

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk and H. Song, "A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions," in *IEEE Transactions on Intelligent Transportation Systems*, 2022, doi: 10.1109/TITS.2022.3220043.

<https://doi.org/10.1109/TITS.2022.3220043>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions

Muhammad Adil¹, Member, IEEE, Mian Ahmad Jan², Senior Member, IEEE,
Yongxin Liu³, Senior Member, IEEE, Hussein Abulkasim⁴, Member, IEEE,
Ahmed Farouk⁵, Member, IEEE, and Houbing Song⁶, Senior Member, IEEE

Abstract—Unmanned aerial vehicles (UAVs) as an intermediary can offer an efficient and useful communication paradigm for different Internet of Things (IoT) applications. Following the operational capabilities of IoTs, this emerging technology could be extremely helpful in the area, where human access is not possible. Because IoT devices are employed in an infrastructure-less environment, where they communicate with each other via the wireless medium to share accumulated data in network topological order. However, the unstructured deployment with wireless and dynamic communication make them disclosed to various security threats, which need to be addressed for their efficient results. Therefore, the primary objective of this work is to present a comprehensive survey of the theoretical literature associated with security concerns of this emerging technology from 2015-to-2022. To follow up this, we have overviewed different security threats of UAV-aided IoT applications followed by their countermeasures techniques to identify the current challenges and requirements of this emerging technology paradigm that must be addressed by researchers, enterprise market, and industry stakeholders. In light of underscored constraints, we have highlighted the open security challenges that could be assumed a move forward step toward setting the future research insights. By doing this, we set a preface for the answer to a question, why this paper is needed in the presence of published review articles.

For novelty and uniqueness, we have performed a comparative analysis section-wise with rival papers to demonstrate that how this paper is different from them.

Index Terms—UAV-aided IoT application, different security threats, security challenges, authentication of UAVs and IoT, data privacy and preservation.

I. INTRODUCTION

NOWADAYS, the proliferation of the Internet of Things (IoT) applications revealed incredible results in several domains such as healthcare, agriculture, military operation, intelligent transportation, smart cities, smart homes, and many more [1], [2], [3]. With reliable results, the deployment of these applications is unhurriedly increasing into the locations, where humanistic access is not possible. To facilitate the communication of such inaccessible locations in the context of IoT applications, Unmanned Aerial Vehicles (UAV) can be used as an integrated technology [4], [5]. With integration, IoT devices are enabled to share their accumulated data with remote destination by means of UAVs, which generally plays the role of an intermediary. At present, UAV-aided-IoT applications technology has emerged in many traditional and new IoT applications. With their productivity, this technology is expected to be a game-changer in the future because it has the potential to improve government and concerned authorities' access to the places, where human access is not possible i.g. flood rescue operations, wildfire monitoring, secret military operations followed by natural avalanches and emergencies rescue operations, etc [6], [7]. Keeping in view the importance of this technology, it is pretty clear that the integration of UAVs and IoT applications can play a remarkable part to intensify the productivity of involved stakeholders and future wireless communication networks.

In UAV-aided-IoT applications, the employed IoT devices gather and share sophisticated information in the network, which is relevant to their assigned task. This information may vary from general to secret, therefore, the importance of authentication, data integrity, confidentiality, and privacy could be assumed as a fundamental factor, while designing, expanding, and integrating IoT technologies [8], [9]. Regrettably, the

Manuscript received 15 May 2022; revised 8 September 2022; accepted 1 November 2022. This work was supported by the National Science Foundation under Grant 2229975, Grant 2150213, and Grant 1956193. The Associate Editor for this article was L. Wang. (Corresponding author: Muhammad Adil.)

Muhammad Adil is with the Department of Computer Science and Engineering, University at Buffalo—The State University of New York, Buffalo, NY 14260 USA (e-mail: muhammad.adil@ieee.org).

Mian Ahmad Jan is with the Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan (e-mail: mianjan@awkum.edu.pk).

Yongxin Liu is with the Department of Mathematics, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA (e-mail: LIUY11@erau.edu).

Hussein Abulkasim is with the Cybersecurity Research Laboratory, Ted Rogers School of Information Technology Management, Toronto Metropolitan University, Toronto, ON M5B 2K3, Canada, and also with the Department of Computer Science, Faculty of Science, New Valley University, El-Kharga 71511, Egypt (e-mail: abulkasim@ryerson.ca).

Ahmed Farouk is with the Department of Computer Science, Faculty of Computers and Artificial Intelligence, South Valley University, Hurghada 83523, Egypt (e-mail: ahmed.farouk@sci.svu.edu.eg).

Houbing Song is with the Department of Information Systems, University of Maryland, Baltimore County, Baltimore, MD 21250 USA (e-mail: h.song@ieee.org).

Digital Object Identifier 10.1109/TITS.2022.3220043

1558-0016 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See <https://www.ieee.org/publications/rights/index.html> for more information.

forementioned security characteristic hasn't been addressed properly in many traditional IoT devices and particularly integrated systems such as UAV-aided IoT applications. In the last couple of years, apart from the productivity of UAV-aided IoT applications, the research community and market stakeholders also kept their eyes on the security risks, which are associated with this emerging technology. As we know, this technology is growing, and have expectedly deployment in sensitive applications such as military operation, wildfire, industrial processes in agriculture, intelligent transportation and many more. To exemplify, some devastating cybersecurity threats that can hamper the performance of UAV-aided-IoT applications include jamming attacks, black-hole attacks, denial of service attacks, flooding attacks, man-in-the-middle attacks, distributed denial service attacks, sink-hole attacks, packet injection attacks, forgery attacks, wormholes attacks, etc [10], [11], [12].

To make UAV-aided IoT applications more unassailable to cyber security threats, the security concerns of this emerging technology must be considered from the design stage [13]. Following this discussion, some good design hardware with security proof is still vulnerable to internal and external security threats, due to wide heterogeneity and communication environment [14], [15], [16]. Keeping in view the limited resources of IoT devices such as energy, computation, and communication capabilities makes these challenges more complicated. These limitations indeed depreciate the adaptability of standard security techniques, that can be productive against adversaries' anticipation in these networks.

To familiarize all stakeholders of UAV-aided IoT applications with the cybersecurity threats, countermeasures, and challenges, in this article, we present an up-to-date survey of the existing literature on security threats scenarios to acknowledge their weak aspects to researchers and enterprise market stakeholders. Furthermore, we will also emphasize on the security requirement of these integrated and constraints-oriented networks to identify the limitation of current literature.

The fundamental contributions of this article are summarized as below:

- 1) In the initial phase, we will give a brief introduction of the security threats that are associated with IoT applications and UAVs. Following this, we will also highlight and discuss some counteraction techniques that could be helpful to tackle the underscore security risks.
- 2) Next, after furnishing the fundamental summary of the security risk to IoT and UAVs, we will extend our discussion to UAV-aided IoT applications to examine the most prevalent authentication, data privacy and preservation schemes that had been used particularly for this integrated technology from 2015 to 2022.
- 3) Consequently, we will underline, discuss and evaluate some attacks and their countermeasure techniques that had been published in the literature to identify their flaws followed by the requirements of this emerging technology. Based on our evaluation, we will highlight the open research challenges to the research community and commercial market stakeholders for redressal.

- 4) Finally, we will move one step ahead to reasoning comparison of this work with the published review articles in this domain to claim its originality and novelty followed by the reply to the question of why this paper is required in presence of existing review papers. With this, we will highlight the conceivable future research directions that could be extremely beneficial in terms of setting security standards, authentication, authorization, access control, data preservation, etc, to achieve optimal results in this integrated technology.

The rest of the paper is managed as below: Section II evaluates different security risks that are associated with UAV-aided IoT applications, while Section III discusses the taxonomy of different security threats. In Section IV, we will discuss the contributions and limitation of existing review articles while Section V demonstrates the comparative analysis of our paper and existing review articles. Section VI, classifies the privacy and data preservation threats associated with UAV-aided IoT applications, whereas Section VII overviews the existing countermeasures techniques of different security threats concerning these networks. The open security challenges connected with these networks are highlighted in Section VIII, while the potential future research directions are discussed in Section IX. Section X, summarizes and concludes the paper.

II. INTRODUCTION OF SECURITY RISK IN IOTs AND UAVs

In the previous section, we have discussed the road map of this paper followed by the importance of IoT applications in the context of UAV's communication assistance. To continue, we have discussed the attacks risk of IoT, and UAV's that could be used simply and easily to break the security of utilized IoT devices and UAV's to capture realistic information of the employed network. Following this, herein, we would like to present a comprehensive overview of IoT and UAVs security requirements followed by different challenges that can hinder their adaptation to create a preprint for the debate of this paper that could be followed in the upcoming sections and subsections to familiarize all stakeholders with current security concerns of IoT and UAVs.

A. Security Requirements of UAV-Aided-IoT Applications

In this part, we will activate our discussion from the current taxonomy of IoT applications and UAVs security requirements by considering its various operational levels such as access control level security, information level security, functional and operational levels security [17], [18]. Figure 1, of the paper visualizes the security requirements of IoT and UAVs.

1) *Access Level Security*: Access level security deals with the policies of the network controlling and access gaining. In particular, it measures and handles the undermentioned security attributes and parameters:

a) *Access control level security*: Access control policies can play a very important role in any network because they ensure that only authorized users are allowed to authenticate with other legal devices followed by network access at the remote location for administrative purposes such as remote

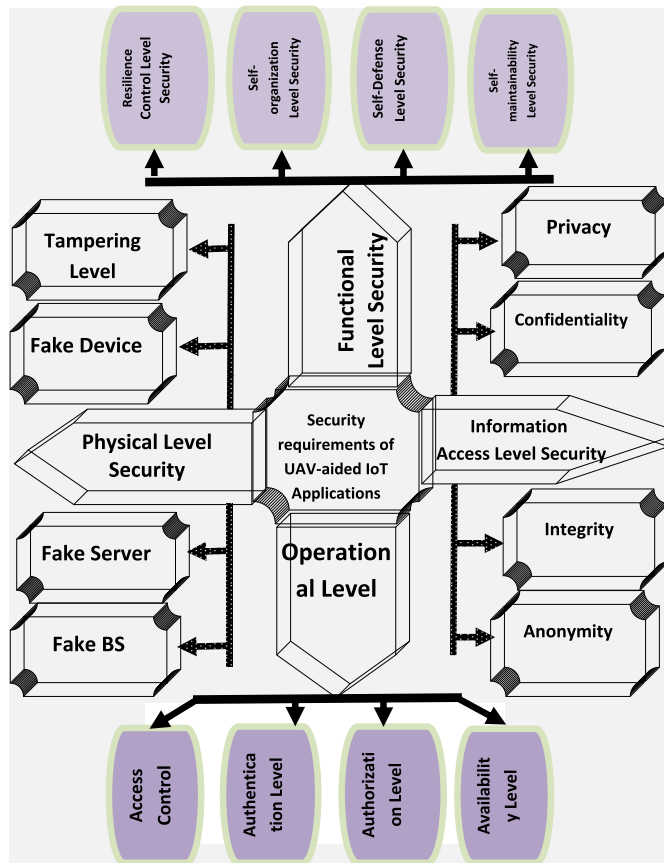


Fig. 1. Security requirement of UAV-aided-IoT applications.

reprogramming, etc [19]. Despite aforestated facts, the access control policies also have a direct role in the operational level security of UAV-aided IoT applications, because they enable the network administrator to allow different people associated with this technology to access the operational hardware, software, and characteristics of the network, and make necessary changes according to their requirements.

b) Authentication control level security: In access control policies the significance of authentication can not be neglected, because it inspects whether an IoT device or UAV has the right to access a network and communicate with other legitimate network entities. When a legal IoT device or UAV joins or registers in the network, it is assumed as the first step toward the legitimacy of the network it does [20]. To resolve security concerns of UAV-aided IoT devices, it is necessary to use robust authentication schemes in these networks. For example, authentication in terms of access level security ensures the things like that if all the IoT devices and UAVs are designed and configured by the same company with the same authentication parameters, then it is very easy for an adversary to hack one device and extract authentication parameters, and apply it on the other connected entities to compromise them.

c) Authorization control level security: In this type of access or authorization, the clients, administrators, and programmers have been given access to the network as per their participation and nature of working requirements. To explore, with this, It is ensured that who is authorized to authenticate

with other legitimate devices and get access to the employed network resources and services [21].

d) Availability control level security: In this type of access control, the transmission of data and messages must be secured against any third-party infiltration from source to destination points [22]. Moreover, it should be ensured to make available legitimate information to the end-users. Following this discussion, it is pertinent to mention that legal users must be enabled to participate in the network from anywhere to view and share information.

2) Information Level Security: In information level security, the undermentioned security requirements should be guaranteed in any UAV-aided IoT application in the context of this work.

a) Information integrity “security”: In information integrity, the information state is to be maintained as it is throughout the transmission process from source to destination [23]. With this, man-in-the-middle would not be able to alter the transmitted data during transmission. To continue, by doing this, the trust among all stakeholders should be maintained in terms of information/data security and the applicability of these applications should be extended to many domains.

b) Information confidentiality: In information confidentiality, the data must be maintained at a level, where the third parties would not be able to read it [24]. Following this, a trustworthy communication environment should be developed among IoT devices and UAVs to share protected information effectively. Apart from this, while maintaining the confidentiality of data, the replicated data and messages must also be identified and recognized.

c) Information privacy: Information privacy basically refers to the client’s/end user’s private data and information that must keep secret and should not be revealed throughout the transmission and data sharing of UAV-aided-IoT applications [25]. For an eavesdropper, it must be very challenging to guess the transmitted information as an identifiable one.

d) Information anonymity: In information anonymity, the identity of the transmitted data in terms of source and destination must be kept hidden or should be remained hidden to man-in-the-middle or third parties [26]. To explore, after launching this type of attack, an adversary blurs users or client-side data very efficiently and it is hard to distinguish between legal and illegal data in an operational network. Therefore, it is extremely important to hide data from third parties during end-to-end communication to avoid such attacks.

3) Functional and Operational Level Security: Functional and operational level security defines the undermentioned security requirements of UAV-aided IoT applications.

a) Functional and operational resilience: These types of security requirements refer to the network capability to process authentication and data preservation algorithm and ensure the security of employed IoT devices and UAVs [27]. Additionally, these are very helpful in case of attacks countering and network failures in the context of attack damage.

b) Functional and operational security parameters self organization: Self-organization in the context of functional and operational security concerns of IoT and UAVs signifies

TABLE I
DESIGN FEATURES AND DIFFERENCES

Description	Communication among IoT-to-IoT	Communication among IoT-to-UAV	Communication with UAV-to-UAV	Security Risk
Communication with mobility model	Random/Dynamic	2D/3D Trajectory-based	Mobility based with 2D/3D	Susceptibility to security risks (High)
Propagation Model	Stable and secure communication	Dynamic & secure communication with	Random and secure communication	Susceptibility to security risks (Average)
Communication density of IoT & UAVs	High Volume	Average Volume	Normal Volume	Susceptibility to security risks (High)
Network Topology	Static or Dynamic	Random	Dynamic	Susceptibility to security risks (Average)
Data volume and traffic	Very High	High	Normal	susceptibility to security risks (High)

the capability of a network to modify itself by keeping the operational parameters as it is, even if certain parts of the system fail due to malicious activities or periodic failures [28].

B. Security Risks With Respect to Communication of IoT and UAVs

In this segment of the paper, we would like to familiarize the reader with the basic dissimilarities between IoT and UAVs, before diving into the detailed discussion of security risks, we would like to familiarize the reader with the global positioning system (GPS) that has an influential role in these networks. Following this, mobile IoT applications such as mobile ad hoc networks (MANET), Intelligent Transportation systems (ITS), and Internet of vehicles (IoV) are commonly used GPS and satellite to ensure accurate communication among employed IoT devices and flying UAVs. Thereafter, we will extend our discussion to the security risk of this emerging technology. To continue, we will highlight the different security concerns that could be immensely useful, while evaluating or designing any security framework for UAV-aided-IoT applications. To do so, in Table I, we will demonstrate, that how much the IoTs and UAVs functionalities defer from each other. Moreover, Rashid et al. [27] present a detailed survey on the security aspects of UAV-aided IoT applications. In this article, the author's considered different communication vulnerability scenarios during the communication, interaction, and authentication of IoTs, UAV, and base station (BS) to highlight the risk statistics. Bera et al. [28] extend this discussion and highlighted some additional security threats that can destroy a well establish UAV-aided IoT network.

III. TAXONOMY OF UAV-AIDED IoT APPLICATIONS SECURITY THREATS

In this section, we will talk about the taxonomy of security threats despite the aforementioned security requirements to understand feasible security vulnerabilities and attacks that can hinder the communication process or network infrastructure of an employed UAV-aided IoT network. Following the open system interconnect (OSI) model, the network and communication architecture of a UAV-aided-IoT application can be divided into Edge Layer, Access Layer, and Application layers [29]. To continue, the edge layer security deals with the physical and media access control layer communication

and network security concerns. Likewise, the access layer is responsible to give access or establish connection among edge devices and network layer entities, where they will performs the role of a mediator such as a middle-ware layer for IoTs, UAVs and other involved stakeholders. Consequently, the application layer took over the responsibility and takes care of the security concerns of service-level interaction and data privacy, preservation, and communication. To explore this, we will present the taxonomy overview of the aforestated OSI model in the context of possible attacks that can be used to target UAV-aided-IoT applications.

A. Edge Layer Security Threats Taxonomy

Edge layer security deals with the end-side or user side devices, where an adversary attempts to launch physical attacks, channel jamming attacks, and tampering attacks to hijack the security of edge devices, and penetrate in the network [30]. The primary objective of these types of attacks is to leak the legitimate network data by analyzing side signals. With this, the attackers would be able to misuse the transmission power of the employed device followed by creating an artificial communication delay that can hamper the interconnected device's authentication process and encryption algorithms. Likewise, these types of attacks are used to attempt and understand the transmission power of legitimate devices and generate an alternative frequency transmission power to disturb the communication process. To tackle such kinds of attacks, differential power analysis could be used as an effective and sophisticated approach [31]. As mentioned in the preceding sentences, at the edge layer, IoTs and UAVs are also susceptible to hardware or physical attacks. By getting access to the network an attacker may misuse the resources of legitimate network components such as unavailability for the hop count communication, exit sleep cycle to drain their batteries, or jam their transmission channel [32].

B. Middle-Ware or Access Layer Security Threats Taxonomy

In UAV-aided IoT applications, the middle-ware or access layer attacks includes eavesdropping, sniffing, non-repudiation, routing, and packet injection attacks, etc [33]. To continue, in these types of attacks, an adversary also tries to spoof, misdirect or redirect the network legitimate traffic. To explore this topic a bit more, in [34], the authors discussed

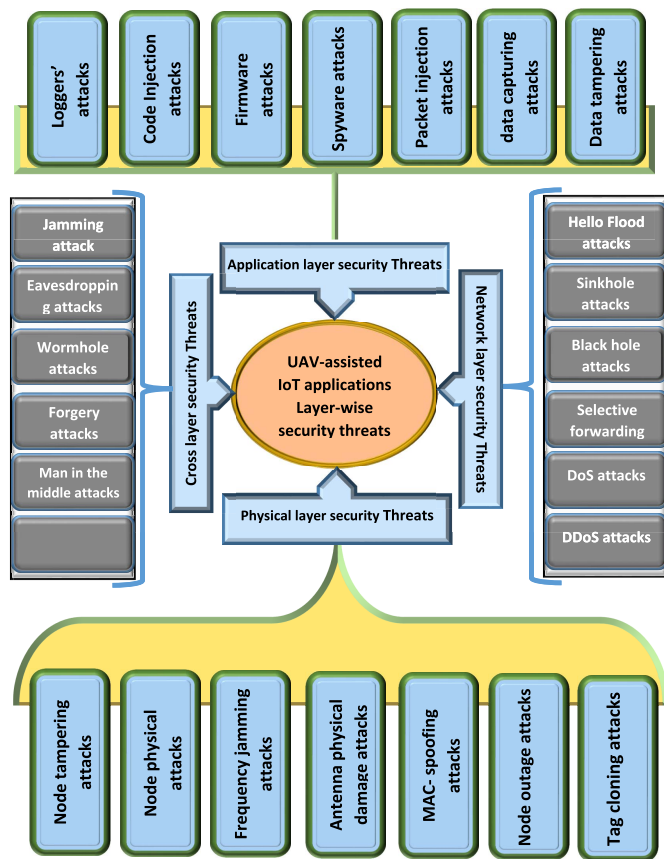


Fig. 2. Layer-wise security threats to UAV-assisted IoT applications.

the integration of UAVs and IoTs application in the context of middleware security threats. Moreover, the authors assumed a cellular network connected with fifth-generation technology to highlight channel side attacks, jamming attacks, and eavesdropping attacks, etc. In [35], this discussion was explored by authors and demonstrated that UAVs have the ability to fulfill the stakeholder's market need in a pervasive aspect and can work as an eye bird to achieve optimal results. Apart from this, they also acknowledged that these UAVs are vulnerable to various internal and external malicious threats that can hinder their performance, which need the research, academia, and enterprise market stakeholder attention for better countermeasures. Before diving into the detailed discussion, herein, first, we would like to visually represent layer-wise security threats of UAV-assisted IoT applications in figure.

C. Application Layer Security Threats Taxonomy

In this segment, we have talked about the application layer security of UAV-assisted IoT applications and their countermeasure schemes by taking into account blockchain technology. In [36], the authors explored to familiarize the readers and other involved stakeholders with the latest adopted counteractions schemes by considering blockchain technology. In the past, the software running on the devices was targeted by adversaries rather than communication technologies as they are happening presently [37]. These attacks target the integrity of the legitimate network algorithm and data such as

manipulation of ML algorithms to disturb the training model and produce irrelevant results. In [38], the authors presented a comprehensive survey regarding the security and vulnerability threats of UAV-aided IoT applications by taking into account the in-depth analysis of existing literature. Following this, the authors highlighted different authentication and data preservation schemes that had been used in the recent past to tackle to security threats of these networks. With this, they also underscore potential research directions that could be very useful to ensure D2D authentication, data privacy, and preservation. This discussion was extended in [39], and the author highlighted possible security threats of UAVs and IoTs in this emerging technology. Moreover, the authors considered various scenarios that how an adversary exploit the security of employed devices these devices.

D. Taxonomy of Security Threat Reducing Functionality

In these types of attacks, an adversary tries to launch an attack on a UAV-aided IoT application to intercept, destroy, or hamper the communication process and functionalities of legitimate devices [40]. To continue, in this type of attack, an adversary exploits the edge-side device's communication process. In [41], the authors talked about the limited communication range of UAV-aided IoT applications in the context of security threats. Furthermore, they extend their discussion to the computation and energy resources of these devices, which could be misused by an attacker to destroy the legitimate operation of this integrated technology. Consequently, they present a Dronemap Planner (DP) based service-oriented communication infrastructure to handle these challenges. Yazdinejad et al. [42] highlighted various security concerns of UAV-aided IoT applications that can degrade or reduce the functionalities of these devices.

E. Taxonomy of Security Threat Concerning Functionality Ignorance

In these types of attacks, the specific functionality of UAVs and IoT devices are ignored or hampered to degrade the communication process or network performance [43]. To continue, bonnet is a simple example of this type of attack, whereas an attacker gets control of the network through compromised UAVs or IoTs to misuse their resources in a meaningless way. Li et al. [44] proposed a Dyna-Q-based reinforcement learning algorithm for UAV-aided IoT applications utilizing UAV flight controller and SDN controller to tackle functionality-related security concerns of this emerging technology. In [45], the authors presented a detailed survey regarding the functional vulnerability threats of UAV-aided IoT applications utilizing Intrusion Detection Systems (IDS) in coordination with software analysis framework.

IV. COMPARATIVE SURVEY PAPERS

In this section, we discuss the existing review articles in the context of their pros and cons. Moreover, we will underline the contributions of these papers to identify their limitations, which could be considered as a footprint for our paper's

TABLE II
COMPARATIVE REVIEW ARTICLES

References	Contributions	Limitations
Chriki et al. [46]	In this paper, the authors present a comprehensive survey related to different challenges associated with UAV-aided IoT applications. To continue, the authors broadly overviewed various problems including security that can depreciate the performance of this emerging technology.	In this paper, the authors fails to present a concrete study about a particular issue including the security of UAV-aided IoT applications that could be helpful for the involved stakeholders to improve the performance or security of this integrated technology. Moreover, they emphasized on the superficial literature rather than concrete or particular domain.
Ilgi et al. [47]	In this paper, the authors discussed the security and privacy challenges associated with UAV-aided IoT applications. Moreover, they only emphasized on the channel sides attacks, which is not sufficient to safeguard these networks again various vulnerability threats.	To highlight the limitation of this paper, we have noted that the authors only focused on the channel side attacks, whereas the rest of the security threats to these networks are ignored.
Noor et al. [48]	In this paper, the authors discussed the communication, interoperability, and security challenges connected with UAV-aided IoT applications. Following this, the authors superficially touch most of the interrelated concepts of these networks, which lives this paper in a fuzzy state.	The limitation of this paper was the superficial evaluation of all interconnected networking aspects as the authors did not talk about a particular challenge.
McCoy et al. [49]	In this review article, the authors overviewed the most contemporary refinements of security vulnerabilities associated with UAV-aided IoT applications by taking into account SDN-enabled mitigation strategies. Furthermore, the writers solely discussed the usefulness of this technology to counter different security threats in operational networks.	The limitation of this paper was that the authors only consider SDN-based authentication, validation, privacy, and data preservation scenarios, whereas the rest of the authentication and countermeasure techniques were ignored.
Liu et al. [50]	In this paper, the authors discussed the hurdles associated with the Space-air-ground integrated networks such as UAV aided IoT applications. With the emergence of this technology, many communication and security challenges arose during the integration phase, which needs to be addressed by the research community and enterprise market stakeholders.	In this work, the authors only introduced the security concerns of UAV-aided IoT applications, which is not sufficient to take preventive measures against different security threats.
Vangala et al. [51]	In this paper, the authors present a rigorous literature review of block-chain-enabled UAV-aided IoT applications deployed in the agriculture sector. Moreover, they highlighted the security concerns of this integrated technology in the context of blockchain-based communication infrastructure.	In this paper, the authors discussed the security concerns of UAV-aided IoT applications in the context of blockchain technology. Following this, the authors considered the authentication aspects of these networks in a decentralized environment.
Qiu et al. [52]	In this survey article, the authors discussed the security concerns related to operator perspective followed by spectrum trading in the context of blockchain-based UAV-aided IoT applications.	In this paper, the authors only considered operator's and spectrum security concerns, while the physical layer and application layer security concerns were ignored, which are the basic need of these networks.
Li et al. [53]	In this survey paper, the authors discussed the security challenges of UAV-aided IoT applications in the context of physical-layer security (PLS). Moreover, they have elaborated various existing authentication and data preservation by particularly considering the physical layer security of this integrating technology.	To elaborate on the limitations of this work, the authors only focused on the PLS and they did not address and highlighted the security challenges network layers and transmission channel.
Wu et al. [54]	In this review paper, the author follows reference [53] discussion and highlighted various PLS challenges that can destroy the legitimate operation of UAV-aided IoT applications.	In this work, the authors mentioned eavesdropping and man-in-the-middle attacks are not very damaging for these networks, but it has some serious impact on the performance of these networks. Therefore, we cannot ignore their importance and consequences in any network.

future research directions. Following these limitations, we will concentrate on relevant literature that how these challenges can be addressed in UAV-aided IoT applications. To continue, we will use this foundation to set future research directions that could be capable to tackle the present security challenges of UAV-aided IoT applications. Table II, contains the present review articles associated with this emerging technology.

V. NOVELTY COMPARATIVE ANALYSIS WITH EXISTING SURVEY PAPERS

In this section, we will exemplify, how our survey paper is distinguishable from the existing review articles associated with security aspects of UAV-aided IoT applications. For this, we have added Table III in the paper, whereas we have performed comparative analysis of different factors that had been discussed in this paper followed by rival review articles. By doing this, we would be in the position to acknowledge the

academia, organization, governments, industry, and enterprise market stakeholders that how our paper is different from the existing ones followed by a response to the query why this review article is novel, in-time and needed in the presence of them. After this, we will focus on the relevant literature followed by the distinguishing factors of our paper to present a complete package to all engaged stakeholders working on the security facets of UAV-aided IoT applications. We are pretty sure that after reading this review article, the people working in this domain will be capable to deal with the existing open challenges of this emerging technology, as we have covered all the aspects of security concerns of these integrated networks with relevant literature. Furthermore, we have highlighted potential research directions that could be used as a move forward step in the redressal of security challenges of these applications. Finally, we would acknowledge that after reading this paper the people working in this domain will find most

of the security concerns and their solutions under one shallow of this article.

VI. SECURITY THREAT BASED DATA PRIVACY AND PRESERVATION CLASSIFICATION

In this section, we will outline the primary security, authentication, and data privacy and preservation threats. Following this, we will highlight the origin of these threats in the context layer-wise model such as OSI (open system interconnection) by taking into account UAV-aided IoT applications communication and interconnection perspectives. To continue this discussion, we go through the most recently published literature to highlight existing security challenges by following the requirements of this emerging technology.

A. Hardware and Software Injection Attacks on UAV-Aided IoT Applications

In these types of attacks, an attacker can add or inject unauthorized software or hardware component in the network at the client-side or application-side to get access to the network and disrupt the legitimate communication process [55], [56]. With this, an adversary is able to use the network's legitimate services and resources to undertake disruptive activity that can hamper the legal operation of the network such as authentication process, data privacy, fake data request, etc. To continue this discussion, we know that there are several types of hardware injection attacks that can be classified as below:

1) *IoT and UAV Replication Attack*: In this type of attack, an adversary insinuates or introduces new malicious IoT devices into the network. Following this, an adversary device initiates a fake route request to interact with genuine devices using the allowed devices IDs, which is the replica of the authorized devices [57]. With this, an adversary would be able to deteriorate, update, steal, or redirect communicating packets arriving at the malicious IoT device. To tackle this, node-revocation and node replica protocols could be used as an influential weapon to detect such malicious devices in the network [58], [59].

2) *IoT and UAV Hardware Trojan Attack*: In this type of attack, an adversary gets unauthorized access to integrated circuits (IC) of IoT and UAV devices. By doing this, the attackers are enabled to manipulate the hardware, software, data, and operating system [60]. To explore this, we know that there are two types of trojan attacks, which can be exercised on UAV-aided IoT applications [61]. First and foremost trojan attacks include externally activated trojan attacks, in which an attacker uses the antenna of legitimate IoTs and UAVs to interact with them and hijack their security to participate in the network. Secondly, trojan attacks can be activated internally, whereas the attacker would be enabled to change the functionality of IoTs and UAVs ICs by triggering rules to achieve desired results [62]. Likewise, camouflage is another type of attack, which belongs to the trojan family. In this type of attack, an attacker injects malicious devices into the network, which act just like legitimate devices to transmit, process, receive, store and share information in the network [63]. To follow this

discussion, the network corrupted or malicious IoT and UAVs could be used by an attacker to gain unauthorized access to the network, and inject deceitful information to disturb the legitimate communication process [64].

3) *DoS and DDoS Attacks on IoTs and UAVs*: Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks are the most common and well-known that had been exercised by attackers in the recent past to hijack the security of IoT applications. These types of attacks include sleep deprivation, misuse of legitimate devices resources, battery draining, and infuriating attacks, etc [65], [66]. To continue, in a sleep deprivation attack, an attacker crushes the IoTs and UAVs with an unwanted set of packets. This kind of attack is very difficult to detect in an operational UAV-aided IoT network. Apart from a sleep deprivation attack, an attacker also targets the battery power of legitimate IoTs during the unauthorized access to exhausted them in a meaningless way, which will incur IoT device failure [67]. To elaborate, on the communication level, the most common type of DoS and DDoS is a transmission channel jamming attack, which includes continuous jamming or partial jamming of legitimate channels.

4) *Physical/Tampering Attacks on IoTs and UAVs*: In this type of attack, an attacker gains physical access to the IoTs or UAVs for the sake of tampering with their authentication parameters [68]. Once, the authentication parameters of legitimate IoTs and UAVs are tampered, then, the whole communication process of the UAV-aided IoT network becomes vulnerable to many security threats. For example, let's assume an adversary gets access to the sensitive cryptographic information of a legal device and alters this information, then the legitimate device of the network would be treated as a malicious device. How costly this kind of attack could be in emerging technology like UAV-aided IoT applications, if proper preventive techniques is not in place to handle them or detect them before any mishap occurrence.

5) *Eavesdropping/Sniffing Attacks on IoTs and UAVs*: In this type of attack, an adversary intercepts the communication channel and starts listening to the private conversation of legitimate devices followed by the extraction of secret information such as private keys, passwords, usernames, etc, [69]. To continue this, if an attacker sniffs legal packets, he can use the authentication parameters to illegally enter into the network, because these packets contain access control information of IoTs and UAVs, such as device configuration, devices identity, and passwords, etc. In [70], the authors proposed an independently programmable packet processor routing protocol for UAV-aided IoT applications to tackle the issue of eavesdropping attacks. In this protocol, the authors used a packet evaluation mechanism in the terms of first, second, and third-party defense lines to effectively detect these attacks.

6) *Non-Network/Side-Channel Attacks on IoTs and UAVs*: These types of attacks can be launched on IoTs and UAVs to reveal critical information, even, if they are not participating in the transmission or communication process of the network [71]. For example, in digital healthcare, the detection of well-known acoustic or electromagnetic signals from

TABLE III
CONTRIBUTING FACTORS COMPARATIVE ANALYSIS WITH STATE-OF-THE-ART REVIEW ARTICLES CONSIDERED/INCLUDED (✓), NOT CONSIDERED/INCLUDED ⊗, PARTIAL CONSIDERED/INCLUDED ⊖

Description of Differ-ent Factors	Chriki et al. [46]	Ilgi et al. [47]	Noor et al. [48]	McCoy et al. [49]	Liu et al. [50]	Vangala et al. [51]	Qiu et al. [52]	Li et al. [53]	Our arti-cle
Security Requirements									
Access Level Security	⊗	✓	⊖	⊗	✓	⊖	⊗	✓	✓
Authentication Control	⊗	✓	⊖	×	✓	✓	✓	⊖	✓
Level Security									
Authorization Control	✓	✓	✓	✓	✓	⊖	⊖	✓	✓
Level Security									
Availability Control	⊖	✓	⊖	✓	⊖	⊖	✓	⊖	✓
Level Security									
Information Level Security	✓	⊖	✓	✓	✓	⊖	⊗	✓	✓
Information Confidentiality	⊖	✓	⊖	⊗	⊗	✓	✓	⊗	✓
Information Privacy & Preservation	✓	⊗	✓	✓	✓	✓	✓	✓	✓
Information Anonymity	⊗	⊗	⊖	✓	⊖	⊗	⊗	⊖	✓
Functional & Operational Level Security	⊖	⊗	⊖	✓	⊗	⊖	✓	✓	✓
Functional and Operational Resilience	✓	⊖	✓	⊗	✓	✓	⊖	⊗	✓
Functional security during Self Organization	✓	⊗	⊖	⊗	⊖	⊖	⊗	⊖	✓
Taxonomy of security threats									
Edge Layer Security	✓	⊖	✓	⊖	✓	⊖	✓	⊗	✓
Middle-ware Layer Security	⊖	⊗	⊖	✓	⊖	✓	⊗	✓	✓
Application Layer Security	⊖	✓	✓	⊖	✓	⊖	✓	✓	✓
Functional Security	⊖	✓	⊖	⊗	✓	✓	⊖	✓	✓
Data and Privacy preservation and classification									
Hardware & Software Attacks	⊖	⊖	✓	✓	⊖	✓	⊖	✓	✓
Replication Attack	⊗	✓	⊖	⊗	✓	⊗	⊖	⊖	✓
Hardware Trojan Attack	✓	✓	⊖	✓	⊖	✓	✓	⊗	✓
Attacks									
DoS and DDoS Attacks	✓	✓	✓	✓	✓	✓	⊖	✓	✓
Routing attacks	⊖	✓	✓	⊖	✓	⊖	✓	⊗	✓
Physical/Tampering Attacks	✓	✓	✓	✓	✓	✓	⊖	✓	✓
Spoofing attacks	✓	⊖	⊗	⊖	✓	⊗	⊖	✓	✓
Forgery Attacks	⊗	⊗	⊖	✓	⊖	✓	⊗	⊖	✓
Replay/Freshness Attacks	⊗	✓	⊗	⊖	×	⊖	✓	⊗	✓
Countermeasure Schemes									
Hardware/Software Countermeasures	✓	✓	✓	⊖	✓	⊖	✓	✓	✓
Policy-Based Countermeasure	⊗	⊖	⊗	⊗	⊖	⊗	⊖	⊗	✓
Firmware based Countermeasures	⊖	⊗	⊖	✓	⊗	✓	⊖	✓	✓
Routing Protocols based Countermeasures	✓	✓	✓	⊖	✓	⊖	✓	✓	✓
Data De-Patterning based Countermeasures	⊗	⊗	⊖	⊗	⊖	⊗	⊖	✓	✓
Information Flooding Attacks Countermeasure	⊗	✓	⊗	✓	⊗	✓	⊖	✓	✓
Future Research Directions									
Machine and Deep Learning based solutions	⊖	⊖	✓	⊗	⊗	⊖	⊖	⊖	✓
Channel based Solution	✓	⊗	⊖	⊖	⊖	⊗	⊖	⊗	✓
Access Control and Authentication based Solutions	⊖	✓	⊖	⊖	✓	⊗	⊖	⊗	✓
Software/Coding Based Solutions	⊗	⊖	⊗	⊗	⊖	⊗	⊗	⊖	✓
Standard Based Solutions	⊗	×	⊖	⊗	⊗	⊗	⊖	⊗	✓

patient embedded IoT devices or medical tools might result in major privacy difficulties when sharing essential information of patient disease and tools in the network.

7) *Forgery Attacks on IoTs and UAVs*: In these types of attacks, an adversary inserts fresh bogus and fake data or routes in the receiver or transmitter that are disastrous and

can cause network damage or failure [72]. To elaborate, an adversary also used additional tactics to insert malicious data packets or manipulate legitimate data in the network to hinder reliable operation between IoTs, UAVs, and other involved commuting entities.

8) *Routing Attacks on IoTs and UAVs*: In these types of attacks, an attacker modifies the routing information of a legitimate UAV-aided IoT network to divert the traffic in a misleading direction or even dump the fair data packets [73]. Blackhole attack is an example of this kind of attack, in which the attacker uses certain tactics to drain all network traffic and disrupt the legitimate operation [74]. Gray Hole is another routing attack, whereas an attacker target certain packets of an operational network to disturb the performance of the network [75]. Following the topic of routing attacks on UAV-aided IoT applications, the devastation of Hello Flood attacks can not be ignored, because an attacker broadcasts fake 'HELLO PACKETS' in the network to create traffic overhead and degrade the network performance [76].

9) *Replay/Freshness Attacks on IoTs and UAVs*: In this type of attack, an adversary capture or record the legitimate traffic/data of the UAV-aided IoT network for a particular period, and then misuse the extracted information by doing activities like amendments in historical data or tampering in the current timestamp of a message [77].

VII. AUTHENTICATION AND DATA PRESERVATION COUNTERMEASURE TECHNIQUES CLASSIFICATION

In this section, we will discuss different countermeasure techniques that had been used in the recent past to combat UAV-aided IoT applications from various external and internal threats. Before diving into this discussion, we would like to acknowledge that in UAV-aided IoT applications, IoTs, UAVs, and other network components collect, process, and store crucial data, which need secure communication infrastructure to maintain the trust of all stakeholders. For this, the literature offers some prominent cryptographic, authentication, data privacy, and preservation schemes, which are summarized in figure 3.

A. Countermeasure of Hardware/Software Malicious Injection Attacks

In the literature, it has been demonstrated that IoTs and UAVs are vulnerable to a variety of hardware and software security threats, including buffer overflow attacks. To tackle hardware and software architectural security threats in UAV-aided IoT applications, Al-Omary et al. [78], present a detailed survey of many susceptibilities threats with their countermeasure techniques. Xu et al. [79] proposed a hardware architecture enhanced model for IoTs to detect and handle buffer overflow attacks in the applications of these devices. This model works in two parts such as one part monitors and verifies the information before its execution, while the other one validates the secure tag to ensure the legitimacy of the communication. To continue, Side-Channel Signal Analysis (SCA) could be used as an effective tool to detect hardware

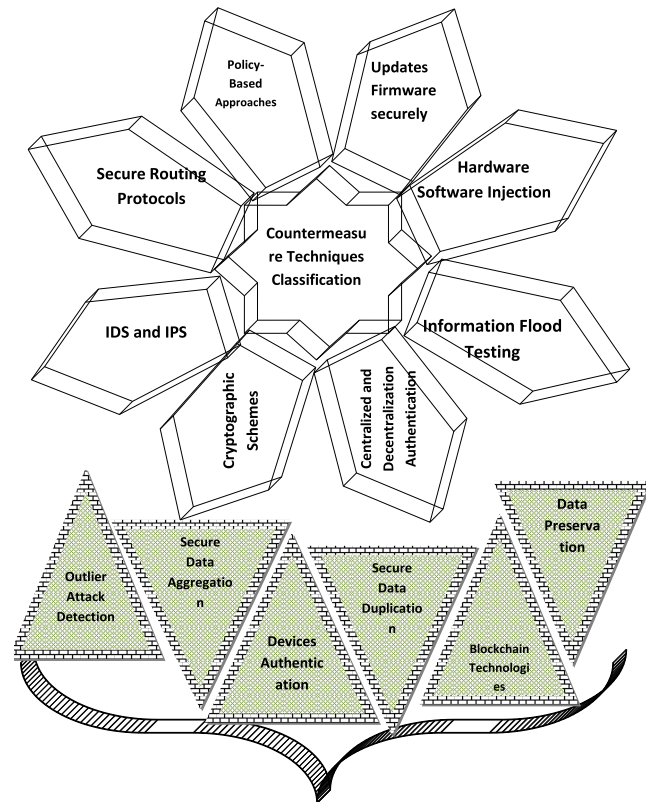


Fig. 3. UAV-aided IoT applications security countermeasures.

trojan followed by malicious firmware used for software hijacking [80].

In [81], the authors used trojan activation methods (TAM), to deal with hardware attacks of IoTs and UAVs by comparing the outputs of devices, communication behavior, and side-channel leakages. This model was checked in the real-time circuit environment by inserting Trojan in the circuits to evaluates its behavior with Trojan-free circuits in the context of results comparison. In [82], the authors demonstrated that circuit modification of IoTs and UAVs is another effective technique that could be used to counter hardware attacks of these networks. In this article, the authors also acknowledged the effectiveness of this model against different types of hardware and software attacks such as external adversary destruction attacks, tampering attacks, and Trojan attacks, etc. In [83], the authors propose a proof-of-work (PoW) based lightweight data preservation scheme for UAV-aided IoT applications to address software attacks utilizing reconfigurable hardware primitives. To continue, the authors used the hash function as an additional constitute to ensure secure communication in a blockchain network. Following this discussion, Zhang et al. [84], proposed a Random Set-based Obfuscation (RSO) authentication model for UAV-aided IoT applications to counter machine learning attacks. In this model, the author's primary objective was to tackle the threats associated with PUF of legitimate devices in these networks.

B. Policy-Based Countermeasure Schemes

In policy-based countermeasure schemes, various traffic rules and data policies to detect illegal traffic in the network.

Moreover, these rules and policies are very effective to ensure the legitimacy of the network followed by reporting of the security breaches. Reference [85], suggests an access control-based security architecture for the healthcare IoT networks. In this model, the author's used a fine-grained-based access mechanism for validation of authorized clients to use the network services and resources. In [86], the authors proposed a ticket-based authentication model for an integrated network of mobile devices and IoTs. Furthermore, the authors claimed that this model can be used in UAV-aided IoT applications because its validity is checked in a mobile and static communication environment. Following this discussion, Karimibiuki et al. [87] suggested a dynamic Policy-based Access Control (DynPolAC) mechanism for mobile IoT networks to resolve the security concerns of these networks effectively. References [88], [99], [90], presents various policy-based approaches to address the security concerns of UAV-aided IoT applications. With this, the author's identified challenges, which can hamper the performance of UAV-IoT applications. Moreover, they also discussed the requirements of this integrated technology, which is very helpful to set future research directions for these networks in the context of policy-based countermeasure data preservation schemes.

C. Firmware Securely Updating Schemes

In this type of countermeasure includes a reliable firmware update of employed UAV-aided-IoT applications either remotely or statically automatically or manually. In [91], the authors proposed a secure PUSH-based model for IoT devices' firmware updates in the blockchain networks. In this model, the firmware up-gradation or updates took place after proper validation and verification process. Zhao et al. [92] proposed a double authentication signature scheme for IoT devices software updates utilizing decentralized network infrastructure. Lu et al. [93], proposed a distributed membership-based firmware update mechanism for blockchain-enabled IoT networks to address the security of concerns of these networks during the IoTs firmware update and upgrade process. To continue this topic, Lo et al. [94], proposed a Message Queuing Telemetry Transport (MQTT) based secure communication framework for IoTs firmware updates in a distributed environment. To elaborate on this discussion, various countermeasure techniques related to the firmware update and upgrade security concerns of IoTs and UAVs are discussed in survey articles [95], [96], [97].

D. Secure and Reliable Routing Protocols

To address and counter security threats against routing protocols and reliable communication in UAV-aided IoT applications, the literature contains various algorithms that had been used to secure these networks. In [98], the authors proposed an authentication and encryption model for UAV-aided IoT applications utilizing eligibility weight function (EWF) to ensure the validation of participating devices and transmitted data. Following this, the author's in [99] presented a comprehensive review of secure routing protocols of UAV-aided IoT applications by considering Low Power and Lossy Networks (RPL) algorithm framework. To continue, Hammi et al. [100]

proposed a secure lightweight routing protocol for UAV-aided IoT applications utilizing a multipath communication infrastructure. In this model, the author's considered two events such as mobility and uncooperative behavior of participating devices to maintain the performance reliability of the network. In [101], the authors present a detailed survey of routing protocols in the context of Disruption Tolerant Networking (DTN) by assuming UAV-aided IoT applications. Furthermore, the authors talked about the current state of the multicasting routing algorithm in the connection of DTN that are targeted and can be targeted by adversaries in an operational network. References [102], [103], [104], presents some important review articles that discussed the security concerns of UAV-aided IoT applications followed by their countermeasure to address them effectively and achieve better results.

E. Intrusion Detection System (IDS), Firewalls, and Intrusion Prevention System (IPS)

In any network, such as wired or wireless and particularly UAV-aided IoT applications, the importance of IDS, Firewalls and IPS cannot be ignored, because of their effective results against various security threats. In [105], it has been discussed that these devices are used in the second line of defense to counter possible security threats such as communication links monitoring, network operation monitoring, routing attacks, monitoring, and reporting of suspicious activities, etc. Pundir et al. [106] extend this discussion and present a comprehensive survey on the security challenges of IDS and IPS in the context of UAV-aided IoT applications. Moreover, the authors also highlighted the possible future research directions that could very useful to address these challenges. In [107], the authors proposed an IDS-based secure communication architecture for UAV-aided IoT applications by creating a trust evaluation framework followed by a balanced dynamics-based service-oriented model. In survey articles [108], [109], [110], the authors discussed the nature of vulnerabilities threats and suggested various technologies such as different types of firewalls, IDS, IPS, etc, that can be productive against them.

F. Cryptographic-Based Countermeasure Schemes

Strong and persuasive encryption countermeasures strategies in UAV-aided IoT applications are very useful to tackle various security threats such as eavesdropping and routing attacks. To follow this topic, the literature contain several encryption/decryption techniques that had been used to counter different data privacy and preservation issues in these networks. To various external security threats associated with data privacy of UAV-aided IoT application, Islam et al. [111] presents a blockchain based data privacy and preservation framework for these applications utilizing mobile edge computing network infrastructure. Wang et al. [112] extend this discussion and proposed a cluster head selection-based secure data sharing framework for UAV-aided IoT applications. References [113], [114], [115], review articles demonstrate various data encryption and decryption schemes that had been used in the recent past for combat UAV-aided IoT applications

against several security threats. In [116], the writer suggested a secure data sharing model for UAV-aided-IoT applications utilizing both public and private key encryption techniques. In this model, the authors used a search technique to allow authorized devices to authenticate and share data securely. In [117], the authors described an architecture-based data preservation framework employing proxy notion for UAV-aided applications. In this framework, the legitimate devices are enabled to use proxy notion through abstraction and ensure the integrity of data in the network.

G. De-Patterning Data Attacks Countermeasure

In these types of countermeasures, malicious bogus are countered through different security techniques in UAV-aided IoT applications. In contrast, an attacker uses fake bogus packets in the network to modify legitimate traffic patterns and destroy the communication process. To handle these kinds of issues in UAV-aided IoT applications, Kerrache et al. [118], proposed an intelligent adaptive detection technique to evaluate the behaviors of the network traffic, and identify malicious bogus and packets. This discussion was followed by Rahman et al. [119], and proposed an intrusion detection system utilizing machine learning algorithms to detect illegal network traffic at the micro-controller level of IoTs, UAVs, and other involved network entities. References [120], [121], also suggested different data pattern detection models to tackle packet modification issues in UAV-aided IoT applications.

H. Information Flooding Attacks Countermeasure

Information flooding countermeasures play a pivotal role to secure employed UAV-aided IoT applications against various external attacks. For this, Oubbati et al. [122], proposed an efficient routing algorithm based on a flooding approach to ensure the legitimacy of network traffic in UAV-aided vehicles network in smart cities. In this model, the authors facilitate the existing vehicular network of smart cities with the help of UAVs to improve the communication infrastructure and maintain data integrity and confidentiality. In [123], an intelligent security model was proposed for the multi-UAVs to evaluate network traffic and identify information flooding attacks. In this article, the author used a tree-based attack-defense approach for data analysis of interconnected UAVs networks to identify information anomalies. Fitwi et al. [124], proposed a mobile agent-based secure data exchange communication framework for UAV-aided IoT applications. In this model, an agent administrator randomly sends clones packets from a secure mobile agent (SMA) to employed IoT devices and or drones to validate and verify their legitimacy.

I. Secure Data De-Duplication Countermeasure

In UAV-aided IoT applications, the removal of redundant data from network traffic securely can improve the performance of the employed network up to a significant level. With the existence of redundant data in the network, the transmission bandwidth is utilized in a meaningless way and assumed as an intentional toward depreciating the network

performance. Sharma et al. [125], proposed a hybrid technique working on the task allocation and secure duplication of UAV-aided IoT applications utilizing transport layer protocols. In this model, the IoT devices and UAVs use their build-in filter to analyze network traffic for redundancy and mitigate concern security threats. Reference [126], suggests a hybrid-stream model for big data analytics by considering the four aspects of the network such as data classification, data pre-processing, data recognition, and reduction. In addition, the authors used a multi-dimensional Convolution Neural Network (CNN) to assess and evaluate each upcoming packet, and eliminate or discard unimportant frames from legitimate traffic with the help of a decision-making algorithm.

J. Interoperable Technologies Vulnerabilities Threats and Countermeasures Techniques

In this subsection, we will follow our discussion of different security threats and their countermeasure to present a complete package to the academia and industry enterprise market stakeholders to address these problems in UAV-aided IoT applications. Although, we are aware of the fact that it is very hard to cover all existing literature associated with the security susceptibility and their countermeasures, but we have discussed the most prevailing and devastating attacks that had been used against UAV-aided IoT applications and discussed their mitigations techniques to maintain the trust of all involved stakeholders. To continue, we will extend our conversation to the interoperability threats and countermeasure of UAV-aided IoT applications. For this, we have used Table IV. In Table V, we have organized attacks related to Table IV interoperable technologies.

VIII. OPEN SECURITY CHALLENGES

Despite the fact that the literature suggests many countermeasure approaches to tackle the security hurdles in UAV-aided IoT applications, but somehow, they fail to manipulate this issue effectively. In Table V, we have demonstrated various security attacks that had been used in the recent past to target UAV-aided IoT applications and even traditional IoT applications. Figure 4, summarizes these challenges, which need enterprise market stakeholders, industry stakeholders, IoT and UAVs hardware producers, and research community working in this domain.

A. Challenge 1

From Table IV, we can undoubtedly observe that Zigbee, LTE, Wi-Fi & Wi-Max technology, which has a great role in the interoperability of UAV-aided-IoT applications suffer against various attacks that are summarized comprehensively. To follow this, we elaborated on the different attacks that are associated with these technology in terms of percentage probability. To continue, we know the consequences of these disruptive attacks particularly connected with these technologies, but we are also aware of the various countermeasure techniques that had been used to mitigate these attacks. However, these countermeasure techniques offer some subjective influences to IoT devices in terms of transmission power

TABLE IV
INTEROPERABILITY TECHNOLOGIES VULNERABILITIES THREATS CLASSIFICATIONS

Name of Technology	Zigbee, LTE, Wi-Fi & Wi-Max	LoWPan, LoRaWAN & CoAP	SHERPA standard & Path planning
Access Control Level Threat	In [127-129], various access level security threats are highlighted that can degrade the performance of Zigbee, LTE, Wi-Fi & Wi-Max connected UAV-aided IoT applications.	These are very prominent technologies that play a considerable role in the interoperability and interconnectivity of UAVs and IoTs. In contrast to the importance of this technology, it has vulnerabilities issues at access level, as mentioned in [130-132].	Integrated networks are vulnerable to SHERPA & Path planning threats, whereas an attacker compromises the legitimate UAV-aided IoT network, and tamper the access level functionality to misguide traffic, authentication, authorization, etc. [133-135].
Information Level Threats	In these types of attacks, an attacker get unauthorized access to the legitimate UAV-aided IoT network to tamper the hardware and legal operation of these networks [136-138].	LoWPan, LoRaWAN & CoAP play an incredible role in the integration and interconnectivity of UAV-aided applications, but it also offers various information level security threats that can destroy the performance of these applications [139-142].	In the recent past, eavesdropping and man-in-the-middle had been used as a weapon against information level security countermeasure in the context of SHERPA standard & Path planning hijacking to disrupt the legitimate operation of UAV-aided IoT applications [143-145].
Functional Level Threat	In these types of attacks, an adversary compromises the Zigbee, Wi-Fi, Wi-Max & LTE technology in the application layer, and penetrates in the legitimate UAV-aided IoT network [146-147].	In the hijacking of LoWPan, LoRaWAN & CoAP, an attacker uses the same tactics of routing protocols hijacking to compromise an employed UAV-aided IoT network at application layer [148-149].	Functional level security threats of UAV-aided IoT application in the context of SHERPA & Path planning are highlighted and discussed in [150-151]

TABLE V
DIFFERENT TYPES OF ATTACKS THAT HAD BEEN USED AGAINST TABLE IV INTEROPERABLE TECHNOLOGIES

Name of Technology	Zigbee, LTE, Wi-Fi & Wi-Max	LoWPan, LoRaWAN & CoAP	SHERPA standard & Path planning
Key Compromised attacks	Extremely High reported in the literature	With high rate routing protocols has been targeted for these attacks	Low rate of attacks has been noted these standard against key compromises.
Password Guessing Attacks	Probability Extremely High	Probability High	Probability Low, as discussed in the literature
DoS & DDoS attacks	With high probability these types of attacks had been recorded	With high probability these types of attacks had been recorded	Low Probability
Black-hole & Wormhole attacks	High Probability	High Probability	Low Probability
Forgery Attacks	Partial Attack Probability had been noted	High Attack Probability had been noted	High Attack Probability had been noted
Jamming Attacks	Partial Attack Probability had been noted	Partial Attack Probability had been noted	High Attack Probability had been noted
Eavesdropping Attacks	Partial Attack Probability had been noted	Partial Attack Probability had been noted	High Attack Probability had been noted
Spoofing Attacks	Had been launched with high probability	Had been launched with high probability	Had been launched with low probability

and computation resource to process an extensive number of forged packets and mitigate their intervention in the legitimate network. Therefore, the utilization of complex authentication techniques can hinder the performance of these networks by two factors such as hardware support and high computations. To manage this issue, the IoTs and UAVs hardware producers (processing chip) and research community are acknowledged to design lightweight authentication schemes for UAV-aided IoT applications that could be computation friendly.

B. Challenge 2

Consequently in Table V, we have highlighted the different attacks that had been used against routing protocols of UAV-aided IoT applications to compromise their security. After compromising the legitimate network, an adversary add supplementary information to the transmitted packets of legal devices to interrupt the authentication process, misdirect the network traffic, create network overhead with short and long message payloads. Therefore, the research community working

in this domain is advised to design secure routing protocols that could be capable to avoid the interception of man-in-the-middle and other adversaries, those aims to disrupt the legitimate communication process.

C. Challenge 3

From Table IV, we can see that public and private key management is another very important task in cryptography. To continue, we have also noted that weak key cryptographic schemes had been targeted through various attacks to compromise the security of employed UAV-aided IoT applications. With this, we have also recorded that the complex key matching or handshaking creates network overhead and consumes extra energy of resources limited IoTs and UAVs. Therefore, we would like to bring the attention of the research community toward this challenging task to rethink about the existing key sharing schemes and design cost-effective key sharing schemes for these networks.

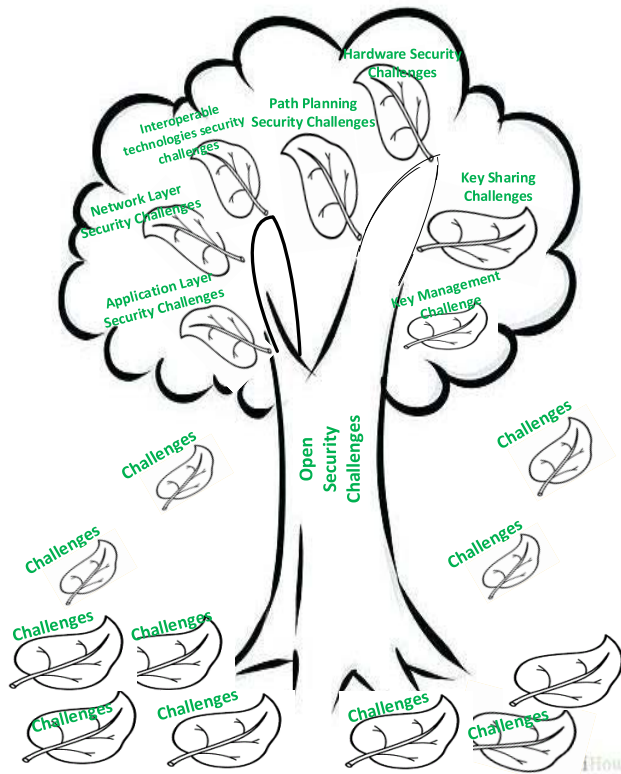


Fig. 4. Visual Representation of different open security challenges.

D. Challenge 4

During literature analysis and review, we have recorded that UAV-aided IoT application has been targeted through different kinds of jamming attacks and SHERPA standard disruption attacks. Although, there exist some preventive techniques to tackle these attacks in operational networks, but somehow, they are unable to handle these attacks efficiently and maintain a high standard of communication metrics. Therefore, we also suggest the research community to take into account this challenging issue and design efficient and productive countermeasure techniques for the attacks associated with transmission channels, path planning, location privacy, and SHERPA standard.

E. Challenge 5

In the literature, there exist various security countermeasures that have been used to mitigate the hardware-based attacks associated with UAV-aided IoT applications. With this, it has also been noted that hardware-based countermeasures are used as a dependable option to ensure the authentication and validation of these devices and create a secure communication environment for them. Moreover, it is very hard for the enterprise market to design hardware based secure IoT and UAV products taking into account their low prices and large scale deployment. Therefore, it is essential for the enterprise market and research community to design secure software-based techniques that can be useful to counter hardware-based attacks on these networks.

F. Challenge 6

In the literature, some machine learning techniques to counter different attacks associated with UAV-aided IoT applications. For this, the researcher used an ML algorithm to detect and prevent different attacks on the UAV-aided IoT networks based on behavioral analysis utilizing mathematical models and expressions. algorithms empower them to assess incoming traffic and differentiate between good and bad. To elaborate on this, these ML algorithms are used in an adoptive manner by considering network layer or application layer to detect anomalies. However, these ML techniques sometimes produce false results, due to wireless and dynamic communication of UAV-aided IoT applications. Therefore, we would like to encourage the research community to pay attention to this important challenge and design reliable ML algorithms that could be capable of producing accurate results and counter different attacks concerning UAV-aided IoT applications.

IX. FUTURE RESEARCH DIRECTIONS

In this section, we will highlight the possible research directions that can be helpful and useful for the research community, IoT and UAV hardware producers, enterprise market stakeholders and concerned organizations to combat different security threats associated with UAV-aided IoT applications in a cost-effective manner. In the under-mentioned subsections, we will discuss distinct these research directions.

A. Security Solutions for Secure Channel Modeling

In UAV-aided IoT applications, communication takes place between IoT-to-IoT, IoT-to-BS, UAV-to-IoT, UAV-to-UAV, and UAV-to-Ground-BS. Keeping in view the wireless communication infrastructure of this integrated technology, efficient and secure channel modeling can assure the integrity of information followed by least latency in the network [152]. In the literature, most of the UAV-aided IoT channel modeling techniques fail to maintain the security of deployed networks with the mobility aspects of UAVs followed by delay sensitivity of these networks [153], [154]. Following this discussion, it has been reported in the literature that most of the existing techniques can be easily targeted through jamming attacks. Therefore, the research community, industry stakeholders, concerned organizations, the enterprise market, IoTs, and UAVs hardware such as processing chip, antennas, transmitters, receivers, etc, producers are advised to design communication efficient devices. Moreover, their devices would be capable to ensure delay-sensitive and secure communication in an operational UAV-aided IoT network. Despite that, these devices would also be capable of following channel triggering rules or changing their transmission and reception communication channels to counter different types of jamming attacks.

B. Security Solutions Utilizing Machine and Deep Learning

In the literature, we have noted that IoT devices have limited resources followed by the least computation capabilities. If advanced or complex authentication models are used for their security, then it can decrease their performance in

terms of communication metrics. Therefore, we would like to acknowledge the importance of ML and DL techniques in resource-limited networks such as UAV-aided IoT applications. Following this, we know that resource restrictions create a trade off between IoTs capabilities and security parameters processing. During the literature review, we recorded various ML and DL approaches that have been used to tackle the security concerns in UAV-aided IoT applications, but most of them were sophisticated and require a significant amount of computing capabilities followed by extra memory and communication resources of IoTs and UAVs to ensure authentication among paired devices. Therefore, the research community are acknowledged to consider this important aspect and determine the pinpoint spot for ML and DL algorithms in the network. To achieve this, extensive experiments and simulations are needed to maintain network efficiency with data privacy and preservation followed by authentication of legitimate devices. In UAV-aided IoT applications, low-cost, robust, trustworthy and reliable authentication and data privacy schemes play an important role, therefore, the research community must take care of it, while developing new ML and DL techniques for this integrated technology.

C. Security Solution for Access Control and Authentication

In UAV-aided IoT applications, authentication and access control policies are the influential factors and requirements of this integrated technology. To maintain this, the legitimate IoTs and UAVs first need to verify each other's authenticity before sharing sensitive information [155], [156], [157]. For this, the literature presents substantial work, but due to the dynamic nature of communication, mobility and wireless communication, this integrated technology demands more attention from the research community to devise communication friendly authentication models for them. Consequently, access control also has a great importance in this technology, just like the IoT applications subject to the data sensitivity followed by services of these applications. Therefore, it is imperative to design intelligent access control policies or schemes, where access should be given to certain users. Therefore, we believe that an adaptive access control mechanism with a proper authentication model could be extremely useful in these applications. Hence, the research community needs to work in this domain and design novel schemes that could be attractive for the consumer market stakeholders in terms of trust reliability on this technology.

D. Software/Coding Based Solutions

In the literature and future research directions, we have noted that hardware-based security solutions can play a major role in the reliable and secure communication of UAV-aided IoT applications, as well as traditional IoT applications [158], [159]. Following the discussion of the preceding sections, we know that designing a hardware-based secure authentication model for UAV-aided IoT applications is not a practical approach because IoT devices have limited processing capabilities followed by low cost and large deployment. Keeping in view these constraints, software-based authentication

schemes can be used as an alternative mechanism, where these low power devices can be configured, updated and upgraded effectively and timely. Therefore, we suggest the research community pay attention toward software-based authentication schemes and resolve the security issues in this emerging technology in a cost-effective way.

E. Settings Security Standard Based Solutions

In the literature review of UAV-aided IoT applications concerning security standards, it had been recorded that these networks are connected in a heterogeneous environment, whereas they communicate with each other through wireless links [160], [161]. Following this discussion, we have noted that IoTs and UAVs hardware are designed with any proper security standards, therefore, the existing security threats need urgent countermeasure techniques that could be used as a standard for these networks. To continue this talk, the existing authentication, key sharing, data preservation, and data encryption schemes are limited to deal with the security threat of UAV-aided IoT applications as standard. To explore, the minimal computation and energy resources of IoTs and UAVs with low cost compel them to use generic authentication, encryption, and data preservation schemes. Therefore, we would like to acknowledge the research community to take these factors into account and develop cost-effective authentication, encryption, data preservation, and key sharing standards for UAV-aided IoT applications.

F. Intelligent and Re-Configurable Surface Based Solution

With the advancement in technology, the role of an intelligent and re-configurable surface (IRS) can not be ignored, because it is appeared as a promising technique to address the security, resource management, and spectrum efficiency issues in UAV-aided IoT applications cost-effectively. Although IRS has a lot of potential, but presently its use is very limited in real environment. Therefore, we suggest, the research community to pay attention to utilization of emerging technology, and resolve many security concerns associated with UAV-assisted IoT applications. To explore, IRS is basically a software controlled surface that is made of a huge number of low cost reflecting elements know as planar array. This is array is capable to randomly manage and adjust the reflective co-efficient of transmitted signals to tackle jamming attack issues and improve the propagation of transmitted signals. Following our future research suggestion, this technology has a lot of potential and can be assumed game-changer for the future of UAV-assisted IoT applications security.

X. CONCLUSION

In this paper, we have presented a systematic survey regarding the security concerns of UAV-aided IoT applications by evaluating the practical literature that highlights the security problems associated with different entities such as industry, academia, enterprise market, organizations and the standardization bodies of this emerging technology. Our survey paper reveals that UAV-assisted IoT applications demonstrated

significant contributions in many traditional IoT applications, and emerged one of the promising technology in the past couple of years. Despite their significant contribution, this burgeoning technology faces a number of challenges, whereas security of the legitimate network components and communication is among the most catastrophic ones. For this, initially, we familiarize the reader with different security taxonomy and risks that can hinder the performance and legitimate operation of a UAV-aided IoT application. Thereafter, we have focused on the existing review articles to highlight their contributions and limitations, which were used in the consequent section as a comparative factor for our paper to exemplify its novelty and uniqueness. Furthermore, we followed up the comparative metrics to comprehensively overview their concerned literature and identify the present challenges that need academia, industry stakeholder, and enterprise market attention. In concatenation with this, we have highlighted the open research challenges in a separate section to set the stage for future directions. Likewise, we used these challenges and acknowledged the potential research direction that could be assumed as a preprint for redressal of the security concerns of UAV-aided IoT applications. To summarize, we have presented a complete package in this paper for all stakeholders working on the security aspects of this emerging technology.

REFERENCES

- [1] M. Adil, M. K. Khan, M. Jamjoom, and A. Farouk, "MHADBOR: AI-enabled administrative-distance-based opportunistic load balancing scheme for an agriculture Internet of Things network," *IEEE Micro*, vol. 42, no. 1, pp. 41–50, Jan. 2022.
- [2] K. L.-M. Ang and J. K. P. Seng, "Application specific Internet of Things (ASIoTs): Taxonomy, applications, use case and future directions," *IEEE Access*, vol. 7, pp. 56577–56590, 2019.
- [3] M. Adil et al., "An intelligent hybrid mutual authentication scheme for industrial Internet of Things networks," *Comput., Mater. Continua*, vol. 68, no. 1, pp. 447–470, 2021.
- [4] X. Xu, H. Zhao, H. Yao, and S. Wang, "A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2431–2443, Feb. 2021.
- [5] Q. Wang, H.-N. Dai, X. Li, M. K. Shukla, and M. Imran, "Artificial noise aided scheme to secure UAV-assisted Internet of Things with wireless power transfer," *Comput. Commun.*, vol. 164, pp. 1–12, Dec. 2020.
- [6] X. Jiang et al., "Covert communication in UAV-assisted air-ground networks," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 190–197, Aug. 2021.
- [7] R. Pakrooh and A. Bohlouli, "A survey on unmanned aerial vehicles-assisted Internet of Things: A service-oriented classification," *Wireless Pers. Commun.*, vol. 119, no. 2, pp. 1541–1575, 2021.
- [8] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.
- [9] A. S. Abdalla, K. Powell, V. Marojevic, and G. Geraci, "UAV-assisted attack prevention, detection, and recovery of 5G networks," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 40–47, Aug. 2020.
- [10] M. Adil, M. Attique, M. M. Jadoon, J. Ali, A. Farouk, and H. Song, "HOPCTP: A robust channel categorization data preservation scheme for industrial healthcare Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7151–7161, Oct. 2022.
- [11] 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.
- [12] V. Chamola, P. Kotes, A. Agarwal, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, 2021, Art. no. 102324.
- [13] M. Golam, J.-M. Lee, and D.-S. Kim, "A UAV-assisted blockchain based secure device-to-device communication in internet of military things," in *Proc. Int. Conf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 1896–1898.
- [14] M. Huang, A. Liu, N. N. Xiong, and J. Wu, "A UAV-assisted ubiquitous trust communication system in 5G and beyond networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3444–3458, Nov. 2021.
- [15] O. S. Oubbati, M. Atiquzzaman, T. A. Ahanger, and A. Ibrahim, "Softwarization of UAV networks: A survey of applications and future trends," *IEEE Access*, vol. 8, pp. 98073–98125, 2020.
- [16] M. Adil et al., "Three byte-based mutual authentication scheme for autonomous internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9358–9369, Jul. 2022.
- [17] B. Liu, Z. Su, and Q. Xu, "Game theoretical secure wireless communication for UAV-assisted vehicular Internet of Things," *China Commun.*, vol. 18, no. 7, pp. 147–157, Jul. 2021.
- [18] W. Wang et al., "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476–4489, Jul. 2020.
- [19] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Oct. 2019.
- [20] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.
- [21] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things security, device authentication and access control: A review," 2019, *arXiv:1901.07309*.
- [22] T. Takada, "Authentication shutter: Alternative countermeasure against password reuse attack by availability control," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, Aug. 2017, pp. 1–9.
- [23] A. Fotouhi et al., "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.
- [24] P. Vamvakas, E. E. Tsiropoulou, and S. Papavassiliou, "Exploiting prospect theory and risk-awareness to protect UAV-assisted network operation," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, Dec. 2019.
- [25] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A. H. Sodhro, and S. C. Mukhopadhyay, "Towards machine learning enabled security framework for IoT-based healthcare," in *Proc. 13th Int. Conf. Sens. Technol. (ICST)*, Dec. 2019, pp. 1–6.
- [26] P. Zhao, H. Jiang, C. Wang, H. Huang, G. Liu, and Y. Yang, "On the performance of k -anonymity against inference attacks with background information," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 808–819, Feb. 2019.
- [27] A. Rashid, D. Sharma, T. A. Lone, S. Gupta, and S. K. Gupta, "Secure communication in UAV assisted HetNets: A proposed model," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Cham, Switzerland: Springer, Jul. 2019, pp. 427–440.
- [28] B. Bera, A. K. Das, S. Garg, M. Jalil Piran, and M. S. Hossain, "Access control protocol for battlefield surveillance in drone-assisted IoT environment," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2708–2721, Feb. 2022.
- [29] A. Rayes and S. Salam, "The internet in IoT—OSI, TCP/IP, IPv4, IPv6 and internet routing," in *Internet of Things From Hype to Reality*. Cham, Switzerland: Springer, 2017, pp. 35–56.
- [30] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, "Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and K -means clustering," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 139–142, Feb. 2020.
- [31] C. O. Nnamani, M. R. A. Khandaker, and M. Sellathurai, "UAV-aided jamming for secure ground communication with unknown eavesdropper location," *IEEE Access*, vol. 8, pp. 72881–72892, 2020.
- [32] H.-M. Wang, X. Zhang, and J.-C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 32–39, Oct. 2019.
- [33] M. Tao, X. Li, H. Yuan, and W. Wei, "UAV-aided trustworthy data collection in federated-WSN-enabled IoT applications," *Inf. Sci.*, vol. 532, pp. 155–169, Sep. 2020.
- [34] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure Internet of Things: ECC comes of age," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 3, pp. 237–248, May/Jun. 2017, doi: 10.1109/TDSC.2016.2577022.

- [35] B. Li, Z. Fei, Y. Zhang, and M. Guizani, "Secure UAV communication networks over 5G," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 114–120, Oct. 2019.
- [36] 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.
- [37] M. Wazid, B. Bera, A. Mitra, A. K. Das, and R. Ali, "Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Sep. 2020, pp. 37–42.
- [38] V. Hassija et al., "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, 4th Quart., 2021.
- [39] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Comput. Commun.*, vol. 162, pp. 102–117, Oct. 2020.
- [40] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, p. 58, Aug. 2019.
- [41] C. Li, Z. Gao, J. Xia, D. Deng, and L. Fan, "Cache-enabled physical-layer secure game against smart UAV-assisted attacks in b5G NOMA networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–9, Dec. 2020.
- [42] A. Yazdinejad, R. M. Parizi, A. Dehghantana, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021.
- [43] B. Shang, L. Liu, J. Ma, and P. Fan, "Unmanned aerial vehicle meets vehicle-to-everything in secure communications," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 98–103, Oct. 2019.
- [44] Z. Li, Y. Lu, Y. Shi, Z. Wang, W. Qiao, and Y. Liu, "A dyna-Q-based solution for UAV networks against smart jamming attacks," *Symmetry*, vol. 11, no. 5, p. 617, May 2019.
- [45] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: A survey," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 560–565.
- [46] 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.
- [47] G. S. Ilgi and Y. K. Ever, "Critical analysis of security and privacy challenges for the Internet of Drones: A survey," in *Drones in Smart-Cities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 207–214.
- [48] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying ad-hoc networks: Key enabling wireless technologies, applications, challenges and open research topics," *Drones*, vol. 4, no. 4, p. 65, Sep. 2020.
- [49] 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.
- [50] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.
- [51] A. Vangala, A. K. Das, N. Kumar, and M. Alazab, "Smart secure sensing for IoT-based agriculture: Blockchain perspective," *IEEE Sensors J.*, vol. 21, no. 16, pp. 17591–17607, Aug. 2021.
- [52] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.
- [53] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.
- [54] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.
- [55] D. Sharma, S. K. Gupta, A. Rashid, S. Gupta, M. Rashid, and A. Srivastava, "A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, Sep. 2020, Art. no. e4114.
- [56] R. R. Gorrepati and S. R. Guntur, "DroneMap: An IoT network security in Internet of Drones," in *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*. Cham, Switzerland: Springer, 2021, pp. 251–268.
- [57] M. M. Alam, Y. L. Moullec, R. Ahmad, M. Magarini, and L. Reggiani, "A primer on public safety communication in the context of terror attacks: The NATO SPS 'COUNTER-TERROR' project," in *Advanced Technologies for Security Applications*. Dordrecht, The Netherlands: Springer, 2020, pp. 19–34.
- [58] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, Jul. 2021.
- [59] H. Tan and I. Chung, "RSU-aided remote V2V message dissemination employing secure group association for UAV-assisted VANETs," *Electronics*, vol. 10, no. 5, p. 548, Feb. 2021.
- [60] I. Tudosa, F. Picariello, E. Balestrieri, L. De Vito, and F. Lam-onaca, "Hardware security in IoT era: The role of measurements and instrumentation," in *Proc. II Workshop Metrol. Ind. 4.0 IoT (MetroInd4.0 IoT)*, Jun. 2019, pp. 285–290.
- [61] I. Butun, A. Sari, and P. Österberg, "Hardware security of fog end-devices for the Internet of Things," *Sensors*, vol. 20, no. 20, p. 5729, Oct. 2020.
- [62] S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware security in IoT devices with emphasis on hardware trojans," *J. Sens. Actuator Netw.*, vol. 8, no. 3, p. 42, Aug. 2019.
- [63] N. Samir et al., "Energy-adaptive lightweight hardware security module using partial dynamic reconfiguration for energy limited Internet of Things applications," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–4.
- [64] C. Meurisch, B. Bayrak, and M. Muhlhauser, "EdgeBox: Confidential ad-hoc personalization of nearby IoT applications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
- [65] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino, and S. E. Quincozes, "Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4569–4578, Mar. 2021.
- [66] V. Attias, L. Vigneri, and V. Dimitrov, "Preventing denial of service attacks in IoT networks through verifiable delay functions," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.
- [67] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect DDoS attacks on VANET system: A survey," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–6.
- [68] R. T. Tiburski et al., "Lightweight security architecture based on embedded virtualization and trust mechanisms for IoT edge devices," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 67–73, Feb. 2019.
- [69] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.
- [70] G. Liu et al., "Softwarized IoT network immunity against eavesdropping with programmable data planes," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6578–6590, Apr. 2021.
- [71] H. Moudoud, L. Khokhi, and S. Cherkaoui, "Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT," *IEEE Netw.*, vol. 35, no. 2, pp. 194–201, Mar. 2021.
- [72] M. Adil and M. K. Khan, "Emerging IoT applications in sustainable smart cities for COVID-19: Network security and data preservation challenges with future directions," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103311.
- [73] M. Adil, M. A. Almaiah, A. O. Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, p. 2311, Apr. 2020.
- [74] M. Adil et al., "MAC-AODV based mutual authentication scheme for constraint oriented networks," *IEEE Access*, vol. 8, pp. 44459–44469, 2020.
- [75] S. Huang, Z. Zeng, K. Ota, M. Dong, T. Wang, and N. Xiong, "An intelligent collaboration trust interconnections system for mobile information control in ubiquitous 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 347–365, Mar. 2020.
- [76] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168825–168853, 2020.
- [77] V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations for critical applications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5391–5402, May 2020.

- [78] A. Al-Omary, A. Othman, H. M. AlSabbagh, and H. Al-Rizzo, "Survey of hardware-based security support for IoT/CPS systems," *KnE Eng.*, pp. 52–70, Oct. 2018.
- [79] B. Xu et al., "A security design for the detecting of buffer overflow attacks in IoT device," *IEEE Access*, vol. 6, pp. 72862–72869, 2018.
- [80] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Nov. 2018, pp. 124–130.
- [81] H. Al-Agrabi, A. P. Johnson, R. Hill, P. Lane, and T. Alsoubi, "Hardware-intrinsic multi-layer security: A new frontier for 5G enabled IIoT," *Sensors*, vol. 20, no. 7, p. 1963, Mar. 2020.
- [82] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT," *J. Parallel Distrib. Comput.*, vol. 134, pp. 198–206, Dec. 2019.
- [83] W. Yan, N. Zhang, L. L. Njilla, and X. Zhang, "PCBChain: Lightweight reconfigurable blockchain primitives for secure IoT applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 10, pp. 2196–2209, Oct. 2020.
- [84] J. Zhang and C. Shen, "Set-based obfuscation for strong PUFs against machine learning attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 1, pp. 288–300, Jan. 2021.
- [85] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, "Policy-based access control for constrained healthcare resources in the context of the Internet of Things," *J. Netw. Comput. Appl.*, vol. 139, pp. 57–74, Aug. 2019.
- [86] A. P. Shrestha, S. M. R. Islam, and K. S. Kwak, "Ticket-based authentication for securing Internet of Things," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2020, pp. 938–941.
- [87] M. Karimibiuki, E. Aggarwal, K. Pattabiraman, and A. Ivanov, "Dyn-PoLAC: Dynamic policy-based access control for IoT systems," in *Proc. IEEE 23rd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2018, pp. 161–170.
- [88] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the Internet of Things era: An overview on security and privacy challenges," *Comput. Netw.*, vol. 179, Oct. 2020, Art. no. 107345.
- [89] D. Kallergis, Z. Garofalaki, G. Katsikogiannis, and C. Douligeris, "CAPODAZ: A containerised authorisation and policy-driven architecture using microservices," *Ad Hoc Netw.*, vol. 104, Jul. 2020, Art. no. 102153.
- [90] G. Katsikogiannis, D. Kallergis, Z. Garofalaki, S. Mitropoulos, and C. Douligeris, "A policy-aware service oriented architecture for secure machine-to-machine communications," *Ad Hoc Netw.*, vol. 80, pp. 70–80, Nov. 2018.
- [91] A. Pillai, M. Sindhu, and K. V. Lakshmy, "Securing firmware in Internet of Things using blockchain," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2019, pp. 329–334.
- [92] Y. Zhao, Y. Liu, A. Tian, Y. Yu, and X. Du, "Blockchain based privacy-preserving software updates with proof-of-delivery for Internet of Things," *J. Parallel Distrib. Comput.*, vol. 132, pp. 141–149, Oct. 2019.
- [93] C.-H. Lu, C.-H. Liu, and Z.-H. Chen, "Secure and efficient firmware update for increasing IoT-enabled smart devices," *J. Ambient Intell. Hum. Comput.*, pp. 1–14, Sep. 2020.
- [94] N. W. Lo and S. H. Hsu, "A secure IoT firmware update framework based on MQTT protocol," in *Proc. Int. Conf. Inf. Syst. Archit. Technol. Cham, Switzerland: Springer*, Sep. 2019, pp. 187–198.
- [95] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.
- [96] N. Yousefnezhad, A. Malhi, and K. Främling, "Security in product lifecycle of IoT devices: A survey," *J. Netw. Comput. Appl.*, vol. 171, Dec. 2020, Art. no. 102779.
- [97] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," *Secur. Privacy*, vol. 1, no. 2, p. e20, Mar. 2018.
- [98] D. B. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Netw.*, vol. 97, Feb. 2020, Art. no. 102022.
- [99] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a secure RPL based Internet of Things routing protocol: A review," *Ad Hoc Netw.*, vol. 101, Apr. 2020, Art. no. 102096.
- [100] B. Hammi, S. Zeadally, H. Labiod, R. Khatoun, Y. Begriche, and L. Khoukhi, "A secure multipath reactive protocol for routing in IoT and HANETs," *Ad Hoc Netw.*, vol. 103, Jun. 2020, Art. no. 102118.
- [101] K.-S. Wong and T.-C. Wan, "Current state of multicast routing protocols for disruption tolerant networks: Survey and open issues," *Electronics*, vol. 8, no. 2, p. 162, Feb. 2019.
- [102] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency Comput., Pract. Exp.*, vol. 32, no. 21, Nov. 2020, Art. no. e4946.
- [103] C. C. Sobin, "A survey on architecture, protocols and challenges in IoT," *Wireless Pers. Commun.*, vol. 112, no. 3, pp. 1383–1429, Jun. 2020.
- [104] M. G. Samaila, J. B. F. Sequeiros, M. M. Freire, and P. R. M. Inácio, "Security threats and possible countermeasures in IoT applications covering different industry domains," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–9.
- [105] N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Sep. 2020, pp. 61–66.
- [106] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.
- [107] P. Royo, E. Pastor, M. Macias, R. Cuadrado, C. Barrado, and A. Vargas, "An unmanned aircraft system to detect a radiological point source using RIMA software architecture," *Remote Sens.*, vol. 10, no. 11, p. 1712, Oct. 2018.
- [108] D. Mishra and E. Natalizio, "A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements," *Comput. Netw.*, vol. 182, Dec. 2020, Art. no. 107451.
- [109] J. J. P. C. Rodrigues, S. Jabbar, M. Abdallah, C. Verikoukis, and M. Guizani, "Future communication trends toward Internet of Things services and applications," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 6–8, Dec. 2019.
- [110] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Comput. Commun.*, vol. 155, pp. 66–83, Jan. 2020.
- [111] A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 491–502, Oct. 2019.
- [112] G. Wang, B. Lee, J. Ahn, and G. Cho, "A UAV-assisted CH election framework for secure data collection in wireless sensor networks," *Future Gener. Comput. Syst.*, vol. 102, pp. 152–162, Jan. 2020.
- [113] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.
- [114] A. Sharma et al., "Communication and networking technologies for UAVs: A survey," *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, Art. no. 102739.
- [115] B. Brik, A. Ksentini, and M. Bouaziz, "Federated learning for UAVs-enabled wireless networks: Use cases, challenges, and open problems," *IEEE Access*, vol. 8, pp. 53841–53849, 2020.
- [116] 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.
- [117] Q. Liao, T. Fischer, J. Gao, F. Hafeez, C. Oechsner, and J. Knode, "A secure end-to-end cloud computing solution for emergency management with UAVs," in *Proc. IEEE Global Commun. Conf. (GLOBE-COM)*, Dec. 2018, pp. 1–7.
- [118] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Veh. Commun.*, vol. 11, pp. 1–11, Jan. 2018.
- [119] M. A. Rahman, M. T. Rahman, M. K. Kısacikoglu, and K. Akkaya, "Intrusion detection systems-enabled power electronics for unmanned aerial vehicles," in *Proc. IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–5.
- [120] B. D. Deebak and F. Al-Turjman, "Aerial and underwater drone communication: Potentials and vulnerabilities," in *Drones in Smart-Cities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 1–26.
- [121] A. Singandhupe, H. M. La, and D. Feil-Seifer, "Reliable security algorithm for drones using individual characteristics from an EEG signal," *IEEE Access*, vol. 6, pp. 22976–22986, 2018.
- [122] 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.
- [123] S. Garg, G. S. Aujla, N. Kumar, and S. Batra, "Tree-based attack-defense model for risk assessment in multi-UAV networks," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 35–41, Nov. 2019.
- [124] A. Fitwi, Y. Chen, and N. Zhou, "An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring," in *Proc. SPIE*, vol. 11018, May 2019, Art. no. 110180L.
- [125] S. Sharma and H. Saini, "Fog assisted task allocation and secure deduplication using 2FBO² and MoWo in cluster-based industrial IoT (IIoT)," *Comput. Commun.*, vol. 152, pp. 187–199, Feb. 2020.

- [126] C. Xu, K. Wang, Y. Sun, S. Guo, and A. Y. Zomaya, "Redundancy avoidance for big data in data centers: A conventional neural network approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 104–114, Jan. 2020.
- [127] T. Gebremichael et al., "Security and privacy in the industrial Internet of Things: Current standards and future challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020.
- [128] Z. Tan, X. Yang, M. Pang, S. Gao, M. Li, and P. Chen, "UAV-assisted low-consumption time synchronization utilizing cross-technology communication," *Sensors*, vol. 20, no. 18, p. 5134, Sep. 2020.
- [129] M. E. Mkiramweni, C. Yang, J. Li, and W. Zhang, "A survey of game theory in unmanned aerial vehicles communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3386–3416, 4th Quart., 2019.
- [130] R. Ch. G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102670.
- [131] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Security challenges and concerns of Internet of Things (IoT)," in *Cyber-Physical Systems: Architecture, Security and Application*. Cham, Switzerland: Springer, 2019, pp. 153–185.
- [132] Z. Kaleem et al., "Amateur drone surveillance: Applications, architectures, enabling technologies, and public safety issues: Part 1," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 14–15, Jan. 2018.
- [133] 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.
- [134] A. Islam and S. Y. Shin, "BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city," in *Proc. 7th Int. Conf. Inf. Commun. Technol. (ICOICT)*, Jul. 2019, pp. 1–6.
- [135] F. Al-Turjman and H. Zahmatkesh, "A comprehensive review on the use of AI in UAV communications: Enabling technologies, applications, and challenges," in *Unmanned Aerial Vehicles in Smart Cities*. USA: Springer, 2020, pp. 1–26.
- [136] C. Tang, X. Wei, C. Liu, H. Jiang, H. Wu, and Q. Li, "UAV-enabled social internet of vehicles: Roles, security issues and use cases," in *Proc. Int. Symp. Secur. Privacy Social Netw. Big Data*. Singapore: Springer, Sep. 2020, pp. 153–163.
- [137] C. Yao, Y. Liu, X. Wei, G. Wang, and F. Gao, "Backscatter technologies and the future of Internet of Things: Challenges and opportunities," *Intell. Converged Netw.*, vol. 1, no. 2, pp. 170–180, Sep. 2020.
- [138] J. P. A. Yaacoub et al., "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Gener. Comput. Syst.*, vol. 105, pp. 581–606, Apr. 2020.
- [139] J. Jiang and G. Han, "Routing protocols for unmanned aerial vehicles," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 58–63, Jan. 2018.
- [140] D. Shumeye Lakew, U. Sa'ad, N.-N. Dao, W. Na, and S. Cho, "Routing in flying ad hoc networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1071–1120, 2nd Quart., 2020.
- [141] M. Kaur and S. Verma, "Flying ad-hoc network (FANET): Challenges and routing protocols," *J. Comput. Theor. Nanosci.*, vol. 17, no. 6, pp. 2575–2581, 2020.
- [142] A. V. Leonov and G. A. Litvinov, "Applying AODV and OLSR routing protocols to air-to-air scenario in flying ad hoc networks formed by mini-UAVs," in *Proc. Syst. Signals Generating Process. Field Board Commun.*, Mar. 2018, pp. 1–10.
- [143] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors*, vol. 20, no. 9, p. 2495, Apr. 2020.
- [144] M. Elbayoumi et al., "NOMA-assisted machine-type communications in UDN: State-of-the-art and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1276–1304, 2nd Quart., 2020.
- [145] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, "Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications," *Automat. Construct.*, vol. 101, pp. 111–126, May 2019.
- [146] Z. Yuan, J. Jin, L. Sun, K.-W. Chin, and G.-M. Muntean, "Ultra-reliable IoT communications with UAVs: A swarm use case," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 90–96, Dec. 2018.
- [147] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband Internet of Things (NB-IoT): Architecture, application and challenges," *IEEE Access*, vol. 7, pp. 16739–16776, 2018.
- [148] Z. Ullah, F. Al-Turjman, and L. Mostarda, "UAVs healthcare applications, communication protocols, deployment strategies, and security challenges," in *Unmanned Aerial Vehicles in Smart Cities*. Cham, Switzerland: Springer, 2020, pp. 27–37.
- [149] A. Nayyar, "Flying adhoc network (FANETs): Simulation based performance comparison of routing protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP," in *Proc. Int. Conf. Adv. Big Data, Comput. Data Commun. Syst. (icABCD)*, Aug. 2018, pp. 1–9.
- [150] X. Ji et al., "E2PP: An energy-efficient path planning method for UAV-assisted data collection," *Secur. Commun. Netw.*, vol. 2020, pp. 1–13, Nov. 2020.
- [151] S. Zhu, L. Gui, N. Cheng, F. Sun, and Q. Zhang, "Joint design of access point selection and path planning for UAV-assisted cellular networks," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 220–233, Jan. 2020.
- [152] J. Xia, Y. Xu, D. Deng, Q. Zhou, and L. Fan, "Intelligent secure communication for Internet of Things with statistical channel state information of attacker," *IEEE Access*, vol. 7, pp. 144481–144488, 2019.
- [153] P. Bhoyar, S. B. Dhok, and R. B. Deshmukh, "Hardware implementation of secure and lightweight Simeck32/64 cipher for IEEE 802.15.4 transceiver," *AEU, Int. J. Electron. Commun.*, vol. 90, pp. 147–154, Jun. 2018.
- [154] X. Sun, W. Yang, and Y. Cai, "Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1884–1897, Mar. 2020.
- [155] S. Sen, J. Koo, and S. Bagchi, "TRIFECTA: Security, energy efficiency, and communication capacity comparison for wireless IoT devices," *IEEE Internet Comput.*, vol. 22, no. 1, pp. 74–81, Jan./Feb. 2018.
- [156] R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, "A steganography algorithm based on CycleGAN for covert communication in the Internet of Things," *IEEE Access*, vol. 7, pp. 90574–90584, 2019.
- [157] T. Wang, D. Wang, and K. Wu, "Chaotic adaptive synchronization control and application in chaotic secure communication for industrial Internet of Things," *IEEE Access*, vol. 6, pp. 8584–8590, 2018.
- [158] U. Bodkhe and S. Tanwar, "Taxonomy of secure data dissemination techniques for IoT environment," *IET Softw.*, vol. 14, no. 6, pp. 563–571, Dec. 2020.
- [159] M. Bansal, I. Chana, and S. Clarke, "A survey on IoT big data: Current status, 13 V's challenges, and future directions," *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–59, Nov. 2021.
- [160] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.
- [161] Y. Zheng, S. S. Dhabu, and C.-H. Chang, "Securing IoT monitoring device using PUF and physical layer authentication," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–5.



Muhammad Adil (Member, IEEE) received the B.S. and M.S. degrees in computer science from the Virtual University of Lahore, Pakistan, in 2017 and 2020, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, University at Buffalo—The State University of New York, USA. He received the Chair's Fellowship from the department in 2022. He has CCNA and CCNP certifications. His research interests include networking, cybersecurity, cyber-physical systems (CPS), unmanned aerial vehicles (UAVs), the Internet of Things (IoT), and wireless sensor networks (WSN). He has many publications in prestigious journals, such as IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE SENSOR JOURNAL, IEEE ACCESS, IEEE Micro Magazine, ACM Transactions on Sensor Networks, Computer Networks (Elsevier), Sustainable Cities and Societies, and Sensor (MDPI). In addition, he is a member of IEEE Computer Society, IEEE Industrial Electronics, IEEE Cybersecurity, IEEE Young Professionals, and London Journal Press Club-U.K., as a Honorary Member. He is reviewing for reputed journals, such as IEEE INTERNET OF THINGS JOURNAL, IEEE SENSORS JOURNAL, IEEE SYSTEMS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, IEEE TRANSACTIONS ON SMS, IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE Communication Magazine, IET Communication, Computer Networks (Elsevier) journals, and Telecommunication System.



Mian Ahmad Jan (Senior Member, IEEE) received the Ph.D. degree from the University of Technology Sydney (UTS), Australia, and the master's degree in mobile computing from the University of Bradford, U.K. He is currently an Assistant Professor at the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. He has published his research in the world leading journals and conferences and has been a guest editor of numerous special issues in various prestigious journals. His research interests include cyber security, energy-efficient and secured communication for wireless sensor networks, and the Internet of Things. He has been among the World's Top 2% scientists in 2021 and 2022, respectively. He has been the general chair of various high-ranked conferences.



Ahmed Farouk (Member, IEEE) is currently an Assistant Professor with the Department of Computer Science, Faculty of Computers and Artificial Intelligence, South Valley University. Before that he was a Post-Doctoral Research Fellow with Wilfrid Laurier University, Waterloo, ON, Canada, and Ryerson University, Toronto, ON, Canada. He is one of the Top 20 technical co-founders of the Quantum Machine Learning Program by Creative Destruction Laboratory, University of Toronto, Toronto. He is also selected as Top 25 of Innovate to 150 Canada to showcase the best of Toronto's next generation of change-makers, innovators, and entrepreneurs. He is exceptionally well-known for his seminal contributions to theories of quantum information, communication, and cryptography. He has authored or coauthored 62 articles in reputed and high-impact journals, such as *Nature Scientific Reports* and *Physical Review A*. The exceptional quality of his research is recognized nationally and internationally. He was selected by the scientific review panel of the Council for the Lindau Nobel Laureate Meetings to participate in the 70th Lindau Nobel Laureate Meeting. His volunteering work is apparent since he was appointed as the Chair of the IEEE Computer Chapter for the Waterloo-Kitchener area and Editorial Board for many reputed journals, such as *Nature Scientific Reports*, *IET Quantum Communication*, and *IEEE ACCESS*. He is also selected for IEEE and IET Young Professional Ambassador and as a Moderator for the new IEEE TechRxiv. He is currently an Associate Editor of *IEEE Canadian Review*.



Yongxin Liu (Senior Member, IEEE) received the Ph.D. degree from the South China University of Technology in 2018 and the Ph.D. degree in computer science from Embry-Riddle in 2021. He is currently an Assistant Professor with the Department of Mathematics, Embry-Riddle Aeronautical University (ERAU), USA. His research interests include cybersecurity, machine learning, the Internet of Things, and unmanned aircraft systems.



Houbing Song (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in August 2012. He is currently a Tenured Associate Professor of AI and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Laboratory) (www.SONGLab.us), University of Maryland, Baltimore County (UMBC), Baltimore, MD, USA. Prior to joining UMBC, he was a Tenured Associate Professor in electrical engineering and computer science at Embry-Riddle Aeronautical University, Daytona Beach, FL, USA. SONG Laboratory, graduates work in a variety of companies and universities. Those seeking academic positions have been hired as a Tenure-Track Assistant Professor at U.S. universities, such as Auburn University, Bowling Green State University, and the University of Tennessee. He is the editor of eight books. He is the author of more than 100 articles and the inventor of two patents (U.S. & WO). His research interests include cyber-physical systems/internet of things, cybersecurity and privacy, AI/machine learning/big data analytics, edge computing, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. He has served as an Associate Technical Editor for *IEEE Communications Magazine* (since 2017), an Associate Editor for *IEEE INTERNET OF THINGS JOURNAL* (since 2020), *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS* (since 2021), and *IEEE JOURNAL ON MINIATURIZATION FOR AIR AND SPACE SYSTEMS (J-MASS)* (since 2020), and a Guest Editor for *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, *IEEE INTERNET OF THINGS JOURNAL*, *IEEE Network*, *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, *IEEE SENSORS JOURNAL*, *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, and *IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS*. His research has been sponsored by federal agencies (including the National Science Foundation, U.S. Department of Transportation, Federal Aviation Administration, Air Force Office of Scientific Research, U.S. Department of Defense, and Air Force Research Laboratory) and industry. His research has been featured by popular news media outlets, including *IEEE GlobalSpec* & 39, *s Engineering360*, Association for Uncrewed Vehicle Systems International (AUUSI), *Security Magazine*, *CXOTech Magazine*, Fox News, U.S. News & amp, World Report, The Washington Times, New Atlas, Battle Space, and Defense Daily.



Hussein Abulkasim (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science from South Valley University in 2004, 2012, and 2016, respectively. From 2006 to 2011, he was a Web Developer with the Center for Information and Communication Technology, South Valley University. From 2012 to 2014, he was with the College of Computer Sciences and Information Systems, Jazan University. From 2019 to 2021, he worked as a Post-Doctoral Researcher with the Cybersecurity Research Laboratory, Toronto Metropolitan University. He is currently working as an Assistant Professor in computer science with the Department of Mathematics and Computer Science, New Valley University. His current research interests include quantum cryptography, cybersecurity, the IoT security, blockchain security quantum computation and communication, blockchain technology, and the IoT security.