applied sciences

MDPI

Review

A Survey on 6G Enabled Light Weight Authentication Protocol for UAVs, Security, Open Research Issues and Future Directions

Adnan Shahid Khan [1,*], Muhammad Ali Sattar [1], Kashif Nisar [2], Ag Asri Ag Ibrahim [3,*], Noralifah Binti Annuar [1], Johari bin Abdullah [1] and Shuaib Karim Memon [4]

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[2] Victorian Institute of Technology, Adelaide, SA 5000, Australia
[3] Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia
[4] Department of Computer Science, University of York, Deramore Lane, Heslington, York YO10 5GH, UK
* Correspondence: skadnan@unimas.my (A.S.K.); awgasri@ums.edu.my (A.A.A.I.)

Abstract: This paper demonstrates a broad exploration of existing authentication and secure communication of unmanned aerial vehicles (UAVs) in a '6G network'. We begin with an overview of existing surveys that deal with UAV authentication in 6G and beyond communications, standardization, applications and security. In order to highlight the impact of blockchain and UAV authentication in 'UAV networks' in future communication systems, we categorize the groups in this review into two comprehensive groups. The first group, named the Performance Group (PG), comprises the performance-related needs on data rates, latency, reliability and massive connectivity. Meanwhile, the second group, named the Specifications Group (SG), is included in the authentication-related needs on non-reputability, data integrity and audit ability. In the 6G network, with blockchain and UAV authentication, the network decentralization and resource sharing would minimize resource under-utilization thereby facilitating PG targets. Furthermore, through an appropriate selection of blockchain type and consensus algorithms, the SG's needs of UAV authentication in 6G network applications can also be readily addressed. In this study, the combination of blockchain and UAV authentication in 6G network emergence is reviewed as a detailed review for secure and universal future communication. Finally, we conclude on the critical identification of challenges and future research directions on the subject.

Keywords: 6G; unmanned aerial vehicles; network; security; topology; authentication; cryptography

Citation: Khan, A.S.; Sattar, M.A.; Nisar, K.; Ibrahim, A.A.A.; Annuar, N.B.; Abdullah, J.b.; Karim Memon, S. A Survey on 6G Enabled Light Weight Authentication Protocol for UAVs, Security, Open Research Issues and Future Directions. *Appl. Sci.* **2023**, *13*, 277. https://doi.org/10.3390/app13010277

Academic Editor: Dimitris Mourtzis

Received: 22 October 2022
Revised: 22 November 2022
Accepted: 23 November 2022
Published: 26 December 2022

1. Introduction

As 5G is heading closer to commercial status, prospects of UAV system integration with future 6G communication models are becoming a significant part of ongoing research in the field [1]. These papers identify a few key UAV systems in 6G flighty applications and administrations such as Human Bond Communication (HBC), Multi-sensory amplified Reality Applications (XR), Wearable Innovation-based Cutting edge Applications (WTech) and Large-scale associated independent frameworks (LS-CAS), and are more noteworthy for a few vertical spaces. All these applications show up in a combinational way beneath the space of the UAV system in 6G-based UAV communication. These applications have remarkably demanding information rates, inactivity and unwavering quality; thus, the nature of the information collected by a few UAV systems in 6G applications will be progressively delicate and fundamental. As 5G is entering the deployment phase, discussion on 6G networks is gradually gaining momentum [2]. The objective of 6G is to support faster connection. Hence, the performance of 6G will be degraded using an inefficient authentication scheme which also brings the possibility towards some security issues. The productive allocation of UAV frameworks in 6G-based UAV structures by the customers would thus require strict data security guarantees. Figure 1 illustrates the UAV paradigm in

5G and beyond networks. This figure symbolizes future employment of UAVs in numerous applications in advanced network environments.

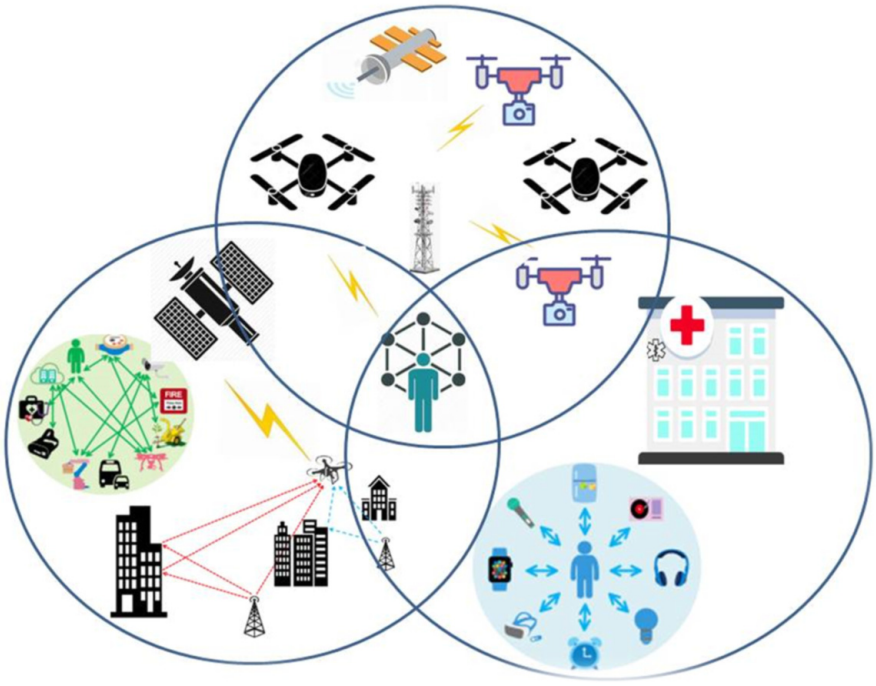

Figure 1. Illustration of future UAV applications in 5G and beyond network environments.

Blockchain could be a disseminated record innovation where cryptography and hash capacities are utilized to make a chain of information [3]. Blockchain, as it was initially utilized in crypto currencies is presently being utilized in other applications such as keen lattice, associated vehicles and Internet of Things [4–6]. The demanding prerequisites of these applications will require bolster of advances such as Reconfigurable Shrewdly Surfaces (RIS), TeraHertz (THz) communication, Artificial Intelligence (AI) and little cell systems. To enable a capable mix of these advances for the game plans of resources to achieve the execution essentials, collaboration and coordination in a straightforward and trustless environment is required [7]. Arranged decentralization will be needed to unravel the coordinate sending. Blockchain will give the required genuineness and verification within the decentralized UAV system in 6G-based UAV arrangements. Blockchain will also give the stern security essentials of the longer-term communication structure due to the built-in security highlights.

In order to tweak blockchain by the selection of suitable blockchain rudiments, its application essentials, decentralization, security and features such as adaptability are vital considerations. Blockchain offers relatively simple solutions to major issues of centralized systems. It is a pertinent fact that centralized systems have concerns including resilience, safety, scalability and privacy. Blocks chained together by a hash in between them is the simplest concept of blockchain. Genesis block is the originating block of blockchain. The key properties such as the number of tokens existing in the system reside in this first block. The last block in blockchain is named tip block. A potential new block must point to tip block. In a blockchain system, all the members that are part of network contribute to consensus and possess a copy of blockchain. In a blockchain system, each block contains a division of information: (i) transactions and account balances, (ii) block hash and (iii) the block ID. Each node in the blockchain requires the validity to be verified of any new transaction, that is added to the blockchain. This aspect of blockchain demonstrates the key properties such as transparency and distributed validations in the system.

Moreover, defense of the blockchain system against attacks is dependent upon number of nodes in the network. As stated above, individual nodes in blockchain networks hold

a copy of the entire blockchain. Certain copies to be legitimized require the same across at least 50% of the blockchain system. If a faction of illegitimate intruders attempts to add fake transactions into a designated blockchain system, they are required to control at least half of its nodes. Hence, to manipulate a blockchain system by a team of hackers, a smaller network is easy to hack or manipulate as relatively fewer number of nodes are required to be added by malicious users to have control over the system. Thus, the larger network ensures the provision of mandatory opposition to malicious users to control the network by populating the system with illegitimate nodes. Moreover, a relatively resource-intensive algorithm is utilized by the blockchain system to acquire BlockID which is acknowledged by all the members of the system. Mining is the method of computing the complex hash. For instance, blockchain entails that every BlockID must start with four zeros and the same criteria to result in longer calculations and increase the safety of blockchain by enhancing the period to build a chain. The agreement is an imperative property in blockchain frameworks which assures that all the hub concurs on the arranged state. By a cautious thought of agreement calculations and conventions, blockchain can achieve extensive and varied security highlights such as non-repudiation, information judgment and audit ability [8]. The fitting option of the communication organization can affect the decentralization and versatility of the framework. For these cases, on the off chance that inactivity is not an issue but decentralization and versatility are required, Proof-of-Work (PoW) can be utilized. On the off chance that the framework is required to converge in a really brief time, a UAV system in 6G can be utilized with communication-intensive components such as Practical Byzantine Fault Tolerance (PBFT).

1.1. Related Previous Works

A wide range of topics is covered in the latest papers, including networking upgrades, applications and security for 6G communication. As technology progresses, UAV communication is moving toward 6G networks and research papers have risen to various degrees in the previous three years. Our research strategy allows us to obtain a bird's eye view of the existing literature on basic 6G UAV communication technologies, with a focus on the research topic we have chosen. Because of the broader scope of research, UAV communication offers potential in a variety of disciplines, including academia, industry and even the military. Since the existence of bitcoin, the globe has seen the great worth of such a decentralized system, that can be implemented in many fields [9]. Similarly, Ethereum blockchain utilizes the concept of smart contracts and is acknowledged as an extension of core blockchain idea [10]. The extension of key properties of blockchain is being realized by the introduction of a smart contract that goes beyond just recording ledger transactions in accounts, which permits the distributed implementation of code. To increase the strength of the blockchain system to not just act as a database, the smart contracts can be implemented in a customized manner to allow enforcement of contracts and storage.

A conventional centralized system serves almost all Internet of Things (IoT) devices over legacy internet. The blockchain has brought up a new concept, in the way that these devices now can communicate with each other, known as a decentralized system. This concept makes the blockchain system even more robust and prevents a single point of failure and ensures immutable data transfer between nodes. The diverse nature of IoT devices presents few challenges to blockchain applications converse to the typical implementation of blockchain that necessitates clusters and powerful computing machines [11]. Moreover, the system can work in entire anonymity, causing increases in its security. An IoT device does not possess enough CPU power to solve cryptographic puzzles that are required to be solved in a blockchain system.

For stated causes, it is unworkable to have an IoT apparatus (e.g., UAVs) executing the typical mining algorithms [12]. Additionally, these devices do not possess the ability for storage of bigger amounts of data due to less storage capacity. In order to allow blockchain to be implemented in relatively low capacity IoT systems, recent studies have suggested a few mechanisms. For example, they can be executed on the basis of partitioning a

single blockchain network in sub-chains under the control of a root-chain [13]. The root-chain at the top contains powerful computers and IoT devices reside at the bottom of this hierarchical system of chains, which connect with each other. Another concept named Tangles that is based on mathematical structures has been proposed in recent studies to adapt a blockchain system by small devices [14]. Subsequently, this new transaction allows two transactions, directly and indirectly, consequently, to perform approval of all transactions that these two tip transactions point to. In this concept, there is no need for miners and no node is neglected as every node gives approval for the transactions, and each node publishes transactions since each new transaction to be linked to Tangle necessitates transaction approval. As stated above, there is no requirement for miners to eliminate the associated fees with every transaction and this permits micro payment economy. One of the pertinent features of the Tangle concept is its high scalability as the trust in a transaction grows around the number of transactions that approve that transaction directly and indirectly [15]. The growth rate of trustfulness in a specific transaction increases as the number of new transactions increases. Hence, the time period for approval of a transaction is less on a network with a high load compared to a low load network. This new concept of decentralization permits to execute a full node on an IoT device with smaller capacity. The idea of running an entire network on devices with low memory and processing power is supported by this approach. Hence, this eliminates the requirement of clusters of powerful computing machines to solve cryptographic puzzles.

Several related studies linking blockchain concepts to robotics and drones/unmanned aerial vehicles (UAVs) are described in subsequent paragraphs. In this study, use of blockchain in groups of robots covering interest and issues has been discussed [16]. Moreover, interests of blockchain for robotic swarm systems have been proposed. Moreover, it discusses the use of blockchain in robotic swarm systems and the advantages it offers in terms of transparency, consensus and security. For the purpose of awards in case of a market-based coordination strategy, this study highlights the utilization of the financial side of blockchain for implementation in such scenarios [17]. Alongside, this study discusses applications that are blockchain-based robotics. It also records shortcomings, such as a system's overall enhanced complexity and difficulty in connection with its implementation on small card computers. A proposal for using a blockchain smart contract for employment of robots for work is also discussed in a comprehensive manner in the stated study. The methodology described in the present study can be classified as one of the applications explained in two previous studies. Security is one of the most vital challenges in the distributed system as specific categories of attacks on groups of robots/UAVs may paralyze the entire network. In this study [18], the main advantages in possible blockchain-embedded UAVs with the perspective of security are the focus. In this study [19], a comprehensive analysis on communication between robot to robot is presented.

Embedding blockchain into a UAV 6G network could result in network fragmentation, that is not typical in conventional blockchains, and is mainly dependent on wired networks. This study [20] focuses on the challenges arising from swarms' divisions. In order to archive stable partitions, the Swarm DAG protocol was proposed to correctly manage the splits and merges of the network during the partitions. This study [21] presents an evaluation on joint effects of 6G, blockchain and IoT; however, a thorough analysis with respect to unmanned aerial vehicles is missing. In this study [22], a comprehensive review on 6G-based systems is presented. The study in [23] presents analysis on implementation of blockchain and edge computing based 6G that can be consequently extended to UAV network. In connection with the above stated previous works, it is ascertained that the security intrinsic to the blockchain provides this kind of service to 6G networks. Therefore, we aim to provide a comprehensive review of blockchain-based implantations, requirements, challenges and futures trends in 6G networks; moreover, we also cover the limitations of previous studies as summarized in Table 1.

Table 1. Previous studies and limitations.

Ref.	Year	Focused Area	Limitations with Respect to Subject
[16]	2020	Blockchain and UAV Swarm	UAV based 3D paradigm in 6G requires further review.
[17]	2019	UAV authentication classes	Focus on 6G-based authentication with respect to UAV requires further deliberations.
[18]	2021	Multi UAV authentication	6G network aspects, challenges and requirements need to be covered.
[14]	2021	UAV-UAV authenticated communication	
[20]	2019	UAV DAG protocol	
[24]	2021	UAVs based IoT and 6G	UAV analysis needs to be covered in detail.
[22]	2021	6G and UAVs	UAV security and blockchain reviews missing.
[23]	2020	Edge computing 6G and UAV authentication	UAV concepts, limitations and security requirements require further review with respect to latest trends.

1.2. Contributions

The major contributions of this paper are as follows:

- This paper considers the blockchain implementation in UAV systems in 6G-based UAV networks. We offer a detailed audit of past work and future directions for the subject domain.
- We isolate UAV systems in 6G application prerequisites into two wide categories with the objective of making the blockchain and UAV network in a 6G combination that is simpler to obtain. This first category, called the Performance Group (PG), is included in Sections 2 and 3.
- We incorporate the execution-related needs on information rates, inactivity, unwavering quality and enormous networks. These performance requirements will help enable ubiquitous communication. This second category, called the Specifications Group (SG), is included in Sections 4 and 5.
- We include the security-focused authentication-based needs on data integrity, non-reputability and audibility. It is worth mentioning that above categories typically classify the highlighted needs and broadly cover the related aspects in the stated sections.

1.3. Paper Structure and Organization

The remainder of this survey is organized as follows: In Section 2, we begin our examination with a discussion of architectural features and fundamental principles in UAV technology. In line 6G, Section 3 offers a review of UAV technology. The two sections broadly discuss aspects categorized in the Performance Group (PG). The light weight authentication protocols are discussed in Section 4. In Section 5, we discuss the most recent developments, difficulties and research directions in the field. These two sections widely include aspects categorized in the Specification Group (SG). As a result, Section 6 concludes the survey. The overall structure and organization of this paper is depicted in Figure 2. In this paper, acronyms are included in Table 2.

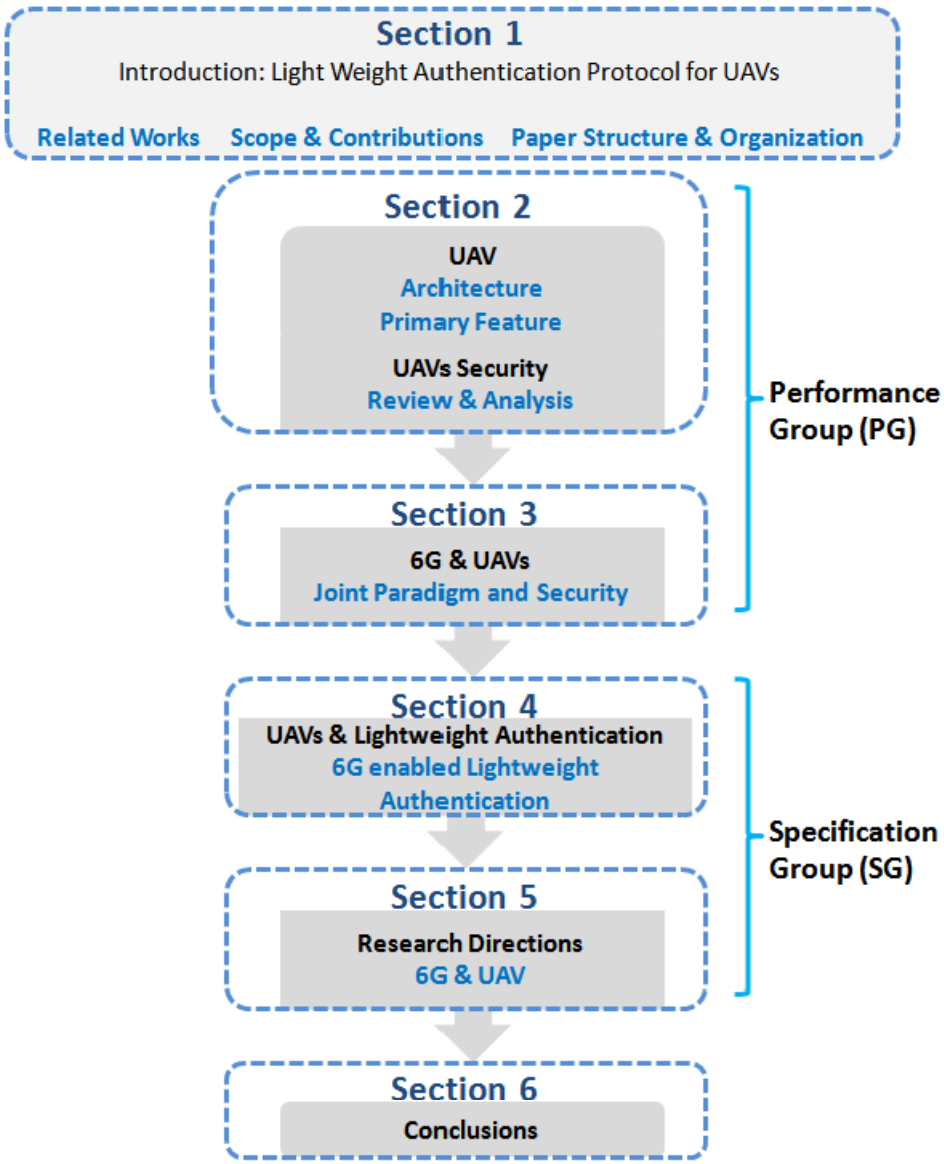

Figure 2. Structure and organization of this paper.

2. UAV Communication

As highlighted in the preceding paragraphs, this section and its sub-sections cover first category, the Performance Group (PG). Unmanned aerial vehicles (UAVs) have enormous potential in the universal domains including civil, defense, media and public domains [25]. They have unprecedented and useful applications where human lives can otherwise be in danger. In addition to this, multi UAV systems are jointly mission capable and can accomplish the same but better economy, precision and efficiency compared with solo UAV systems. However, there are many concerns that are required to be resolved before the effective use of unmanned aerial vehicles for the provision of reliable, assured and context-focused networks. In view of the distinctive characteristics of the UAV networks and the need to address related issues, considerable work is yet to be carried out in this area. Current progress in the domain of mobile adhoc networks (MANETs) and vehicular adhoc networks (VANETS) is not sufficient to address the peculiar nature of UAV networks. UAV networks may vary from slow dynamic to dynamic as some have intermittent links and topology that is relatively fluid. Meanwhile, it is considered that adhoc mesh networks may be one of the most appropriate domains for UAV networks. Moreover, it is a pertinent fact that the topology of multi UAV networks has been a less researched area.

Software defined networking (SDN) can be the answer to enable flexible deployment and management of future applications [26,27]. Moreover, the stated technology may achieve benefits such as availability and security in networks and cost reduction [28,29]. Moreover, fundamental characteristics such as flexibility and reach demands of UAV networks go beyond the scope of MANETS and VANETS. Furthermore, future UAV network application necessitates protocols that would cater needs of intermittent links, high mobility, power constraints, dynamic topology and varying link quality [30]. UAVs may be utilized for different profiles and missions depending upon their size. Smaller UAVs may be used in swarms while large UAVs may be used in solo missions. Stated roles of UAV networks have diverse as well as enormous potential in civilian applications. The authors of [31] state that UAVs are going to possibly be an invaluable addition in the operations of security organizations including fire brigades and police departments. However, future progress in the domain of sensors and electronics technology has enhanced the scope of UAV network applications [32]. This will likely include applications such as remote sensing, remote damage assessment, traffic monitoring and diverse traffic monitoring [33,34].

The primary challenge in all the distributed systems such as UAVs, drones or mobile IoTs is a robust authentication mechanism. We characterize the UAV communication in the following paragraphs for presenting a holistic understanding of authentication requirements in diverse domains of UAV systems.

2.1. Characterizing the UAV Network

It is necessary to characterize a network to comprehend its nature, authentication-related limitations and opportunities [35]. How does the topology of the UAV network affect the authentication requirements?

As nodes fail or migrate away, how often does the network become partitioned? What can be done to extend the network's life? Is it necessary to have self-organizing and self-healing abilities? What kind of structure would be more appropriate? Which authentication protocols can be executed at various layers? Is it possible to dynamically add and remove nodes with authentication? Are the connections intermittent and how good are they? In this section, we present a comprehensive view of the characteristics that run across all of the works, as well as the research trajectory in UAV networks. This section presents the emerging UAV network requirements to comprehend the security-related work in subsequent sections.

2.1.1. Multi UAV Network

The utilization of a single large UAV for a mission was common in the early days of UAV use. As a result, in these systems, the UAV-based communication network only had one aerial node and one or more terrestrial nodes. The UAVs in a multi UAV system are smaller and less expensive and they have the ability to work together. multi UAV systems may now be used to carry out most public and civic applications more efficiently [36]. The communication network, which ensures communication between UAVs and between UAVs and ground nodes, constitutes a key component in most multi UAV systems. These UAVs can be designed to cooperate together to provide services and function as relays to extend network coverage. The mobility of UAVs is determined by the application. For example, in order to provide communication in an earthquake-stricken area [37], UAVs would hover over the operation area and the linkages would be slow and dynamic. The fact that the UAVs may go out of service due to failure or battery drain demonstrates the dynamic nature of the network setup and connectivity. Agricultural and forest monitoring applications, on the other hand, demand UAVs to move across a vast region, with links breaking and reestablishing often. This is also true for UAVs that must hover over an area for extended periods of time. To take their place, new unmanned aerial vehicles must be launched.

Some of the UAVs may be pulled out of operation to save power until a more appropriate time comes. As a result, it would be a requirement that the linkages immediately

reconfigure themselves in all such circumstances. Multi UAV systems, while beneficial in many ways, complicate the UAV communication network. Reliability and survivability through redundancy are two significant advantages of multi UAV systems. When a single UAV fails in a multi UAV system, the network must reorganize and retain communication through other nodes. In a single UAV system, this would be impossible. However, in order to gain the full benefits of numerous UAVs operating together in a multi UAV topology, the protocols in place must address concerns such as power limits, mobility and changing topology [38]. Figure 3 illustrates the multi UAV system; each UAV struggles to address mobility and varying link' quality dividends in an ever changing topology during the flying role. As per interference requirements, the UAV link selection and topology should be dynamically optimized. The phenomenon is a governing element in terms of authentication protocol implementation in a multi UAV network. A single UAV system would have to maintain communication linkages with the control station(s), servers and base stations as well as provide access for functionality. The limited battery power and bandwidth are severely hampered as a result.

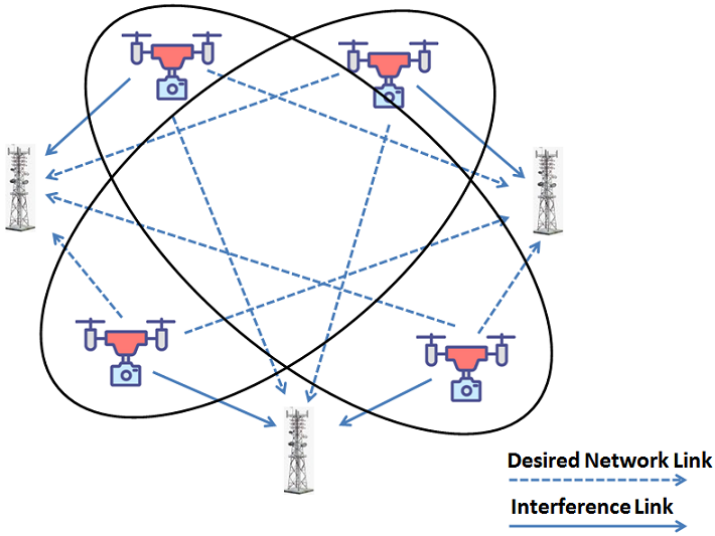

Figure 3. Multi UAV system and varying links' quality demands.

In a multi UAV system, one or two UAVs can be utilized for the provision of feed to other UAVs in the network. Moreover, some can connect to control the network [39]. In order to provide access ability for voice, data and video, the UAV network will have to retain the mesh architecture. Additionally, maintenance and operational cost of multi UAV systems is relatively less expensive than their legacy equivalents. In this study [40], it is stated that the communication umbrella range provided by multi UAV infrastructure can be easily enhanced by adding more UAVs to the mesh. Missions carried out through small UAV systems are usually cost effective compared to solo UAVs. Moreover, missions are completed with even better efficiency and speed [36]. The authors of [41] have elucidated the results of the successful accomplishment of missions by explaining multi UAV networks based on PRoPHET routing protocol attaining the capability of finding a path, even if two end points are not directly connected. In the study by [42], the authors present their research on multi UAV systems and explain how multi UAV systems are reliable and even robust to loss. The vital benefits emerging from multi UAV systems result in the enhanced use in civilian applications [43].

2.1.2. Infrastructure-Based or Adhoc UAV Networks

UAV networks are usually referred to as ad hoc networks in the existing literature. Most of the discussion in available research relates VANETs to UAV networks; moreover, MANETs are also related to UAV networks. However, the stated studies do not address the

explicit properties of UAV networks entirely. Depending upon the utilization and nature of the mission, the UAV network could be attributed to slow moving, feature-like hovering, high mobility missions and slow mobility profiles. One of the pertinent applications of UAV nodes is to function as a sky-based communication-based station, ensuring provision of reliable coverage over a good span of area [44]. UAV networks could perform functions such as infrastructure-based systems for applications dissimilar to VANET and MANET networks. In such scenarios, UAVs would exchange data with one another in parallel with designated control centers [45]. Such network would be identical to a wireless network that is fixed with UAVs acting as aerial base stations. The infrastructure-based UAV network clearly diversified the authentication requirements. Moreover, there is a group of roles in which nodes have high mobility and collaborate, construct and communicate with the network in an ad hoc manner [45]. The aerial network of UAVs demonstrating adhoc base station systems is illustrated in Figure 4. In this scenario, the architecture and nodes involved in data forwarding can be ascertained on a dynamic basis. A considerable number of challenges are faced by both UAV adhoc and UAV infrastructure-based networks [46]. Such as replacing power exhausted nodes or failing nodes by new nodes.

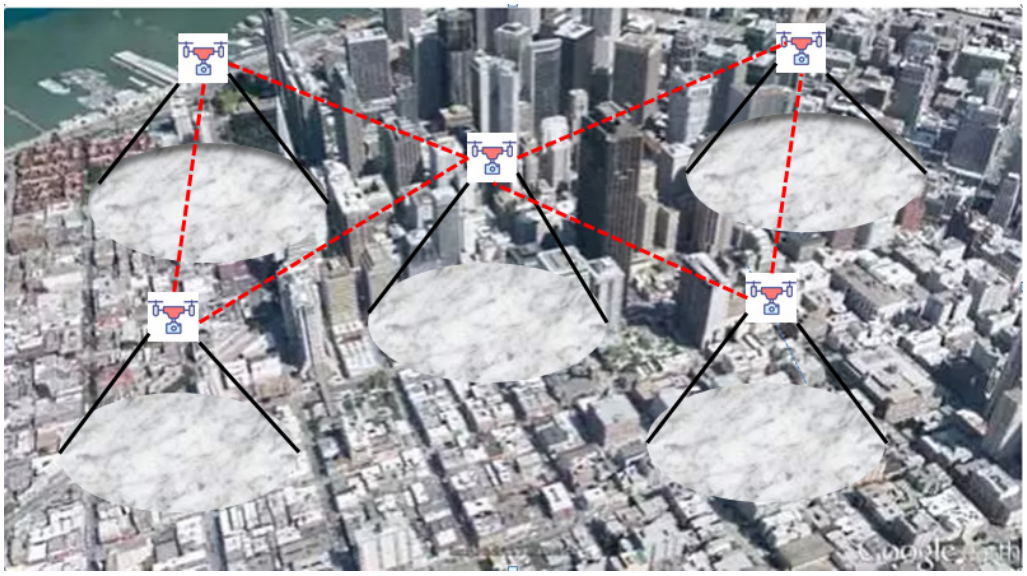

Figure 4. UAVs serving as aerial adhoc base stations.

Any wireless mobile network is vulnerable to link disruptions. The networks of unmanned aerial vehicles (UAVs) are no exception. In situations where UAVs provide communication coverage across a large region, the UAVs hover, thus the likelihood of disruptions is low. On the other hand, disruptions are more likely in applications that require rapid UAV mobility [47]. The amount of disruption is determined by the mobility of the UAVs, the amount of power transmitted, inter-UAV distances and external noise. Delays in data transmission could be caused by low network quality or by one or more UAV nodes holding the data due to a lack of an end-to-end path [48].

2.1.3. Server or Client?

Whether the node is in the role of server or client is another distinction. In vehicular networks, the nodes are usually servers and in adhoc networks, the nodes usually act as clients [49]. UAV nodes usually act as servers and perform relaying functions of sensor data and packet forwarding [50]. They are also utilized for provision of data forwarding to other UAV clients. Figure 5 is a depiction of a widely used server–client implementation of UAV network is surveillance mode.

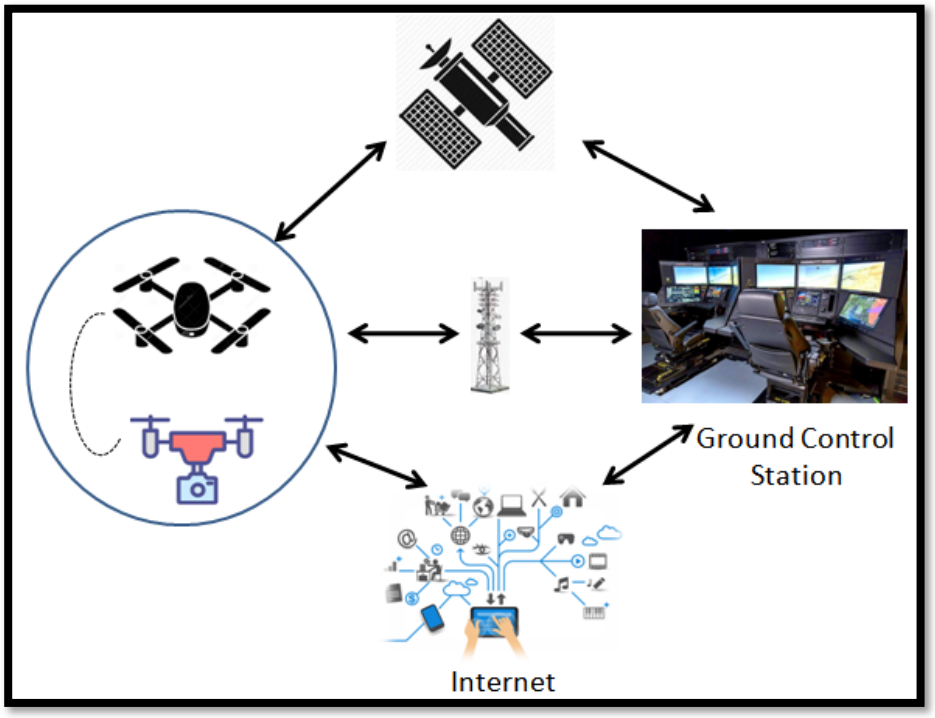

Figure 5. UAVs relaying packets for clients/sensor data to control centers.

2.1.4. Star or Mesh?

UAV network topology for communication applications is an area that has received little focus yet. A solo UAV driven by a single command and control station is the most fundamental system. Multi star, hierarchical mesh, star and mesh are network architectures that can be realized in a multi UAV system. In a star topology, all UAVs connect directly to ground nodes. Moreover, all types of communication are ensured through ground nodes between UAVs. In this scenario, there is the possibility of latency, intermittency in links and need for high capacity downlinks. Moreover, in view of the mobility aspect, steerable and direction-seeking antennas may be needed to keep a correct point of reference towards the ground node.

In some of existing literature, the researchers argue that legacy network technologies will not meet the demanding needs of UAV networks. In related studies, employment of mesh networks is advocated for civilian applications [50]. Multiple considerations including alterations in topology, interference, transmission deviations due to power constraints, multiple links on antennas, variation in number of network nodes, topography and weather constraints are all familiar. There are several challenges related to adhoc networks including formations that do not maintain symmetry, network nodes shifting away during mission profiles and intermittent connectivity. However, optimally configured mesh network systems would be capable of addressing some of the known issues [51]. In order to have fully converged networks and address the above stated issues, future networks necessitate self-healing attributes. Moreover, networks must ensure reconfiguration capability over wrecked links and consistent connectivity for successful accomplishment of mission profiles. Figure 6 depicts the star and mesh topology of UAV networks.

2.2. Security in UAV Communication

Internet of Things (IoT) acts as an interface between the physical world and computing systems; IoTs perform this role by transfer of information regarding the physical atmosphere after sensing and necessary analysis. Internet of Drones (IoD) is a classic mobile IoT system [52,53].

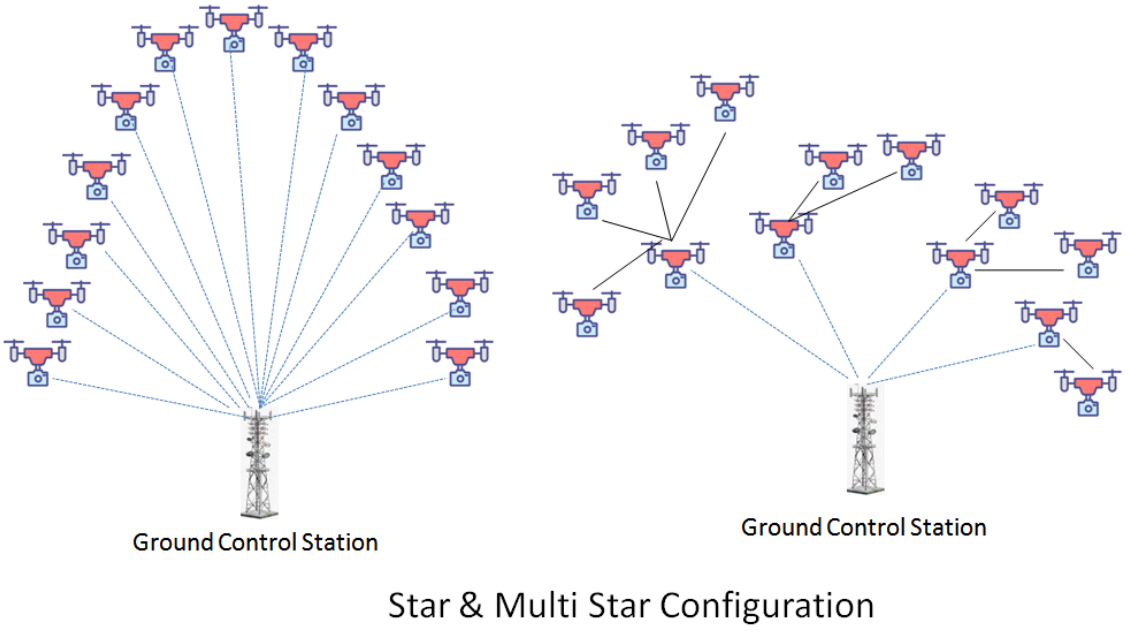

Figure 6. UAVs wireless mesh networks.

In the latest years, unmanned aerial vehicles and drones have become a popular application in several fields due to its inherent characteristics including reach, exploratory abilities, flexibility, speed, life safety in case of difficult missions and coverage, etc. Keeping in mind advancements in this domain, the public's demand has invariably increased. Moreover, there is increased demand against consumer grade drones across the globe as engagement of UAVs in different applications and roles is becoming widespread. The employment of UAVs in various fields has increased manifold, including in shooting movies, drone selfies, agriculture businesses, and security objectives; all are utilizing these aerial devices. Growth in UAV commerce is expected to accelerate upwards at a rate of at least 29.9% per annum in upcoming years. Moreover, the industry volume is expected to rise to approximately 4.9 billion dollars at the end of the coming three years [54].

The prominent progress UAVs have made is in the IoTs, and they have promising applications in the future that will accompany generations to come. One of the major concerns that needs to be addressed before time is security of communication in the employment of Internet of Drones (IoD). For example, to accomplish unlawful border breaches in 2016, drug dealers from Mexico carried out signal spoofing of navigation satellite and attacked border patrolling aerial carriers. In July 2016, Nils Rodday cautioned very clearly that drones without encryption features are prone to hijacking, raising serious security concerns of drones. Nils Rodday is a well-known security expert from IBM and presented this important concern in a security summit held in Asia. Similarly, the Iranian military caused a serious loss of information when they successfully hijacked and seized US MQ-9 UAV in 2019. Therefore, communication security of unmanned aerial vehicles during different roles such as patrolling and surveillance necessitates immediate and robust measures to ensure the same [55].

Two critical properties of UAVs as a smart IoT apparatus are resource limitations and the varying environment. Moreover, UAV network connection conditions including AP servers are subject to constantly changing position and environments. Consequently, the identity of every element of the UAV network must be periodically authenticated in multiple cycles. Moreover, due to the mobility of these smart devices, which are embedded with smart features, they face noteworthy limitations such as power constraints and processing power. Furthermore, the endurance of these devices and other abilities will be adversely affected if an excessively recurrent and sophisticated authentication scheme is defined for them [56]. In the IoD paradigm, avoiding mishaps such as loss of assets, loss of

the drone itself, and most importantly loss of life and vital information due to breach of network and any compromise, ensuring the overall protection of the IoD environment is currently a decisive issue. Pertinent threats to the IoD environment include jamming [57], spoofing, Denial of Service (DoS), eavesdropping and MiTM. Figure 7 symbolizes major issues relating to the IoD security environment.

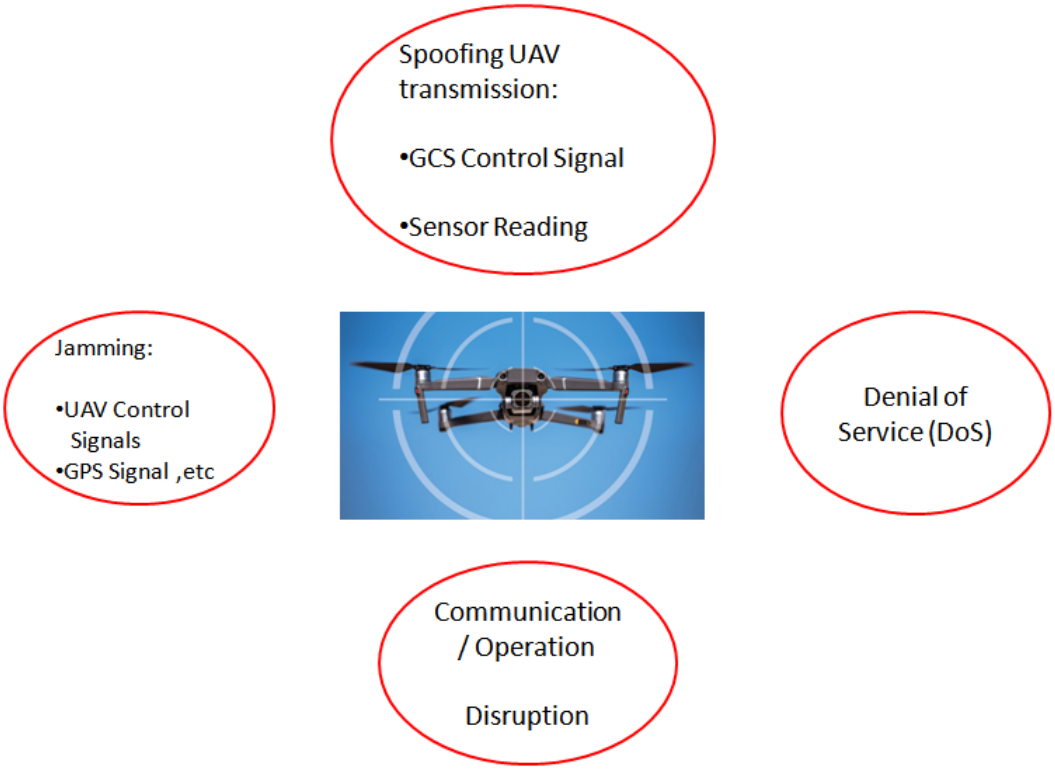

Figure 7. Security challenges in UAV communication.

There is a considerable boost in utilization of UAVs in different applications as stated above and this aspect has surfaced potential security concerns, specifically in networking and communication protocols [58,59]. Zhao et al. [18] have highlighted that, in order to detect the invasion of proletarian UAVs, 60 GHz frequency band have relatively superior performance than the over-cluttered frequencies, i.e., 2.5–5 GHz. One of the major hazards, named the Jelly Fish Attack, has been investigated by Thomas et al. [60] by utilizing MANET in combination with UAV networks. They have devised a multicast protocol-based system that provides resistance to such attacks. On the basis of most stable and secure paths, the routing algorithm determines trustworthy nodes [61]. Cryptography is another foundation to ensure protection of information in vehicles. In their study [60], Ramdhan et al. have offered a data collection mechanism that is based on optical code word. Some others have suggested layered unmanned aerial vehicle network topology with drone nodes, sensor and data collection nodes at different levels.

In such scenarios, network-related concerns are catered through two approaches, firstly by utilizing the above mentioned idea of optical code words to classify network nodes and secondly, transportation of designated data from UAV node to root node for mandatory required supplementary processing and subsequent decision formulation. Homomorphic cryptography controller-based security appraisal has been investigated by Cheon et al. [62] by devising a realistic linearly homomorphic Authenticated Encryption (LinHAE) for implementation of the controller. The Advanced Encryption Standard (AES) encryption key [63] extracted from the operator's EEG (electroencephalogram) signal was utilized by [64]. In the study [65], Quist et al. utilized a quantum key allocation procedure to generate secret keys., in order to encrypt video. The keys are distributed and their identity

is known by two persons on opposite channel end. Without being detected, it is difficult for any eavesdropper to capture messages, as each photon is altered instantaneously once read and corresponds to a qubit. In the study [66], Steinmann et al. describe that, by utilizing an encryption key negotiation method, protection and validation of data carried out on UAVs in partitions and transferred in between ground station can be ensured.

3. UAV 6G Networks

The explanation on aspects classified in our first category, Performance Group (PG), continues in this section and its sub-sections. In this segment, we present a few of the futuristic applications related to 6G. Figure 8 depicts future advanced applications that will work hand in glove with UAVs in 6G and beyond networks. Moreover, mandatory requirements in connection with the subject are also discussed. It is pertinent to mention that UAVs will be an integral part of such future applications in connection with several aspects of application needs. Most importantly, in many future scenarios, drones will act as Aerial base stations for the provision of wide area coverage of 6G networks.

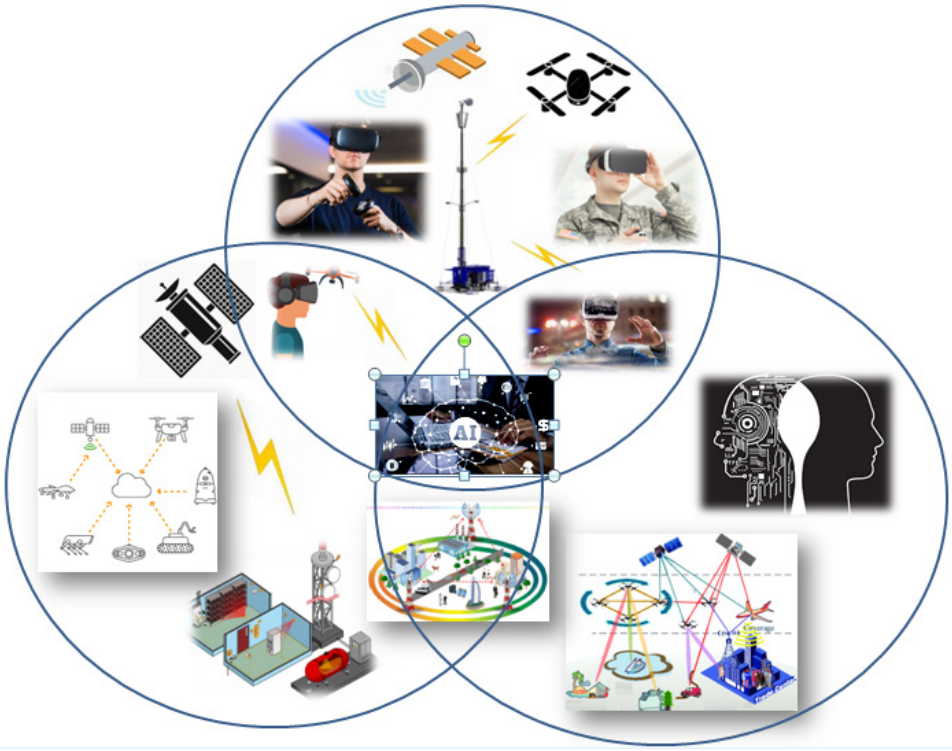

Figure 8. Future applications supported by UAV system in 6G environment.

3.1. 6G Applications

Future advanced applications will work hand in glove with UAVs in 6G environments. Imagining the role of drones in futuristic applications in 6G environments has unprecedented dimensions. UAVs will have countless employment roles in future applications.

3.1.1. Human Bond Communication

This subject matter relates to data commencing from the five senses of humans to permit robots, drones and humans to share even expressive, comprehensive and realistic communication. Because a lot of personal information will be transferred, this application would necessitate stringent security measures.

3.1.2. Wearable Technology Based Futuristic Applications

Brain computer interface, wearable clothing and technology are futuristic ideas that demand robust security for sharing the data. Current wireless networks including 5G are not capable to utilize numerous future prospects that are beyond the traditional medical ways.

3.1.3. XR Apps with Multi-Sensory

Extended reality multi-sensory applications are designed in a way for the provision of user experience that is entirely enchanting by amalgamating the reception from human sensory, environment and, human body moves, and several data originators. In view of the above, the aspect of data integrity is mandatory for such applications, as any malicious attack can be devastating and can spoil the user experience.

3.1.4. Autonomous Systems Connected through a Wide Range Network

Networked together autonomous devices including self-driven vehicles, delivery methods based on drones and robots based on autonomous technology are part of ancillary field, where 6G has potential uses. These applications require all three 5G service classes at the same time. In order to meet this end, 5G slicing cannot be a possible solution.

3.1.5. Support for Vertical Domains

The KPIs identified by 3GPP against secondary and core QoS for vertical commerce, in which identical services and artifacts are offered, include energy, automation, health and manufacturing. In the near future, 5G will reveal its inability to cater the ever increasing number of networked devices in vertical industries, when we discuss mMTC.

3.2. 6G Application Requirements

With the goal of making blockchain utility more understandable, in this study 6G applications are separated into two major groups. Ultra-reliability, low latency, increased data speeds and huge connection are among the typical criteria. I view of the pertinent factor in almost entire wireless communication generations, these needs are made part of the first category. These are referred as Qualification Group-I (QG-I). QG-I standards necessitate considerable improvement for potential 6G applications. The prime features for any reliable and secure network include non-reputability, confidentiality, defined level of secrecy, data integrity and auditability. These features are catered in second group named Qualification Group-II (QG-II).

Based on the literature review and future application requirements, it is established that applications based on the 6G network in the future will be bandwidth hungry and will utilize abundant data originating from different sources, including all senses of human being, other devices. Said requirement will demand employment of requirements as divided in QG-I and QG-II. There is a lot of discussion in 6G vision papers about various technologies that can help with additional improvements in QG-I values. A few of the important 6G technologies include AI, Reconfigurable Intelligent Surface and THz communication [67]. We predict that improvements in these upcoming technologies and communication models will certainly facilitate 6G systems for the provision of high broadband capacity to even a bigger number of network nodes ensuring low latency and improved reliability. On the other hand, there is little mention of QG-II in the 6G literature. This is attributable to a number of factors. The scope and description of the security feature may change in connection with scenarios in different applications, on the basis of character of different units concerned that include machines, devices and controller. Hence, assigning responsibility for meeting these needs is therefore not straightforward. Fixing QG-II values will become more difficult as the complexity in requirements related to potential 6G applications increases.

UAVs will be employed with prominent roles in futuristic 6G communication models due to their low cost and flexibility of deployment. In said, context, unmanned aerial vehicles (UAVs) have received a lot of press recently, both for military and commercial

purposes. 6G is designed to be an all-coverage network that can connect people in space, on the ground and underwater. UAVs can provide wireless coverage from the air in a variety of ways, such as Aerial base stations for users globally, relays to provide coverage to dispersed nodes and typical mobile network end users. Small UAVs have limited onboard power that results in limited capability of these devices for provision of temporary wireless communication. It becomes a significant problem to extend the lifetime of UAVs and produce green UAV communication with low power consumption.

For future air transportation, 6G technology can make use of non-terrestrial networks (NTNs). "Connectivity from the sky" is one of the most groundbreaking 6G networking trends. In 6G communication, non-terrestrial network amalgamation is one the potential aspect. NTN provides aerial vehicle networking in air space for ensuring worldwide omni-present communication services [60]. Currently, TNs have limited capacity to ensure required connectivity as well as coverage to UAVs that are mobile with faster speeds. Consequently, Air-to-Air and Air-to-Ground are employed for commercial airlines and are not expected to serve networking facilities to future populated aerial vehicles. As a result, 6G is a suitable and enabling technology for UTM systems. In the studies [50,51,60], communication technologies such as NR, 4G, 5G and futuristic 6G technology including other future revolutionized technologies including artificial intelligence, integrated radar, smart detectors, XR, autonomous systems such as UAVs, brain computer interface based on wireless and AI-based future communication models are studied and compared. 6G is anticipated to provide 100 times more coverage for connectivity and multiple times the performance. The pertinent revolutionary features in the upcoming 6G communication model are AI, machine learning, TeraHertz communication, drone connectivity through terrestrial and non-terrestrial networks [52,65,67] and wireless power transfer [53,64]. This will serve max of 1 Tbps per device data transfer speed. Moreover, ensuring at least 1000 km/h mobility support to airborne vehicle flying in a densely populated metropolitan environment. The communication requirements for UAVs, as well as their capabilities and 6G functions, are listed below.

3.2.1. High-Precision Positioning and Seamless Coverage

Unmanned aerial vehicles performing operations while airborne at various level of air space necessitate accurate positioning, precise navigation and excellent network coverage and the same aspects are vital for the network's growing infrastructure, expansion and convergence as shown in Figure 9. While the UAVs are flying independently, a secure connection and vast network coverage ensures uninterrupted connectivity. Covering a wide range of coverage at varied elevations while maintaining seamless connectivity is a critical problem for 4G/5G cellular networks. Positioning based on high precision is expected to be provided by 6G while employing radar technology. Moreover, utilization of modern concepts such as 3D placement permits the accurate locating of unmanned aerial vehicles and moving devices in the sky [68]. Upcoming, 6G communication networks may enhance the quantity of connected unmanned aerial vehicles in densely populated scenarios by 107 devices/km^2 which is 10 times greater than its predecessor, wireless communication model density. Beyond the vision line of sight, improved quality, robust, reliable and secure networks with vast speedy coverage, the 6G network is expected to provide connectivity that is efficient, cost effective and speedy, promising the future needs of the world [69]. The high-speed OWC system's high-capacity backhaul network enables a significant volume of UAV traffic data.

In the study [70], 6G multilayer architecture comprising of terrestrial layer, airborne layer and space layer is discussed. Marko et al. describe satellite communications asnow undergoing significant advancements and 6G technology is being integrated into satellite networks. This is paving the way for a significant global turning point in the satellite-enabled service industry. 6G communication model integrated with satellites will provide enveloping services worldwide to support both dense and less-dense areas. In order to materialize the same, 6G systems are required to amalgamate terrestrial, airborne assets

including drones/ UAVs and satellite infrastructure in different orbits. 6G technologies are to offer dependable, guaranteed bandwidth connections to users on ships in the sea, in the air, trains and in cars covering entire globe. Satellites assist operations with the provision of the desired bandwidth connection. Without existence of significant terrestrial infrastructure, satellites would be able to provide connections that are considered reliable in a sustainable manner.

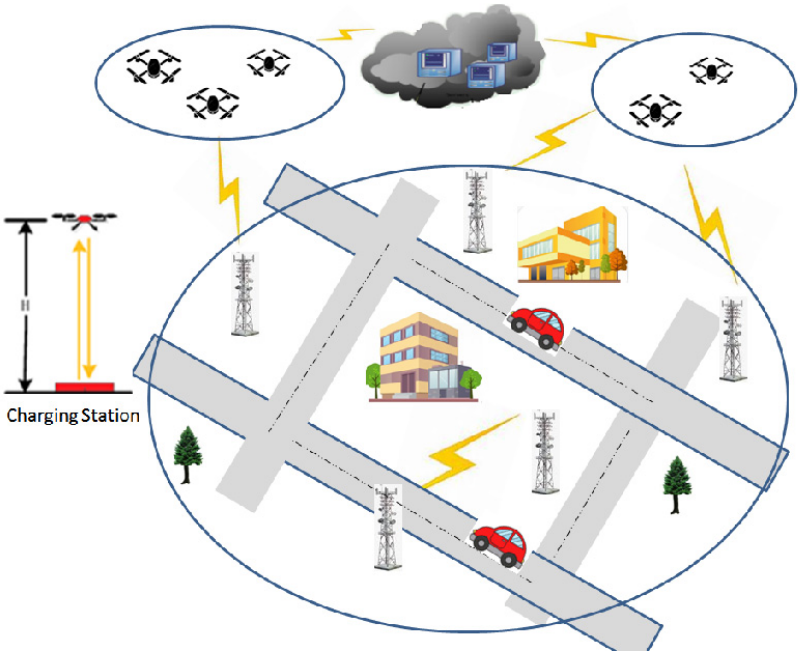

Figure 9. Multiple layers of the airspace with high-precision positioning.

In the study [71], space–air–ground (SAG) integrated network is discussed in detail. It states that UAV systems can be employed as a service to supplement the idea of 6G-SAG in future. Moreover, blockchain technology is a vital requirement for 6G-SAG, in order to store network activity logs in an immutable, decentralized manner. Through employment of cryptographic hash drones, ground stations and satellites can serve as the block storage media.

In the study [72], it is envisaged that 6G network would ensure the provision of numerous services and unblemished network coverage for everyone and everything. The integrated satellite–terrestrial network architecture promises to provide worldwide broadband connectivity by combining advantages of both types of networks, to a wide range of users around the globe. The stated perceived communication model has already received attention from both academia and business.

3.2.2. Remote and Real-Time Control (RRC)

Unmanned aerial vehicles are operated through remote and real-time links and a continuous feedback from designated UAVs is received by establishing links through this media. Equipment status, location and other sensory data are received at ground stations from UAVs. In order to ensure seamless command and control of UAVs over wireless communication media, latency and data rate are pertinent considerations and specific required criteria must be fulfilled. In potential 6G networks, a bigger number of unmanned aerial vehicles can be operated and even these machines can accomplish different mission profiles in autonomous mode without direct operator control [73]. Integration of 6G communication infrastructure with satellites can result in vast coverage and required level of remote command and control. Moreover, a latency value of less than 1 ms is also promised in 6G networks, which can bring significant improvement in future UAV networks.

3.2.3. Multimedia Transmission

Based on mission profiles and to ensure the prompt provision of data to ground stations, unmanned aerial vehicles transport live data such as video, other sensors data for timely analysis and subsequent decision making. In future, modern multimedia services will be one of major demands through UAV platforms. These include multimedia applications related to virtual reality, 4K and beyond films, holograms, etc. These advance multimedia services require high data rates and bandwidth to provide true experience to users in connection with applications such as virtual reality and 3D holograms. The envisaged 6G network is capable of providing high bandwidth and throughput in UTM [74]. In order to ensure, seamless communication of UAVs with the ground control station and reliable traffic between the two ends, mandatory high bandwidth requirements are required to be promised, which will be offered by 6G in future. A data rate of 10 Gbps is anticipated in upcoming 6G technology [75]. The multimedia application of UAV is depicted in Figure 10.

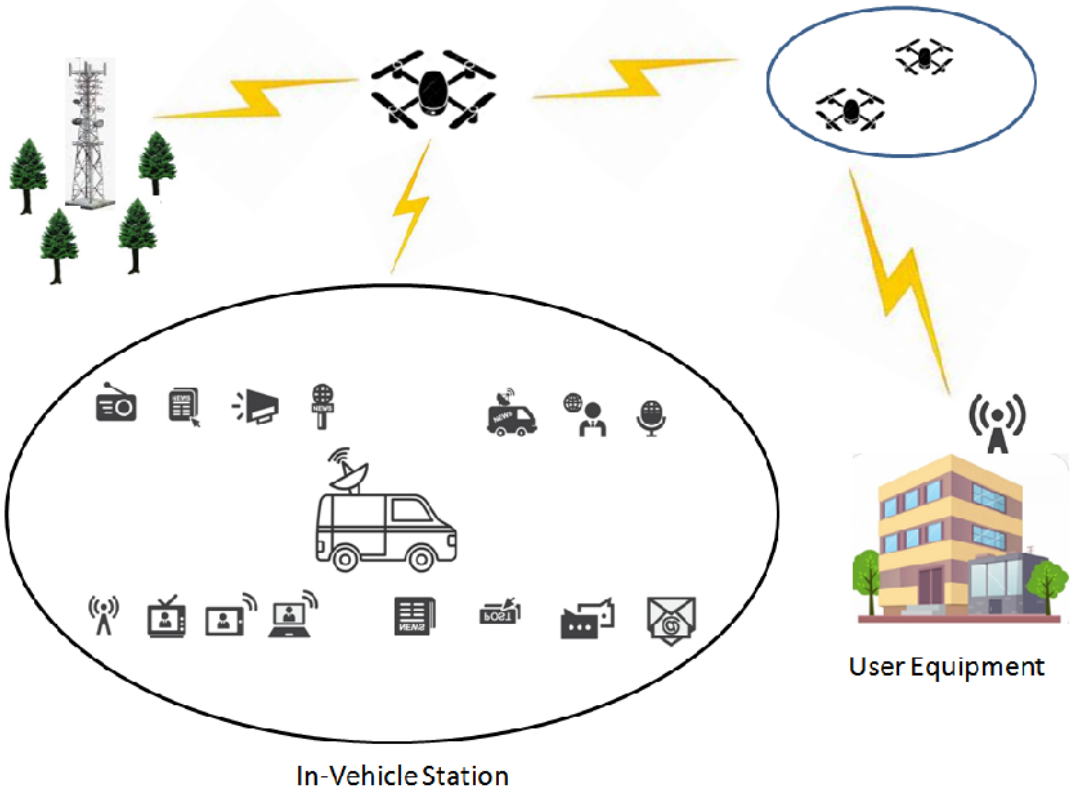

Figure 10. Multimedia application of UAVs.

3.2.4. Aircraft Identification and Regulation

An automated dependent surveillance broadcast (ADS-B) system is utilized for the identification of commercial aircrafts. Because of the increased number of UAVs in future applications, the usage of ADS-B may inundate the designated frequency band [58]. In view of this fact, a new scheme for the identification of commercial flights is deemed necessary. Radio waves are used to convey the remote ID. Registration, identification, tracking and regulation of aircraft all require reliable cellular network connectivity. In the same way, remote ID data can be utilized in the integration with future 6G networks. By effective monitoring of UAVs status data, positioning and related information, early warning along with subsequent remedial measures can be executed on the basis of monitoring parameters. Probable threats can also be contained after due analysis of the received data [76]. Low altitude authorization and notification capability (LAANC) for UAVs allows UAV operators to approach controlled airspace near the landing strips, air bases, Commercial

airports through valid authorization based on real-time system for management of active geofencing [77]. The prominent UAV Regulations Domains are depicted in Figure 11.

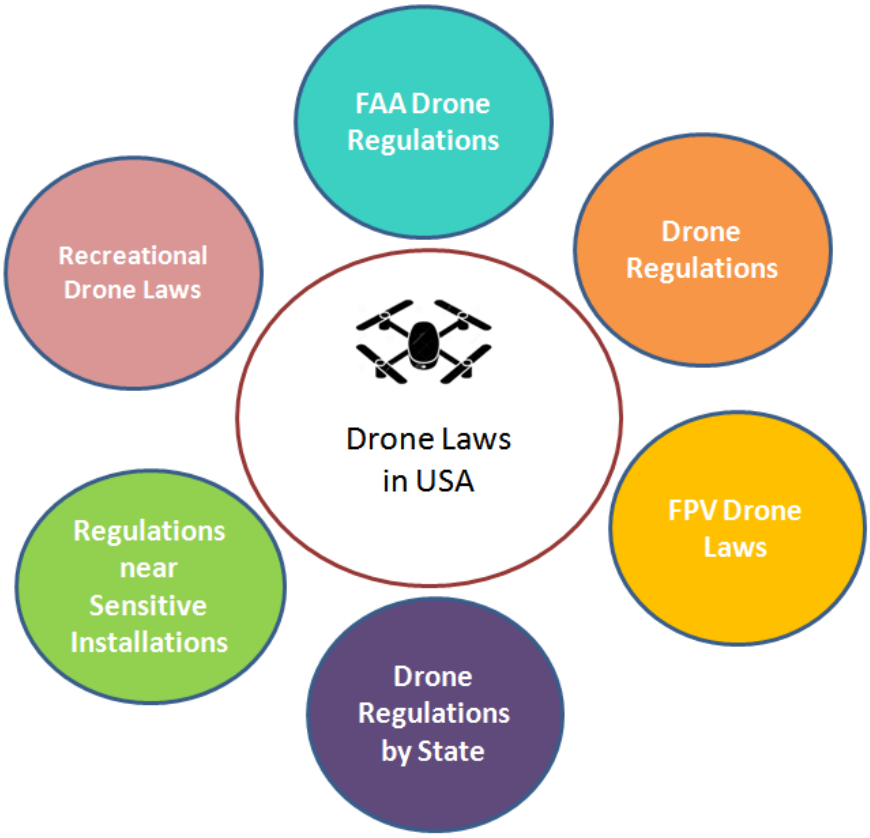

Figure 11. UAV regulations domains.

4. Authentication in UAV Networks

Unmanned aerial systems (UASs) consist of one or more than one UAVs. The stated unmanned aerial vehicles are operated and controlled through a reliable communication channel by GCS [78]. Utilization of UAVs is found in commercial, civilian and military uses. From surveillance to reconnaissance, security purposes, traffic monitoring, items delivery, etc., all are applications of UAVs employing modern communication networks in the future. Swarm employment is providing promising advantages in multiple civilian applications [79]. Graceful degradation is achieved in case of any technical fault as alternate UAV can take over the mission role and task in such scenarios. Moreover, robustness as well as availability of communication with GCS is ensured beyond the line of sight through establishment of the Adhoc network [80]. The probability of mission failure is minimized as in the swarm system, multiple UAVs are employed which act as system redundancy.

One of the pertinent advantages of these systems is reduced maintenance cost. Communication is of key importance in a flock of UAVs. The major reasons for communication needing to be robust and reliable in operation of such UAV networks is the high mobility of UAVs, irregular distance between each UAV nodule which results in inconsistent link quality, limited capacity of UAVs in terms of onboard available power and the ever-changing topology of the UAV network due to the mobile nature. Moreover, due to limited battery storage, unmanned aerial systems communication becomes challenging [81]. Secure networks are an essential requirement of worldwide users in connection with different applications and have been an unvarying challenge for researchers in ever-evolutionary modern communication models. Similarly, it has been a growing concern in unmanned aerial vehicle systems. It is a significant consideration in wireless networks that they are intrinsically insecure [82].

Wireless networks can be victim of sniffing, eavesdropping and other related wireless network attacks that include MitM, impersonation attacks, DoS [83] and Sybli. These attacks are vulnerable as they compromise privacy; moreover, they can result in major denial of the overall system by exhausting system bandwidth, memory, power, etc. [84]. The jamming of wireless communication between unmanned aerial vehicle system elements can be devastating. Functional as well as operational control of the unmanned vehicle can be lost through such attacks, causing overall system hacking by the enemy [85]. The classic example of eavesdropping is through man in the middle attacks as malicious element records and the transport of information is through passive means to attacker. Each eavesdropped information packet can be altered in Man in the middle active attack to take over the command and control of the UAV system or to inject manipulated data into the network system [86]. In the same way, such MitM attacks can be excessively destructive as the same can cause a complete crash of UASs by failing the complete authentication mechanism of the UAV network [87]. Replay attacks can result in overall compromise of the system as they target authentication systems by replay technique of already captured data to gain unauthorized access from the legitimate system server [88]. It is quite a successful approach by the attackers to obtain unauthorized system access. One of the techniques used by attackers is Sybil, in which a malevolent node plays to be numerous different people in the system. This attack allows for the injection of fake data and routing disruption [89,90]. This section covers elements broadly categorized in second category of Specification Group (SG).

UASs work with a minimum or no human interaction and the authentication process in such system is node to node. Approaching GCS by any node in UAS, it is vital that all nodes are authenticated. However, the limited computing and power resources of UAVs make off-the-shelf security solutions impractical [91]. To construct a secure communication channel, authentication and encryption are essential security features [63]. Cryptography is frequently employed in authentication systems. Typical authentication systems utilize cryptography during the basic steps of verification and certification [92,93]. In resource-constrained contexts, joint authentication is prone to man in the middle attacks. However, encryption prevents the denial of service attacks [94]. The authentication paradigm of UAVs is shown in Figure 12.

4.1. Light Weight Authentication Protocols

The use of WiFi has significantly increased over the years both at individual and commercial levels. Due to no complexity involved in installation and operational use of WiFi technology, the popularity of this wireless communication system is ever-increasing [95]. Moreover, it is a cost-effective solution in comparison to typical cable network. wireless sensor nodes are exploding in popularity, with applications as diverse as in any possible fields for the future [96]. These sensors are expected to be a ground-breaking addition in the consumer and business world. For example, the information collected by these sensors in a market place, in a particular section of a store, can turned into meaningful data for targeted advertisement, thus engaging visitors through tapped data by these small sensors for attracting customers and providing better services in consumer field [97].

In a wireless sensor network (WSN), each sensor collects a query from numerous wireless nodes and transports it to a database for subsequent analysis for converting data into meaningful information. The vital requirement in a secure network is authentication of network nodes. Similarly, in WSN, valid authentication of each element is vital. Light weight authentication is considered to be one of the time efficient schemes, mandatory in a heterogeneous network to reduce the period required for authentication process [98]. Reducing handoff latency is thought to be a difficult task. Once a mobile user requires to maintain utilizing the wireless service uninterrupted and remain connected while during a journey across the diverse communication network, this issue arises. For example, the access networks are switched by a user during traveling, staying connected on internet and accessing real-time mobile applications [99]. Interruptions, link quality and reliability

issues, security concerns, loss of data packets is experienced whenever there is delay in vertical handoff. Security, reliability, negligible interruption, appropriate handoff scheme are demanded in such applications [100]. In this arena, a number of strategies for reducing authentication delays have been presented. These solutions, on the other hand, do not entirely solve all of the concerns in the problem area; for example, they have security, monetary cost, signaling cost and packet latency flaws.

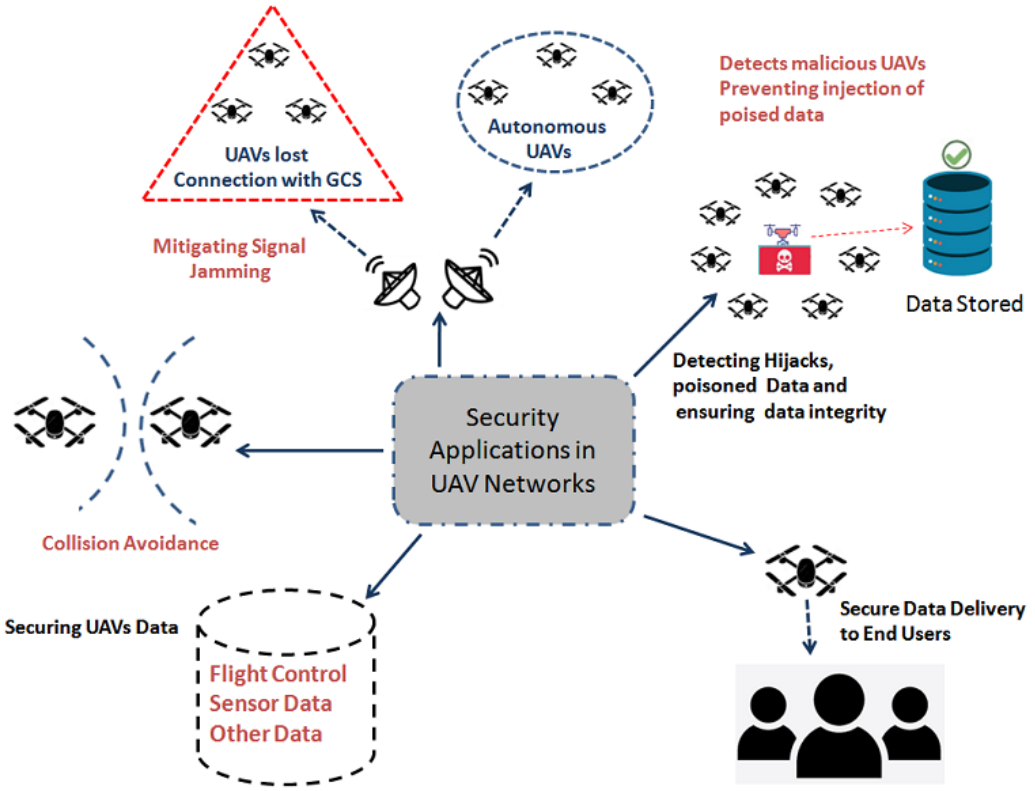

Figure 12. Authentication in UAV systems.

Table 2. Lightweight authentication.

Ref.	Concept	Description
[96]	UAV application	Military, business analysis, health and traffic analysis.
[97]	WSN-based applications	Business requirements for targeted advertisements and to show you how well you convert outside traffic into engaged visitors.
[98]	Data-sensitive communication	Techniques proposed to shorten the time necessary for authentication during vertical handoff across heterogeneous networks.
[99]	Handoff latency	Switch access networks while performing tasks such as accessing the internet. Using real-time applications, or working in cooperative information systems
[100]	Real-time applications	seamless and efficient handoff, service continuity with light weight authentication.

4.2. 6G Enabled Light Weight Authentication Protocols

In this study [101], a light weight authentication protocol is described that promises the privacy and security of a wireless network that is 6G enabled and supports a maritime IoT-based transportation mechanism. In order to critically verify the security features, methods such as real or random oracle scheme are employed. IoT integrated with blockchain schemes is one of the promising designs in connection with future applications ensuring

inherent requirements including security-focused authentication-based needs on data integrity, non-reputability and audibility.

Existing literature presents ideas related to IoT coupled with blockchain technology. However, a number of issues arise once pertinent considerations such as calculation burden and power limitations, thus other network overheads are examined in relation with blockchain technology implementation with IoT. In this study [102], integration shortcomings of blockchain with IoT are reviewed by assessing challenges and major inadequacies of these technologies. The main challenges include the inherent feature of authentication protocols to provide defense against probable attacks and other protocol implementation complexities. This paper [103] presents a light weight authentication scheme for Internet of Things. The protocol is spelled as "Light Edge" employing a hierarchy comprising of three layers. The three layers include a device layer, a secondary edge layer related to a clearinghouse for information about practices, policies and procedures on privacy, security, transparency and compliance and a third layer corresponds to the cloud service operator. The detailed examination in the paper describes the effectiveness of the suggested protocol against other methods in terms of protection against network attacks, cost effectiveness in respect to the overall communication model and time. An efficient and smart way of managing assets of a smart city is the development of state infrastructure that may cater requirements of numerous potential network technologies and huge data that flows through said networks. This research [104] describes a network topology for SCNM-LSM. The term SCNM-LSM stands for smart city networking model environments utilizing the light weight security module. This paper appends details regarding proposed artificial intelligence-based security features that are adapting to an IoT-6G environment [105]. In this network model, IoT devices are converged with mobile communication networks through various frequencies that include mm and THz waves. Major light weight authentication domains in UAV systems are shown in Figure 13.

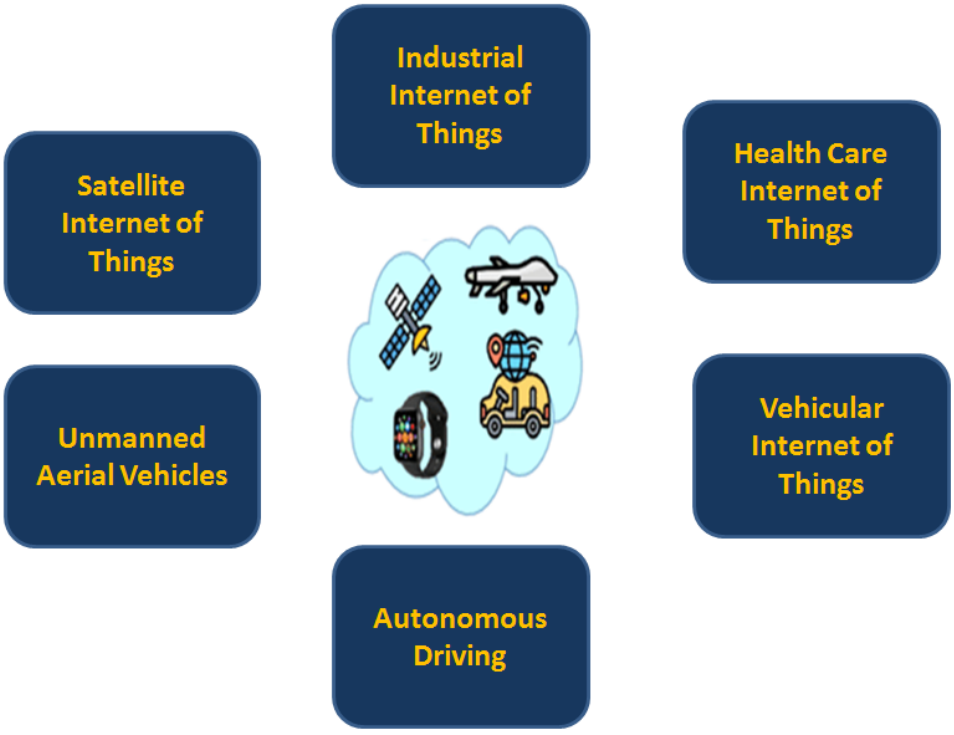

Figure 13. UAV systems light weight authentication domains.

In the study [106], in order to predict future yielding power, the EKF technique was employed. EKF stands for extended kalman filter. In the future 6G communication model, IoT devices are supposed to maintain a power yielding method. This aspect has a wide scope of utilization to meet energy limitations in the 6G environment. In the above stated

paper, a mathematical method was devised to compute energy requirements in parallel with several security models and finally adopt the best possible protection strategy as per network security requirement and to minimize energy depletion. In this paper [107], an authentication mechanism based on a set of rules that includes an authenticated key exchange and digital signature is devised to cater to security requirements of transported data. Furthermore, a thorough security examination was conducted that concludes that in the industry 4.0 environment, the proposed authentication mechanism offers protection against various attacks. Additionally, the detailed verification in this study proves the higher ranking of the proposed scheme once compared with existing studies. Due to limitations in frequency band resources, proficient management of this limited asset and judicious sharing holds fundamental importance. One possible scheme to address all this is blockchain technology. The inherent advantages offered by blockchain technology makes it the best choice for the security of future networks and data exchange and the upcoming 6G communication model is no exception An efficient employment model of blockchain technology in 6G networks will result in better network resource management, effective network monitoring and efficient resource sharing. In the study [108], the inherent capabilities of blockchain technology are examined in connection with 6G network resource sharing and management, in view of different scenarios. The different applications and circumstances that are discussed in this study include network slicing, IoTs, blockchain ecosystems and D2D communication.

Routinely, Internet of Things networked together employs a relatively weak model of security in use of the communication link. The communication is encrypted through the utilization of session keys. Moreover, in networked IoTs, the limitation of resource utilization is experienced which gives way to inefficient algorithms such as dynamic key generation. Secure interoperability and operation of IoT protocols is a significant issue in embedded devices with several resource limitations. This study offers a new scheme of dynamic key generation that is capable of functioning and producing a hefty number of keys that are unique. The suitability of such key generation algorithms is principally proven for Internet of Things modules and dependent conditions in which such devices cannot depend upon re-utilization of already in use keys for encryption and on unvarying key conciliation [109]. Light weight authentication in UAV systems is shown in Figure 14.

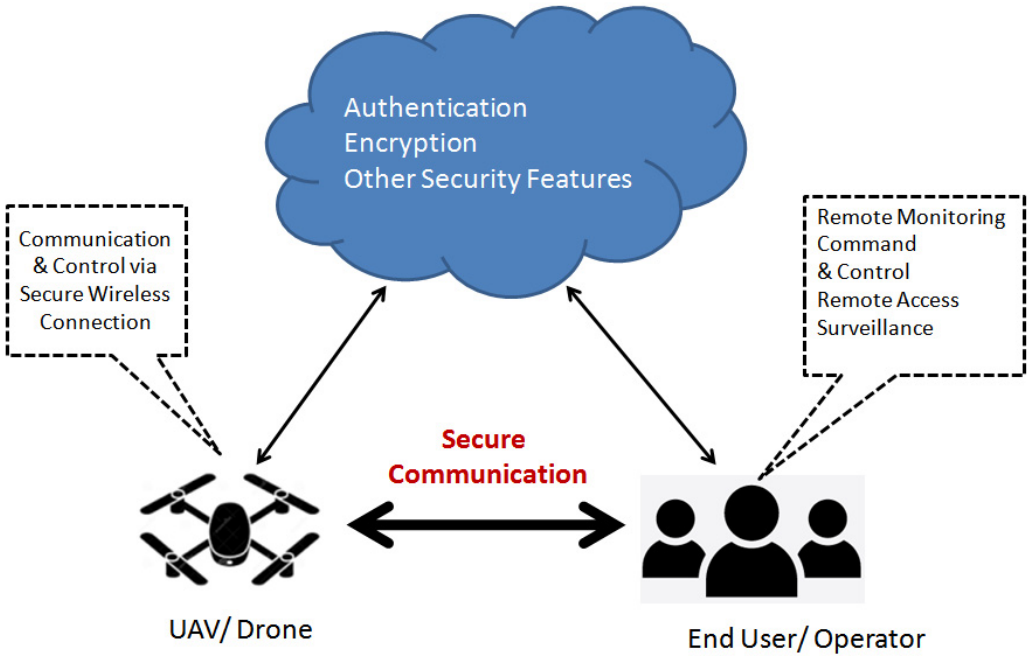

Figure 14. Light weight authentication in UAV systems.

This paper highlights the technicalities involved in the employment of BCT methods in conjunction with 6G networks. Moreover, the parallel working of IoT devices in blockchain enabled environment is presented in this study for smart convergence and distribution in industrial Internet of Things. Additionally, this paper describes the techniques, interesting challenging areas and potential research dimensions that may reveal technical horizons to pursue this research idea in an accelerated and right direction [110]. This paper presents a few fundamental characteristics of the 6G communication model. These include smart radio, artificial intelligence (AI), channel reliability and live edge computing. Moreover, some of popular technologies in each field in consultation with related privacy and security challenges are discussed. The report finally describes the potential use of 6G networks [111]. In this study, diverse blockchain implementation solutions were investigated to cater to future expected issues. At the outset, the role and task of DM team members in blockchain structural design is investigated and discusses the scalability schemes along with consensus algorithms. Subsequently, Access, Authentication, Authorization (AAA) requirements by DM members are discussed. Thirdly, blockchain models for mutual information processing are explained. Moreover, privacy needs of DM are discussed.

Lastly, research issues and possible solutions are presented to meet prospects for 6G-based DM in the blockchain model [112]. In this research, a communication model is suggested that comprises of Internet of Drones (IoD) and Internet of Healthcare (IoH) in conjunction with future wireless networks including 5G and 6G. Information is combined through access networks and is processed through a set of UAVs at the edge layer. In this study [113], a software defined network is perceived, in order to transport data in between edge and cloud layers. Moreover, to achieve accelerated process to accomplish the authentication role and to ensure privacy protection of moving vehicles, a P4C protocol (Privacy-Preserving Parallel Pedersen Commitment) was devised. This research further suggests the DPBFT (Diffused Practical Byzantime Fault Tolerance) model to achieve consensus that can significantly cut down latency involved in the consensus process and can achieve even better operational efficiency. The suggested cyber-chain model and related methods were assessed by qualitative evaluation and replication. The assessment outcome concluded that the suggested model brings considerable improvement in performance related to the authentication process. The key factors with improved performance include storage cost, latency in authentication, different overheads in communication and privacy [114].

In this paper [115], the suggested scheme meets all security-related concerns and addresses pertinent issues of privacy as well. The proposed model is capable of accomplishing an authentication sequence, however, with a slight increment in computation cost. The security feature of this suggested model was evaluated by informal and formal means in this paper, which concluded significant improvement in results. This paper [116], carried out a comprehensive exercise related to the incorporation of wireless communication models with blockchain, keeping several integration and performance aspects in consideration. Moreover, a unified structure named Blockchain radio access network (B-RAN) is suggested in this study for 6G networks employing a blockchain scheme as a reliable, secure and efficient model. During the recent work on blockchain in combination with IoT, multiple challenges have surfaced. One of vital challenges is concern of low throughput while employing blockchain with IoTs. Few assessments regarding transaction efficiency of blockchain versions have been carried out and it has been found that Ethereum blockchain is able to perform 12–15 transactions/s. This transaction processing speed of the Ethereum blockchain does not meet demands of future IoT networks, as the same requires a higher value of throughput in future scenarios.

Hence, blockchains have limitation in capability for supporting and operating IoT networks based on 5G. The pertinent limitation regarding blockchain throughput is their network. In point-to-point networks, miners and verifiers do not have the liberty to mine and verify new blocks in a fast pace due to a relatively slow propagation pace of blocks and transactions in such networks. In said context, network scalability is foreseen as a

prominent factor in IoT networks employing blockchain technology. In this article, the Raft consensus algorithm is discussed and it has determined that solution of network scalability can be materialized by employing blockchain distributed topology and consequently achieving the increased blockchain throughput. Privacy is one of the major issues in the list of challenges related to future IoT networks. One of the limitations in distributed blockchain is that ledgers are public and availability of perceptive information to everyone is private. In this scenario, in order to carry out third party editing, it is only possible once original content is revealed.

In this paper [117], in order to address privacy-related concerns, zkLedger is utilized that relies on zero knowledge-based cryptography. Academia–industry linkage is carrying out a widespread study on the employment of modern technology of machine learning (ML) in network of vehicles and mobility enabled devices. This research is revealing the possible ways for equipping 6G vehicular networks with much needed intelligence in future applications [118]. This paper [119], presents a survey on techniques related to vehicular networks in modernizing the ways they operate in a network enabled with due intelligence in the backdrop of machine learning technology. This article further elaborates on the utilization of this advanced technique in optimized networking, the security portion and information transportation in vehicular networks. Moreover, AI employment to achieve smart radios, intelligent learning and hands-on exploration in vehicular networks is an informative part of this study.

This paper [120] suggests a network architecture sliced up into the communication and blockchain plane in relation to having an in-depth view of future blockchain enabled networks and related applications. A framework based on blockchain scheme is proposed that is capable to supervise the authority; moreover, the suggested model can administer the identity certificates of network elements. This proposed solution is named as "Unified Identity Authentication Framework". This paper [121], highlights the usefulness of blockchain while dealing with data security. This further elaborates the effectiveness of this technology referring to a report on indoor navigation systems. This study further describes an overall intelligent network model that can be achieved by appropriate employment of AI and blockchain together. Additionally, in this study, a number of open issues regarding information security in future 6G communication models are elaborated. In this paper [122], a number of major concerns and challenges regarding blockchain application in IoV are discussed. Multiple possible scenarios of IoV employment are also elaborated in this study. Additionally, this study explains further research dimensions in the field of IoV and offers details of possible opportunities for the modern world in the said field. IoV is discussed in paving the way towards an Intelligent Transportation System (ITS). In [123], three layered scheme which includes IoT device layer, trust centre at the edge layer and cloud layer are provided to add the security concern. The discussion of in this section in summarized in Table 3.

Table 3. 6G-Based Lightweight Authentication.

Ref.	Concept	Description
[102]	(ROR) oracle model	Formal security assessment method for UAV security analysis.
[103]	Light-Edge	Three-layer scheme, including IoT device layer, trust center at the edge layer and cloud service providers.
[124]	SCNM-LSM	An artificial intelligence (AI)-based adaptive security specification method for 6G IoT networks.
[106]	Extended Kalman filtering	Predicts future harvesting power to calculate the required energy of different security strategies.
[107]	Privacy-preserving authentication	A digital signature and authenticated key exchange protocol resist several attacks in the industry 4.0 environment.
[108]	Integration of the blockchain in 6G	Blockchain for resource management and sharing in 6G
[109]	Key generation model	A novel dynamic key generation scheme that uses the entropy and performs various operations to continuously generate a large set of unique keys.

Table 3. *Cont.*

Ref.	Concept	Description
[110]	Deployment of BCT schemes	Convergence of IoT in blockchain to enable intelligent distribution in the technical model of 6G networks.
[111]	Four key aspects of 6G networks	Real-time intelligent edge computing, distributed artificial intelligence, intelligent radio and 3D intercoms.
[112]	DM privacy requirements	Research issues and potential solutions for blockchain-based DM toward 6G.
[113]	Edge-enabled UAVs	a Software Defined Network (SDN) model for data transfer the within the edge and cloud layers.
[114]	P4C algorithm	Protection of the privacy of vehicles and accelerate the authentication process.
[115]	Formal and informal security methods	Authentication cycle with a minor increase in computation cost but provides all security goals along with privacy.
[116]	B-RAN	Secure paradigm for 6G networking by utilizing blockchain technologies.
[117]	zkLedger	Blockchain distributed ledgers solution based on zero knowledge-based cryptography.
[119]	Network intelligence and self-learning	AI toward a future 6G vehicular network.
[120]	Unified identity authentication framework	Blockchain technology to manage the identity certificates of entities in the network and supervise the authority.
[121]	Indoor navigation system	AI and blockchain to evaluate and optimize the quality of intelligent service
[122]	key enabler of ITS	blockchain application for key generation in IoV.

5. Challenges and Future Research Directions

The following are the subject's future research directions. For timely adaption of 6G technology, both academics and industry must pay special attention to these selected areas. This section also covers a discussion on fundamentals categorized in the Specification Group (SG).

5.1. Blockchain Technological Limitations

The lightning network has been threatened because of increased centralization and the complete coverage of blockchain is yet unknown [6]. Although blockchain increases network security when data are fraudulently transferred or tampered with, the decentralized nature of blockchain will render the data irreversible or altered, potentially resulting in irreparable effects [125]. Therefore, a highly decentralized UAV 6G network has challenges in blockchain implementation.

5.2. Mobility Management

In order to achieve a sufficient link budget when operating at mm waves to sustain high-capacity connections, directionality is essential. Fine beam alignment has serious consequences for the design of control procedures such as user tracking, handover and radio link failure recovery in this situation. These issues are especially pressing in the non-terrestrial sector, where the fast speed of UAV aerial/space platforms may cause beam alignment to be lost before a data transfer is completed. The higher Doppler experienced at high speeds may also cause the channel to become non-reciprocal, reducing the feedback over a broadcast channel in 6G enabled UAV networks [126].

5.3. Security Risks

As per our survey, we discussed various emerging technologies that can be employed for secure authentication in next generation UAV communication such as blockchain. However, there are still several security risks associated with these technologies which require further research.

Blockchain relies in part on transparent transactions. Hence, user privacy may be jeopardized in blockchain-based systems. Further, other attacks against blockchain include selfish mining [127] and Sybil attacks [128]. In a Proof-of-Work consensus mechanism,

selfish mining is a means to obtain more reward while wasting honest miners' resources and energy, whereas a Sybil attack is when a user creates several blockchain identities in order to control it. Finally, smart contracts on the blockchain have considerably increased the application of the blockchain by allowing software-defined contracts between participants to be transacted as transactions [129]. Smart contracts, however, as versatile as they are, may inject a number of new attack surfaces into the system. Vulnerabilities in the blockchain, the smart contract and the virtual machine executing code are the three main attack surfaces for blockchain-based smart contracts in 6G enabled UAV communication [130]. These above discussed aspects must attract future researchers' attention for comprehensive research, in order to achieve blockchain-based light weight authentication model resistant to vital threats as highlighted above. The most optimum and finest blockchain model addressing existing limitations can be a reliable and functional solution for authentication of future UAV networks in terms of lightweightness as well as robust security [131].

5.4. Quantum Computing

Commercial quantum computation is expected to already be available in the near future [132]. A certain amount of quantum computation, in particular, can be expected to become a reality, the time it takes for a new node to download the entire blockchain. Throughout the lifespan of 6G enabled UAV networks, the arrival of large-scale quantum computing necessitates the replacement of some current public-key primitives with quantum-resistant ones in the blockchain in 6G enabled UAV networks [133]. Due to Shor's quantum polynomial time integer factoring algorithm [134], factoring and discrete logarithm-based cryptographic primitives, such as the elliptic curve signature algorithm (ECDSA) [135], are rendered vulnerable once large-scale quantum computation becomes a reality. In the post-quantum environment, post-quantum resistant alternatives must be used to replace these security methods. Fortunately, symmetric primitives, such as cryptographic hash functions used in block formation, are not affected in the same way, based on current knowledge.

5.5. Performance Evaluation in Federated Learning

Investigating the implications of transmission bandwidth on Federated Learning (FL) delay performance is one of the primary challenges in 6G enabled UAV networks. Despite the fact that processing capacity are becoming more capable, wireless communication bandwidth has not increased considerably. As a result, the bottleneck has migrated away from compute and toward communication. As a result of the limited communication capacity, there may be a greater communication delay, resulting in extended FL convergence times. As a result, communication-efficient FL is a hot topic for research right now and in the future [136].

5.6. Standardization

The prominent organizations such as IEEE and ITU have not yet finalized the standardization and regulation of blockchain technology. As a result, adequate rules, guidance and regulations are required in the real-time deployment of blockchain with the UAV network. Thus, it is necessary to develop technological standards and recommendations that will make the deployment of UAVs over 6G communication channels simple and efficient. It is difficult to acquire blockchain in real-world 6G enabled UAV networks without the blockchain technology standardization [13].

5.7. THz Deployment

Although THz communication systems are still in their early stages of development, some standardization and regulating processes have already begun. IEEE 802.15.3d-2017, for example, is the first standard for THz, aiming an alternate PHY layer at frequencies between 252 and 321 GHz as an addition to 802.15.3-2016. Furthermore, the WRC 2019 conclusions offer a regulatory framework for the operation of fixed service (FS) and land

mobile service (LMS) applications in frequency bands between 275 GHz and 450 GHz. On the other hand, the growing interest in THz communications naturally raises concerns about the health risks connected with high-frequency radiation, particularly as some non-scientific people still have a bad image of 5G technologies, particularly mm wave and beam forming [2]. In fact, radio frequency electromagnetic fields (EMFs) below 3×1016 GHz are non-ionizing in nature and hence do not have enough energy to ionize cells, avoiding cancer and death hazards [137]. However, they have enough energy to propel electrons and ions into higher energy levels. Because the ensuing thermal effects may cause health problems, regulatory authorities (ICNIRP, FCC, EC, IEEE and others) set maximum RF exposure limits to prevent dangerous heating effects. However, in THz, it is more critical to enforce RF exposure rules for large antenna arrays since beam forming might result in higher power density levels than omnidirectional transmissions. Nevertheless, UAV-assisted communications can increase the distance between THz radiation and human bodies, reducing RF exposure to a degree. There is no evidence of any serious health problems that has been supported by the scientific community to date [138]. However, this aspect requires significant research and experimental studies across various domains to analyze and discover any health-related issues which may arise due to THz applications.

6. Conclusions

While our understanding of UAV cellular communications has improved in recent years, there are still numerous fundamental hurdles to overcome. We conducted a trip from authentication in 6G UAV application cases, requirements and enabling technologies in this essay, blending academic and industrial perspectives. We demonstrated how NR improvements will considerably aid in meeting the rigorous control and payload data demands of network-connected UAVs throughout this decade through real results. In terms of sidelobe-based association, beamformed control signals make UAV cell selection and handovers easier. In both UMa and denser UMi scenarios, mMIMO combined with UAV-aware null steering or UAV-based beam shaping is required to ensure stable cellular connectivity. Surprisingly, this is because to a favorable mix of antenna sidelobes and powerful reflections, NR mm wave networks can also provide enough sky coverage. Such coverage could be further extended by rooftop-mounted uptilted mm wave cells, albeit this is subject to regulations. Underlaying these direct links with the ground uplink incurs little mutual interference for UAV-to-UAV applications, but this becomes more noticeable as UAVs fly higher. UAV-specific power control can efficiently balance UAV-to-UAV performance with ground-link performance. In this article, we have presented the detailed information on the blockchain-envisioned UAV communication using 6G networks. A discussion on the architecture, requirements and use cases of 6G technology was carried out. A solution taxonomy of several applications of UAV communication was discussed. Various unsolved issues were extracted from the study among UAVs and provide a viable solution by providing a view on the blockchain-envisioned UAV communication using 6G networks. Then, we discussed some future research directions based on our study. Finally, we presented a case study of package delivery in industry 4.0 applications that explores the role of the blockchain-envisioned UAV communication using 6G networks.

Author Contributions: Conceptualization: A.S.K. and M.A.S.; Methodology: M.A.S. and K.N.; Visualization: A.A.A.I. and N.B.A., Writing—original draft preparation: M.A.S., A.S.K. and K.N.; Writing review and editing: A.S.K., J.b.A. and S.K.M.; supervision, A.S.K., K.N. and J.b.A.; project administration, A.S.K., K.N. and S.K.M.; Funding acquisition: A.A.A.I., K.N. and A.S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research is fully funded by Universiti Malaysia Sarawak under Grant number F08/GRADUATES/2188/2021.

Informed Consent Statement: Not applicable.

Acknowledgments: This research was conducted in collaboration with Universiti Malaysia Sarawak, Malaysia, Victorian Institute of Technology, Adelaide, Australia, University Malaysia Sabah, Malaysia and University of York, UK. Article Processing Charges (APC) is paid by University Malaysia Sabah.

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

References

1. Popovski, P.; Chiariotti, F.; Huang, K.; Kalør, A.; Kountouris, M.; Pappas, N.; Soret, B. A perspective on time toward wireless 6G. *Proc. IEEE* **2022**, *110*, 1116–1146. [CrossRef]
2. Khan, A.; Javed, Y.; Abdullah, J.; Nazim, J.; Khan, N. Security issues in 5G device to device communication. *Int. J. Comput. Sci. Netw. Secur.* **2017**, *17*, 366.
3. Premkumar, R.; Priya, S.S. Blockchain and Internet of Things: Applications and practices. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Pichanur, India, 25–27 March 2021; pp. 1376–1380.
4. Gupta, R.; Nair, A.; Tanwar, S.; Kumar, N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Commun.* **2021**, *15*, 1352–1367. [CrossRef]
5. Moşteanu, N.; Faccia, A. Digital Systems and New Challenges of Financial Management–FinTech, XBRL, Blockchain and Cryptocurrencies. *Qual.-Access Success J.* **2020**, *21*, 159–166.
6. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef]
7. Safdar, H.; Fisal, N.; Ullah, R.; Maqbool, W.; Asraf, F.; Khalid, Z.; Khan, A. Resource allocation for uplink M2M communication: A game theory approach. In Proceedings of the 2013 IEEE Symposium on Wireless Technology & Applications (ISWTA), Kuching, Malaysia, 22–25 September 2013; pp. 48–52.
8. Gürpinar, T.; Austerjost, M.; Kamphues, J.; Maaßen, J. Blockchain technology as the backbone of the internet of things—An introduction to blockchain devices. In Proceedings of the Conference on Production Systems and Logistics: CPSL 2022, Vancouver, BC, Canada, 17–20 May 2022.
9. Jalan, A.; Matkovskyy, R.; Urquhart, A. What effect did the introduction of Bitcoin futures have on the Bitcoin spot market? *Eur. J. Financ.* **2021**, *27*, 1251–1281. [CrossRef]
10. Oliva, G.A.; Hassan, A.E.; Jiang, Z.M.J. An exploratory study of smart contracts in the Ethereum blockchain platform. *Empir. Softw. Eng.* **2020**, *25*, 1864–1904. [CrossRef]
11. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Netw.* **2020**, *34*, 8–14. [CrossRef]
12. Rana, A.; Sharma, S.; Nisar, K.; Ibrahim, A.A.A.; Dhawan, S.; Chowdhry, B.; Hussain, S.; Goyal, N. The Rise of Blockchain Internet of Things (BIoT): Secured, Device-to-Device Architecture and Simulation Scenarios. *Appl. Sci.* **2022**, *12*, 7694. [CrossRef]
13. Kathole, A.B.; Katti, J.; Dhabliya, D.; Deshpande, V.; Rajawat, A.S.; Goyal, S.B.; Raboaca, M.S.; Mihaltan, T.C.; Verma, C.; Suciu, G. Energy-Aware UAV Based on Blockchain Model Using IoE Application in 6G Network-Driven Cybertwin. *Energies* **2022**, *15*, 8304. [CrossRef]
14. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
15. Khan, A.S.; Javed, Y.; Abdullah, J.; Zen, K. Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–18. [CrossRef]
16. Strobel, V.; Castelló Ferrer, E.; Dorigo, M. Blockchain technology secures robot swarms: A comparison of consensus protocols and their resilience to Byzantine robots. *Front. Robot. AI* **2020**, *7*, 54. [CrossRef] [PubMed]
17. Afanasyev, I.; Kolotov, A.; Rezin, R.; Danilov, K.; Mazzara, M.; Chakraborty, S.; Kashevnik, A.; Chechulin, A.; Kapitonov, A.; Jotsov, V. Towards blockchain-based multi-agent robotic systems: Analysis, classification and applications. *arXiv* **2019**, arXiv:1907.07433.
18. De Campos, M.G.S.; Chanel, C.P.; Chauffaut, C.; Lacan, J. Towards a Blockchain-Based Multi-UAV Surveillance System. *Front. Robot. AI* **2021**, *8*, 557692. [CrossRef]
19. Söderlund, M. The robot-to-robot service encounter: An examination of the impact of inter-robot warmth. *J. Serv. Mark.* **2021**, *35*, 15–27. [CrossRef]
20. Tran, J.A.; Ramachandran, G.S.; Shah, P.M.; Danilov, C.B.; Santiago, R.A.; Krishnamachari, B. Swarmdag: A partition tolerant distributed ledger protocol for swarm robotics. *Ledger* **2019**, *4*, 25–31. [CrossRef]
21. Li, M.; Pei, P.; Yu, F.R.; Si, P.; Li, Y.; Sun, E.; Zhang, Y. Cloud–Edge Collaborative Resource Allocation for Blockchain-Enabled Internet of Things: A Collective Reinforcement Learning Approach. *IEEE Internet Things J.* **2022**, *9*, 23115–23129. [CrossRef]
22. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.* **2021**, *9*, 359–383. [CrossRef]
23. Sekaran, R.; Patan, R.; Raveendran, A.; Al-Turjman, F.; Ramachandran, M.; Mostarda, L. Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation. *IEEE Access* **2020**, *8*, 143453–143463. [CrossRef]
24. Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* **2021**, *172*, 102–118. [CrossRef]

25. Kazmi, S.H.A.; Masood, A.; Nisar, K. Design and Analysis of Multi Efficiency Motors Based High Endurance Multi Rotor with Central Thrust. In Proceedings of the 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 13–15 October 2021; pp. 1–4.
26. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K.; Chowdhry, B.S. Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions. *Res. Sq.* **2022**. [CrossRef]
27. Barakabitze, A.A.; Ahmad, A.; Mijumbi, R. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Comput. Netw.* **2020**, *167*, 106984. [CrossRef]
28. Waseem, Q.; Alshamrani, S.S.; Nisar, K.; Wan Din, W.I.S.; Alghamdi, A.S. Future Technology: Software-Defined Network (SDN) Forensic. *Symmetry* **2021**, *13*, 767. [CrossRef]
29. Shaikh, M.R.; Khuhawar, F.Y.; Nisar, K.; Memon, A.A.; Khan, A.S. Vulnerability Assessment & Analysis of Software-Defined Networking using a Virtual Testbed. In Proceedings of the 2022 Global Conference on Wireless and Optical Technologies (GCWOT), Malaga, Spain, 14–17 February 2022.
30. Khan, A.; Abdullah, J.; Zen, K.; Tarmizi, S. Secure and Scalable Group Rekeying for Mobile Multihop Relay Network. *Adv. Sci. Lett.* **2017**, *23*, 5242–5245. [CrossRef]
31. Schwartz, S.C. The Promise and Challenge of Drones in Homeland Security. In *The Role of Law Enforcement in Emergency Management and Homeland Security*; Emerald Publishing Limited: Bingley, UK, 2021.
32. Alsamhi, S.H.; Afghah, F.; Sahal, R.; Hawbani, A.; Al-qaness, M.A.; Lee, B.; Guizani, M. Green internet of things using UAVs in B5G networks: A review of applications and strategies. *Ad Hoc Netw.* **2021**, *117*, 102505. [CrossRef]
33. Byun, S.; Shin, I.-K.; Moon, J.; Kang, J.; Choi, S.-I. Road traffic monitoring from UAV images using deep learning networks. *Remote Sens.* **2021**, *13*, 4027. [CrossRef]
34. Chan, K.Y.; Abdullah, J.; Khan, A.S. A framework for traceable and transparent supply chain management for agri-food sector in malaysia using blockchain technology. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 149–156. [CrossRef]
35. Kumar, A.; Ridha, S.; Narahari, M.; Ilyas, S.U. Physics-guided deep neural network to characterize non-Newtonian fluid flow for optimal use of energy resources. *Expert Syst. Appl.* **2021**, *183*, 115409. [CrossRef]
36. Raja, G.; Anbalagan, S.; Ganapathisubramaniyan, A.; Selvakumar, M.S.; Bashir, A.K.; Mumtaz, S. Efficient and secured swarm pattern multi-UAV communication. *IEEE Trans. Veh. Technol.* **2021**, *70*, 7050–7058. [CrossRef]
37. Li, T.; Hu, H. Development of the Use of Unmanned Aerial Vehicles (UAVs) in Emergency Rescue in China. *Risk Manag. Healthc. Policy* **2021**, *14*, 4293. [CrossRef] [PubMed]
38. Zhu, K.; Han, B.; Zhang, T. Multi-UAV Distributed Collaborative Coverage for Target Search Using Heuristic Strategy. *Guid. Navig. Control* **2021**, *1*, 2150002. [CrossRef]
39. Dalal, S.; Seth, B.; Jaglan, V.; Malik, M.; Surbhi; Dahiya, N.; Rani, U.; Le, D.; Hu, Y. An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. *Soft Comput.* **2022**, *26*, 5377–5388. [CrossRef]
40. Akhloufi, M.A.; Couturier, A.; Castro, N.A. Unmanned aerial vehicles for wildland fires: Sensing, perception, cooperation and assistance. *Drones* **2021**, *5*, 15. [CrossRef]
41. Du, Z.; Wu, C.; Yoshinaga, T.; Chen, X.; Wang, X. A routing protocol for UAV-assisted vehicular delay tolerant networks. *IEEE Open J. Comput. Soc.* **2021**, *2*, 85–98. [CrossRef]
42. Yao, P.; Wei, X. Multi-UAV Information Fusion and Cooperative Trajectory Optimization in Target Search. *IEEE Syst. J.* **2021**, *16*, 4325–4333. [CrossRef]
43. Yavariabdi, A.; Kusetogullari, H.; Celik, T.; Cicek, H. FastUAV-net: A multi-UAV detection algorithm for embedded platforms. *Electronics* **2021**, *10*, 724. [CrossRef]
44. Khan, I.U.; Shah, S.B.H.; Wang, L.; Aziz, M.A.; Stephan, T.; Kumar, N. Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. *Int. J. Commun. Syst.* **2021**, e4885. [CrossRef]
45. Ji, J.; Zhu, K.; Niyato, D. Joint Communication and Computation Design for UAV-Enabled Aerial Computing. *IEEE Commun. Mag.* **2021**, *59*, 73–79. [CrossRef]
46. Agrawal, J.; Kapoor, M. A comparative study on geographic-based routing algorithms for flying ad-hoc networks. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6253. [CrossRef]
47. Kemp, S.; Rogers, J. UAV-UGV Teaming for Rapid Radiological Mapping. In Proceedings of the 2021 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR), New York, NY, USA, 25–27 October 2021; pp. 92–97.
48. Ruby, R.; Yang, H.; Pham, Q.-V.; Wu, K. Delay Performance of UAV-Based Buffer-Aided Relay Networks under Bursty Traffic: Mobile or Static? In Proceedings of the 2021 IEEE 22nd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Pisa, Italy, 7–11 June 2021; pp. 51–60.
49. Nagpal, S.; Aggarwal, A.; Gaba, S. Privacy and Security Issues in Vehicular Ad Hoc Networks with Preventive Mechanisms. In *Proceedings of the International Conference on Intelligent Cyber-Physical Systems*; Springer: Singapore, 2022; pp. 317–329.
50. El Haber, E.; Alameddine, H.A.; Assi, C.; Sharafeddine, S. UAV-aided ultra-reliable low-latency computation offloading in future IoT networks. *IEEE Trans. Commun.* **2021**, *69*, 6838–6851. [CrossRef]
51. Çabuk, U.C.; Tosun, M.; Dagdeviren, O. MAX-Tree: A Novel Topology Formation for Maximal Area Coverage in Wireless Ad-Hoc Networks. *IEEE/ACM Trans. Netw.* **2021**, *30*, 162–175. [CrossRef]
52. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]

53. Jan, S.U.; Abbasi, I.A.; Algarni, F.; Khan, A.S. Corrections to "A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET". *IEEE Access* **2022**, *10*, 105496. [CrossRef]
54. Lei, Y.; Zeng, L.; Li, Y.-X.; Wang, M.-X.; Qin, H. A lightweight authentication protocol for UAV networks based on security and computational resource optimization. *IEEE Access* **2021**, *9*, 53769–53785. [CrossRef]
55. Ko, Y.D.; Song, B.D. Application of UAVs for tourism security and safety. *Asia Pac. J. Mark. Logist.* **2021**, *33*, 1829–1843. [CrossRef]
56. Oteafy, S.M. Resource augmentation in Heterogeneous Internet of Things via UAVs. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021.
57. Khan, A.S.; Ahmad, Z.; Abdullah, J.; Ahmad, F. A spectrogram image-based network anomaly detection system using deep convolutional neural network. *IEEE Access* **2021**, *9*, 87079–87093. [CrossRef]
58. Mitkas, D.Z.; Lovell, D.J.; Venkatesh, S.; Young, S. Activity Identification using ADS-B data at General Aviation Airports. In Proceedings of the AIAA AVIATION 2021 FORUM, Virtual Event, 2–6 August 2021.
59. Azari, M.M.; Solanki, S.; Chatzinotas, S.; Bennis, M. THz-Empowered UAVs in 6G: Opportunities, Challenges, and Trade-offs. *IEEE Commun. Mag.* **2022**, *60*, 24–30. [CrossRef]
60. Hong, H.; Zhao, J.; Hong, T.; Tang, T. Radar-communication integration for 6G massive IoT services. *IEEE Internet Things J.* **2021**, *9*, 14511–14520. [CrossRef]
61. Karim, F.A.; Aman, A.H.M.; Hassan, R.; Nisar, K.; Uddin, M. Named Data Networking: A Survey on Routing Strategies. *IEEE Access* **2022**, *10*, 90254–90270. [CrossRef]
62. Nozari, H.; Szmelter-Jarosz, A.; Ghahremani-Nahr, J. The Ideas of Sustainable and Green Marketing Based on the Internet of Everything—The Case of the Dairy Industry. *Future Internet* **2021**, *13*, 266. [CrossRef]
63. Maikol, S.O.; Khan, A.S.; Javed, Y.; Bunsu, A.L.A.; Petrus, C.; George, H.; Jau, S. A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. *Int. J. Integr. Eng.* **2021**, *13*, 127–135.
64. Rukhsar, L.; Bangyal, W.H.; Nisar, K.; Nisar, S. Prediction of insurance fraud detection using machine learning algorithms. *Mehran Univ. Res. J. Eng. Technol.* **2022**, *41*, 33–40. [CrossRef]
65. Sher, A.; Sohail, M.; Shah, S.B.H.; Koundal, D.; Hassan, M.A.; Abdollahi, A.; Khan, I.U. New Trends and Advancement in Next Generation Mobile Wireless Communication (6G): A Survey. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9614520.
66. Wang, Y.; Su, Z.; Xu, Q.; Li, R.; Luan, T.H. Lifesaving with RescueChain: Energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021.
67. Ahmad, Z.; Shahid Khan, A.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.R.; Tarmizi, S.; Rodrigues, J.J. Anomaly detection using deep neural network for IoT architecture. *Appl. Sci.* **2021**, *11*, 7050. [CrossRef]
68. Gandra, C.; Hansson, J. *Application of Value Proposition Design to a High-Tech Business Market Product*; Lund University: Lund, Sweden, 2021.
69. Baltaci, A.; Dinc, E.; Ozger, M.; Alabbasi, A.; Cavdar, C.; Schupke, D. A Survey of Wireless Networks for Future Aerial Communications (FACOM). *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2833–2884. [CrossRef]
70. Höyhtyä, M.; Boumard, S.; Yastrebova, A.; Järvensivu, P.; Kiviranta, M.; Anttonen, A. Sustainable Satellite Communications in the 6G Era: A European View for Multi-Layer Systems and Space Safety. *arXiv* **2022**, arXiv:2201.02408.
71. Ray, P.P. A review on 6G for space-air-ground integrated network: Key enablers, open challenges, and future direction. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *34*, 6949–6976. [CrossRef]
72. Zhu, X.; Jiang, C. Integrated satellite-terrestrial networks toward 6g: Architectures, applications, and challenges. *IEEE Internet Things J.* **2021**, *9*, 437–461. [CrossRef]
73. Zhang, T.; Wang, Z.; Liu, Y.; Xu, W.; Nallanathan, A. Joint Resource, Deployment, and Caching Optimization for AR Applications in Dynamic UAV NOMA Networks. *IEEE Trans. Wirel. Commun.* **2021**, *21*, 3409–3422. [CrossRef]
74. Kaiser, M.S.; Zenia, N.; Tabassum, F.; Mamun, S.A.; Rahman, M.A.; Islam, M.; Mahmud, M. 6G access network for intelligent internet of healthcare things: Opportunity, challenges, and research directions. In *Proceedings of the International Conference on Trends in Computational and Cognitive Engineering*; Springer: Singapore, 2021; pp. 317–328.
75. Hamza, B.J.; Saad, W.K.; Shayea, I.; Ahmad, N.; Mohamed, N.; Nandi, D.; Gholampour, G. Performance enhancement of SCM/WDM-RoF-XGPON system for bidirectional transmission with square root module. *IEEE Access* **2021**, *9*, 49487–49503. [CrossRef]
76. Ahmad, Z.; Shahid Khan, A.; Wai Shiang, C.; Abdullah, J.; Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4150. [CrossRef]
77. Gope, P.; Millwood, O.; Saxena, N. A provably secure authentication scheme for RFID-enabled UAV applications. *Comput. Commun.* **2021**, *166*, 19–25. [CrossRef]
78. Munusamy, R.; Kumre, J.; Chaturvedi, S.; Bandhu, D. Design and Development of Portable UAV Ground Control and Communication Station Integrated with Antenna Tracking Mechanism. In *Intelligent Infrastructure in Transportation and Management*; Springer: Singapore, 2022; pp. 193–212.
79. Adnan, W.H.; Khamis, M.F. Drone use in military and civilian application: Risk to national security. *J. Media Inf. Warf.* **2022**, *15*, 60–70.

80. Mohammed, I.; Collings, I.B.; Hanly, S.V. Line of sight probability prediction for UAV communication. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
81. Tang, S.; Zhou, W.; Chen, L.; Lai, L.; Xia, J.; Fan, L. Battery-constrained federated edge learning in UAV-enabled IoT for B5G/6G networks. *Phys. Commun.* **2021**, *47*, 101381. [CrossRef]
82. Sehrawat, H.; Siwach, V. Security vulnerabilities in Wireless Sensor Networks. *J. Inf. Assur. Secur.* **2010**, *5*, 31–44.
83. Javed, Y.; Khan, A.S.; Qahar, A.; Abdullah, J. Preventing DoS attacks in IoT using AES. *J. Telecommun. Electron. Comput. Eng. (JTEC)* **2017**, *9*, 55–60.
84. Nazir, M.; Sabah, A.; Sarwar, S.; Yaseen, A.; Jurcut, A. Power and resource allocation in wireless communication network. *Wirel. Pers. Commun.* **2021**, *119*, 3529–3552. [CrossRef]
85. Ly, B.; Ly, R. Cybersecurity in unmanned aerial vehicles (UAVs). *J. Cyber Secur. Technol.* **2021**, *5*, 120–137. [CrossRef]
86. Bakare, B.; Ekolama, S. Preventing Man-in-The-Middle (MiTM) Attack of GSM Calls. *Eur. J. Electr. Eng. Comput. Sci.* **2021**, *5*, 63–68. [CrossRef]
87. de Melo, C.F.E.; e Silva, T.D.; Boeira, F.; Stocchero, J.M.; Vinel, A.; Asplund, M.; de Freitas, E.P. Uavouch: A secure identity and location validation scheme for uav-networks. *IEEE Access* **2021**, *9*, 82930–82946. [CrossRef]
88. Satyanarayana, P. Detection and Blocking of Replay, False Command, and False Access Injection Commands in SCADA Systems with Modbus Protocol. *Secur. Commun. Netw.* **2021**, *2021*, 8887666.
89. Tesfay, D.; Tiwari, B.; Teka, M.e.J.; Tiwari, V. An Intrusion Prevention System embedded AODV to protect Mobile Adhoc Network against Sybil Attack. In Proceedings of the International Conference on Data Science, Machine Learning and Artificial Intelligence, Windhoek, Namibia, 9–12 August 2021; pp. 57–64.
90. Chaubey, N.K.; Yadav, D. Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance. *Int. J. Electr. Comput. Eng.* **2022**, *12*, 1703–1710. [CrossRef]
91. Chierici, A.; Malizia, A.; Di Giovanni, D.; Ciolini, R.; d'Errico, F. A High-Performance Gamma Spectrometer for Unmanned Systems Based on Off-the-Shelf Components. *Sensors* **2022**, *22*, 1078. [CrossRef] [PubMed]
92. Balan, K.; Abdulrazak, L.; Khan, A.; Julaihi, A.; Tarmizi, S.; Pillay, K.; Sallehudin, H. RSSI and public key infrastructure based secure communication in autonomous vehicular networks. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 298–304. [CrossRef]
93. Mahmood Saqib, R.; Shahid Khan, A.; Javed, Y.; Ahmad, S.; Nisar, K.; Abbasi, I.A.; Haque, M.R.; Ahmadi Julaihi, A. Analysis and intellectual structure of the multi-factor authentication in information security. *Intell. Autom. Soft Comput.* **2022**, *32*, 1633–1647. [CrossRef]
94. Riyadi, E.H.; Putra, A.E.; Priyambodo, T.K. Improvement of nuclear facilities DNP3 protocol data transmission security using super encryption BRC4 in SCADA systems. *PeerJ Comput. Sci.* **2021**, *7*, e727. [CrossRef]
95. Memon, S.K.; Nisar, K.; Hijazi, M.H.A.; Chowdhry, B.; Sodhro, A.H.; Pirbhulal, S.; Rodrigues, J.J. A survey on 802.11 MAC industrial standards, architecture, security & supporting emergency traffic: Future directions. *J. Ind. Inf. Integr.* **2021**, *24*, 100225.
96. Uribe-Leitz, T.; Matsas, B.; Dalton, M.K.; Lutgendorf, M.A.; Moberg, E.; Schoenfeld, A.J.; Goralnick, E.; Weissman, J.S.; Hamlin, L.; Cooper, Z. Geospatial analysis of access to emergency cesarean delivery for military and civilian populations in the US. *JAMA Netw. Open* **2022**, *5*, e2142835. [CrossRef]
97. Talpur, M.R.H.; Talpur, M.S.H.; Talpur, F.; Haseeb, A.; Kehar, A.; Fatima, S. A Model for Secure Inter-Institutional Communication Based on Artificial Intelligence (AI) and Blockchain. *Int. J. Comput. Intell. Control* **2021**, *13*, 145–154.
98. Javed, Y.; Khan, A.S.; Qahar, A.; Abdullah, J. EEoP: A lightweight security scheme over PKI in D2D cellular networks. *J. Telecommun. Electron. Comput. Eng. (JTEC)* **2017**, *9*, 99–105.
99. Deebak, B.D.; Fadi, A.-T. Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Gener. Comput. Syst.* **2021**, *116*, 406–425. [CrossRef]
100. Lafta, S.A.; Abdulkareem, M.M.; Ibrahim, R.K.; Kareem, M.M.; Ali, A.H. Quality of service performances of video and voice transmission in universal mobile telecommunications system network based on OPNET. *Bull. Electr. Eng. Inform.* **2021**, *10*, 3202–3210. [CrossRef]
101. Chaudhry, S.A.; Irshad, A.; Khan, M.A.; Khan, S.A.; Nosheen, S.; AlZubi, A.A.; Zikria, Y.B. A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System. *IEEE Trans. Intell. Transp. Syst.* **2021**. [CrossRef]
102. Zuo, Y.; Jin, S.; Zhang, S.; Zhang, Y. Blockchain storage and computation offloading for cooperative mobile-edge computing. *IEEE Internet Things J.* **2021**, *8*, 9084–9098. [CrossRef]
103. Shahidinejad, A.; Ghobaei-Arani, M.; Souri, A.; Shojafar, M.; Kumari, S. Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment. *IEEE Consum. Electron. Mag.* **2021**, *11*, 57–63. [CrossRef]
104. Beebe, N.H. *A Complete Bibliography of Publications in ACM Computing Surveys*; University of Utah: Salt Lake City, UT, USA, 2022.
105. Rana, S.K.; Rana, S.K.; Nisar, K.; Ag Ibrahim, A.A.; Rana, A.K.; Goyal, N.; Chawla, P. Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. *Sustainability* **2022**, *14*, 9471. [CrossRef]
106. Mao, B.; Kawamoto, Y.; Kato, N. AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 7032–7042. [CrossRef]
107. Soleymani, S.A.; Goudarzi, S.; Anisi, M.H.; Movahedi, Z.; Jindal, A.; Kama, N. PACMAN: Privacy-Preserving Authentication Scheme for Managing Cybertwin-based 6G Networking. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4902–4911. [CrossRef]

108. Xu, H.; Klaine, P.V.; Onireti, O.; Cao, B.; Imran, M.; Zhang, L. Blockchain-enabled resource management and sharing for 6G communications. *Digit. Commun. Netw.* **2020**, *6*, 261–269. [CrossRef]
109. Pothumarti, R.; Jain, K.; Krishnan, P. A lightweight authentication scheme for 5G mobile communications: A dynamic key approach. *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–19. [CrossRef]
110. Jahid, A.; Alsharif, M.H.; Hall, T.J. The Convergence of Blockchain, IoT and 6G: Potential, Opportunities, Challenges and Research Roadmap. *arXiv* **2021**, arXiv:2109.03184.
111. Wang, M.; Zhu, T.; Zhang, T.; Zhang, J.; Yu, S.; Zhou, W. Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.* **2020**, *6*, 281–291. [CrossRef]
112. Shen, X.S.; Liu, D.; Huang, C.; Xue, L.; Yin, H.; Zhuang, W.; Sun, R.; Ying, B. Blockchain for Transparent Data Management Toward 6G. *Engineering* **2021**, *8*, 74–85. [CrossRef]
113. Haque, M.R.; Tan, S.C.; Yusoff, Z.; Nisar, K.; Lee, C.K.; Chowdhry, B.; Ali, S.; Memona, S.K.; Kaspin, R. SDN architecture for UAVs and EVs using satellite: A hypothetical model and new challenges for future. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–6.
114. Chai, H.; Leng, S.; He, J.; Zhang, K.; Cheng, B. CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-preserving Authentication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *71*, 4620–4631. [CrossRef]
115. Chaudhry, S.A.; Irshad, A.; Yahya, K.; Kumar, N.; Alazab, M.; Zikria, Y.B. Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment. *ACM Trans. Internet Technol. (TOIT)* **2021**, *21*, 1–19. [CrossRef]
116. Wang, J.; Ling, X.; Le, Y.; Huang, Y.; You, X. Blockchain-enabled wireless communications: A new paradigm towards 6G. *Natl. Sci. Rev.* **2021**, *8*, nwab069. [CrossRef]
117. Dhar Dwivedi, A.; Singh, R.; Kaushik, K.; Rao Mukkamala, R.; Alnumay, W.S. Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Trans. Emerg. Telecommun. Technol.* **2021**, e4329. [CrossRef]
118. Aqeel, S.; Shahid Khan, A.; Ahmad, Z.; Abdullah, J. A comprehensive study on DNA based Security scheme Using Deep Learning in Healthcare. *EDPACS* **2022**, *66*, 1–17. [CrossRef]
119. Tang, F.; Kawamoto, Y.; Kato, N.; Liu, J. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. *Proc. IEEE* **2019**, *108*, 292–307. [CrossRef]
120. Chen, M.; Tan, C.; Zhu, X.; Zhang, X. A Blockchain-Based Authentication and Service Provision Scheme for Intemet of Things. In Proceedings of the 2020 IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
121. Li, W.; Su, Z.; Li, R.; Zhang, K.; Wang, Y. Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Netw.* **2020**, *34*, 31–37. [CrossRef]
122. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.-Y.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2020**, *8*, 4157–4185. [CrossRef]
123. Chen, C.-M.; Chen, Z.; Kumari, S.; Lin, M.-C. LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things. *Sensors* **2022**, *22*, 5401. [CrossRef] [PubMed]
124. Kamruzzaman, M. *6G-Enabled Smart City Networking Model Using Lightweight Security Module*; Jouf University: Sakaka, Saudi Arabia, 2021.
125. Ji, B.; Han, Y.; Liu, S.; Tao, F.; Zhang, G.; Fu, Z.; Li, C. Several key technologies for 6G: Challenges and opportunities. *IEEE Commun. Stand. Mag.* **2021**, *5*, 44–51. [CrossRef]
126. Giordani, M.; Zorzi, M. Non-terrestrial networks in the 6G era: Challenges and opportunities. *IEEE Netw.* **2020**, *35*, 244–251. [CrossRef]
127. Sapirshtein, A.; Sompolinsky, Y.; Zohar, A. Optimal selfish mining strategies in bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; pp. 515–532.
128. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J.* **2014**, *1*, 372–383. [CrossRef]
129. Ma, X.; Liao, L.; Li, Z.; Lai, R.X.; Zhang, M. Applying Federated Learning in Software-Defined Networks: A Survey. *Symmetry* **2022**, *14*, 195. [CrossRef]
130. Duan, L.; Sun, Y.; Zhang, K.; Ding, Y. Multiple-Layer Security Threats on the Ethereum Blockchain and Their Countermeasures. *Secur. Commun. Netw.* **2022**, *2022*, 5307697. [CrossRef]
131. Khan, A.S.; Javed, Y.; Saqib, R.M.; Ahmad, Z.; Abdullah, J.; Zen, K.; Abbasi, I.A.; Khan, N.A. Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. *IEEE Access* **2022**, *10*, 31273–31288. [CrossRef]
132. Feng, G.; Hou, S.-Y.; Zou, H.; Shi, W.; Yu, S.; Sheng, Z.; Rao, X.; Ma, K.; Chen, C.; Ren, B. SpinQ Triangulum: A commercial three-qubit desktop quantum computer. *arXiv* **2022**, arXiv:2202.02983. [CrossRef]
133. Asim, J.; Khan, A.S.; Saqib, R.M.; Abdullah, J.; Ahmad, Z.; Honey, S.; Afzal, S.; Alqahtani, M.S.; Abbas, M. Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. *Appl. Sci.* **2022**, *12*, 3551. [CrossRef]
134. Yahui, W.; ZHANG, H. Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point. *Wuhan Univ. J. Nat. Sci.* **2021**, *26*, 489–494.
135. Khan, S.; Abdullah, J.; Khan, N.; Julahi, A.; Tarmizi, S. Quantum-elliptic curve cryptography for multihop communication in 5G networks. *Int. J. Comput. Sci. Netw. Secur.* **2017**, *17*, 357–365.
136. Yang, Z.; Chen, M.; Wong, K.-K.; Poor, H.V.; Cui, S. Federated learning for 6G: Applications, challenges, and opportunities. *Engineering* **2021**, *8*, 33–41. [CrossRef]

137. Averbeck, D. Does scientific evidence support a change from the LNT model for low-dose radiation risk extrapolation? *Health Phys.* **2009**, *97*, 493–504. [CrossRef]
138. Bell, M.L.; Fong, K.C. Gender differences in first and corresponding authorship in public health research submissions during the COVID-19 pandemic. *Am. J. Public Health* **2021**, *111*, 159–163. [CrossRef]