarized as follows:

- A brief overview of the background information on the UAV-aided MEC-enabled IoT, PLS, and authentication issues is provided. Also, the role of ML, Blockchain, and their combination in strengthening the security aspects is underlined.
- Indicative use cases concerning secure computation offloading are discussed.
- An exhaustive overview of recent security solutions from all possible categories ranging from PLS schemes to emerging ML-inspired and Blockchain-based methods is comprehensively presented.
- Lightweight methods for the authentication of heterogeneous network nodes within the UAV-aided MEC-enabled IoT are described.
- Current limitations and open issues are highlighted.

Fig. 1 classifies the security methods, which are comprehensively reviewed in this paper.

### *B. STRUCTURE*

The remainder of this paper is organized as follows. Section II investigates relevant review and survey papers and indicates their goals and shortcomings. Section III provides an overview of the UAV-aided MEC-enabled IoT and examines several representative use cases in different application domains. Section IV studies the role of PLS and node authentication for secure operations and also provides insights into ML and Blockchain. Section V emphasizes the recently proposed PLS mechanisms and Section VI presents ML-inspired and Blockchain-based techniques. Software- and hardware-based authentication schemes are outlined in Section VII. Section VIII identifies fertile areas for future research. Finally, Section IX concludes this paper.

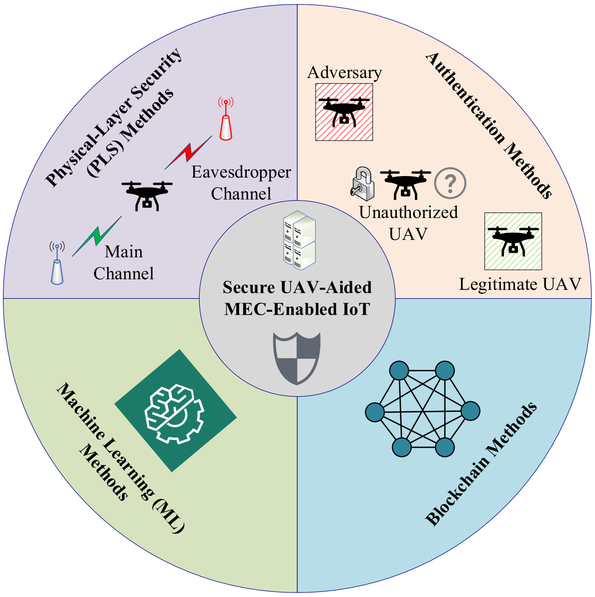


**FIGURE 1. The major security approaches for the UAV-aided MEC-enabled IoT.**

## II. PREVIOUS REVIEW AND SURVEY WORKS

Previously, a wide range of reviews, surveys, and tutorials investigating IoT, MEC, UAVs, and security issues, as well as their interplay, has been published. This section provides a literature review concerning these works, which are also synopsized in Table 1.

### A. MEC-ENABLED IOT

In [23], the fundamental features of MEC technology were underlined in a holistic manner, indicative use case scenarios were investigated, and both theoretical and experimental research activities were analyzed. In this respect, the integration and interaction of MEC with 5G enabling technologies were considered and the role of NOMA, WPT, energy harvesting, UAVs, IoT, heterogeneous Cloud Radio Access Network (C-RAN), and ML was discussed. Insight on potential MEC-enabled IoT applications and relevant technical aspects (e.g., scalability, communication, computation offloading, resource allocation, mobility management, security, privacy, and trust management) was given in [24]. However, the works in [23] and [24] partially studied the security issues and the integration of UAVs in MEC-enabled IoT scenarios. From a cyber-physical security perspective, potential threats and vulnerabilities were identified in [17]. These threats were classified based on the intrusion target, that is the access network, mobile edge network, and core network. Furthermore, state-of-the-art mechanisms that can mitigate security threats and preserve privacy were outlined. Nevertheless, the work in [17] did not invoke UAVs as network nodes towards establish a secure MEC-enabled IoT and did not include relevant research activities.

### B. UAV-AIDED NETWORKS

The concept of the Internet of Flying Things (IoFT) for Beyond 5G (B5G) networks was introduced in [25] and its major characteristics were discussed. In addition, certain obstacles towards the realization of IoFT scenarios were designated, such as collision avoidance, interference mitigation, path planning, energy consumption, security, privacy, and control and management of the UAVs. To tackle the strict requirements of enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and massive Machine Type Communications (mMTC), the adoption of advanced techniques (e.g., NOMA, massive MIMO, RIS, short packet transmission, energy harvesting, radio-based sensing, and ML) was considered in [26]. Although flying edge-computing network architectures were envisioned in [27] and [28], the MEC technology was not the main research objective of these works, possible UAV-aided MEC-enabled network schemes were partly investigated, and up-to-date research works were not provided. The integration of UAVs into cellular networks was also considered in [29] and the corresponding core technologies and challenges were surveyed without taking into account computation offloading.

### C. UAV-AIDED MEC-ENABLED NETWORKS

On the other hand, a wide variety of UAV-aided MEC-enabled network architectures and algorithms were comprehensively reviewed, classified, and evaluated from a computation offloading perspective in [30]. Additionally, issues related to computation, security, cost, and mobility were discussed. In this respect, both single-UAV and multi-UAV deployments were considered and relevant applications and case studies were underlined to emphasize the emergence of combining UAVs and MEC. The survey paper in [31] investigated the role of UAVs as MEC servers, users or relays in three different MEC-enabled network architectures and described the recent advances and the indicative scenarios, i.e., hotspots, remote and complex terrains, battlefields, and areas suffering from natural disasters. In this regard, the major implementation challenges were underlined with respect to the operation mode, the local computing techniques, the offloading techniques, and the resource allocation. The benefits and drawbacks of several research efforts in the field of UAV-aided MEC-enabled networks were categorized in [32] and particular categories were identified, which are associated with energy efficiency, resource allocation, security, architecture, and latency. The integration of these networks into B5G networks and Industry 5.0 was also discussed as an extension of cloud computing and edge computing, emerging use cases were described, and future research perspectives were identified to further enhance the QoE and QoS. In [33], various AGMEN architectures were extensively reviewed and the corresponding communication, computation, and edge caching techniques were discussed. In this direction, the characteristics and components of the Unmanned Aerial Systems (UASs) were described and challenges regarding

**TABLE 1.** Relevant review and survey papers.

| Reference | Year | Short Description | UAVs | MEC | Security |
|---|---|---|---|---|---|
| Ranaweera et al. [17] | 2021 | Survey on security and privacy aspects, threats and solutions of MEC | ✗ | ✓ | ✓ |
| Michailidis et al. [18] | 2022 | Review on software- and hardware-based authentication schemes for the IoD | ✓ | Partially | Partially |
| Bithas et al. [21] | 2019 | Survey on ML methods for UAV-based communications | ✓ | ✗ | Partially |
| Mehta et al. [22] | 2020 | Survey on authentication and privacy issues in UAV-based networks and Blockchain-based solutions | ✓ | ✗ | ✓ |
| Pham et al. [23] | 2020 | Survey on key enabling technologies and applications for the MEC-enabled B5G networks | Partially | ✓ | Partially |
| Porambage et al. [24] | 2018 | Survey on key enabling technologies and applications for the MEC-enabled IoT | ✗ | ✓ | Partially |
| Zaidi et al. [25] | 2021 | Survey on characteristics, applications, and taxonomy of the IoFT | ✓ | Partially | Partially |
| Wu et al. [26] | 2021 | Overview of key enabling technologies for the UAV-based B5G networks | ✓ | Partially | Partially |
| Fotouhi et al. [27] | 2019 | Survey on challenges, standardization activities, field tests, and security issues for UAV-based cellular communications | ✓ | Partially | ✓ |
| Huda et al. [28] | 2022 | Survey on design issues, network architectures, and offloading techniques for UAV-aided MEC-enabled systems | ✓ | ✓ | Partially |
| Zhou et al. [29] | 2020 | Review on advances, challenges, and open issues for UAV-aided MEC-enabled networks | ✓ | ✓ | Partially |
| Fatima et al. [30] | 2022 | Review on key findings, enabling technologies and open issues for UAV-aided MEC-enabled networks | ✓ | ✓ | Partially |
| Zhang et al. [31] | 2020 | Survey on applications, challenges, and research advances of AGMEN | ✓ | ✓ | Partially |
| Yazid et al. [32] | 2021 | Review on AI methods for UAV-aided MEC-enabled IoT | ✓ | ✓ | Partially |
| Abrar et al. [33] | 2021 | Review on research work for energy-efficient UAV-aided MEC-enabled IoT | ✓ | ✓ | Partially |
| Shakeri et al. [34] | 2019 | Review on design challenges of multi-UAV systems for cyber-physical applications | ✓ | ✗ | ✓ |
| Shafique et al. [35] | 2021 | Survey on security protocols, vulnerabilities, and solutions in UAVs | ✓ | ✗ | ✓ |
| Mekdad et al. [36] | 2021 | Survey on security and privacy issues of UAVs and systematic classification at hardware-level, software-level, communication-level, and sensor-level. | ✓ | ✗ | ✓ |
| Lagkas et al. [37] | 2018 | Review on UAV-aided 5G IoT applications, security and privacy issues, and solutions | ✓ | ✗ | ✓ |
| Yaacoub et al. [38] | 2020 | Review on vulnerabilities of drone-based networks in military and civilian domains | ✓ | ✗ | ✓ |
| Altawy et al. [39] | 2017 | Survey on security, privacy, safety aspects, and physical and cyber threats during the operation of civilian drones | ✓ | ✗ | ✓ |
| Syed et al. [40] | 2021 | Review on optimal techniques based on Blockchain, ML, and watermarking for securing UAVs | ✓ | ✗ | ✓ |
| Hassija et al. [41] | 2021 | Review on security-critical drone applications, security challenges, and countermeasures based on Blockchain, SDN, ML, and fog/edge computing | ✓ | Partially | ✓ |
| Challita et al. [42] | 2019 | Review on wireless and security challenges of UAV-based delivery systems, real-time multimedia streaming, and, intelligent transportation systems. Application of AI methods | ✓ | ✗ | ✓ |
| McCoy et al. [43] | 2019 | Review on advances, vulnerabilities, and SDN-based security solutions for UAV-based networks | ✓ | ✗ | ✓ |
| This paper | 2022 | Review on security mechanisms for UAV-aided MEC-enabled IoT | ✓ | ✓ | ✓ |

channel modeling, mobility, trajectory planning, energy efficiency, and harvesting were analyzed. In [34], ML and Deep Learning (DL) were seen as cornerstones for implementing intelligent UAV-aided MEC-enabled networks and revolutionizing the decision-making process from massively generated, collected, or exchanged data. As a substantial amount of energy can be consumed during local computation and data offloading, a wide range of energy-aware methods was recently proposed to keep the energy consumption at a low level thus prolonging the battery life of ground terminals and increasing the endurance of resource-limited UAVs. These methods were thoroughly reviewed in [35], computation offloading access schemes were summarized, and the underlying types of optimization problems that lead to optimal, sub-optimal, near-optimal, or global optimal solutions were studied. However, the works in [30], [31], [32], [33], [34], and [35] did not focus on security-based mechanisms.

### D. SECURE UAV-AIDED NETWORKS

In recent years, the research area of security for UAV-based deployments has received several contributions. A summary of security issues and indicative use cases was provided in [27]. However, security was not the main research objective of this work. Moreover, the UAV-aided networks were exhaustively reviewed in [34], [35], and [36], and a discussion about vulnerabilities, threats, cyber-physical security applications, and security protocols was included. The use of drones as "flying" things was suggested in [37], the security challenges were summarized, and a secure IoT architectural framework was proposed. In [38], certain weaknesses of the UAVs were underlined, the security issues were studied in the context of the civilian and military domain, and an indicative use case involving an attack life cycle was described. A high-level insight on the network architecture of a communication system that includes civilian drones was given in [39] and the deployment and security issues were highlighted. As different UAV-based network layers may be exposed to attacks in military and disaster scenarios, the role of Blockchain, ML, and watermarking was pointed out in [40], whereas relevant application scenarios involving ML, Blockchain, SDN, and edge computing were discussed in detail in [41]. A thorough review of relevant research works for heterogeneous B5G UAV-based networks was provided in [21] and emphasis on ML-based methods was given to enhance the secrecy level during data communication. The use of Artificial Neural Networks (ANNs) as potential countermeasures against security attacks at higher communication layers of UAV-based delivery systems, Intelligent Transportation Systems (ITS), and real-time multimedia streaming was suggested in [42]. The security and privacy challenges in UAV-aided networks were surveyed in [22] and a Blockchain-based scheme was presented. Nevertheless, this paper is currently outdated and does not invoke recent research activities. Various security solutions for SDN-enabled UAV networks were presented in [43]. In [18], up-to-date research studies on authentication mechanisms for UAV-based networks were presented. To this end, the adoption of conventional technologies and methods, such as the widely used hash functions, Public Key Infrastructure (PKI), and Elliptic-Curve Cryptography (ECC), was discussed along with emerging technologies, including MEC, ML, and Blockchain. Additionally, a review of effective hardware-based solutions for the identification and authentication of network nodes was provided and the use of Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), and Physically Unclonable Functions (PUFs) as effective security solutions was indicated. Nevertheless, the role of authentication was only studied in [18], whereas the use of MEC was not considered in [21], [22], [27], [34], [35], [36], [37], [38], [39], [40], [41], [42], and [43].

To reconcile the shortcomings of the aforementioned works and extensively study the ambiguous landscape concerning the available security solutions for the UAV-aided MEC-enabled IoT, contemporary review papers are requisite. Therefore, this paper focuses on the investigation and comparison of a broad set of security solutions.

## III. OVERVIEW OF MEC-ENABLED IOT AND UAV-AIDED NETWORKS

The notion of MEC technology was initially introduced by the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) [44] as a key enabler for the execution of computation-intensive and latency-sensitive tasks at the edge of the networks, as well as for the storage of a huge number of datasets. MEC stands for an extension of cloud computing and intends to surpass network congestion issues, enhance resource optimization, and bring benefits to mobile operators, third parties, and end-consumers. As the IoT applications evolve, the computing and storage requirements increase and there is a need for auxiliary computing capacity. In this regard, centralized cloud computing cannot meet the growing demands for ultra-low latency, mobility, flexibility, scalability, and location awareness. Since a large number of connected devices consecutively generate data, the collaborative and complementary combination of MEC and IoT is highly suggested to construct novel applications in the civilian and military domains [3]. More importantly, the use of MEC servers with sufficient computing capabilities as integral elements of IoT is expected to fulfill the requirements for computation and storage of massive data by enabling efficient computation offloading and providing a host of analytics applications, whereas IoT can provide a wide range of heterogeneous smart objects and sensors. Apart from meeting the computation demands of static nodes, MEC also intrinsically supports the mobility of moving IoT nodes (e.g., vehicles and trains) across different cells. Moreover, two operation modes can be adopted for computation offloading, the partial offloading mode and the binary computation mode [28]. In the former, which ensures dynamic and flexible task allocation based on the available resources, part of the computation task is locally processed and the remaining part is computed at the MEC server. On the contrary, the latter is simpler and considers that the nodes perform only task computation offloading or local computing, thus leading to mediocre computation performance.

On the other hand, the Low-Altitude Platforms (LAPs) operating at modest altitudes, in the troposphere, can act as aerial Base Stations (BSs), relays, or Access Points (APs) and enhance the coverage, the connectivity between data collection points and sensors, and the reliability, in cases where the links of the terrestrial communication infrastructure are severely attenuated or blocked [45]. The fixed-wing and rotary-wing UAVs, commonly known as drones, constitute the main representative type of LAPs and were initially introduced into the national airspace system in 2016 by the Radio Technical Commission for Aeronautics (RTCA) [46]. It is noted that the integration of UAVs into the airspace system of the United States was also suggested by the National Aeronautics and Space Administration (NASA) and Federal Aviation Administration (FAA) [47]. Various UAV-based network architectures have been previously proposed. Apart from typical single-UAV deployments, more sophisticated network configurations have also been envisioned to provide extended scalability, reliability, survivability, efficient task distribution, and coordination, such as the Flying Ad-hoc Networks (FANETs) that involve interconnected drones configured in groups [48] and the IoD paradigm that combines heterogeneous aerial and ground interconnected network segments [18]. Among the main benefits of the UAVs are the flexibility, the rapid deployment, and the movement on-demand.

However, the UAVs typically represent resource- constrained devices and usually have insufficient computation, storage, and energy resources stemming from their restrained battery capacity and stringent size limitations. These practical constraints may discourage the use of the UAVs as MEC servers, the application of powerful computation-intensive security mechanisms, and the decision-making on the fly. Hence, the implementation of low-complexity and energy-efficient security solutions is necessary. On the other hand, the UAVs can partly or fully perform task offloading to ground MEC servers to keep their energy consumption at a low level, prolong their flight time, and satisfy the latency requirements. As the ground MEC servers are usually embedded in fixed APs, BSs, or Road-Side Units (RSUs) in the case of a Vehicular Ad hoc Network (VANET), the UAVs can be also used for effective data collection and communication in MEC-enabled IoT networks, especially in areas with obstacles and dispersed and highly mobile nodes. Depending on the application scenario, the UAVs can play the following roles:

- **UAVs as MEC servers:** In this case, there are no ground MEC servers in the vicinity of the nodes. Thus, the UAVs operate as MEC servers and assist the Ground Users (GUs) to accomplish task computation.
- **UAVs as users:** In this case, the UAVs offloads their own computation tasks to MEC servers due to their limitations in terms of energy and computation capacity.
- **UAVs as relays:** In this case, the UAVs guarantee reliable and secure offloading by acting as aerial relays forwarding the computation tasks received from GUs to ground MEC servers.
- **UAVs as data collectors or dispatchers:** In this case, the UAVs gather tasks and aggregate data from GUs that are eventually processed by MEC servers.
- **UAVs as supporting entities:** In this case, the UAVs transmit artificial noise toward malicious entities.
- **UAVs as attackers:** In this case, the UAVs may be malicious entities (e.g., eavesdroppers).

Also, the GUs can have the following roles:

- Devices with limited or moderate computational capabilities (e.g., remote IoT devices) that require MEC assistance.
- Connected vehicles (ITS nodes) supported by UAVs.
- Supporting ground nodes transmitting artificial noise towards malicious entities.
- Malicious entities (e.g., eavesdroppers).

Overall, the potential roles of the aerial and ground nodes are shown in Fig. 2.

### A. USE CASES FOR SECURE UAV-AIDED MEC-ENABLED IOT

As the application domains of UAV-aided networks expand, novel exciting use cases combining UAVs with MEC-enabled IoT systems are predicted to emerge in the near future. In particular, a variety of application scenarios have been envisioned, where providing flexible and extended radio coverage in dynamic propagation scenarios, as well as enhanced computational resources at the network's edge is of utmost importance. In these scenarios, attaining security is crucial but challenging, particularly for real-time applications, where there is a clear trade-off between security and latency. Because edge devices have limited resources, they may be vulnerable to security attacks. Therefore, it is vital to employ lightweight yet effective security solutions. In this section, relevant use cases are described.

#### 1) ENHANCED COVERAGE AND CONNECTIVITY

In current cellular networks, the integration of MEC with the network's edge nodes, i.e., the BSs, is already becoming a reality to significantly reduce latency, especially in real-time data streams, and enhance the end user's QoS and QoE. MEC enables the placement of multimedia content closer to the user, while BSs with MEC capabilities can locally run computationally intensive applications (e.g., intelligent video analytics or augmented reality-based applications), thereby relieving the strain on the core network. In this context, a compelling use of UAVs as aerial BSs or aerial relays is their ability to be flexibly deployed and operated to enhance the edge network's connectivity, caching, and computational capabilities. This can be beneficial in scenarios such as the following:

- **Confrontation of significant and rapid fluctuations in network traffic volume:** Current and future mobile networks must deal with temporal and spatial fluctuation in network traffic, which frequently results in localized traffic load bursts. This condition is intensified in hotspot areas and crowded venues (e.g., large athletic events and music festivals), when the network infrastructure confronts substantial challenges due to intense and concentrated network traffic. In this regard, UAVs can form overlaying aerial networks that have a flexible

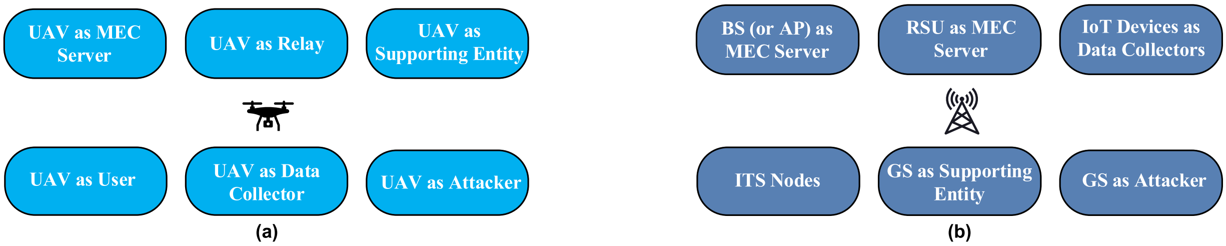


**FIGURE 2.** The role of (a) aerial and (b) ground network nodes in security scenarios.

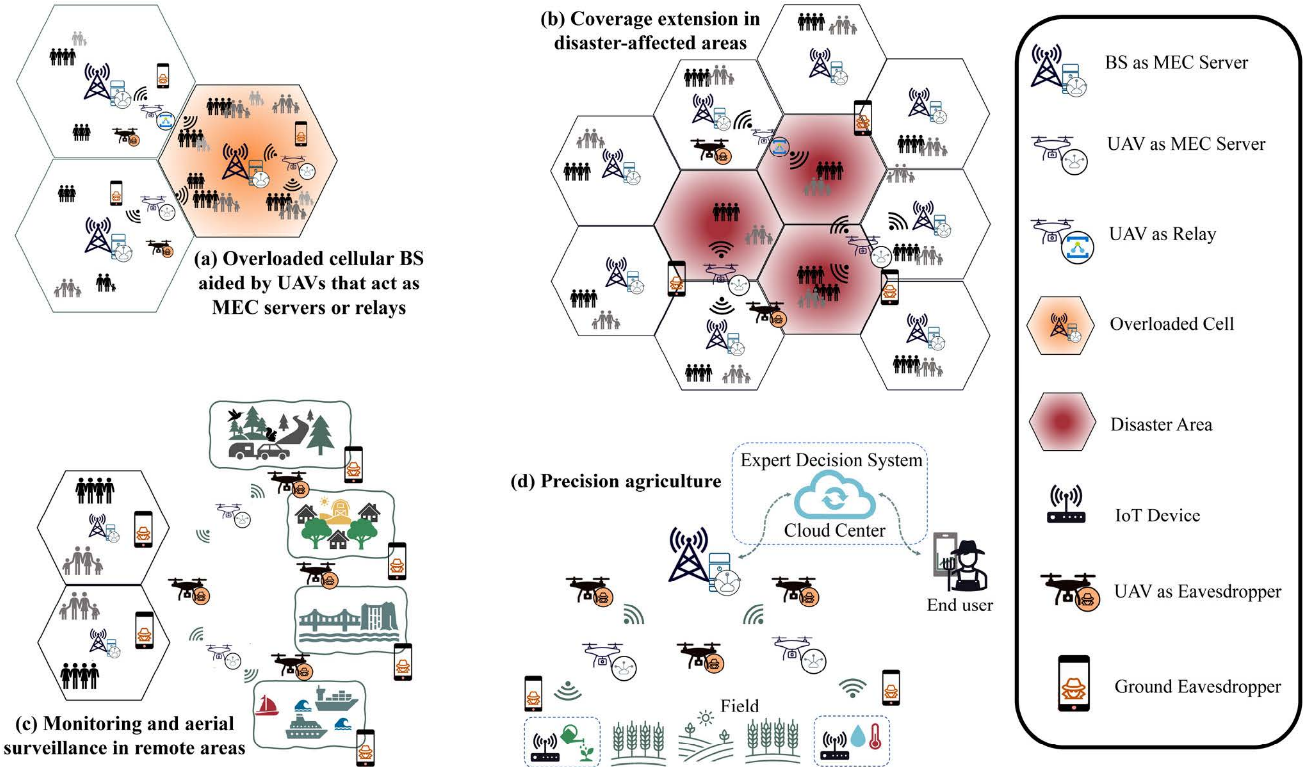

(a) Overloaded cellular BS aided by UAVs that act as MEC servers or relays
(b) Coverage extension in disaster-affected areas
(c) Monitoring and aerial surveillance in remote areas
(d) Precision agriculture
Expert Decision System
Cloud Center
End user
Field
BS as MEC Server
UAV as MEC Server
UAV as Relay
Overloaded Cell
Disaster Area
IoT Device
UAV as Eavesdropper
Ground Eavesdropper

**FIGURE 3.** Indicative use cases of secure UAV-aided MEC-enabled IoT.

structure and can be strategically deployed wherever and whenever needed to handle service requests of a massive number of GUs [49]. Thus, by acting as aerial relays UAVs should be able to guarantee reliable and secure distribution of the traffic load from an overloaded cell to the adjacent BSs with MEC capabilities, as shown in Fig. 3(a). Furthermore, emerging 5G wireless networks should be able to offer real-time eMBB services, such as live video and music streaming, and support the resource-intensive processing and orchestration of high-quality on-demand multimedia streams at the network's edge. Even more challenging can be the support of services that require URLLC network connectivity, such as AR/VR-based applications that can be used for both entertainment and non-entertainment purposes, such as online gaming, teaching, and training. The remote control of autonomous and semi-autonomous vehicles of the near future can also be rather challenging due to the requirements for ultra-low latency, high reliability, availability, and security. Consequently, the UAVs should not only act as relays, but also have significant storage and computational capabilities allowing them to locally execute computation-intensive tasks or operate as MEC nodes. Thus, they could reduce strain on the underlying network infrastructure by providing additional data caching, handling, and forwarding features. However, wireless communication is vulnerable to security threats that can compromise the overall network security. Various malicious actors can perform passive or active attacks to get access to users' private data or degrade network performance. The primary targets of these attacks are the GU-UAV and UAV-BS links, as well as the UAVs themselves, as they are considered to be more vulnerable than the BSs. These malicious actors can be either at both ground and aerial levels or they can also utilize UAVs to gain greater flexibility. Thus, the most important aspect of incorporating UAVs into 5G mobile networks is that they can be part of a robust and security-oriented communication system that ensures confidentiality, data integrity, and availability [50].

- **Extending cellular connectivity to disaster-affected areas:** Natural or man-made disasters (e.g., warfare, water contamination, earthquakes, hurricanes, and flash floods) pose a challenge to societies all over the globe. In the aftermath of such horrific events, the terrestrial communication infrastructure may be either totally or partially damaged. In such a situation, the flexible and rapid deployment of networks that exploit UAVs as aerial BSs or relays to the remaining functional MEC-enabled BSs could be a valuable solution for ensuring a steady flow of information. This is critical in preventing human fatalities by properly directing emergency vehicles (e.g., fire trucks, patrol cars, and ambulances) and maintaining communication with rescue authorities [51]. Reliable and real-time transmission of emergency data is crucial for keeping coordinators informed and plays an important role in facilitating effective and rapid decision-making. Thus, the network must be able to support the real-time transmission of commands, reports, and vital statistics, as well as real-time video monitoring of disaster zones. Furthermore, in special emergency situations, video conferencing may also be utilized to provide remote medical assistance. Evidently, an emergency communication network should be both horizontally and vertically scalable, secure, and employ adequate authentication and authorization control techniques. Also, the confidentiality of the transmitted data should be guaranteed, since an external attacker might take advantage of the vulnerabilities that could be revealed during an emergency situation to gain access to confidential data, as depicted in Fig. 3(b). Besides, terrorists may attempt to prevent the first responders from controlling the disaster's consequences by getting access to critical information, such as the location of the rescue units. Hence, it is crucial to be able to defend the deployed emergency communication network, especially at the physical layer, against a variety of threats (e.g., eavesdropping, traffic analysis, tampering attack, forgery attack, and Denial of Service (DoS)). Consequently, the employed UAVs should have the adequate processing power to implement all necessary preventative measures against both passive and active attacks.

### 2) MONITORING AND AERIAL SURVEILLANCE IN REMOTE AREAS

It is critical to ensure mobile coverage in difficult-to-reach areas (e.g., remote historical sites, natural parks, or isolated small and rural communities) not only for permanent residents who live in these areas, but also for tourists or scientists who wish to access or visit these areas. In addition, because of their valuable ecosystems that may include historical monuments and artifacts, or critical infrastructure (e.g., dams and bridges), several of these regions should be continuously monitored and protected. Real-time monitoring, particularly in the case of critical infrastructure failures, can aid in the delivery of effective and timely response, which is crucial given the propensity for these malfunctions to worsen rapidly over time. However, monitoring exclusively via terrestrial equipment is both cost-inefficient and limited in scope [52]. In this respect, UAVs could be used to monitor the aforementioned areas in a cost-efficient manner and provide extended radio coverage, as illustrated in Fig. 3(c). Following the same concept, UAVs could be used to provide radio coverage to ships situated close to the shore, as well as surveillance of maritime routes [53]. Additionally, real-time maritime surveillance provides data to support human activity at sea for a variety of operations, including maritime security, law enforcement, and monitoring of sea borders. Consequently, it enhances situational awareness, aids decision-making, and reduces reaction times. Moreover, the UAVs may collect data from wearable biomedical sensors that detect aberrant health conditions, such as body temperature and heart rate, and thus they can be utilized for monitoring epidemics or pandemics, particularly in remote areas, as demonstrated by the recent COVID-19 outbreak [54]. This concept can also be applied to the real-time remote monitoring of patients with chronic diseases (e.g., cardiovascular disease, epilepsy, or diabetes) who are located far from healthcare facilities. In the event of a medical emergency, such as a diabetic coma, cardiac arrest, or epileptic seizure, the patient's data can be transmitted to a clinical center to initiate a prompt reaction. MEC is an essential technology that should be implemented at the BSs for the aforementioned use cases, particularly for real-time IoT services that require low latency, such as surveillance and long-distance medical monitoring. As far as difficult-to-reach areas are concerned, UAVs, which are placed far from the network's cell edge, can act as relays and forward computation-intensive tasks to MEC-enabled BSs. However, it would be essential for these UAVs to have enhanced processing capabilities to perform data caching, handling, and forwarding operations. Moreover, it is also evident in this scenario that the establishment of wireless communication links over large distances could be a point of vulnerability that poses a potential security risk. Therefore, it could be easier for malicious actors to gain access to the deployed UAV communication networks and conduct a variety of active and passive attacks (e.g., data tampering, Global Positioning System (GPS) spoofing, eavesdropping, data injection, DoS and replay attacks, or even jamming attacks). To ensure that data is delivered in a secure, timely, and confidential manner, UAVs should be equipped with adequate computing capacity to support sophisticated and computation-intensive security mechanisms.

By leveraging UAVs as effective remote sensing technology, the monitoring of crops and the management of the spatio-temporal variability within fields can be facilitated. This can be beneficial in scenarios that necessitate the provision of enhanced connectivity and data gathering from remote areas such as the following:

- **Precision agriculture:** Precision agriculture aims to improve the quantity and quality of agricultural products, while also reducing production costs by integrating conventional agricultural methods with emerging technologies. Localized microclimate data (e.g., rainfall level, barometric pressure, temperature, and humidity) can be acquired in real-time by employing IoT monitoring devices. At the same time, UAVs can be utilized in a range of crop management applications, either autonomously by capturing high temporal and spatial resolution images for disease identification, growth monitoring, and yield estimation, or in cooperation with the underlying IoT network by collecting data from deployed monitoring devices in the field. As low-cost IoT devices typically have limited computational capabilities, they can take advantage of both ground MEC servers, as well as UAVs operating as both communication and MEC nodes [55]. In this direction, the various types of gathered data can be stored on an edge-based node and then can be subsequently evaluated. Also, an expert decision system can exploit big data and ML techniques, assess the data, and then recommend necessary agricultural procedures or automatically take action by activating or deactivating the appropriate actuators (e.g., irrigation system). Additionally, farmers can have a complete and real-time view of their field's data and the ability to perform actions remotely, but most importantly, they can have a valuable tool at their disposal that makes recommendations based on localized data and enables the forecast and application of appropriate inputs at an optimized time and scale. To illustrate this point, the process of applying fertilizer to the field is considered. Instead of distributing fertilizer evenly throughout the entire field, farmers can apply it on demand, resulting in lower costs, higher efficiency, and reduced environmental pollution. Consequently, more efficient use of input data can sustainably intensify food production, increase yields, and decrease environmental impact. Moreover, we should also consider emergency situations in which real-time monitoring at a local scale could provide valuable information and facilitate a rapid and well-informed response to effectively manage a hazard, such as nascent infestations of agricultural pests like fruit flies and infection by plant diseases such as botrytis. However, agriculture is unavoidably susceptible to various security threats, like any other technology-based industry [56], [57], [58]. Firstly, the IoT devices in the field are physically accessible, which poses a significant risk, since any malicious entity may access them to cause damage or glitch. As wireless networks are a prime target for passive attacks (e.g., eavesdropping, traffic analysis) and active attacks (e.g., message modification, masquerading), the wireless data exchange can also be a security concern, especially for resource-constrained IoT devices, as shown in Fig. 3(d). In this regard, the use of UAVs as intermediate nodes can lead to short-range transmissions and limit the exposure of the IoT devices to potential attackers. However, the UAVs should have the required computational capabilities to be part of a secure communication system. Overall, protecting data privacy and ownership is a key security issue for the agriculture industry, since data breaches may cause serious financial and personal implications. Also, intentional data falsification might have a substantial impact on the overall precision agricultural system, particularly in terms of the decisions and recommendations provided by ML and inference algorithms embedded in automation systems, leading to inferior products or even production loss. Additionally, erroneous data may result in harmful situations for both the environment and the farmer's and consumer's health owing to the misuse of farming inputs, such as fertilizers or pesticides.

## IV. OVERVIEW OF SECURITY METHODS

### A. THE ROLE OF PLS

Despite the promising capabilities of the UAV-aided MEC-enabled IoT, critical issues exist regarding security and privacy that should be effectively handled in real-time. More importantly, this type of network is inherently vulnerable owing to the wide distribution of heterogeneous nodes in challenging and harsh environments, whereas the network topology dynamically changes and the communication channels are usually insecure and unencrypted. By taking advantage of the significantly constrained resources of the UAVs, several malicious entities may perform various invasive, non-invasive, and semi-invasive attacks [35], [36], [37], [38], [39], [40], [41], including active and passive eavesdropping, hijacking, spoofing, impersonation/Sybil attacks, man-in-the-middle attacks, replay attacks, DoS, and data tampering. During the last few years, significant research effort has been spent on the investigation of information-theoretic PLS in the UAV-aided MEC-enabled IoT. Information-theoretic security refers to the calculation of limits that verify the existence of security measures against adversaries with unlimited computing resources and time, while PLS refers to the exploitation of physical randomness and properties of the channel to obtain secure communications and achieve the security goals [20]. When investigating PLS, the main quantity of interest is the secrecy rate – or the maximum achievable rate, which is called secrecy capacity. For the studies and use cases included in this paper and since the communication objective concerns the MEC principle, various "flavors" of secrecy rate can be found, i.e., secure calculation rate, secure computation rate, secure offloading rate, etc. The terms are used to express the secrecy rate during the data offloading process, while sometimes the local computations may also be included in the calculation as secure computation bits. Other relevant

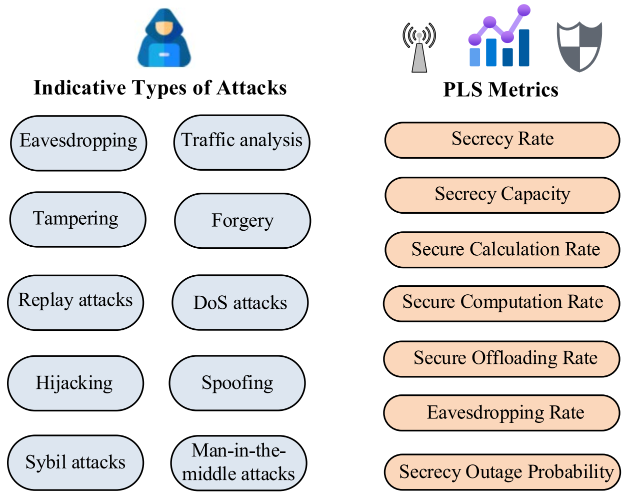


**FIGURE 4.** Various types of attacks and PLS metrics.

security metrics are the leakage or eavesdropping rate, i.e., the average amount of information that can be extracted by a malicious entity and the secrecy outage probability, i.e., the probability that the achievable secrecy rate is less than a given secrecy code rate. Fig. 4 shows the main security attacks and security metrics for the UAV-aided MEC-enabled IoT.

Apart from including the aforementioned security metrics, the notion of secure communications has been investigated in conjunction with other metrics that are relevant to either the UAV or the MEC operation. Specifically, multi-variate optimization problems have been formulated, where some quantities have been used to define the cost function, other quantities have been set as variables and others have been defined as constraints. The (non-exclusive) set of quantities/variables includes:

- The transmission power for offloading, relaying
- The transmission power for jamming
- The UAV position or trajectory definition
- The offloading ratio
- The task, power, and resource allocation
- The energy/power consumption or efficiency
- The beamformer configuration
- The latency
- The task processing or completion time
- The local and offloading computation capabilities
- The computation overhead

Besides the variety of quantities and metrics that compete with each other, a large number of configurations and use cases can be defined to implement the UAV-aided MEC-enabled IoT paradigm. The configurations may include one or multiple UAVs, dual configurations with UAV supporting jammers, one or multiple UAVs acting as relays, multiple ground or flying users requiring offloading, one or multiple MECs at the legacy network edge, one or multiple ground or flying malicious nodes, etc. Clearly, a huge number of problem formulations is possible.

PLS relies on the intrinsic randomness of the wireless channel to achieve secrecy, for example by concealing or shielding transmissions, avoiding malicious nodes, and generating and distributing secret keys. The techniques employed incur significantly lower latency, making PLS an ideal match for real-time applications. Additionally, PLS implementation has significantly lower complexity, which is extremely useful for the IoT ecosystem and UAV-aided networks. On the other hand, the provision of URLLC is defined as a key service area for 5G and 5BG communications, and PLS seems to be a perfect fit. Together with the use of UAVs for adhoc and reliable connectivity in hostile environments, as well as the utilization of MEC for computational offloading and fast content delivery, PLS has the potential to serve as a security enabler for URLLC and real-time applications, such as vehicle-to-everything (V2X) communications, tactile internet, and industrial IoT.

### B. THE EMERGENCE OF ML AND BLOCKCHAIN

Although a wide range of conventional security approaches for the UAV-aided MEC-enabled networks has been proposed, there have also been recently various works relating security and privacy with emerging technologies, such as ML and Blockchain. By avoiding human intervention, ML has been recognized as an effective method to contain security flaws and confront possible security barriers in complex, dynamic, and heterogeneous environments, as well as large-scale network deployments with a massive number of devices (e.g., IoT scenarios) by learning the behavior of network entities and predicting cyber-threats [16], [21]. In this sense, the ML-based methods have the potential to intelligently and in real-time manage and analyze the data flow in an IoT ecosystem. Generally, ML relies on a pattern recognition framework, where the nonlinearities from massive datasets can be characterized and the correlation among a set of data and/or previous action sequences can be exploited. By systematically mining and analyzing collected information data from different sources and setting these data as input of ML-based methods, the networks can be optimally managed and autonomously coordinated, whereas the latency and security requirements can be simultaneously satisfied. In general, ML can be categorized depending on the learning method as [45]:

- Supervised Learning
- Semi-Supervised Learning
- Unsupervised Learning
- Reinforcement Learning (RL)

Besides, evolutionary and forceful types of ML are the DL and the Deep RL (DRL). In DL, multiple layers are employed to build multi-layered ANNs capable of making intelligent decisions and adapting to undefined and unprecedented conditions without guidance from external supervisors. Although ML can revolutionize the decision-making process within the IoT domain and increase the possibility of achieving highly autonomous UAV operations, a centralized collection of raw datasets for training is usually required, which in turn triggers security and privacy issues. As the resource-constrained UAVs cannot usually perform heavy computations and process the collected data, the Federated Learning (FL) paradigm has been introduced as an efficient means to enable collaborative learning in a decentralized fashion with local training [59]. On the other hand, the MEC can reduce the training time required by ML algorithms and address computation-intensive issues, as the computing requirements for timely handling large datasets are significantly high. More specifically, dedicated edge infrastructure can expedite the process of large amounts of data, as UAVs have stringent processing capabilities. However, this strategy should be carefully considered, since it may lead to additional latency and increased signaling overhead due to the data exchange between the UAVs and the MEC servers in harsh propagation environments.

Beyond centralized deployments of record-keeping, Blockchain has also been recently proposed as an unchangeable, tamper-resistant, and tamper-evident digital ledger capable of ensuring secure and trustworthy transactions in a decentralized and transparent manner [22]. More importantly, in Blockchain, only trusted data blocks with specific sizes are recorded and verified and these valid sets of records are immutable and form the Blockchain itself. To attain the integrity of data in each block, unique hash values are used. In this respect, the robust one-way cryptographic Secure Hash Algorithm-256 (SHA-256) and SHA-512 are typically employed to rapidly map message data of arbitrary sizes to bit arrays of fixed, compressed sizes. Besides, the block validity is confirmed using consensus algorithms, which require consensus among the participants. Also, the proper addition of blocks is controlled by the smart contract (i.e., a self-executing set of codes that runs on Blockchain). Based on the ownership and the audience that is certified to verify and add a block, the Blockchain systems can be classified into three major types as follows [60]:

- The less-efficient but highly immutable **Public Blockchain**, where the public has access to all the records and participates in the consensus process.
- The highly efficient but easily tampered **Private Blockchain**, where only specific nodes have access to the network and participate in the consensus process.
- The partially decentralized **Consortium Blockchain**, where a small number of selected organizations can participate in the consensus process.

However, the adoption of Blockchain technology in UAV-aided MEC-enabled IoT is challenging, since there are certain onboard energy, computation and data storage resource constraints. This issue becomes more significant, as the number of network nodes increases and massive datasets are generated. To maintain an adequate Blockchain operation, partial or full task offloading to MEC servers is suggested [60]. On the other hand, integrating Blockchain in UAV-based systems constitutes a complex task and requires extended experimentation, testing, and verification, before practical implementation.

Recently, the Blockchain and ML synergy was also envisioned [61], [62], [63], where the Blockchain facilitates the verification of the training processes of ML, while reducing the risk of failures. Also, the Blockchain network can be used to store the training data sets that are used by the learning models to eliminate or minimize the data faults and errors. By enhancing the capabilities of Blockchain and its decentralized nature with the intelligence introduced by ML-based methods, prescriptive and real-time predictive analytics can be performed to large data volumes generated from sensors or collected from IoT devices, leading to timely and precise data classification and identification. In other words, combining these two technologies (i.e., ML and Blockchain) can lead to highly accurate outcomes.

In Fig. 5, a MEC-compliant network architecture with trustful and secure computation offloading and seamless coverage, where FL and Blockchain work cooperatively, is demonstrated [61], [62], [63]. To maintain trustful, secure, and transparent transactions of legitimate nodes, a Consortium Blockchain is considered that exploits the features of smart contracts, data consensus, and shared ledgers. The underlying network consists of multiple resource-limited IoT devices dispersed over a wide area that collect sensed data from their local physical environment. Such data originating from the IoT devices may need to be rapidly processed in real-time or fully explored. The MEC servers ensure the availability of powerful resources to timely handle the delay-tolerant and computation-intensive tasks of the IoT devices. However, it is considered that the direct communication of these devices with the MEC servers is not always feasible owing to blockage and/or fading effects in the propagation environment. In this regard, the IoT devices can forward their computation tasks to UAVs in their vicinity, which are equipped with onboard computing processors. As the UAVs have limited energy resources, they should determine the portion of the offloaded tasks that can locally process and then act as aerial relays to forward the remaining part of these tasks to the ground MEC servers for computing. It is considered that Blockchain interconnects the UAVs and the MEC servers together in a decentralized manner with low-latency response and a low possibility of errors. Besides, the MEC servers support data services, such as data mining and big data analytics, whereas the UAVs not only support partial task execution, but can also participate in the local training of the FL functions or data mining. Towards this end, the MEC servers choose a set of UAVs as learning clients to perform collaborative training using their data. The UAVs upload the computed update to the MEC servers for aggregation and global computation in an iterative way without revealing sensitive information. Besides, the MEC servers broadcast the global model to all UAVs for the next round of training, until accurate results are obtained.

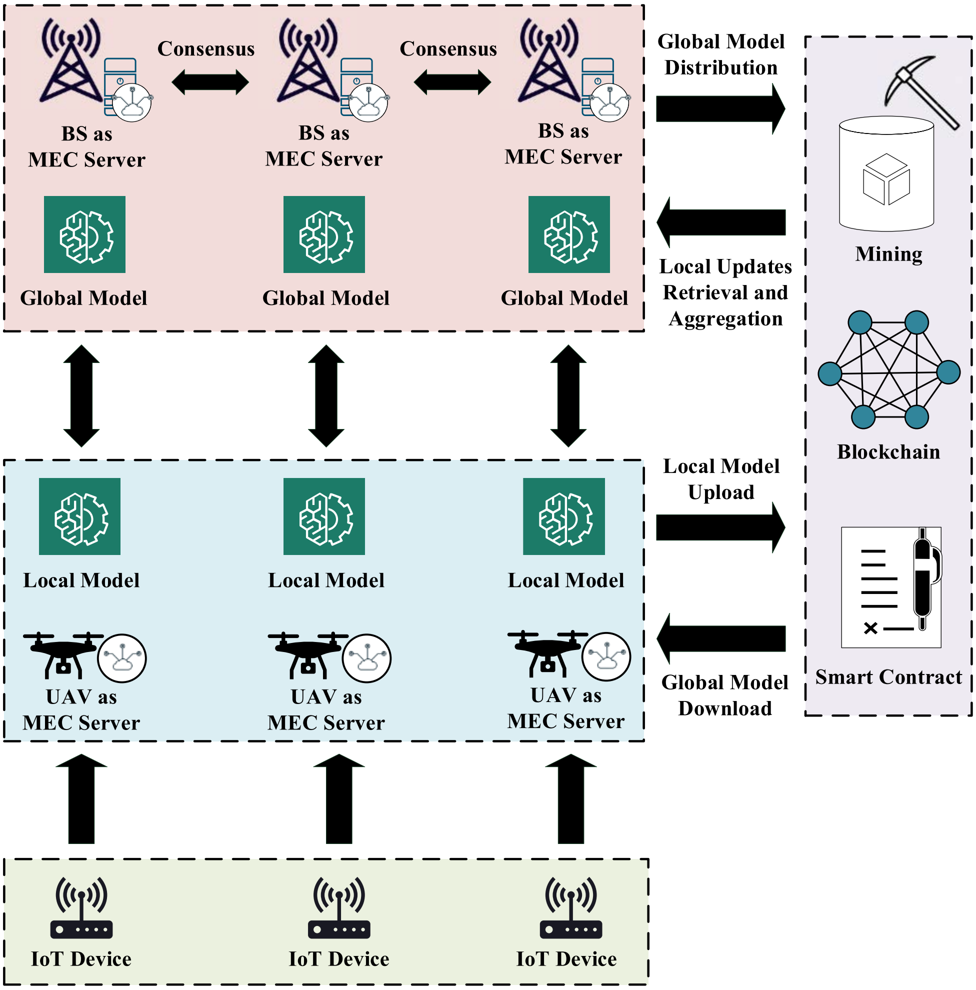


**FIGURE 5.** Simple representation of a prospective network architecture for the UAV-aided IoT with the synergetic integration of MEC, FL, and Blockchain.

### C. THE ROLE OF AUTHENTICATION

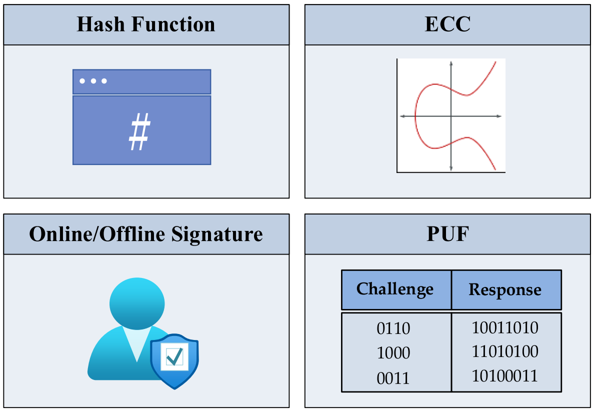
Apart from PLS, succesfully authenticating the network nodes is also critical [18]. In such volatile and decentralized network deployments, as those studied in this paper, the aerial and ground nodes can dynamically join or leave the network. As only authorized nodes should gain access to the network, the authentication plays a crucial role in confirming the identity of these nodes and preventing malicious entities from joining the network and using network resources. During the authentication process multiple phases are invoked, where cryptographic keys are exchanged between the network entities, as follows:

- **Setup Phase:** Initialization of the security parameters
- **Registration Phase:** Registration of the partially trusted nodes
- **Authentication Key Aggrement Phase:** Mutual authentication and key agreement among the nodes
- **Update Phase:**Authorization or revocation of nodes

Although node authentication stands for the main requirement for secure network operation, no unified security standards for UAV-aided networks exist. Also, applying sophisticated security methods is infeasible owing to the computation and energy constraints of IoT devices and UAVs. Thus, lightweight and efficient authentication mechanisms should be designed and MEC can provide additional computation resources. Beyond software-based schemes that depend on mathematical and algorithmic methods, the robustness and effectiveness of the authentication procedure can be further expanded by using dedicated Integrated Circuits (ICs) and computing devices, such as PUF chips [18]. In Fig. 6, potential lightweight authentication mechanisms are presented.

## V. REVIEW OF PLS SOLUTIONS

In this section, several research works are reviewed that focus on information-theoretic security and take into account metrics, such as secrecy capacity and secrecy rate for communication and offloading in the UAV-aided MEC-enabled IoT environment. Additionally, the use of PLS is investigated through interference avoidance or artificial noise injection



| Challenge | Response |
|---|---|
| 0110 | 10011010 |
| 1000 | 11010100 |
| 0011 | 10100011 |

**FIGURE 6.** Software- and hardware-based authentication mechanisms.

techniques. In these works, the UAVs may facilitate MEC operation by either hosting the MEC capabilities or playing the role of a relay. Also, the UAVs themselves may be the resource-limited nodes that require the offloading capabilities of a MEC. The state-of-the-art analysis revealed that there are several studies investigating UAVs acting as MEC servers in conjunction with other interesting and challenging research topics, including NOMA, RIS, and ITS. More specifically, a multitude of complicated problems can be formulated – usually leading to non-convexity, which consequently means that special techniques should be applied to reach a solution. Fig. 7 presents different network configurations for the UAV-aided MEC-enabled IoT, when PLS is concerned. Also, Table 2 briefly summarizes the reviewed works.

### A. UAVS AS MEC SERVERS

In [64], a UAV acted as a MEC server and its main task was to support through computational offloading several GUs, while sending jamming signals against potential eavesdroppers to fulfill both qualitative and security requirements. The eavesdropper was assumed to be located on the ground, while the system was time-slotted and the UAV had full-duplex capabilities. The objective function of the optimization problem aimed to maximize the secure computation efficiency, which was defined as the ratio of the achievable secrecy rate over a number of slots to the energy for communication and computing assuming full offloading. To tackle the optimization problem, two sub-problems were defined and iteratively solved by adjusting the transmission power, the computation capability, and the UAV's trajectory, until the algorithm converged. The algorithms, which were evaluated through simulations in MATLAB, showed superiority to other schemes (i.e., non-jamming and ground relay) approaching the system performance in the absence of a malicious party.

The collaboration of a UAV with MEC functionalities with Ground Stations (GSs) in the presence of multiple (down-to-earth) eavesdroppers was studied in [65]. Partial offloading was supported in a Time-Division Multiple Access (TDMA) sharing scheme, and the exact location of the eavesdroppers was considered known. The formulated optimization problem had the objective to minimize the UAV energy consumption using as optimization variables the transmit power of GS, the UAV's trajectory, and the task allocation. Also, the secrecy rate of the offloading channel was used as a constraint together with the transmit power and the trajectory boundaries. To tackle the non-convexity, the Successive Convex Approximation (SCA) and Block Coordinate Descent (BCD) were utilized by dividing the problem into three convex sub-problems: task allocation for given transmit power and trajectory; transmit power given task allocation and trajectory; and trajectory given power and allocation. The CVX modeling system for convex optimization was used [66] to tackle the optimization problems in the numerical results. Then, the scheme was compared to methods with less dimensionality, but the security rate improvement was relatively small.

In [67], the role of the MEC was shared between a UAV and a BS, i.e., the UAV was able to carry some of the offloading efforts. The use case included several GSs and malicious, eavesdropping UAVs. In this regard, a Decode-and-Forward (DF) policy was used to transfer part of the offloading tasks to the BS. Additionally, the legitimate UAV had full-duplex capabilities and it was also capable of sending jamming signals to eavesdroppers. The formulated optimization problem used the maximum secrecy capacity as the objective function, whereas a two-stage partial computation offloading model was investigated based on DF. The joint optimization problem was complicated and non-convex; thus, it was separated into four sub-problems and solved with SCA and branch-and-bound methods. Each sub-problem was associated with: UAV path/position, UAV transmit power, offloading ratio, and computing scheduling among users. The provided simulation results showed that the scheme could effectively obtain high secrecy capacity.

A similar, but more generalized use case, was investigated in [68], where a UAV was used to serve multiple GSs as a MEC server, under the threat of multiple eavesdropping UAVs. In a more realistic approach, the knowledge of the location of the eavesdroppers was considered imperfect and jamming signals were transmitted to increase secrecy from the legitimate full-duplex UAV, as well as the non-offloading GSs. In this direction, a max-min optimization problem was formulated targeting the minimum secrecy capacity with imposed constraints, like latency, total power consumption, and minimum offloading. As variables of the problem, the authors consider the legitimate UAV path/position, the GS transmit power, the jamming power, the communication capacity, the possible use of local computation resources of GS (user association), and the offloading ratio, i.e., the ratio of the offloaded processing to the overall data processing. The results indicated that the joint optimization can provide significant benefits when considering various locations, packet sizes and self-interference (SI) efficiencies of the legitimate UAV. Additionally, these results confirmed the existence of a fundamental tradeoff between secrecy and latency.

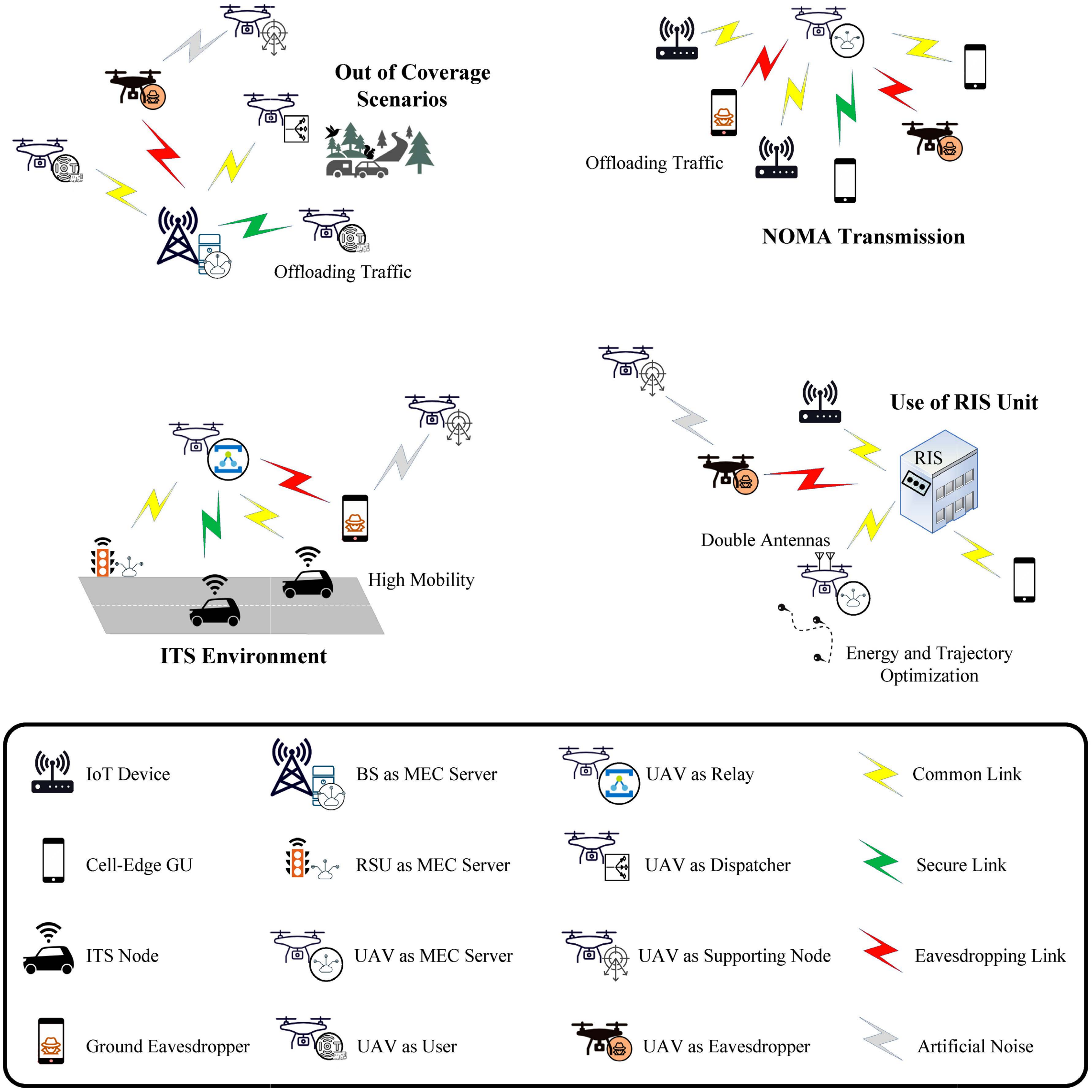


**FIGURE 7.** Potential PLS issues in various network configurations of the UAV-aided MEC-enabled IoT.

In [69], a use case was studied, where power-limited IoT devices were served from UAVs with MEC capabilities that also acted as data collectors due to assumed limited coverage from the ground devices. The underlying system was threatened by multiple eavesdroppers located also on the ground. In this scenario, the IoT devices could be used for regional situation awareness, which means that identity and location information was critical. This work proposed a method, where the IoT devices did not share identity or location information that could then be estimated by using beamforming, time-of-arrival, and deployment information at the UAVs (multiple antennas at the UAV were required). The UAVs forwarded data (e.g., to the BS) using the identity and location information of multiple IoT devices as an encryption key. Moreover, the trajectory of the UAVs was designed by minimizing the power consumption among the UAV clusters, while the secrecy capacity at each cluster was also maximized. To increase security, encryption through beam hopping randomization per cluster was performed implementing a space-time key structure. In addition, the use of satellites was suggested for the transmission of the keys (identity, location, beam hopping sequence) as a feedback channel.

A UAV acted as a MEC server in [70], while a second UAV had the role of an eavesdropper attempting to intercept offloading information. However, a GS was used as a jammer, providing support and an advantage to the legitimate UAV to achieve secure communication. It was assumed that the MEC-enabled UAV was able to cancel the jammer interference and increase the secrecy capacity under the secure offloading rate measure and then increase the secure

**TABLE 2.** Summary of recent research works on PLS solutions.

| Reference | Year | Configuration of the Network | Wireless Communications Techniques | Type of the Network | Advantages |
|---|---|---|---|---|---|
| Amos et al. [64] | 2021 | UAV as MEC server to support the GUs and also as jammer towards potential ground eavesdroppers | Time-slotted communications, full-duplex transmission, single antennas | UAV-aided MEC-enabled network | Low energy consumption, maximized secure computation efficiency |
| Li et al. [65] | 2021 | UAV as MEC server for partial computation offloading and multiple ground eavesdroppers with known exact location | TDMA, single antennas | UAV-aided MEC-enabled network | Low energy consumption, optimized secrecy rate |
| Han et al. [67] | 2020 | UAV and BS as MEC servers to support the GSs, UAV as eavesdropper, and UAV as jammer towards potential eavesdroppers | DF relaying, full-duplex transmission, double antennas (legitimate UAV), single antennas (GUs and eavesdropper UAV) | UAV-aided MEC-enabled network | Maximized secrecy capacity |
| Zhou et al. [68] | 2020 | UAV as MEC server to support the GSs with partial computation offloading, multiple eavesdroppers UAVs, and unknown exact location of jammers | Full-duplex transmission, double antennas (legitimate UAV), single antennas (eavesdropper UAV and GUs) | UAV-aided MEC-enabled network | Maximized secrecy capacity |
| Han et al. [69] | 2021 | UAVs as MEC servers and data collectors, multiple ground eavesdroppers. The UAVs use location information from clustered ground IoT nodes as encryption key | Identity-free transmission, encryption via beam hopping randomization, double antennas (UAV), single antennas (IoT nodes) | UAV-aided MEC-enabled IoT | Low energy consumption, maximized secrecy capacity, and low latency for real-time applications |
| Lu et al. [70] | 2022 | UAV as MEC server to support the GSs, UAV as eavesdropper, and GS as jammer | TDMA, single antennas | UAV-aided MEC-enabled network | Low energy consumption and maximized secrecy capacity |
| Liu et al. [71] | 2021 | UAVs as MEC servers to support the GSs with partial computation offloading, multiple GSs, and UAV as flying eavesdropper | Single antennas (legitimate UAV, GSs), multiple antennas (eavesdropper UAV) | UAV-aided MEC-enabled network | Low energy consumption, minimized eavesdropping rate |
| Bai et al. [72] | 2022 | UAVs and BSs as MEC servers, UAVs as relays and multiple legitimate and malicious IoT nodes | Single antennas | UAV-aided MEC-enabled IoT | Maximized task completion rate, minimized average task completion time, low energy consumption, and support of real-time applications |
| Xu et al. [73] | 2021 | UAV as MEC server to support the GSs, UAV as supporting node for artificial noise transmission, ground eavesdroppers | TDMA, NOMA, SIC, single antennas | Dual-UAV-aided MEC-enabled network | Maximized secure computing capacity |
| Yang et al. [74] | 2022 | UAVs as MEC servers and data collectors, GSs as IoT nodes, and UAV as jammer towards eavesdroppers at the ground | RIS unit, half-duplex transmission, single antennas | Dual-UAV-aided MEC-enabled network | Low energy consumption, secure transmission |
| Bai et al. [75] | 2019 | UAV as user, BSs and APs as MEC servers for zero, full and partial computation offloading, BS as jammer towards malicious entities, ground active and passive eavesdroppers | Full-duplex transmission with no self-interference issues, single antennas | Aerial offloading MEC-enabled network | Low energy consumption (for local computation and offloading), secure transmission |
| Gu et al. [76] | 2021 | UAV as user, BSs and APs as MEC servers for partial and full computation offloading, and BS as jammer towards malicious entities | Single antennas (UAV and eavesdroppers), multiple antennas (BS) | Aerial offloading MEC-enabled network | Low energy consumption, enhanced secrecy capacity |

**TABLE 2.** ***(Continued.)*** **Summary of recent research works on PLS solutions.**

| | | | | | |
|---|---|---|---|---|---|
| Gu et al. [77] | 2022 | UAV as user, BSs and APs as MEC servers, ground eavesdropper | Full-duplex transmission, single antennas, energy harvesting capabilities | Aerial offloading MEC-enabled network | Energy efficiency, enhanced secrecy capacity |
| Lu et al. [78] | 2022 | UAV as MEC server to support the GSs with partial computation offloading, UAV as eavesdropper, ground node as jammer transmitting artificial noise to the eavesdropper | NOMA, SIC, single antennas | UAV-aided MEC-enabled network | Optimized secure computing capacity |
| Wang et al. [79] | 2021 | UAV as relay for cellular coverage extension, UAV as MEC server to support cell-edge users, UAV as eavesdropper targeting cellular traffic | NOMA, SIC, full-duplex transmission, single antennas | UAV-aided MEC-enabled network | Enhanced secrecy driven transmission |
| Yan et al. [83] | 2022 | UAV as MEC server to support the GSs, UAV as transmitter of interfering signals towards eavesdroppers | RIS unit, full-duplex transmission, multiple antennas | UAV-aided MEC-enabled network | Energy efficiency, maximized secrecy rate |
| Wang et al. [84] | 2022 | UAVs as users, BS as MEC server to support the UAVs, ground eavesdroppers | IOS, single antennas | Aerial offloading MEC-enabled network | Maximized SEE and support of real-time applications |
| Garg et al. [85] | 2018 | UAV as dispatcher and BSs (or RSUs) as MEC servers to support connected vehicles | Single antennas | ITS | Low computational time and storage for authentication and data encryption/decryption, and support of V2X real-time applications |
| Sedjelmaci et al. [86] | 2019 | UAV as data collector and BSs (or RSUs) as MEC servers to support connected vehicles | 802.11b and 802.11p protocols, single antennas | UAV-based edge computing network | Low energy consumption, low computation overhead, secure transmission, and support of V2X real-time applications |
| He et al. [91] | 2021 | UAV as MEC server to support connected vehicles, Poisson-generated vehicles, ground eavesdropper | VANET, IEEE 802.11p protocol (CSMA/CD), single antennas | VANET | Optimized task offloading, secure transmission, and support of V2X real-time applications |

calculation capacity. Assuming a TDMA scheme, an optimization problem was formulated to maximize the minimum secure calculation capacity. This was practically obtained through the optimization of the resources and trajectory of the legitimate UAV, while taking into account certain constraints of the MEC/IoT environment (e.g., local computation, power consumption, etc.). Due to problem non-convexity, optimization was performed using the SCA and BCD techniques.

In [71], a network consisting of multiple UAV-based MEC servers (called helpers), multiple GSs and a flying eavesdropper was proposed. Based on this network, an offloading mechanism was presented that relies on the minimization of energy consumption and the eavesdropping rate, which constitutes a metric for PLS. The constraints involved the task's overall processing time and the local and offloading computation capabilities. As the optimization problem was proved to be non-convex (distributed, mixed-integer non-linear programming) a two-stage solution scheme was applied. The first stage involved a reformulated convex sub-problem of the task assignment process. Besides, the second stage included a learning-based distributed algorithm for joint assignment of computing and channel resources mainly based on the Fading Memory Joint Strategy Fictitious Play (FM-JSFP) with inertia. Extended simulations were carried out using MATLAB. As verified through these simulations, the proposed scheme outperformed local computation and random offloading schemes.

The subject of security via trust was examined in [72]. A UAV could act either as a relay interconnecting resource-limited IoT devices with an edge server or as a MEC node itself. It was considered that multiple GSs that can be legitimate or malicious (the number of malicious nodes was assumed smaller) were positioned in a large geographical area and a trust-based active task offloading scheme was proposed that identifies credible and suspicious areas in the network. More importantly, the optimization problem aimed to maximize the task completion rate and also minimize the average task completion time and the energy consumption of the UAV.

To notify the UAV for task offloading requests, an IoT device spread Task Offloading Notices (TONs) to adjacent devices. However, malicious devices discarded the TON messages and degrade the system performance. The area was divided into a grid and the "trust" was defined as the ratio of TONs from a grid point with and without malicious entities. According to the results, the proposed method outperformed other similar techniques and had significant benefits in terms of the completion rate, service time, and flight path.

It is noted that the respective use cases described in [67], [69], and [70] included multiple UAV setups, where the UAVs could be either legitimate or malicious. However, two or more UAVs can coordinate with each other to achieve their objectives and increase secrecy. Towards this end, relevant scenarios were studied in [73] and [74] and are analyzed in Subsection C and Subsection D, respectively. More specifically, a UAV with MEC capabilities was supported by another UAV that transmitted artificial noise to eavesdroppers in [73], while a similar setup was considered in [74] with the UAVs equipped with advanced antennas.

### B. UAVS AS USERS

Beyond network architectures with UAVs acting as MEC servers, previous works investigated the role of the UAVs as users with significantly limited resources that may need a MEC server to perform computation offloading.

In [75], the limited computation capacity of a UAV was mitigated through computational offloading to a MEC server located at a terrestrial BS or AP. Also, an eavesdropper was considered at the ground level. To cope with this eavesdropper, the ground BS was jammed with artificial noise (assuming full-duplex wireless communication with no self-interference issues). Then, energy efficiency in resource allocation was studied with the formulation of two optimization problems, assuming: (a) active eavesdropper (i.e., known location and channel state information from the eavesdropper) and (b) passive eavesdropper (i.e., only location information is known). In both problems, the attempt was to minimize the total power consumption (for local computation and offloading transmission), while latency, power, and offloading data volume constraints were set. Additionally, to ensure secrecy, in (a) the secrecy capacity was required to be higher than the offloading rate, while in (b) since the eavesdropper channel was unknown, the secrecy outage probability was considered as a constraint and provided as a function of offloading and jamming power. Also, fixed (for (a) and (b)), and random (for (b)) location of the eavesdropper was assumed. After some transformation, the problems were proven convex and were successfully solved. An analysis of zero, full and partial offloading, as well as overloaded computation, was performed and the results were numerically verified for various offloading strategies in terms of energy and security.

A similar setup with a ground eavesdropper was also investigated in [76], where the UAV offloaded tasks at a MEC located at the BS (or AP). Partial offloading was considered, i.e., a portion of the computation task was locally executed, while the complementary was offloaded to the MEC. Both the UAV and the eavesdropper were assumed to have single antennas, while the BS was equipped with multiple antennas and was capable of performing jamming towards the malicious party without self-interference. The formulated optimization problem had the objective of energy consumption minimization by properly performing computation and communication resource allocation with constraints in the secrecy (offloading) rate, the transmit power, the latency, and the Central Processing Unit (CPU) capabilities of the UAV. After manipulation, the problem was transformed into a convex equivalent, and simulations were carried out to highlight the benefits of the proposed scheme against other schemes (i.e., full-offloading, fixed UAV, no eavesdropper).

In [77], a UAV with moderate computational capabilities was considered and energy harvesting was taken into account with the assumption of full-duplex operation at both this UAV and a BS. It is noted that the control instructions for the harvesting also played the role of artificial noise that could confuse a potential eavesdropper. Moreover, the computational and communication resource allocation (i.e., offloading data size, offloading time duration, and transmitted power) were optimized with respect to the minimization of the UAV energy consumption, including the harvested energy. Also, secrecy was introduced as a constraint together with computation latency. More specifically, the worst-case secrecy offloading rate was used. The non-convex formulated optimization problem was converted through transformations to a convex one. Additionally, semi-closed expressions for the offloading time, offloading data size, and transmit power were extracted. The numerical results for various benchmarking configurations (i.e., no offloading, full offloading, no eavesdropping) validated the advantages of the proposed approach.

### C. NOMA SCHEMES

In previous works, NOMA schemes were leveraged in the context of the UAV-aided MEC-enabled IoT as key enablers for simultaneously supporting the wireless connectivity of a vast number of IoT nodes. More specifically, in NOMA, multiple nodes can utilize non-orthogonal resources concurrently by yielding a high spectral efficiency, while allowing some degree of multiple access interference.

In [73] a dual UAV-assisted MEC configuration was considered, where one UAV carried the MEC serving GSs and a second one transmitted jamming signals to eavesdroppers on the ground. The analyzed optimization problem maximized the minimum secure computing capacity for both TDMA and NOMA schemes (power multiplexing with Successive Interference Cancellation (SIC)), where the average achievable number of secure computing bits was defined as secure computing capacity, considering the secrecy offloading rate and the local computations. The optimizations took jointly into account the computation and communication resources, as well as the UAV trajectories. After transformations, the problems could be solved using the BCD algorithm, as well as a penalized BCD. Besides, the convex subproblems were efficiently solved using CVX [66]. The simulations showed improvement in the security computing capacity performance of the system, as well as, that the NOMA outperforms the conventional TDMA method, as far as the security improvement is concerned.

The main particularity in [78] is that NOMA was applied in a setup, where one UAV acted as a MEC node serving GSs, while a second UAV was a flying eavesdropper. Simultaneously, a ground jammer transmitted artificial noise to this eavesdropper. The targeted security metric was the secure computing capacity, under the following constraints; system energy, computation capabilities of GSs and MEC, UAV flight movement (and collision prevention between UAVs), and the minimum computation requirements of the GSs. Besides, the formulated problem took into account the transmit power, the CPU computation capabilities, the local computation, and the UAV's trajectory. On the other hand, the location of the eavesdropper was considered uncertain. Based on this scenario, the formulated problem was non-convex and both the SCA and BCD methods were used to iteratively solve this problem. For the numerical calculations, CVX [66] was used to tackle the decomposed subproblems. To cope with the uncertainty of the eavesdropper's position, the worst-case NOMA conditions were considered by using the upper bound of the eavesdropping rate. The algorithm was compared with various other schemes (e.g., straight trajectory, UAV both MEC and jammer, fixed transmit power, etc.) and its superiority was confirmed.

In [79], several cell users (located at the cell edge) were considered and had the responsibility to communicate with the BS and process a specific workload. In this environment, a UAV was used as a relay for cellular connectivity and as an edge-server for task offloading. Moreover, the proposed network included a flying eavesdropper that intercepted the cellular traffic, while the idea of using the offloading traffic from the edge users to the UAV-based MEC server as a cooperative jammer for the eavesdropper emerged. Towards this end, a joint optimization problem was formulated to minimize the overall energy consumption for the UAV and the cell-edge users, considering the UAV position, the transmission duration, and the computation offloading. All cell-edge users were assumed to form a NOMA cluster to send their data to the UAV. In addition, the process was performed in two distinct phases. In Phase 1, the users sent through NOMA their cellular data to the relay. Then, in Phase 2, the UAV relayed the packets to the BS, but also the cell-edge users transmitted through NOMA their offloading tasks, which were cooperatively used as jamming signals to protect the UAV–BS link from the eavesdropper. The optimization problem was non-convex and thus the study proposed an algorithm that converged to the optimal solution. First, a polyblock approximation-based algorithm was used to optimize the transmission and the offloading process at a specific UAV position, and then the position was optimized using a precoding-based cross-entropy algorithm. The numerical results demonstrated the efficiency of the proposed algorithm in conjunction with the achieved secrecy in the UAV–BS path. Besides, the accuracy and efficiency of the algorithms were evaluated using LINGO as a benchmark [80].

### D. USE OF RIS UNITS

As the Radio Frequency (RF) Micro Electromechanical Systems (MEMS) rapidly evolve, the use of programmable and reconfigurable meta-surfaces has been recently suggested [81]. In this direction, the RIS technology can offer energy efficiency, low complexity, and cost-effectiveness.

In [74], the dual UAV setup presented in [73] was considered with an eavesdropper positioned on the ground. Specifically, one UAV collected data from the GSs, while the second UAV acted as an interferer/jammer to enable secure communication. In the underlying network, a RIS unit was used as a passive beamformer with a large number of small reflecting elements that were jointly adjusted to reconfigure the wireless propagation environment in favor of signal transmission [82]. The main objective of this paper was to minimize the total energy consumption. However, in the analysis, the minimum secrecy rate requirement was also considered and the formulated optimization problem jointly adjusted the GU power, the jamming UAV transmission power, and the phase shifters of the RIS reflecting elements. In addition, the BCD method was leveraged to deal with the non-convexity of the formulated problem. The occurred convex subproblems were treated using CVX [66].

A quite similar problem was treated in [83], where only one UAV was used to collect offloading data from the GS and transmit interfering signals towards the eavesdropper. Once again, the communication was supported by a RIS unit. The formed optimization problem had the goal of maximizing energy efficiency and trajectory design with respect to the secrecy rate, taking into account the RIS elements. Also, the non-convexity of the formulated problem is resolved through transformations and approximations. For the calculation of the numerical results, CVX solvers [66] were used.

The use of Intelligent Omni Surfaces (IOSs) in the UAV-aided MEC-enabled IoT environment was also envisioned in [84]. These surfaces can both reflect and transmit to serving stations on both sides of the surface, constituting a full-space smart radio environment. The considered use case examined the UAVs as the stations requiring MEC support through aerial offloading, while a MEC was hosted at the serving BS. In the proposed network setup, multiple UAVs and ground eavesdroppers were considered. This paper tried to optimize the Secrecy Energy Efficiency (SEE) with constraints in terms of the delay, energy, and security requirements. Also, iterative algorithms were used for computing and communication scheduling. The SEE generally balanced information security and energy efficiency, and it was defined as the ratio of the secrecy rate to the total power consumption. In addition, the CVX [66] framework was adopted for tackling the specified optimization subproblems.

### E. ITS SCENARIOS

The construction of future smart cities necessitates the development of efficient ITS with integrated connected and autonomous vehicles. By adding an extra degree of freedom compared with the ground RSUs owing to their 3-D positioning, the UAVs have the potential to better support the transportation infrastructure in terms of connectivity.

The role of UAVs and edge computing in ITS was addressed in [85], where a smart city with multiple UAVs and multiple vehicles was considered. In this environment, several edges were assumed that acted as data processing and decision-making centers for the UAVs' data. Each UAV was assigned a domain and it hovered over the vehicles of the domain collecting data. The UAVs did not process, but they deliver the data to an entity called dispatcher, which acted as a workload distribution center and dispatched the data to the edge with minimum load. After analysis, the decisions (e.g., regarding the UAV trajectory) were sent to the UAVs through the aggregator, which ensured that the edge's decision was not hacked or leaked to any third party. The proposed scheme relied on Bloom filters (BF), which were used in three steps. In the first step, the UAV validated the authenticity of vehicles hashed to the BF. Then, in the second step, the load was balanced among all edges by the dispatcher, after authenticating the UAVs (2nd BF). In the third step, data processing was performed and the edges informed the dispatcher of the processing status. In case of abnormality in a vehicle behavior, the edge securely conveyed its decision to the respective UAV. Consequently, the aggregator accepted the data from the edge after validating the keys (3rd BF), and eventually the decision reached the vehicle. The process was refined through optimization that maximized the processing capabilities, minimized the delay, and maximized the security. Also, the simulations of the proposed framework were conducted via MATLAB, while the hash functions were calculated using the CityHash 64-bit library.

The security was dealt with through a different prism in [86], where a reputation-based scheme was used. First, the UAVs were considered as mobile devices and part of a vehicular ecosystem to collect measurements from the environment. Moreover, a MEC server was located at the BSs or APs of the network, where RSUs could play the role of the AP. The UAVs transmitted the collected information to the server, whenever an infrastructure network was available. Each UAV had the responsibility to monitor the network and detect misbehaviors that were then disseminated to the neighboring users, whereas all UAVs retained reputation metrics from their monitored neighbors. More importantly, the UAV-based edge offloading in conjunction with DoS attacks detection was examined, while taking into account the energy consumption and the computation overhead of the UAVs. In this respect, each UAV had security agents that detected suspicious activities, whereas the misbehavior detection was either performed locally or through offloading. The system-scale problem was analyzed with a zero-sum game based on a Stackelberg [87] methodology with two types of non-cooperative players (i.e., the agents and the attackers). To simulate the IEEE 802.11p transmission, the NS-2 network simulator [88] was used, while the mobility of vehicles was generated by the SUMO simulator [89]. As revealed by the results, the proposed game-theoretic method showcased significant benefits in the detection accuracy and energy efficiency.

Although the VANETs stand for a basic structural element for ITS deployments, the UAVs can assist VANETs to fulfil the requirements for improved connectivity, reliability, and stability [90]. In this respect, a VANET was supported by multiple UAVs operating as MEC servers in [91]. It was considered that multiple Poisson-generated vehicles were moving along a road and offloaded computation tasks to the UAVs, while keeping a subset of them for local computation. Among the vehicles, an eavesdropper existed. A particularity of the study was that the IEEE 802.11p protocol was used for car-to-car communications. Since this protocol is a Carrier Sense Multiple Access protocol with Collision Avoidance (CSMA/CA), the process contained collisions, back-off, and retransmissions. It is noted, however, that even though this protocol was used to specify the task computation model, the security was measured through the secrecy capacity. By assuming that each vehicle can select and use one MEC node, an optimization problem was formulated to minimize the overall serving time using latency, secrecy/security, and compute resource constraints at the MEC servers. To obtain a solution for this problem, the problem was decoupled into two sub-problems: a) optimization of task-offloading and b) optimization of resource allocation. Then, the problem was iteratively solved using the relax-and-rounding method together with the Lagrangian method. A system simulator was implemented in MATLAB and the simulation results demonstrated significant gains in comparison with local computing or computation at MEC servers located on the ground (e.g., MEC servers at RSUs).

### F. SUMMARY

As far as PLS is concerned, there is a vast range of scenarios, configurations, requirements, and metrics to take into account in the UAV-aided MEC-enabled operation. This section has investigated PLS in three axes:

- Calculation of information-theoretic security metrics under a specific topology without any actual security measure.
- Achievement of PLS through eavesdropper and/or interference avoidance.
- Achievement of PLS through artificial noise transmission to remove any advantage from the eavesdropper.

Also, PLS has been investigated in conjunction with communication or offloading requirements (e.g., throughput, offloading rates, reliability). As indicated in this section, the UAVs may have different roles. They may host the MEC, they may relay data flows towards an edge unit located at the BSs, they may have the role of a data dispatcher, they may act as an

**TABLE 3.** Summary of recent research works on ML-inspired and blockchain-based security solutions.

| Reference | Year | Key Technologies | Type of the Network | Advantages |
|---|---|---|---|---|
| Wang et al. [59] | 2021 | FL, Blockchain | Multi-UAV-aided MCS | High-quality model sharing, improved utilities for UAVs, converged strategies, and privacy protection |
| Tang et al. [92] | 2021 | FL, DRL | UAV-aided edge computing-based IoT | Data privacy, low power consumption, and low latency |
| Zhao et al. [93] | 2021 | DQN | MEC-enabled network | Secure data transmission, low price, low latency, low energy consumption, and support of real-time control systems |
| Wei et al. [94] | 2021 | DP-DQL | UAV-aided IoT | Privacy protection and cost efficiency |
| Lu et al. [96] | 2022 | RL | Multi-UAV-aided MEC-enabled network | Secure offloading and maximized system utility |
| Li et al. [97] | 2020 | DQN, Blockchain | Multi-UAV-aided IoT with M2M communications | Increased system rewards |
| Islam et al. [98] | 2021 | DL, Blockchain | IoD | Robustness and low service execution time |
| Islam et al. [100] | 2022 | FL, Blockchain | Multi-UAV-aided MEC-enabled IoT | Enhanced security, low mean absolute error in the local model, low execution time, and increased data transmission rate |
| Luo et al. [101] | 2021 | Blockchain | Multi-UAV-aided MEC-enabled IoT | Flexible task offloading |
| Li et al. [104] | 2022 | Blockchain | UAV-aided delivery system | Enhanced security and openness, transparency, traceability in the delivery process, and support of real-time navigation for UAVs |
| Xu et al. [105] | 2021 | Blockchain | Multi-UAV-aided MEC-enabled network | Enhanced security, optimal edge computing resource pricing, optimal allocation of computing resources |
| Islam et al. [106] | 2019 | Blockchain | Multi-UAV-aided MEC-enabled IoT | Real-time data collection from IoT devices, enhanced security, increased throughput, low processing time, energy consumption, and latency |

active jammer protecting the communication, or they may be malicious nodes. Therefore, there is a large pallet of possibilities that should be considered for next-generation networks. The common part in all previous investigations has been the formulation of optimization problems, where information-theoretic variables (e.g., secrecy, secure rate, secrecy outage probability) are considered either as part of the cost function or as constraints. In this respect, this section has presented an extensive review of studies that jointly considered PLS, communication quality, offloading efficiency, radio/network resource allocation, energy consumption, UAV trajectory, etc.

## VI. REVIEW OF ML-INSPIRED AND BLOCKCHAIN-BASED SECURITY SOLUTIONS

In previous research works, the importance of distilling intelligence through ML-based methods in heterogeneous, complex, and dynamic UAV-aided MEC-enabled IoT networks with a large number of nodes has been underlined. On the other hand, the emergence of Blockchain has revolutionized the security sector by ensuring decentralization, immutability, and transparency, as well as secured and legitimate data. This section studies the recent works that are predominantly associated with either ML, Blockchain, or both. In these works, which are outlined in Table 3, the execution of computation tasks is facilitated by the MEC nodes.

To avoid raw data exchange in UAV swarms and protect data privacy, the Federated Edge Learning (FEEL) method was used in [92], in which the training data of a particular task is stored in a decentralized way across the UAVs in the swarm and the optimization problem is addressed cooperatively. However, the UAVs usually have batteries with a limited life, which may lead to an untimely dropping of these UAVs from FEEL training. Thus, an optimization strategy for time-varying channel conditions was presented, where the UAVs could extend their flight endurance by adaptively adjusting the frequency of their onboard CPU. In this respect, the computational resources and the wireless bandwidth were jointly allocated and a non-convex optimization problem was formulated and solved through a DRL-based Deep Deterministic Policy Gradient (DDPG)-based method, which was implemented using the well-known open-source PyTorch framework. Using this method, the total latency and energy consumption were linearly combined to estimate the system cost and their linear combination was minimized.

By combining the RL-based Q-learning advances with Deep Neural Networks (DNNs), an efficient deep Q-network (DQN) algorithm was proposed in [93] to dynamically optimize the computation offloading procedure and the bandwidth allocation, as well as enable the secure and green design of a MEC network. In the DQN algorithm, the DNN was used to approximate the Q-function and the RL was adaptive to many states. It was considered that the mobile devices in this network had limited computation capacity and could partly and locally execute their tasks with their onboard computing processors. The remaining part of these tasks should be offloaded to Computational Access Points (CAPs), which acted as MEC servers with powerful computation capacity to obtain a reduced system cost in terms of latency, energy consumption, and price. However, owing to the broadcast nature of the radio channel, a malicious UAV intended to perform a security attack and act as an eavesdropper during data transmission. The effectiveness of this DQN scheme was confirmed through extensive simulation results for Rayleigh flat fading channels.

Although ML-based schemes, e.g., DRL, can decrease energy consumption and time delay in dynamic and complex computation offloading scenarios without requiring prior radio channel knowledge [21], the feasibility of these schemes is confined owing to possible privacy issues and leakage of sensitive information. Specifically, adversaries may monitor the offloading decision-making process by capturing the status of the communication link and infer the value function of the learning algorithm, which in turn leads to an unprotected UAV's computation offloading preference. To preserve privacy during partial computation offloading, an online Differential Privacy (DP)-based Deep Q-Learning (DP-DQL) scheme for UAV-aided MEC-enabled IoT networks was presented in [94]. In this scheme, the DQL represented the primal learning mechanism, a generated Gaussian noise safeguarded the offloading preference, and the Prioritized Experience Replay (PER) technique [95] expedited the learning process. The network consisted of multiple fixed BSs with powerful computation capacity and grid power supply as well as a UAV, which flew above the area of interest and gathered data. Experimental results were provided to compare the performance of this scheme with the results obtained using full and partial offloading without the DP mechanism. It was considered that the UAV had limited resources and could locally perform task computation using a Raspberry Pi 3B+. Moreover, Pytorch and Python were adopted to implement the DP-DQL scheme. Based on the results, the proposed scheme surpassed other existing schemes with respect to cost-efficiency and privacy protection.

In [96], a secure offloading scheme for multi-UAV-aided MEC-enabled networks was proposed. In this direction, the UAVs were optimally deployed to serve all the GUs, under LoS propagation conditions, using a spiral placement algorithm. In addition to the legitimate UAVs, another UAV played the role of the eavesdropper, whereas a ground jammer tried to intercept the malicious UAV by transmitting artificial noise. To maximize the system utility, a non-convex optimization problem with a variety of constraints (i.e., transmission rate, latency, energy consumption, and type of task) was formulated and the low-complexity single-agent and multi-agent RL-based methods were adopted to solve this problem. The performance analysis demonstrated that the multi-agent method outperforms the single-agent method and the random offloading method in terms of the achieved system utility.

In [59], a decentralized Blockchain-based secure FL scheme, in which the UAVs trained their data locally to avoid several security and privacy issues, was leveraged for a Mobile Crowdsensing (MCS) scenario. The MSC comprised multiple mobile devices acting as task publishers, a group of resource-constrained UAVs acting as workers, powerful MEC nodes deployed at the BSs, and a consortium Blockchain, which designated the authorized nodes within the network that registered at a trusted Certification Authority (CA). It was considered that the devices initially published the sensing tasks to MEC nodes in their proximity and then the tasks were published to the UAVs that were also equipped with specialized sensors. By using the local sensing data of the UAVs, which were locally kept, a global model was collaboratively trained and the local model updates were forwarded to the MEC nodes to build this global model. More importantly, the UAVs aimed to enhance the QoS of MCS in a flexible, rapid, and cost-effective fashion, as long as challenging and emergency situations (e.g., earthquakes or flooding) took place. To mitigate privacy threats during the update of UAVs' local data and obtain aggregate accuracy, a specially designed privacy-preserving algorithm was proposed that relied on Local Differential Privacy (LDP). On the other hand, an RL-based incentive method was exploited to optimize the Quality of Local Model (QoLM) update during the FL procedure in the underlying highly dynamic network. According to the simulation results, which were obtained using Python, the proposed scheme outperforms other existing schemes in terms of the utilities for UAVs, model sharing, privacy preservation, and QoLM.

It is well known that the IoT enables the deployment of a massive number of Machine-Type Devices (MTDs), which interact and cooperate without human intervention through Machine-to-Machine (M2M) communications. Nevertheless, large-scale unexpected events or natural disasters may devastate the terrestrial M2M communication infrastructure. In this respect, the use of UAVs as BSs or aerial relays can restore the communication links, whereas combining Blockchain and MEC enables trustful data exchange and execution of data-intensive computing tasks, respectively. In [97], the data computation capacity and the throughput of a Blockchain system for multi-UAV-aided MEC-enabled M2M communications were jointly maximized and the optimization problem was formulated as a Markov Decision Process (MDP). More specifically, a DQN algorithm was developed to handle mission-critical, dynamic and complex application scenarios with variability and uncertainty. It is noted that the DQN combined an offline deep Convolutional Neural Network (CNN) and an online dynamic DP-DQL phase. It was considered that the UAVs could perform task computation with their onboard processor, as long as the computing requirements were not demanding. Otherwise, full task offloading to MEC servers was necessary. Also, these UAVs acted as Blockchain nodes and forwarded the data received from the MTDs. The performance of the proposed method was tested using Tensorflow with Python on Ubuntu and the simulation results revealed that the optimization framework can significantly enhance the system performance.

By leveraging an IoD network architecture and the powerful capabilities of DL and Blockchain, a swarm of drones was used in [98] for autonomous monitoring of pandemics in urban and rural areas with insufficient wireless connectivity. In this regard, a lightweight authentication scheme that combines a cuckoo filter and a digital signature algorithm was proposed to avoid security attacks (i.e., spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege). Also, the recent COVID-19 outbreak was considered as a use case. In this scheme, surveillance drones were used to remotely check face masks and social distances. Also, bumblebee drones in close proximity to the ground users were deployed to record people's body temperature in real-time through Forward-looking infrared (FLIR) cameras and provide delivery services. To improve the QoS during the execution of computation tasks and maintain low latency, the IoD network included an edge server. In addition, the drones were equipped with dew servers [99] to enable the local offline execution of the computation tasks. Besides, a consortium Blockchain system securely managed sensitive information and a DL-based algorithm was adopted to accurately detect face masks. To obtain experimental results, the DJI Mavic 2 Pro and Parrot Bebop 2 were used as surveillance and bumblebee drones, respectively. Furthermore, the Blockchain network was built using Multichain (https://www.multichain.com/) and 15 local computers acting as miners, whereas the DL-based mask detection was realized using the "you only look once (YOLO)" real-time object detection system. The experimental results in terms of service execution time and block transmission rate validated the feasibility of the proposed scheme.

In [100], an FL method and a Blockchain framework were successfully combined and a secure drone-aided data accumulation IoT scheme was proposed, namely FBI. To surpass connectivity issues in remote areas, the drones were used as intermediate nodes with onboard dew servers [99] and preserved the end-to-end communication between IoT devices and edge servers. The IoT devices were equipped with sensors and collected data to train the local models, which were securely stored in Blockchain. These models were verified using a Hampel filter and loss checks, while the privacy was maintained using a DP approach. In addition, the authentication of the network nodes involved two phases, where a cuckoo filter was used in Phase 1 and a timestamp nonce was used in Phase 2. The experiments were carried out using a DJI Mavic Pro 2 as a drone and a Jetson Xavier NX board as a dew server, whereas the Jetson TX2 and the Raspberry Pi 4 Model B were used as IoT devices. Also, PyTorch and PySyft were exploited to provide an FL environment for the proposed scheme and the open-source Multichain platform was adopted to construct the Blockchain network. The results confirmed the effectiveness of the proposed scheme with respect to the mean absolute error in the local model, the execution time, and the data transmission rate.

In [101], drones were used to expand the radio coverage of a MEC-enabled IoT network in remote locations beyond the outdoor coverage of conventional cellular networks. Also, a private Blockchain was exploited to safeguard computation offloading and increase reliability. In this direction, a decentralized three-layer network architecture was proposed. The first layer involved Wireless Sensor Networks (WSNs), which were deployed in different areas to gather sensed data. Moreover, the second layer included registered battery-operated rotary-wing drones as intermediate network entities that received the sensed data from the authorized IoT nodes of the WSNs and forwarded this data to MEC servers. In addition, the third layer comprised the MEC servers that performed task execution as well as the private Blockchain network between these servers that recorded the network data in a decentralized manner and allowed or restricted the participation of particular nodes in the network through a smart contract, which designated the offloading policy operations. The Ethereum-based Ropsten testnet was used to evaluate the smart contracts, which were implemented using the object-oriented high-level Solidity language (https://docs.soliditylang.org/en/v0.8.15/). To identify security threats, the STRIDE threat model [102] was adopted. The simulation results verified the performance, feasibility, and flexibility of the proposed offloading scheme.

Recently, the UAVs have been recognized as an inexpensive, sustainable, and affordable component of parcel delivery systems compared to conventional ground vehicles [103]. In this regard, UAVs can be used as "last-mile" aerial nodes and extend connectivity. As the delivery process involves operation among untrusted or malicious entities (i.e., the sender, the receiver, the intermediate node or the administrator of the UAV), securing this process is challenging and of high importance. To solve the "last mile" problem in logistics via a cost-effective and secure approach, a UAV-aided delivery system that adopts the MEC and Blockchain advances was presented in [104]. In particular, a network architecture was presented, where Blockchain nodes were positioned on the edge servers to mitigate potential security threats and these edge servers handled computation-intensive and latency-critical tasks (e.g., real-time UAV navigation) and ensured sufficient storage. By designating the rights and responsibilities of different nodes and automating the transaction process via the smart contract technology, the UAVs were successfully authenticated, the delivery process was monitored and access control, accountability, and traceability were provided. To verify the performance of the proposed delivery solution in terms of the access time and the transaction processing time, a UAV-aided MEC-enabled delivery system prototype was implemented. In this respect, the OpenAirInterface (OAI)-based MEC platform (https://openairinterface.org) and an Ethereum-based private Blockchain network were used. According to the experimental results, the proposed delivery solution is efficient and practically realizable.

In [105], a resource pricing and trading optimization scheme was proposed for a UAV-aided MEC-enabled network and the allocation of the edge computing resources between the Edge Computing Stations (ECSs) and the UAVs in their proximity was dynamically optimized to enhance the

QoS for the users. More importantly, the resources price of the edge computing resources was adjusted by the ECSs, whereas the requests for additional computing resources were reconciled by the UAVs. In this context, a Stackelberg dynamic game [87] was considered to characterize the trading interactions of the edge computing resources and construct the optimization problem with the ECSs and UAVs acting as leaders and followers, respectively. To solve this problem under open loop and feedback situations, the Lagrangian method and the Bellman dynamic programming were used. Also, the Blockchain technology was adopted, where the ECSs had the role of the mining tasks issuers to record the information about the trading interactions (e.g., requests for resources and price) and simultaneously handle the security and privacy threats. The numerical results highlighted the efficacy of the proposed scheme, under varied services demands of the users and different required resources of the UAVs. The equilibrium solutions of the ECSs, which are related to the optimal pricing strategies, were also depicted along with the optimal objectives of the UAVs and the optimal profit of the ECSs.

A swarm of UAVs was considered in [106] to facilitate data collection from IoT devices and a Blockchain-based data acquisition system, namely BUS, was proposed. As this system may be vulnerable to a wide range of security attacks (e.g., man-in-the-middle attacks, spoofing, and replay attacks), a shared key was used and data encryption was performed to obtain secure data transmission between the UAVs and the IoT devices. Before forwarding the data to a proximate server and storing these data on Blockchain, the UAV swarm performed an authentication process through a $\pi$-hash bloom filter and a digital signature algorithm. To efficiently perform data acquisition, two types of UAVs were used, i.e., the Minion UAVs that are located close to the IoT devices and the Emissary UAVs that transmit the data received from the Minion to the servers. Moreover, a MEC server provided additional computational resources and enabled real-time data collection, whereas a Ground Control Station (GCS) remotely controlled the UAVs during their operation. By using MATLAB and Python on the server and UAV side, respectively, and an Ethereum-based decentralized Blockchain platform, extended experimental results were obtained. In the experiments, the DJI Mavic 2 Pro and Parrot Bebop 2 were deployed to act as UAVs, whereas the Raspberry Pi 3 model b+ represented an IoT device. The results indicated that BUS can provide superior performance with respect to the throughput, processing time, energy consumption, and latency.

### A. SUMMARY

ML-based security methods have opened up new chances for safeguarding security, under complex and unpredictable conditions. In this regard, this section has reviewed recent ML-based research efforts and highlighted how different learning algorithms have been adopted and evaluated depending on the optimization target, such as the power consumption and latency. As long as vast amounts of data from multiple sources are available for training, the most powerful DL-based learning solutions can satisfactorily reveal useful correlations among heterogeneous data toward optimizing the security aspects of UAV-aided MEC-enabled IoT. However, solutions entailing lower complexity, i.e., RL and FL, may be preferable, when the computation resources are inadequate or inaccessible. Besides, the role of Blockchain as a protector of shared data against security threats has been underlined and relevant research works have been reviewed. As underlined in this section, Blockchain can provide transparency, flexibility, and an extra layer of security without the need for a centralized authority.

## VII. REVIEW OF AUTHENTICATION SOLUTIONS

As UAV-aided networks are highly dynamic, a large number of ground and aerial nodes may unexpectedly join or leave these networks. However, only the legitimate nodes should gain access to sensitive information. In this section, recently proposed software- and hardware-based authentication schemes are presented that aim to prevent in real-time unauthorized access to the IoT network by leveraging the MEC capabilities. These schemes, which are summarized in Table 4, involve MEC capabilities to expedite the authentication process and reduce the authentication cost.

In [107], the privacy information (i.e., identity, location, and flying routes) of UAVs in a highly mobile MEC-enabled IoD network was efficiently protected against external and internal threats (i.e., malicious UAVs) using a predictive and scalable authentication method for the UAV-to-UAV (U2U) communication links. In this respect, modular arithmetic operations were carried out in the authentication process to reduce the computation requirements. A lightweight online/offline signature design for the UAVs was also adopted [108] to enable self-control of signature key generation and avoid key escrow. The IoD consisted of a Trusted Authority (TA) that generated the certificates, the trusted MEC devices with powerful storage and computation capabilities, and the untrusted UAVs. The authentication procedure involved four distinct steps. The first step included the registration of MEC devices and UAVs by the TA and the initialization of the system. In the second step, the UAVs were allowed to join the network, whereas the MEC devices facilitated the rapid authentication of U2U communication in the third step. Moreover, the privacy of the UAVs was ensured in a non-interactive manner using a Pseudonym and Key Update design in the fourth step. To investigate the performance of the proposed authentication method, a Raspberry Pi 3 (Model B+) was used as the UAVs' onboard computer and a desktop running OS X was used as the MEC device. The MEC devices and the TA applied RSA-2048 digital signature techniques, while the modular arithmetic operations were implemented using the Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) [109]. Numerical and simulation results were provided to verify the

**TABLE 4. Summary of recent research works on authentication solutions.**

| Reference | Year | Authentication Mechanisms | Type of the Network | Advantages |
|---|---|---|---|---|
| Tian et al. [107] | 2019 | Modular arithmetic operations, online/offline signature design | IoD | Support of real-time authentication, low computation, communication, and storage costs |
| Khan et al. [110] | 2019 | HECC | FANET | Real-time response, low computation and communication costs |
| Khan et al. [111] | 2020 | HECC | FANET | Low computation and communication costs |
| Yahuza et al. [114] | 2021 | ECC | IoD | Low energy consumption, low computation and communication costs |
| Gope et al. [115] | 2020 | PUF, hash functions | IoD | Low power consumption, low storage and communication costs, and execution efficiency |

superior performance of this method in terms of computational cost, communication cost, and storage overhead.

To avoid public-key certificates and the key escrow issue, the provably verified certificateless blind signature (CL-BS) scheme for resource-constrained 5G-enabled FANETs was proposed in [110] for a surveillance application scenario. This scheme relies on hyperelliptic curves and uses keys of relatively small size. A three-layer network architecture was considered, where Layer 1 comprised the BS and the ground-based IoT devices that were connected with a raspberry pi-based multi-access edge computing UAV (RMEC-UAV) with adequate computing resources for the execution of the security mechanism. Also, Layer 2 included monitoring UAVs (M-UAVs) that were equipped with cameras, Inertial Measurement Unit (IMU), sensors, and GPS. These M-UAVs were interconnected via Bluetooth and collected images and videos from the area of interest. In addition, Layer consisted of the RMEC-UAV, which authenticated the M-UAVs and also forwarded the collected data of the M-UAVs and the IoT devices to a BS along with their flight information and features. The test of the runtime of the cryptographic operations using MIRACL [109], the informal security analysis, and the formal security analysis using the Automated Validation for Internet Security Validation and Application (AVISPA) tool indicated that CL-BS can outperform other schemes with regard to computational and communication costs.

An identity-based generalized signcryption scheme was proposed in [111] to prevent the risk of unauthorized access and preserve confidentiality in multi-UAV FANETs. In this scheme, both 5G and Wi-Fi technologies were leveraged to enable backhaul and fronthaul connectivity, respectively. Since UAVs typically have low onboard computational and energy resources, the implementation of cryptographic protocols with low complexity is required. To this end, this scheme adopted the Hyperelliptic Curve Cryptography (HECC) and used very small size keys during key exchange. Apart from the monitoring UAVs, this scheme also included UAVs that acted as MEC servers and provided offloading services to other UAVs. Based on the Dolev and Yao (DY) threat model [112] and the AVISPA tool, security analysis was realized. Also, MIRACL [109] was exploited to investigate the performance of the proposed scheme, and precision agriculture was considered as a case study. The results indicated that the proposed scheme was effective against known and unknown attacks and could surpass other schemes in terms of computational and communication costs.

The certificateless-based and Elliptic-Curve Cryptography (ECC)-based SLPAKA (Secure Lightweight Proven Authenticated Key Agreement) authentication method, which can cope with the widely used Canetti–Krawczyk (CK) adversary model [113], was presented in [114]. In this model, a probabilistic polynomial adversary was considered that could affect the communication channel. Apart from the drones that were dynamically added, the IoD network consisted of the Trusted Authority Center (TAC) that facilitated the key generation, the MEC devices that assisted the drones during computation tasks, and the GCS. To implement SLPAKA and investigate its energy and computational efficiency, the Python programming language was used. In this regard, the security was analyzed both informally and formally (via the ProVerif tool), and the advantages of SLPAKA were demonstrated.

As key management is challenging in large-scale IoD networks and the network nodes are usually resource-constrained, exploiting the intrinsic characteristics of hardware can strengthen the identification, authentication, and access control [18]. In this direction, embedded PUF chips can be used to authenticate individual nodes without using costly cryptographic methods. In [115], a simple key agreement scheme was proposed to efficiently preserve privacy and handle the authentication process in the MEC-enabled IoD. In this scheme, invasive and non-invasive attacks could be prevented, while minimum computing resources were required by exploiting PUFs to store cryptographic keys and hash functions. More importantly, the use of memory-based devices was avoided, since they are vulnerable to physical attacks. In particular, an IoD consisting of multiple UAVs was considered. These UAVs used third-party edge devices susceptible to various threats (e.g., authentication, privacy, location, session-key security, and physical security threats). In this regard, the MEC operators could validate the legitimacy of a particular UAV owing to a double-PUF-based configuration at each UAV, where the first PUF was located in the memory unit and the second PUF was placed in the main control circuit. In the performance evaluation of the proposed authentication mechanism, a 128-bit arbiter PUF circuit and the SHA-256 were considered. Additionally, the cryptographic operations were carried out using an ATMel ATMega2560 machine with an MSP430 micro-controller on the UAV side and a powerful desktop computer with an Intel Core i7 processor at the server side. The results, which were obtained using the Java Cryptography Extension (JCE) library, verified the superior performance of this authentication scheme in terms of the total authentication time for a varying number of UAVs.

### *A. SUMMARY*

As authentication stands for one of the major requirements towards security for a UAV-aided MEC-enabled IoT network, this section has discussed relevant authentication mechanisms. These mechanisms allow for optimized real-time authentication owing to the powerful capabilities of MEC servers. The primal goal of these mechanisms is to compensate the energy, communication, computation, and storage costs. Beyond the conventional cryptographic methods (e.g., hash functions and ECC), the PUFs enable the successful authentication of the network nodes efficiently and cost-effectively.

## VIII. FUTURE RESEARCH DIRECTIONS

The emergence of novel deployment paradigms for UAV-assisted MEC-enabled IoT systems is anticipated over the next decade, as UAV, MEC, and IoT technologies continue to mature. Within the environment of future computing-aware networks, the cooperation of the network nodes will be far more effective as well as complex, allowing for the formation of novel security vulnerabilities. Although current work provides a convenient methodological framework for maintaining security in UAV-aided MEC-enabled IoT, future supplementary work and further advancements in this area, from PLS, ML, Blockchain, and authentication perspective, are required. To foster further advancements in this research field, still many open research issues require critical attention as follows.

### *A. OPEN ISSUES IN PLS*

In the vast majority of the relevant studies on secrecy and PLS, the encountered threat was the existence of eavesdroppers/men-in-the-middle. Besides, few studies investigated DoS misbehavior/anomaly detection based on trust or reputation-based metrics. This fact indicates that there are still open issues and challenges in tackling other types of threats like jamming, Sybil attacks, spoofing, and tampering. Additional investigation on the secrecy-key rate estimation and coding for secrecy is also required. Moreover, the analysis of PLS under outdated channel state information (CSI) conditions should be considered in future work, since the CSI may be outdated in UAV-based scenarios due to the high mobility and fast channel fading. Also, one of the main challenges of designing RIS-aided networks is to determine the proper location of the RIS units that leads to optimal or near-optimal performance. Thus, optimizing the location of multiple RIS units to maximize the secrecy performance is also suggested.

### *B. OPEN ISSUES IN THE ADOPTION OF ML AND BLOCKCHAIN*

As the integration of ML and Blockchain is in its infancy, additional research efforts should be devoted to investigating the computation efficiency and software/hardware design issues. In this direction, the scheduling of the computation tasks can lead to reduced execution time. Furthermore, the trustworthiness of the IoT nodes during Blockchain transactions should be ascertained, whereas incentive schemes that recompense the MEC providers should be established to motivate them to allocate computing resources. Besides, sophisticated ML techniques can be adopted to enable efficient vision-based detection and tracking of aerial and ground objects.

### *C. OPEN ISSUES IN THE AUTHENTICATION PROCEDURE*

The increased mobility and the dynamic distribution of the network nodes during data exchange should be taken into account in future authentication solutions along with decentralized scenarios. Instead of using public key cryptosystems, sophisticated hybrid Blockchain-based and quantum-based schemes are also envisioned to increase the robustness of the authentication procedure.

### *D. OPEN ISSUES IN THE EXPERIMENTAL TESTING*

Currently, there is a gap in acquiring measured data from real-world experiments in various scenarios and dynamically changing propagation environments with high resiliency requirements and real-world constraints. Thus, small-scale experimental campaigns that involve various ML algorithms, a real Blockchain testbed, different adversaries, and various attacks constitute the basis for the verification of the hitherto theoretical outcomes.

## IX. CONCLUSION

Since long-range radio coverage, uninterrupted connectivity, and sufficient computation capacity have been deemed a necessity in a wide variety of novel IoT applications and services, the UAVs together with the MEC technology can significantly enhance the QoS and QoE and strongly promote the evolution of IoT. As UAVs have limited onboard processing resources and limited battery capacity, dedicated infrastructures with MEC capabilities can facilitate the processing of large amounts of data. Cellular BSs, for example, can use MEC to deliver next-generation services and applications more flexibly. Multimedia content, such as video games and movies, can be placed closer to the end-user, lowering latency and bandwidth requirements. In addition, applications requiring powerful computing capacity (e.g., intelligent video analytics that automatically recognize temporal and spatial events in videos or augmented reality-based applications) can be performed efficiently at the edge node. Using the same reasoning, we can also conclude that by introducing cloud computing to the edge of the radio access network, MEC can be a crucial component for real-time IoT systems and services, such as surveillance and long-distance medical monitoring. Nevertheless, there exists a quest for an equilibrium between satisfying the computation demands and developing effective countermeasures to mitigate security threats. Therefore, this paper has provided an extensive overview and classification of recently proposed security solutions. To this end, the major outcomes of this paper can be summarized as follows:

- Specific use cases were identified, in which the employment of UAV-assisted MEC-enabled IoT systems can be not only beneficial, but also essential for meeting end-user QoS and QoE requirements. Specifically, the issue of significant and rapid fluctuations in cellular network traffic volume was discussed, as well as the extension of cellular coverage and connectivity, especially in disaster-affected and remote areas. Also, due to its strategic significance in modern society, a detailed overview of UAV-assisted MEC-enabled IoT systems for precision agriculture was provided.
- In general, there exists a trade-off between security and system costs (i.e., communication, computation, and storage costs) in practical implementations of the UAV-aided MEC-enabled IoT.
- Although PLS is generally computationally more efficient than conventional cryptosystems, IoT imposes strict computational requirements. Therefore, a UAV-based MEC node can play the role of PLS enabler in such configurations.
- The possibilities and capabilities of PLS heavily rely on the topology, i.e., the number of eavesdroppers, the location of the eavesdroppers (i.e., airborne or ground), the number of UAVs cooperating to achieve secure communications, and the number and location of the user terminals.
- Elaborate techniques to increase PLS, while retaining an acceptable rate of communication, require multiple antennas and are significantly benefited by the use of state-of-the-art techniques, such as the use of NOMA, RIS, etc.
- Although DL algorithms require remarkable computing power, running DL algorithms on MEC servers significantly increases the response and efficiency of the network.
- Considering the varying processing capabilities of UAVs, their energy constraints, and the need for secure network operation, exploiting decentralized privacy-preserving collaborative ML methods, such as FL, can ensure feasibility in practical scenarios and lead to adequate protection of the node privacy, less experienced latency, and decreased energy burden.
- Blockchain can be further optimized and become more accurate using ML methods.
- In general, traditional cryptographic methods, including hash functions and ECC, can satisfactorily mitigate malicious attacks. However, adopting PUFs or hybrid schemes with software- and hardware-based mechanisms can drastically improve the security level and leads to cost-effective, scalable, and robust authentication solutions.

## REFERENCES

[1] N. Nomikos, E. T. Michailidis, P. Trakadas, D. Vouyioukas, H. Karl, J. Martrat, T. Zahariadis, K. Papadopoulos, and S. Voliotis, "A UAV-based moving 5G RAN for massive connectivity of mobile users and IoT devices," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100250, doi: 10.1016/j.vehcom.2020.100250.

[2] P. Boccadoro, D. Striccoli, and L. A. Grieco, "An extensive survey on the Internet of Drones," *Ad Hoc Netw.*, vol. 122, Nov. 2021, Art. no. 102600, doi: 10.1016/j.adhoc.2021.102600.

[3] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-edge computing architecture: The role of MEC in the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016, doi: 10.1109/MCE.2016.2590118.

[4] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020, doi: 10.1109/JIOT.2020.3004500.

[5] P. Zhang, C. Wang, C. Jiang, and A. Benslimane, "UAV-assisted multi-access edge computing: Technologies and challenges," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 12–17, Dec. 2021, doi: 10.1109/IOTM.001.2100092.

[6] N. Cheng, W. Xu, W. Shi, Y. Zhou, N. Lu, H. Zhou, and X. Shen, "Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 26–32, Aug. 2018, doi: 10.1109/MCOM.2018.1701092.

[7] J. Ji, K. Zhu, and D. Niyato, "Joint communication and computation design for UAV-enabled aerial computing," *IEEE Commun. Mag.*, vol. 59, no. 11, pp. 73–79, Nov. 2021, doi: 10.1109/MCOM.101.2100229.

[8] W. Lin, T. Huang, X. Li, F. Shi, X. Wang, and C.-H. Hsu, "Energy-efficient computation offloading for UAV-assisted MEC: A two-stage optimization scheme," *ACM Trans. Internet Technol.*, vol. 22, no. 1, pp. 1–23, Feb. 2022, doi: 10.1145/3430503.

[9] Z. Yu, Y. Gong, S. Gong, and Y. Guo, "Joint task offloading and resource allocation in UAV-enabled mobile edge computing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3147–3159, Apr. 2020, doi: 10.1109/JIOT.2020.2965898.

[10] L. Zhang and N. Ansari, "Latency-aware IoT service provisioning in UAV-aided mobile-edge computing networks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10573–10580, Oct. 2020, doi: 10.1109/JIOT.2020.3005117.

[11] Z. Hu, F. Zeng, Z. Xiao, B. Fu, H. Jiang, and H. Chen, "Computation efficiency maximization and QoE-provisioning in UAV-enabled MEC communication systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1630–1645, Apr./Jun. 2021, doi: 10.1109/TNSE.2021.3068123.

[12] W. Feng, J. Tang, N. Zhao, X. Zhang, X. Wang, K.-K. Wong, and J. A. Chambers, "Hybrid beamforming design and resource allocation for UAV-aided wireless-powered mobile edge computing networks with NOMA," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3271–3286, Nov. 2021, doi: 10.1109/JSAC.2021.3091158.

[13] C. Lin, G. Han, S. B. H. Shah, Y. Zou, and L. Gou, "Integrating mobile edge computing into unmanned aerial vehicle networks: An SDN-enabled architecture," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 18–23, Dec. 2021, doi: 10.1109/IOTM.001.2100070.

[14] E. T. Michailidis, N. I. Miridakis, A. Michalas, E. Skondras, and D. J. Vergados, "Energy optimization in dual-RIS UAV-aided MEC-enabled Internet of Vehicles," *Sensors*, vol. 21, no. 13, p. 4392, Jun. 2021, doi: 10.3390/s21134392.

[15] E. T. Michailidis, N. I. Miridakis, A. Michalas, E. Skondras, D. J. Vergados, and D. D. Vergados, "Energy optimization in massive MIMO UAV-aided MEC-enabled vehicular networks," *IEEE Access*, vol. 9, pp. 117388–117403, 2021, doi: 10.1109/ACCESS.2021.3106495.

[16] Z. Yang, M. Chen, X. Liu, Y. Liu, Y. Chen, S. Cui, and H. V. Poor, ''AI-driven UAV-NOMA-MEC in next generation wireless networks,'' *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 66–73, Oct. 2021, doi: 10.1109/MWC.121.2100058.

[17] P. Ranaweera, A. D. Jurcut, and M. Liyanage, ''Survey on multi-access edge computing security and privacy,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3062546.

[18] E. T. Michailidis and D. Vouyioukas, ''A review on software-based and hardware-based authentication mechanisms for the Internet of Drones,'' *Drones*, vol. 6, no. 2, p. 41, Feb. 2022, doi: 10.3390/drones6020041.

[19] D. He, S. Chan, and M. Guizani, ''Security in the Internet of Things supported by mobile edge computing,'' *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 56–61, Aug. 2018, doi: 10.1109/MCOM.2018.1701132.

[20] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, ''Physical layer security in UAV systems: Challenges and opportunities,'' *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019, doi: 10.1109/MWC.001.1900028.

[21] P. S. Bithas, E. T. Michailidis, N. Nomikos, D. Vouyioukas, and A. G. Kanatas, ''A survey on machine-learning techniques for UAV-based communications,'' *Sensors*, vol. 19, no. 23, p. 5170, 2019, doi: 10.3390/s19235170.

[22] P. Mehta, R. Gupta, and S. Tanwar, ''Blockchain envisioned UAV networks: Challenges, solutions, and comparisons,'' *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020, doi: 10.1016/j.comcom.2020.01.023.

[23] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W.-J. Hwang, and Z. Ding, ''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, doi: 10.1109/ACCESS.2020.3001277.

[24] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, ''Survey on multi-access edge computing for Internet of Things realization,'' *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018, doi: 10.1109/COMST.2018.2849509.

[25] S. Zaidi, M. Atiquzzaman, and C. T. Calafate, ''Internet of flying things (IoFT): A survey,'' *Comput. Commun.*, vol. 165, pp. 53–74, Jan. 2021, doi: 10.1016/j.comcom.2020.10.023.

[26] Q. Wu, J. Xu, Y. Zeng, D. W. K. Ng, N. Al-Dhahir, R. Schober, and A. L. Swindlehurst, ''A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence,'' *IEEE J. Sel. Areas Commun.*, vol. 39, no. 10, pp. 2912–2945, Oct. 2021, doi: 10.1109/JSAC.2021.3088681.

[27] 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 Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019, doi: 10.1109/COMST.2019.2906228.

[28] S. M. A. Huda and S. Moh, ''Survey on computation offloading in UAV-enabled mobile edge computing,'' *J. Netw. Comput. Appl.*, vol. 201, May 2022, Art. no. 103341, doi: 10.1016/j.jnca.2022.103341.

[29] F. Zhou, R. Q. Hu, Z. Li, and Y. Wang, ''Mobile edge computing in unmanned aerial vehicle networks,'' *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 140–146, Feb. 2020, doi: 10.1109/MWC.001.1800594.

[30] N. Fatima, P. Saxena, and M. Gupta, ''Integration of multi access edge computing with unmanned aerial vehicles: Current techniques, open issues and research directions,'' *Phys. Commun.*, vol. 52, Jun. 2022, Art. no. 101641, doi: 10.1016/j.phycom.2022.101641.

[31] W. Zhang, L. Li, N. Zhang, T. Han, and S. Wang, ''Air-ground integrated mobile edge networks: A survey,'' *IEEE Access*, vol. 8, pp. 125998–126018, 2020, doi: 10.1109/ACCESS.2020.3008168.

[32] Y. Yazid, I. Ez-Zazi, A. Guerrero-González, A. El Oualkadi, and M. Arioua, ''UAV-enabled mobile edge-computing for IoT based on AI: A comprehensive review,'' *Drones*, vol. 5, no. 4, p. 148, Dec. 2021, doi: 10.3390/drones5040148.

[33] M. Abrar, U. Ajmal, Z. M. Almohaimeed, X. Gui, R. Akram, and R. Masroor, ''Energy efficient UAV-enabled mobile edge computing for IoT devices: A review,'' *IEEE Access*, vol. 9, pp. 127779–127798, 2021, doi: 10.1109/ACCESS.2021.3112104.

[34] R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. K. Al-Ali, K. A. Harras, and M. Guizani, ''Design challenges of multi-UAV systems in cyber-physical applications: A comprehensive survey and future directions,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3340–3385, 4th Quart., 2019, doi: 10.1109/COMST.2019.2924143.

[35] 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, doi: 10.1109/ACCESS.2021.3066778.

[36] 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,'' 2021, *arXiv:2109.14442*.

[37] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, ''UAV IoT framework views and challenges: Towards protecting drones as 'things,''' *Sensors*, vol. 18, no. 11, p. 4015, Nov. 2018, doi: 10.3390/s18114015.

[38] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, ''Security analysis of drones systems: Attacks, limitations, and recommendations,'' *Internet Things*, vol. 11, Sep. 2020, Art. no. 100218, doi: 10.1016/j.iot.2020.100218.

[39] R. Altawy and A. M. Youssef, ''Security, privacy, and safety aspects of civilian drones: A survey,'' *ACM Trans. Cyber Phys. Syst.*, vol. 1, no. 2, p. 1–25, Nov. 2016, doi: 10.1145/3001836.

[40] F. Syed, S. K. Gupta, S. H. Alsamhi, M. Rashid, and X. Liu, ''A survey on recent optimal techniques for securing unmanned aerial vehicles applications,'' *Trans. Emerg. Telecommun. Technol.*, vol. 32, p. e4133, Jul. 2021, doi: 10.1002/ett.4133.

[41] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, ''Fast, reliable, and secure drone communication: A comprehensive survey,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, 4th Quart., 2021, doi: 10.1109/COMST.2021.3097916.

[42] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, ''Machine learning for wireless connectivity and security of cellular-connected UAVs,'' *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 28–35, Feb. 2019, doi: 10.1109/MWC.2018.1800155.

[43] J. McCoy and D. B. Rawat, ''Software-defined networking for unmanned aerial vehicular networking and security: A survey,'' *Electronics*, vol. 8, no. 12, p. 1468, Dec. 2019, doi: 10.3390/electronics8121468.

[44] Y.-C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, ''Mobile edge computing—A key technology towards 5G,'' 1st ed., ETSI, Sophia Antipolis, France, ETSI White Paper 11, Sep. 2015, pp. 1–16.

[45] E. T. Michailidis, S. M. Potirakis, and A. G. Kanatas, ''AI-inspired non-terrestrial networks for IIoT: Review on enabling technologies and applications,'' *IoT*, vol. 1, no. 1, pp. 21–48, Jul. 2020.

[46] Radio Technical Commission for Aeronautics (RTCA). *Drone Advisory Committee (DAC)*. Accessed: May 18, 2022. [Online]. Available: http://www.rtca.org/content/drone-advisory-committee

[47] *Armstrong Flight Research Center*. Accessed: May 18, 2022. [Online]. Available: https://www.nasa.gov/centers/armstrong/images/UAV/index.html

[48] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, ''FANET: Communication, mobility models and security issues,'' *Comput. Netw.*, vol. 163, Nov. 2019, Art. no. 106877, doi: 10.1016/j.comnet.2019.106877.

[49] Z. Zhao, P. Cumino, C. Esposito, M. Xiao, D. Rosário, T. Braun, E. Cerqueira, and S. Sargento, ''Smart unmanned aerial vehicles as base stations placement to improve the mobile network operations,'' *Comput. Commun.*, vol. 181, pp. 45–57, Jan. 2022, doi: 10.1016/j.comcom.2021.09.016.

[50] M. Aloqaily, Y. Jararweh, and O. Bouachir, ''Trustworthy cooperative UAV-based data management in densely crowded environments,'' *IEEE Commun. Standards Mag.*, vol. 5, no. 4, pp. 18–24, Dec. 2021, doi: 10.1109/MCOMSTD.0001.2000039.

[51] K. G. Panda, S. Das, D. Sen, and W. Arif, ''Design and deployment of UAV-aided post-disaster emergency network,'' *IEEE Access*, vol. 7, pp. 102985–102999, 2019, doi: 10.1109/ACCESS.2019.2931539.

[52] B. Bollard, A. Doshi, N. Gilbert, C. Poirot, and L. Gillman, ''Drone technology for monitoring protected areas in remote and fragile environments,'' *Drones*, vol. 6, no. 2, p. 42, Feb. 2022, doi: 10.3390/drones6020042.

[53] Y. Liu, C.-X. Wang, H. Chang, Y. He, and J. Bian, ''A novel non-stationary 6G UAV channel model for maritime communications,'' *IEEE J. Sel. Areas Commun.*, vol. 39, no. 10, pp. 2992–3005, Oct. 2021, doi: 10.1109/JSAC.2021.3088664.

[54] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, ''A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact,'' *IEEE Access*, vol. 8, pp. 90225–90265, 2020, doi: 10.1109/ACCESS.2020.2992341.

[55] D. C. Tsouros, S. Bibi, and P. G. Sarigiannidis, ''A review on UAV-based applications for precision agriculture,'' *Information*, vol. 10, no. 11, p. 349, Nov. 2019, doi: 10.3390/info10110349.

[56] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming," *Sensors*, vol. 20, no. 22, p. 6458, Nov. 2020, doi: 10.3390/s20226458.

[57] X. Yang, L. Shu, J. Chen, M. A. Ferrag, J. Wu, E. Nurellari, and K. Huang, "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 2, pp. 273–302, Feb. 2021, doi: 10.1109/JAS.2020.1003536.

[58] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020, doi: 10.1109/ACCESS.2020.2973178.

[59] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for UAV-assisted crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1055–1069, Apr./Jun. 2021, doi: 10.1109/TNSE.2020.3014385.

[60] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100249, doi: 10.1016/j.vehcom.2020.100249.

[61] S. H. Alsamhi, F. A. Almalki, F. Afghah, A. Hawbani, A. V. Shvetsov, B. Lee, and H. Song, "Drones' edge intelligence over smart environments in B5G: Blockchain and federated learning synergy," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 295–312, Mar. 2022, doi: 10.1109/TGCN.2021.3132561.

[62] D. Saraswat, A. Verma, P. Bhattacharya, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions," *IEEE Access*, vol. 10, pp. 33154–33182, 2022, doi: 10.1109/ACCESS.2022.3161132.

[63] C. Feng, B. Liu, K. Yu, S. K. Goudos, and S. Wan, "Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3582–3592, May 2022, doi: 10.1109/TII.2021.3116132.

[64] P. Amos, P. Li, W. Wu, and B. Wang, "Computation efficiency maximization for secure UAV-enabled mobile edge computing networks," *Phys. Commun.*, vol. 46, Jun. 2021, Art. no. 101284, doi: 10.1016/j.phycom.2021.101284.

[65] Y. Li, Y. Fang, and L. Qiu, "Joint computation offloading and communication design for secure UAV-enabled MEC systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6, doi: 10.1109/WCNC49053.2021.9417457.

[66] M. Grant, S. Boyd, and Y. Ye. (2013). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.0 Beta*. Accessed: Jul. 19, 2021. [Online]. Available: http://cvxr.com/cvx

[67] D. Han and T. Shi, "Secrecy capacity maximization for a UAV-assisted MEC system," *China Commun.*, vol. 17, no. 10, pp. 64–81, Oct. 2020, doi: 10.23919/JCC.2020.10.005.

[68] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Secure communications for UAV-enabled mobile edge computing systems," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 376–388, Jan. 2020, doi: 10.1109/TCOMM.2019.2947921.

[69] R. Han, L. Bai, J. Liu, J. Choi, and Y.-C. Liang, "A secure structure for UAV-aided IoT networks: Space-time key," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 96–101, Oct. 2021, doi: 10.1109/MWC.111.2100087.

[70] W. Lu, Y. Ding, Y. Gao, S. Hu, Y. Wu, N. Zhao, and Y. Gong, "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2704–2713, Apr. 2022, doi: 10.1109/TII.2021.3087726.

[71] W. Liu, Y. Xu, D. Wu, H. Wang, X. Zheng, and X. Chen, "Distributed energy-efficient and secure offloading in air-to-ground MEC networks," *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, pp. 1–18, Dec. 2021, doi: 10.1186/s13634-021-00785-9.

[72] J. Bai, Z. Zeng, T. Wang, S. Zhang, N. N. Xiong, and A. Liu, "TANTO: An effective trust based unmanned aerial vehicle computing system for the Internet-of-Things," *IEEE Internet Things J.*, early access, Feb. 11, 2022, doi: 10.1109/JIOT.2022.3150765.

[73] Y. Xu, T. Zhang, D. Yang, Y. Liu, and M. Tao, "Joint resource and trajectory optimization for security in UAV-assisted MEC systems," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 573–588, Jan. 2021, doi: 10.1109/TCOMM.2020.3025910.

[74] H. Yang, "Secure energy efficiency maximization for dual-UAV-assisted intelligent reflecting surface system," *Phys. Commun.*, vol. 52, Jun. 2022, Art. no. 101622, doi: 10.1016/j.phycom.2022.101622.

[75] T. Bai, J. Wang, Y. Ren, and L. Hanzo, "Energy-efficient computation offloading for secure UAV-edge-computing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6074–6087, Jun. 2019, doi: 10.1109/TVT.2019.2912227.

[76] X. Gu, G. Zhang, and J. Gu, "Offloading optimization for energy-minimization secure UAV-edge-computing systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6, doi: 10.1109/WCNC49053.2021.9417527.

[77] X. Gu, G. Zhang, M. Wang, W. Duan, M. Wen, and P.-H. Ho, "UAV-aided energy-efficient edge computing networks: Security offloading optimization," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4245–4258, Mar. 2022, doi: 10.1109/JIOT.2021.3103391.

[78] W. Lu, Y. Ding, Y. Gao, Y. Chen, N. Zhao, Z. Ding, and A. Nallanathan, "Secure NOMA-based UAV-MEC network towards a flying eavesdropper," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3364–3376, May 2022, doi: 10.1109/TCOMM.2022.3159703.

[79] T. Wang, Y. Li, and Y. Wu, "Energy-efficient UAV assisted secure relay transmission via cooperative computation offloading," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 4, pp. 1669–1683, Dec. 2021, doi: 10.1109/TGCN.2021.3099523.

[80] J. X. Xie and Y. Xue, *Optimization Modeling and LINDO/LINGO Software*, vol. 18, no. 4. Beijing, China: Tsinghua Univ. Press, 2005, pp. 67–73.

[81] H. Hashida, Y. Kawamoto, and N. Kato, "Intelligent reflecting surface placement optimization in air-ground communication networks toward 6G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 146–151, Dec. 2020, doi: 10.1109/MWC.001.2000142.

[82] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, 3rd Quart., 2021, doi: 10.1109/COMST.2021.3077737.

[83] L. Yan, C. Wang, and W. Zheng, "Secure efficiency maximization for UAV-assisted mobile edge computing networks," *Phys. Commun.*, vol. 51, Apr. 2022, Art. no. 101568, doi: 10.1016/j.phycom.2021.101568.

[84] W. Wang, W. Ni, H. Tian, and L. Song, "Intelligent Omni-surface enhanced aerial secure offloading," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5007–5022, May 2022, doi: 10.1109/TVT.2022.3150769.

[85] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart vehicles," *IEEE Netw.*, vol. 32, no. 3, pp. 42–51, May/Jun. 2018, doi: 10.1109/MNET.2018.1700286.

[86] H. Sedjelmaci, A. Boudguiga, I. B. Jemaa, and S. M. Senouci, "An efficient cyber defense framework for UAV-edge computing network," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101970, doi: 10.1016/j.adhoc.2019.101970.

[87] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5549–5561, May 2020, doi: 10.1109/TVT.2020.2982000.

[88] *The Network Simulator-NS*. Accessed: Jul. 25, 2022. [Online]. Available: https://sourceforge.net/projects/nsnam/files/

[89] P. A. Lopez, E. Wiessner, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flotterod, R. Hilbrich, L. Lucken, J. Rummel, and P. Wagner, "Microscopic traffic simulation using SUMO," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 2575–2582, doi: 10.1109/ITSC.2018.8569938.

[90] O. S. Oubbati, N. Chaib, A. Lakas, P. Lorenz, and A. Rachedi, "UAV-assisted supporting services connectivity in urban VANETs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3944–3951, Apr. 2019, doi: 10.1109/TVT.2019.2898477.

[91] Y. He, D. Zhai, F. Huang, D. Wang, X. Tang, and R. Zhang, "Joint task offloading, resource allocation, and security assurance for mobile edge computing-enabled UAV-assisted VANETs," *Remote Sens.*, vol. 13, no. 8, p. 1547, Apr. 2021, doi: 10.3390/rs13081547.

[92] S. Tang, W. Zhou, L. Chen, L. Lai, J. Xia, and L. Fan, "Battery-constrained federated edge learning in UAV-enabled IoT for B5G/6G networks," *Phys. Commun.*, vol. 47, Aug. 2021, Art. no. 101381, doi: 10.1016/j.phycom.2021.101381.

[93] R. Zhao, J. Xia, Z. Zhao, S. Lai, L. Fan, and D. Li, "Green MEC networks design under UAV attack: A deep reinforcement learning approach," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1248–1258, Sep. 2021, doi: 10.1109/TGCN.2021.3073939.

[94] D. Wei, N. Xi, J. Ma, and L. He, "UAV-assisted privacy-preserving online computation offloading for Internet of Things," *Remote Sens.*, vol. 13, no. 23, p. 4853, Nov. 2021, doi: 10.3390/rs13234853.

[95] T. Schaul, J. Quan, I. Antonoglou, and D. Silver, "Prioritized experience replay," 2015, *arXiv:1511.05952*.

[96] W. Lu, Y. Mo, Y. Feng, Y. Gao, N. Zhao, Y. Wu, and A. Nallanathan, "Secure transmission for multi-UAV-assisted mobile edge computing based on reinforcement learning," *IEEE Trans. Netw. Sci. Eng.*, early access, Jun. 22, 2022, doi: 10.1109/TNSE.2022.3185130.

[97] M. Li, F. R. Yu, P. Si, R. Yang, Z. Wang, and Y. Zhang, "UAV-assisted data transmission in blockchain-enabled M2M communications with mobile edge computing," *IEEE Netw.*, vol. 34, no. 6, pp. 242–249, Nov./Dec. 2020, doi: 10.1109/MNET.011.2000147.

[98] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using internet of drone things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 166–173, Aug. 2021, doi: 10.1109/MWC.001.2000429.

[99] P. P. Ray, "An introduction to dew computing: Definition, concept and implications," *IEEE Access*, vol. 6, pp. 723–737, 2018, doi: 10.1109/ACCESS.2017.2775042.

[100] A. Islam, A. Al Amin, and S. Y. Shin, "FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things," *IEEE Wireless Commun. Lett.*, vol. 11, no. 5, pp. 972–976, May 2022, doi: 10.1109/LWC.2022.3151873.

[101] S. Luo, H. Li, Z. Wen, B. Qian, G. Morgan, A. Longo, O. Rana, and R. Ranjan, "Blockchain-based task offloading in drone-aided mobile edge computing," *IEEE Netw.*, vol. 35, no. 1, pp. 124–129, Jan./Feb. 2021, doi: 10.1109/MNET.011.2000222.

[102] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Threat modeling-uncover security design flaws using the stride approach," in *MSDN Magazine-Louisville* (MSDN Magazine is the Microsoft Journal for Developers). USA: Microsoft, 2006, pp. 68–75.

[103] R. She and Y. Ouyang, "Efficiency of UAV-based last-mile delivery under congestion in low-altitude air," *Transp. Res. C, Emerg. Technol.*, vol. 122, Jan. 2021, Art. no. 102878, doi: 10.1016/j.trc.2020.102878.

[104] X. Li, L. Gong, X. Liu, F. Jiang, W. Shi, L. Fan, H. Gao, R. Li, and J. Xu, "Solving the last mile problem in logistics: A mobile edge computing and blockchain-based unmanned aerial vehicle delivery system," *Concurrency Comput. Pract. Exp.*, vol. 34, no. 7, p. e6068, 2022, doi: 10.1002/cpe.6068.

[105] H. Xu, W. Huang, Y. Zhou, D. Yang, M. Li, and Z. Han, "Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3107–3121, May 2021, doi: 10.1109/TWC.2020.3047496.

[106] A. Islam and S. Y. Shin, "BUS: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in Internet of Things," *IEEE Access*, vol. 7, pp. 103231–103249, 2019, doi: 10.1109/ACCESS.2019.2930774.

[107] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354, doi: 10.1016/j.jisa.2019.06.010.

[108] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 435, G. Brassard, Ed. New York, NY, USA: Springer, 1989, doi: 10.1007/0-387-34805-0_24.

[109] *Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL)*. Accessed: Jul. 21, 2022. [Online]. Available: https://github.com/miracl/MIRACL

[110] M. A. Khan, I. M. Qureshi, I. Ullah, S. Khan, F. Khanzada, and F. Noor, "An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing," *Electronics*, vol. 9, no. 1, p. 30, Dec. 2019, doi: 10.3390/electronics9010030.

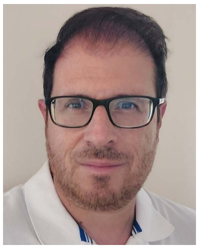
[111] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. Khanzada, H. Khattak, and M. A. Aziz, "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Inf. Syst.*, vol. 2020, Jul. 2020, Art. no. 8861947, doi: 10.1155/2020/8861947.

[112] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983, doi: 10.1109/TIT.1983.1056650.

[113] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 2045, B. Pfitzmann, Ed. Berlin, Germany: Springer, 2001, doi: 10.1007/3-540-44987-6_28.

[114] M. Yahuza, M. Y. I. Idris, A. W. A. Wahab, T. Nandy, I. B. Ahmedy, and R. Ramli, "An edge assisted secure lightweight authentication technique for safe communication on the Internet of Drones network," *IEEE Access*, vol. 9, pp. 31420–31440, 2021, doi: 10.1109/ACCESS.2021.3060420.

[115] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13621–13630, Nov. 2020, doi: 10.1109/TVT.2020.3018778.



**EMMANOUEL T. MICHAILIDIS** (Member, IEEE) was born in Athens, Greece. He received the M.Sc. degree in digital communications and networks from the Department of Digital Systems, University of Piraeus, Piraeus, Greece, in 2006, and the Ph.D. degree with specialization in "aerospace communication systems" from the University of Piraeus, in 2011. Since 2018, he has been an Adjunct Lecturer with the Department of Electrical and Electronics Engineering, School of Engineering, University of West Attica, Egaleo, Greece. Since 2021, he has been a Postdoctoral Researcher with the Department of Information and Communication Systems Engineering, University of the Aegean, Samos Island, Greece. He has published more than 50 scientific articles and received several best paper awards in his areas of research. His current research interests include the channel modeling and performance analysis of next-generation terrestrial wireless, aerial, and satellite communication systems.

**KONSTANTINOS MALIATSOS** graduated from the School of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Greece, in 2003. He received the M.B.A. degree from the Postgraduate Program "Technoeconomic Systems" (co-organized by NTUA, National and Kapodistrian University of Athens, and University of Piraeus), in 2005, and the Ph.D. degree in design, analysis and transmission techniques for cognitive radio systems, in 2011. In 2003, he began his collaboration with the Mobile Radio Communications Laboratory (NTUA) as an Engineer in various research projects. Since 2013, he collaborates with the Telecommunication Systems Laboratory, University of Piraeus, as a Senior Researcher in various projects, mainly EU-funded. In 2015, he co-founded the technology SME, FERON TECHNOLOGIES, in which he served as the Director of research and development programs. In 2020, he was elected as an Assistant Professor at the ICSD. He is currently an Assistant Professor at the Department of Information and Communication Systems Engineering (ICSD), University of the Aegean, Greece. He was/is actively involved in more than 17 European projects, with a key role in many of them (indicatively, technical manager, steering committee member, and WP leader). His research interests include MIMO systems, cognitive radio, information-theoretic security, vehicular communications, and risk modeling and analysis.

**DIMITRIOS N. SKOUTAS** (Senior Member, IEEE) received the Ph.D. degree in communication networks and the Dipl.-Eng (five-year degree) degree in electrical and computer engineering with a major in telecommunications. He currently holds the position of an Assistant Professor with the Department of Information and Communication Systems Engineering (ICSE), University of the Aegean, Greece. His research activities are currently focused on the development of cooperative transmission schemes that can be extended to multiple networks in a HetNet environment as well as on the IoT networks. He has also been keenly working on the areas of resource management and quality of service provisioning in mobile and wireless broadband networks, where he has proposed several algorithmic and architectural optimizations. He is a member of the Editorial Boards for *Wireless Networks* (Springer), *Journal of Wireless Communications and Networking* (EURASIP), and *Internet Technology Letters* (Wiley). He had previously served on the editorial boards for *Advances in Electrical Engineering* and *The Scientific World Journal* (subject area: Communications and Networking), both of which are published by Hindawi. He also serves on the technical program and organizing committees for several conferences.

**DEMOSTHENES VOUYIOUKAS** (Senior Member, IEEE) received the five-year Diploma and Ph.D. degrees in electrical and computer engineering and the Joint Engineering-Economics M.Sc. degree from the National Technical University of Athens (NTUA), in 1996, 2003, and 2004, respectively. He is currently a Professor and the Director of the Computer and Communication Systems Laboratory, Department of Information and Communication Systems Engineering, University of the Aegean, Greece. His research interests include mobile and wireless communication systems, channel characterization and propagation models, machine learning techniques for pathloss prediction, performance modeling of wireless networks, cooperative wideband systems with relays, UWB indoor localization techniques, UAV and aerial communications, next generation mobile and satellite networks, MIMO and 5G and beyond/6G technologies, and network security and privacy policies. In this area, he has over 130 publications in scientific journals, books, book chapters, and international conference proceedings. He is a member of the IEEE Communication Society of the Greek Section, a member of IFIP and ACM, and a member of the Technical Chamber of Greece.

**CHARALABOS SKIANIS** (Senior Member, IEEE) received the B.A. degree in physics from the University of Patras, Greece, and the Ph.D. degree in computer science from the University of Bradford, U.K. He is currently a Professor at the Department of Information and Communication Systems Engineering, University of the Aegean. His work has been published in magazines, conference proceedings, and book chapters, while it has been presented in numerous conferences and workshops. He has extensive experience in attracting funding and managing international consortia in the ecosystem of information, network and communication systems. He is a member of scientific and organizational committees for numerous conferences and workshops and has edited special publications for scientific journals. He is a member of the editorial/scientific committee of several journals, a member of professional communities, and an active reviewer in scientific journals and he participates and chairs international technical committees.

• • •