symmetry

MDPI

Review

Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions

Syed Hussain Ali Kazmi [1], Rosilah Hassan [1], Faizan Qamar [1,*], Kashif Nisar [2] and Ag Asri Ag Ibrahim [3,*]

[1] Center for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Selangor, Malaysia
[2] Victorian Institute of Technology, Adelaide, SA 5000, Australia
[3] Faculty of Computing and Informatics, University Malaysia Sabah, Jalan UMS, Kota Kinabalu 88400, Sabah, Malaysia
* Correspondence: faizanqamar@ukm.edu.my (F.Q.); awgasri@ums.edu.my (A.A.A.I.)

Abstract: Challenges faced in network security have significantly steered the deployment timeline of Fifth Generation (5G) communication at a global level; therefore, research in Sixth Generation (6G) security analysis is profoundly necessitated. The prerogative of this paper is to present a survey on the emerging 6G cellular communication paradigm to highlight symmetry with legacy security concepts along with asymmetric innovative aspects such Artificial Intelligence (AI), Quantum Computing, Federated Learning, etc. We present a taxonomy of the threat model in 6G communication in five security legacy concepts, including Confidentiality, Integrity, Availability, Authentication and Access control (CIA^3). We also suggest categorization of threat-countering techniques specific to 6G communication into three types: cryptographic methods, entity attributes and Intrusion Detection System (IDS). Thus, with this premise, we distributed the authentication techniques in eight types, including handover authentication, mutual authentication, physical layer authentication, deniable authentication, token-based authentication, certificate-based authentication, key agreement-based authentication and multi-factor authentication. We specifically suggested a series of future research directions at the conclusive edge of this survey.

Keywords: communication; security; vulnerabilities; 6G; authentication; threats; countermeasures

Citation: Kazmi, S.H.A.; Hassan, R.; Qamar, F.; Nisar, K.; Ibrahim, A.A.A. Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions. *Symmetry* **2023**, *15*, 1147. https://doi.org/10.3390/sym15061147

Academic Editors: Yuan Zhang, Wei Quan, Anjia Yang and Xiaojun Zhang

Received: 22 December 2022
Revised: 19 January 2023
Accepted: 20 January 2023
Published: 25 May 2023

1. Introduction

6G will surface symmetry of a completely mobile and linked human–machine civilization by transforming asymmetric unconventional services in a modern symmetric era. The Sixth Generation (6G) mobile network communication will envelop the whole world in future decades or even earlier. 6G, in comparison to Fifth Generation (5G), is aimed at high bit rates with a multitude level of gigabits per second and expanded bandwidth with extremely reduced latencies; therefore, 6G is the emerging motive of the billions of interconnected devices in terms of the Internet of Things (IoT). 6G-enabled intelligent IoT systems will achieve effectivity and efficiency by employing the properties of "symmetry" as well as "asymmetry" [1]. 6G technological evolution is based on emerging modern trends in network communication regimes such as Software Defined Networking (SDN), Fog Computing and Network Function Virtualization (NVF) [2]. In a 6G environment, the inclusion of symmetry in wireless technologies will allow network users to switch among various service providers and technologies alongside maintaining a seamless Quality of Service (QoS), fast 3D handover, cognitive networking and a generalized openness. Table 1 summarizes the latest prominent 6G communication projects by multiple organizations.

Table 1. The Prominent Research Projects on 6G communication.

Year	Project	Scope
2019	6G Flagship	Formed and finished an academic and industrial consortium aiming at developing key enabling technologies for 6G [3]
2021	Hexa-X	6G European flagship initiative of future [4]
2021	RISE-6G	RISE-6G project aims at investigating innovative solutions [5]
2021	6G Sentinel Lighthouse	Targeting improvements to device antennas and front-end modules [6]
2021	6G UT (University of Texas)	New sensing methods, wireless-specific machine learning algorithms and networking innovations [7]
2020	6G Brazil project	Allowing the construction of a nation-wise view for the future mobile network [8]

The modern futuristic 6G environment is envisaged in categories such as enhanced Mobile Broad-Band (eMBB), Un-Conventional Data Communications (UCDC), Secure Ultra-Reliable Low-Latency Communications (SURLLC), Three-Dimensional Communications (3DCom) and Big Communications (BigCom) [9]. Primarily, eMBB comprises multifeatured smartphones, highly dynamic real-world gaming, high-resolution multi-media applications and many more similar applications [10]. However, eMBB lacks symmetry due to huge variations in data rate requirements from a few Mbps to 1 or more Gbps [11]. Moreover, eMMB-based massive bandwidth and huge data impacts the security requirement in terms of an optimized implantation of intrusion detection in Bigdata traversing over the network. Similarly, eMMB also impacts the security in terms of authentication mechanism implementation and cryptographic requirements in low processing devices such as IoTs. Likewise, SURLL covers modern machine tools, smart industry, smart health care, etc., also creating security challenges in authentication and cryptographic processing. 3Dcom consists of airborne and high-rise smart platforms such as underwater communication, drones, Unmanned Aerial Vehicles (UAVs), etc. [12]. Due to spatiotemporal characteristics of 3Dcom, the security areas related to availability and confidentiality are most vulnerable. Moreover, drones, UAVs and underwater autonomous systems face limitations related to power-efficient cryptographic processing. UCDC is an open-ended technological edge that covers futuristic smart human bond applications. The dynamic nature of UCDC causes major difficulties related to attribute selection for security implementations such as authentication and confidentiality. Thus, BigCom formulates a holistic communication paradigm at the global level, as illustrated in Figure 1. Moreover, 6G will emerge as a global phenomenon due to futuristic concepts such as mobile fog computing, Unmanned Mobile Systems, blockchain revolutionization, smart cities, etc. [13]. BigCom is a completely unconventional paradigm in mobile communication, resulting in security challenges primarily in the domain of authentication and cryptographic processing. The majority of telecommunication experts consider that the commercialization of 6G will be initiated in 2032 [14].

This 6G multi-dimensional expansion surfaces serious challenges related to threats in cyberspace [15,16]. Hence, a 6G-based unconventional communication environment will generate several fundamental security threats related to Confidentiality, Integrity and Availability (CIA), known as the CIA triad [17]. Furthermore, IP-based network architecture will also entail specific conventional vulnerabilities. These findings show the requirement of a state-of-the-art security architecture for authentication in 6G networks [18]. The concept of 3D handover will allow devices to remain holistically connected; they will formulate a notion of social nodes in the 6G network [19]. The clusters will be easily trackable and vulnerable in various terms such as impersonation, eavesdropping, Distributed Denial of Service (DDoS), Man-in-the-middle (MitM), repudiation and replay attacks. Communication networks that ensure the least latency and seamless bandwidth are prone to becoming unmanageable once integrated with secure and privacy-preserving architectures. Thus,

formulation of global level security ensured QoS architecture is substantially critical in achieving a systematic emergence of 6G communication.

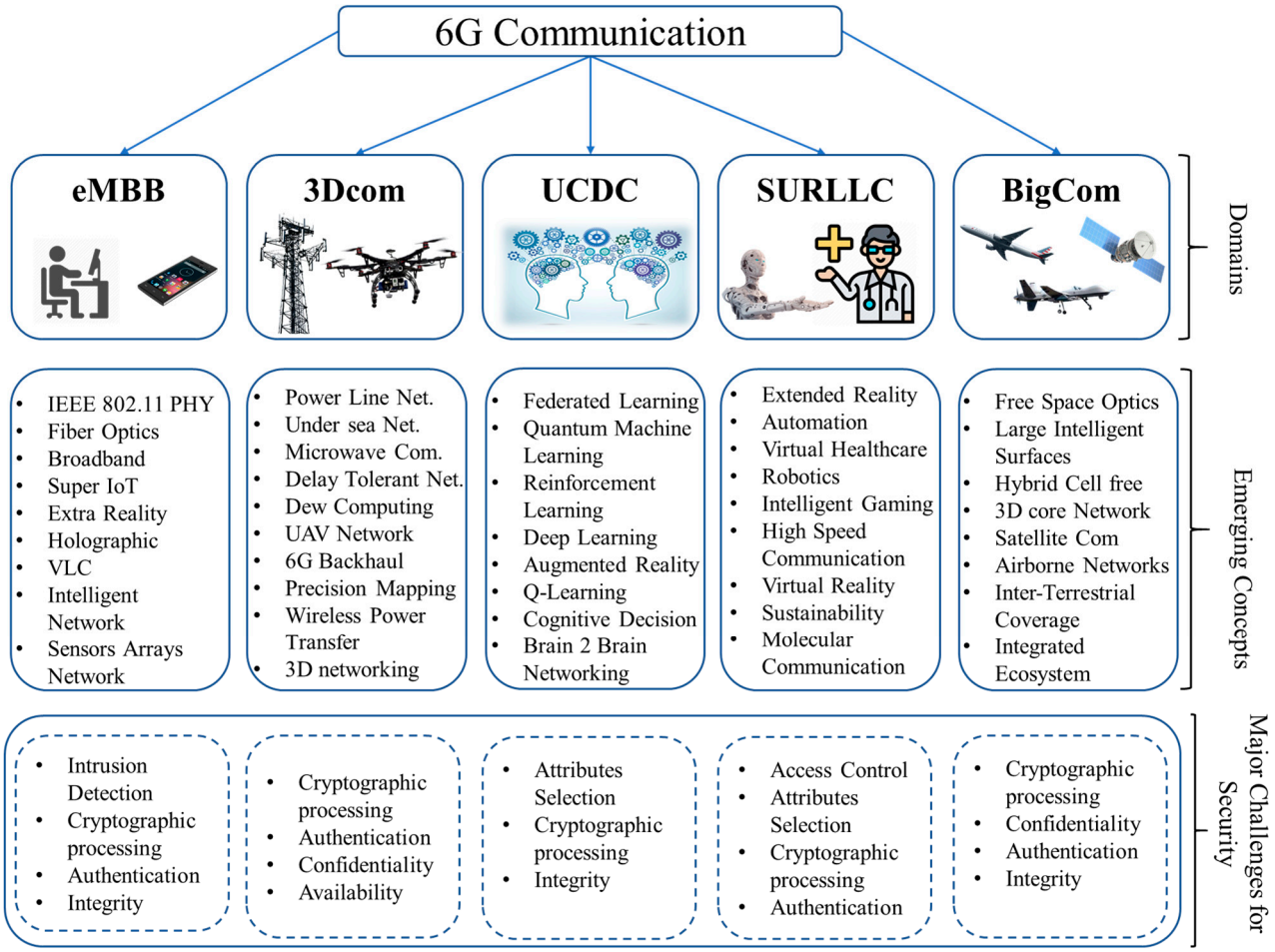

Figure 1. 6G communication paradigm.

1.1. Existing Previous Work in Literature

The number of articles published in recent times spread across a wide spectrum of topics that focus on 6G communication-related networking refinements, applications and security. With the progression in technologies, computer communication is evolving towards 6G networks and the research articles are reaching a multitude of levels in the last three years. We shortlisted publications from SCOPUS and Web of Science related to the topic. The previous surveys are presented from 2019 to 2022, and only eight are focused on security and authentication in 6G networks as shown in Table 2. In contrast, this survey is the first of its kind that presents the threat model, countermeasures and authentication techniques in 6G networks.

Table 2. Comparative analysis related to surveys in the previous literature.

Ref.	6G	Auth.	Observations	
[20]	√	0	Only specific authentication and privacy-preserving schemes are reviewed. It lacks a review concerning the threat spectrum.	None of the previous surveys cover the CIA^3 triad-based Threat Model to analyze authentication and privacy in 6G Security.
[21]	√	0		
[22]	√	0	Focus only on ML-based techniques. Moreover, it lacks threat model-based analysis.	
[23]	√	X	Only privacy is covered with a general overview. Aspects related to various attacks and techniques require further review.	
[24]	√	X		
[25]	√	X		
[26]	√	X	Limited coverage to the security perspective.	
[27]	√	X		

√: indicates Complete support; X: indicates no support; 0: indicates partial support.

In previous surveys, the security issues related to 6G networks were analyzed in [20–27], but threats, countermeasures and techniques were only partially focused. This survey concentrates explicitly on security implementation for 6G networks. With this premise, we further analyzed the open issues and future research directions that cover novel implementations and innovative solutions in combination with techniques from interdisciplinary domains. We strongly believe that this survey will provide a comprehensive review of the current aspects of emerging security issues in 6G communication.

1.2. Scope and Contributions

Mainly, the focus of the literature review in this paper was based on a keyword search, namely, "threats"," counter measures", "security schemes", "authentication techniques", "authentication system" and "authentication framework". These terminologies were used to search the latest literature on various platforms such as SCOPUS, Web of Science, IEEE Xplore Digital Library and ACM Digital Library. Specifically, the proposed authentication schemes of 6G networks were shortlisted at the start. Thereby, each shortlisted work was reviewed with a focus on distinct criteria: (1) reputation, (2) relevance, (3) originality, (4) date of publication (between 2019 and 2022) and (5) most significant literature in the specific area. The explanatory portion of this survey primarily comprises papers in the field of 6G that specifically discuss security mechanisms as their main subject. We initialized our search on 11 July 2022 and proceeded until the submission for acceptance. The significant contributions of the survey are:

1. We presented a threat model for the vulnerabilities in 6G cellular networks in five classifications: threats against Confidentiality, Integrity, Authentication, Availability and Access control (CIA^3).
2. We presented a categorization for countermeasures used in 6G networks into three types based on asymmetries: (1) Cryptographic Methods (CM), (2) Entity Attributes (EA) and (3) Intrusion Detection Systems (IDS).
3. We suggested a taxonomy of authentication techniques for 6G networks in eight types: handover authentication, mutual authentication, physical layer authentication, deniable authentication, Token-based authentication, Certificate-based authentication, key agreement-based authentication and multi-factor authentication.
4. We specifically highlighted future research directions on the basis of overall discussion on the topic, including, (1) Privacy Preservation in 6G network-based 3D Fog Computing, (2) 6G-enabled secure smart Infrastructures and Augmented Reality, (3) SDN-based privacy-protected architecture in 6G networks, (4) Optimized secure routing in 6G networks, (5) 6G Physical Layer security and (Tera-Hertz) THz spectrum, (6) 6G security in Quantum computing and (7) Blockchain-based distributed security in 6G.

1.3. Paper Structure and Organization

The review proceeding of this paper is structured as follows. Section 2 discusses the prevailing CIA^3 triad-based threat taxonomy in 6G communication. Section 3 provides a categorized review of security countermeasures. Section 4 discusses a taxonomy of authentication techniques for 6G networks in eight types: handover authentication, mutual authentication, physical layer authentication, deniable authentication, token-based authentication, certificate-based authentication, key agreement-based authentication and multi-factor authentication. Section 5 provides future research directions related to security in 6G communication. In the end, we conclude our survey in Section 6. Figure 2 illustrates the overall structure and organization of this paper.

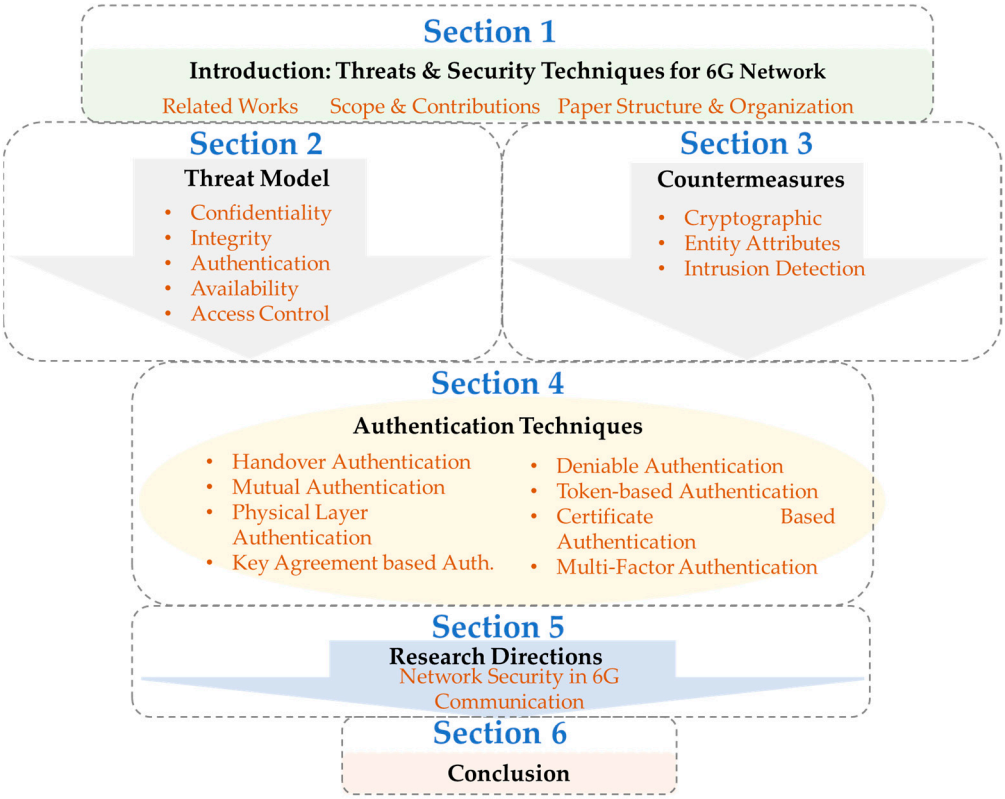

Figure 2. Paper Structure and Organization.

2. Taxonomy for the Threat Model

This portion presents the prevailing threat model in 6G communication. Here, we reviewed thirty-two attacks related to authentication and privacy-preserving schemes for 6G mobile network communication security. Due to symmetry in behavior of wireless network threats, multiple distinct criteria are available in the literature to produce a taxonomy of the threat model [28–31]. Our survey categorized threats in 6G mobile networks into five categories, as shown in Figure 3. The threat model is an extended CIA triad that includes threats related to Confidentiality, Integrity, Availability, Authentication and Access Control (CIA3).

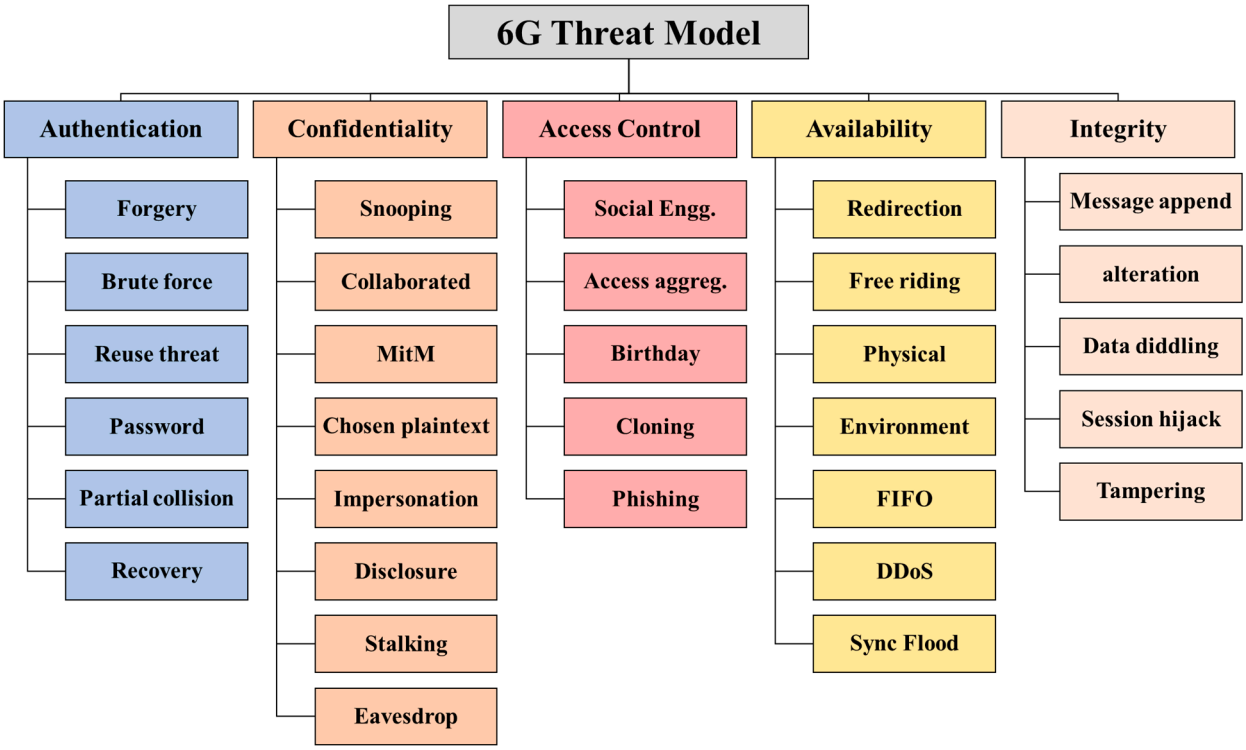

Figure 3. Taxonomy of threats in 6G Mobile Networks.

2.1. Threats against Confidentiality

We shortlist eight attacks in this domain, including MitM, eavesdropping, snooping, chosen text, impersonation, stalking, collaboration and disclosure. The most venerable area is related to MitM threats. MitM threat is considered a realistic vulnerability to mobile communication where attackers can take a middle position between two communicating parties. Various challenges have prevailed in the vulnerabilities related to False Base Station Attacks (FBSA)-based MitM in modern cellular networks [32]. Most of the solutions use public-key cryptographic techniques for countering different threats related to MitM. Likewise, asymmetric information-based intelligent routing and collision avoidance techniques are also suitable for countering MitM attacks in modern 6G networks based on UAV communication [33,34]. Various unconventional techniques such as Artificial Intelligence (AI)-based Machine Learning (ML) can be employed for ensuring security in 6G network-based smart cities, which counters many vulnerabilities, including MitM [35]. Blockchain-based authentication mechanisms are also widely researched for protection against issues related to MitM attacks in 6G-based ad hoc networks. For example, eavesdropping results in compromised confidentiality through data transmission on unsecured channels. In [36], the authors presented a blockchain-based confidentiality probability matrix to estimate data confidentiality level in 6G networks with a specific focus on eavesdropping.

6G communication is vulnerable to edge server snooping attacks, resulting in compromised data confidentiality in the Cybertwin architecture [37]. Confidential information can be compromised through statistically chosen text attacks in wireless networks [38]. Therefore, data aggregation through multiple statistical functions is used to obtain a single result of an information unit. This technique provides security against several types of chosen text attacks against confidentiality [39]. Impersonation attacks can trick users into revealing vital information on unsecured wireless channels. A massive communication paradigm in 6G can result in several possibilities of impersonation at various levels in the communication chain. Likewise, the emerging 6G communication environment will result in a huge challenge for regulatory authorities to assist common users against bullying/stalking attacks concerning confidential information [40]. Similarly, these massive

communication scenarios may create a wide span of vulnerabilities related to collaborative attacks on confidential information in 6G networks. In [41], the authors suggested blockchain-based transparent data management for 6G-enabled networks for countering vulnerabilities related to intentional or unintentional disclosure of confidential data.

2.2. Threats against Integrity

We categorized these threats into five types: message append threats, message alteration threats, tampering threats, session hijack and data diddling threats. These attacks can be categorized in other hierarchies; however, the presented taxonomy is most appropriate as per the prevailing security paradigm in 6G communication. Integrity-related threats have severe implications in the 6G network [21]. Several risks are related to the unconventional implementation of the Internet of Things (IoTs), such as intelligent water quality management for a healthy ecosystem [42]. Various techniques, especially blockchain, are widely considered for integrity measures in 6G-enabled IoTs.

Similarly, unconventional approaches such as machine learning-based blockchain techniques can cover several security prospects, especially data integrity [43]. Implementing various cryptographic techniques to counter message append, message alteration and message tampering attacks may result in massive processing overheads in ultra-dense communication, which will become a challenge for resource constraints of 6G-enabled IoTs [44]. Time-specific session hijack attacks compromise the integrity of whole data communication. Similarly, session hijacking is considered a broad attack that may result in several simultaneous security incidents in a 6G-enabled fog computing environment [45]. Likewise, data diddling also transforms into many attack formats such as infecting malicious data devices to create integrity issues in massive communication. In [46], the authors suggest QR code-based secret sharing in 6G-enabled industrial IoTs to prevent attackers from data diddling.

2.3. Threats against Availability

This categorization contains seven types of threats: redirection threat, physical threat, DDoS, environmental threat, First-In-First-Out (FIFO) threat, free riding threat and syn flood threat. In [47], the authors proposed a DDoS attack identification technique in machine-to-machine 6G networks. The proposed technique is an energy-efficient topology for the mitigation of DDoS attacks in the 6G network. The concept of virtual shadow networks is emerging in 6G network security architecture to counter traffic redirection attacks in virtual networks [48]. 6G-enabled smart infrastructures are bringing unconventional security-sensitive implementations such as smart grids. Physical layer attacks or interventions may result in catastrophic incidents in less secure 6G-enabled smart grid cyber-physical systems [49].

Similarly, the 6G massive communication requires intelligent interference mitigation to avoid an RF-saturated environment that may otherwise create serious network availability threats [50]. FIFO attacks occur when data or communication process entry/exit time intervals are gathered or correctly predicted by the adversary. In [51], the authors suggested an ML-enabled IDS system to counter several attacks, including FIFO functionalities-based vulnerabilities in 6G-enabled networks. 6G will entail ubiquitous AI to incorporate data-driven ML solutions [52]. Therefore, intense employment of Federated Learning is inevitable in 6G communication. However, the free-rider attack has prevailed as a common vulnerability in Federated Learning-based models [53]. Similarly, 6G communication requires the incorporation of intelligent mechanisms to counter conventional flooding attacks related to weakness in existing implementations such as Transport Control Protocol (TCP), HyperText Transfer Protocol (HTTP) and Internet Control Message Protocol (ICMP) [54].

2.4. Threats against Authentication

In this category, we covered seven types of threats, which include brute force, replay, reuse, forgery-based, partial collision, password and recovery-based threats. The primary

focus of threats against authentication is to disturb the client—server authentication mechanism. The password-based authentication schemes are primarily attacked by entities which are portrayed to be legitimate in a communication environment. In the partial collision, an attacker can employ various cryptographic methods to extract the secret keys, hash, etc. Similarly, 6G-enabled Radio Access Network (RAN) is vulnerable to collision attacks on control signals from intelligent spectrum controllers [12]. In [37], the authors presented a lightweight authentication scheme for a 6G-enabled maritime transport system to avoid forgery attacks. The scheme is a lightweight message exchange protocol to counter trust issues in public channels of communication. Anonymous mutual authentication and key establishment protocols can improve security against message recovery-based attacks in 6G-enabled IoT networks. Traditional communication protocols such as the Voice over Long-Term Evolution (VoLTE) protocol contain vulnerabilities related to keystream reuse. Therefore, transition to 6G requires critical analysis of previous protocols to avoid security incidents related to reuse attacks [13]. AI-based joint QoS and security schemes are designed with proven strength against brute force attacks [38]. In combination with the electronic Subscriber Identity Module (eSIM), Public Key Cryptography can provide resilience against replay attacks [39].

2.5. Threat against Access Control

We include five threats related to social engineering, data mining, birthday, cloning and phishing in this category. Access control-related threats are most common, especially in organizations that contain proprietary or sensitive information related to products, possesses, customers and operations. Organizations must implement computer-based solid access control for continuity and minimum potential destruction to prevent their vital information from intentional or accidental unauthorized access. In these scenarios, intentional threats are very sophisticated and advanced. In [55], the authors discussed a blockchain-based application for establishing various security mechanisms, including access control in 6G-based ecosystems. Social engineering is considered a serious threat to heterogenous integrated smart infrastructure in 6G-enabled IoTs. Therefore, blockchain-based key management protocols must be designed to attain a decentralized traceable security impression in 6G [56]. Similarly, malicious collection of apparently insensitive or unclassified data from heterogeneous 6G-enabled networks may result in various kinds of data mining attacks. Moreover, the post-quantum era of 6G communication requires the design of unconventional birthday attack-resistant algorithms [57]. Similarly, no-cloning theorem-based quantum computing can prevail as a potential solution against cloning attacks in 6G heterogeneous networks [58]. In [59], the authors suggested an adversarial learning algorithm to mitigate 6G mm-Wave beam prediction attacks. Here, phishing attacks can exploit data to affect the performance of AI-based models in 6G spectrum management.

3. Countermeasures

This section focuses on various mechanisms related to countermeasures against threats to authentication and privacy-preserving schemes for 6G mobile networks. These countermeasures are categorized into three types: Cryptographic, Entity Attributes and Intrusion Detection. Moreover, our categorization provides a comparative overview of existing countermeasures, as shown in Figure 4.

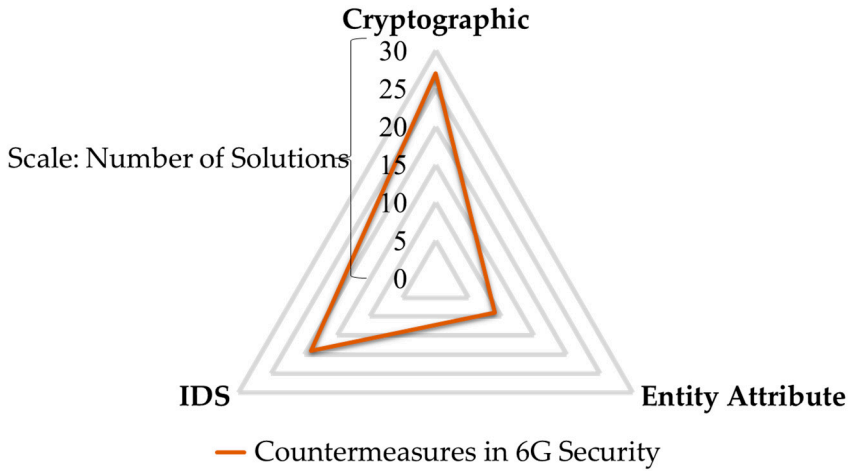

Figure 4. Number of papers vs. countermeasures.

3.1. Cryptographic-Based Countermeasures

Cryptographic techniques encompass the majority of primary conventional as well as unconventional measures to achieve a reliable level of security architecture in emerging mobile communication scenarios. Cryptography contains classical concepts of symmetry as well as asymmetry [60]. Several techniques are structured on Public Key Infrastructure (PKI) for identification of Access Points (AP) or Base Stations (BS) in the 6G mobile networks [61]. In [41], the authors suggested the Paillier cryptosystem composed of three algorithms: generation of keys, encryption and decryption. A traditional approach of two large independent and random prime numbers is used in this technique. Although the proposed scheme is targeting 6G communication, it requires extended analysis for estimation of the processing power requirement and MitM vulnerability related to quantum computing-based factorization. A group signature scheme is suitable for incorporating conditional anonymity. Likewise, a short group signature scheme is ideal for group RSA-based strong signatures. Therefore, applications for 6G-based IoTs networks are researched iteratively for group-based signature architecture efficacy in quantum computing [57]. However, RSA implementation in low processing sensors communication will be a challenging problem for attaining resistance to quantum computing-based attacks.

There are several symmetric key-based schemes for privacy preservation in the 6G network. Cybertwin is a novel unconventional network architecture in 6G [62]. This unusual framework establishes itself as a network assistant, communication behavior logger, caching mechanism, resource coordinator, support localization and embedded security architecture for the 6G mobile communication system. Cryptographic-centric reference security architecture is considered appropriate for the Cybertwin-driven 6G environment [37]. Similarly, the authors in [63] discussed several challenges, methods, applications and security issues related to Cybertwin-driven 6G architecture. Moreover, the authors in [64] presented a post-quantum secure ring signature based on chameleon hash function to enhance security and privacy in the Cybertwin-driven 6G network. However, limited scalability in commercial applications is major drawback of the ring signature due to linear growth of signature size [65]. Moreover, the chameleon hash algorithm may create compatibility issues in 6G, where the domain including eMBB, UCDC, SURLLC, 3DCom and BigCom requires a holistic integration with a broad range of modern user elements. In [37], the authors proposed reference architecture for security of a Cybertwin-driven 6G vehicle-to-everything network. The proposed scheme includes a handover authentication between vehicle and edge server with a proxy ring signature technique. Proxy ring signature overcomes scalability issues due to decentralization. However, the concept has major challenges for handling the insecure data at the edge server, processing cost at the edge server and historical data migration problems. The elliptic curve-based non-conventional cryptographic technique is capable of recovering RSA's prime factors [66]. Cybertwin-based

cloud-centric network architecture incorporates an enhanced and compatible always-on connection in 6G communications; however, this brings several cloud-specific vulnerabilities. In [67], the authors suggested the use of a digital signature-based authentication key exchange protocol with provable reliance against several attacks in 6G Cybertwin network architecture. However, the proposed strategy requires typical evaluation related to typical 6G challenges of processing issues in IoT devices, MEC exploitation with quantum computing and authentication delay.

Advanced Encryption Standard (AES)-based schemes are widely suggested for privacy-preserving and authentication protocols in 6G networks. In combination with AI-based QoS, AES encryption provides joint network optimization in 6G. In [68], the authors proposed lightweight cryptography with the color image-based scheme for privacy preservation in 6G networks. The authors used the Hybrid Particle Swarm Optimization-based Cuckoo Search Optimization Algorithm scheme for multiple secret sharing. However, this steganographic approach requires evaluation for implementation in non-image related applications of the 6G era, such as dense sensors network, tactical drone swarm, etc. Similarly, further analysis is required for cryptanalysis and threat spectrum coverage of the proposed scheme. Likewise, the authors in [69] suggested random number generation with a single Central Processing Unit (CPU) for 23.8 Tbit per second, which is employable in various security-related implementations in high-speed communication such as 6G. Although the proposed solution targets the eMBB scenario of 6G communication, it will contain trivial vulnerabilities specific to the stream cipher. Moreover, further research is required for secure management of memory and key sharing mechanisms. The authors in [70] proposed a secure, lightweight cryptography-based eHealth system for the 6G network, which also addressed vulnerabilities related to MitM in low-latency D2D communication. The solution focused on the security of Mobile Edge Computing (MEC) integration in 6G architecture for private data management in Internet of Medical Things (IoMT) devices. However, the proposed solution requires elaboration to analyze the role of Certification Authority (CA), key generation and the management process. In [71], the authors proposed a reconfigurable Field Programmable Gate Array (FPGA)-based stream cipher for 6G-based high speed and massive throughput data streaming hardware applications. The scheme is a potential countermeasure for resource constraints related to security challenges in smart devices. However, the scheme has a complex design, therefore, memory management will be a challenge. Moreover, the scheme is vulnerable to cryptanalysis attacks. Similarly, 6G physical layer provisions the implementation of a Delta-Orthogonal Multiple Access (D-OMA)-based security scheme through distributed encryption with a low intercept probability [72]. However, D-OMA-based physical layer encryption will cause challenges related to compatibility with the upper layer and integration issues with non-OAM devices in heterogenous network environments. Visible Light Communication (VLC) arose as an effective option for data communication. Therefore, VLC is considered as a potential medium for handling 6G-based high-throughput applications. In [73], the authors suggested use of asymmetric encryption for optimum error rate in comparison to conventional symmetric encryption in 6G-enabled VLC-based indoor applications. 6G technology is being designed with the aim to achieve a 1Tbps throughput with less than 100us latency. Therefore, it is imperative to analyze related challenges and design a corresponding Next Generation Transport-layer Protocol (NGTP).

The authors in [74] presented an AI-empowered AES encryption for joint network optimization. The solution employs Kalman filtering to predict future harvesting power and key length switching. However, the proposed solution requires further research to ascertain the vulnerabilities in case of relatively short keys; similarly, the proposed solution requires a compatibility analysis for implementation in a multi-tier heterogeneous network.

The authors in [75] discuss the cryptographic limitations in the use of user identifiers, the Subscriber Concealed Identifier (SUCI), during the post-quantum 6G era. They proposed a SUCI for SIM card security based on the post-quantum Key Encapsulation Mechanisms (KEM) standard declared by NIST. Although the solutions have been highlighted as

potential countermeasures to quantum attacks, the research work requires further extension for analysis related to processing and delay requirements in 6G domains. Table 3 presents an evaluation of the prevailing security cryptographic countermeasure mechanisms in 6G mobile networks.

Table 3. Cryptographic countermeasures for 6G communication.

Ref.	Threat Area	Countermeasure	Attributes	Limitations
[41]	Confidentiality	Paillier cryptosystem	• Employs three algorithms: generation of keys, encryption and decryption • Traditional approach of random prime numbers	• Processing Power requirement • MitM vulnerability • Quantum Computing-based Factorization
[57]	Authentication	RSA	• Group-based signature architecture	• Processing in IoT • Resistant to Quantum Computing
[64]	Authentication	Quantum secure ring signature	• Chameleon hash function • Accumulator and ZK arguments	• Limited scalability • Linear growth of signature size • Backward compatibility issues
[37]	Authentication	Proxy ring signature	• Handover authentication • ECC algorithm	• Unsecure data at edge server • Processing cost at edge server • Historical data migration problem
[67]	Authentication	Key exchange	• Digital signature-based key exchange • AES encryption	• Processing issue at IoT device level • MEC exploitation with quantum computing • Authentication delay is above 1ms
[68]	Confidentiality	Lightweight cryptography	• Cryptography with the color image-based scheme • Multiple secret sharing • Hybrid Particle Swarm Optimization-based Cuckoo Search Optimization Algorithm	• Specific application of multimedia data • Does not cover network exploits
[69]	Confidentiality	Random number generation	• PRNG algorithm • XOR-shift operation • 23.8 Tbps throughput	• Specific to stream cipher • Does not explain memory and key sharing • Does not cover network exploits
[70]	Authentication	Lightweight cryptography	• MEC integration in 6G architecture • Device-to-Device (D2D) communications	• Role of CA not explained • Key generation and management
[71]	Confidentiality	Stream cipher	• FPGA-based stream cipher • Reconfigurable Logic • Aims at a lower hardware utilization	• Complex design • Memory limitations • Cryptanalysis attacks
[72]	Confidentiality	Distributed encryption	• D-OMA • Low intercept probability • Physical Layer Security	• Compatibility with upper layer in network • Compatibility with non-OMA capable devices
[73]	Confidentiality	Asymmetric encryption	• VLC-based indoor applications • Optimum error rate • RSA encryption keys and data lengths	• Line of sight • RSA in quantum computing • Integration issues
[74]	Confidentiality	AES encryption	• AI-based QoS, AES encryption for joint network optimization • Kalman filtering to predict future harvesting power • Key length switching	• Key distribution in heterogenous IoT • Short keys are vulnerable
[75]	Confidentiality	Post quantum KEM	• Countermeasure to quantum attacks	• Processing requirements in IoTs • Delay requirements of 6G

3.2. Entity Attributes-Based Countermeasures

This category contains several traditional and unconventional entity attributes based on technological and theoretical evolution over the years. In [32], the authors evaluated and discussed the communication attribute of context-aware security schemes for the 6G wireless network. Due to symmetric nature of wireless networks, context-aware and adaptive data traffic control schemes are considered optimum for network management as well as

security [76]. However, context-aware security has limitations related to backward compatibility, processing in resource constraint devices and degradation in interference/jamming. SDN technology contains several examples of context-aware security in northbound Application Programming Interface (API) [77]. Distributed SDN has been researched for intelligent interference mitigation and DDoS detection schemes; however, scalability and consistency management is a major challenge in distributed architecture. [78]. Similarly, the authors in [46] suggested a joint implementation of secret sharing and QR-based authentication schemes for 6G mobile networks. QR-based security and management applications have revolutionized the wireless network domain due to ease-of-use. Quick Response (QR) payload base visual cryptographic methods are ideal for IoTs' authentication and privacy preservation in 6G networks. However, QR codes are vulnerable to specific attacks such as Q phishing and replacement of the QR code.

Quantum communication is an unconventional emerging attribute of communication technologies [79]. In [80], the authors proposed a novel approach for quantum key distribution between IoTs and severs in the 6G networks. The authors demonstrated the efficacy of the key distribution mechanism through MitM-based simulation by placing an attacker between IoT devices and the server. However, currently, quantum experiments require analysis beyond the simulation solution to ascertain the limitations related to integration with higher layers in the network. Moreover, the proposed scheme is specific to MitM only.

Three-dimensional location-based resource management and optimization is widely studied for 6G-based heterogeneous UAV networks. Therefore, attributes such as 3D location, resource utilization and system behavioral characteristics are potential candidates for the implementation of security solutions [81]. However, location-based schemes are vulnerable to GPS spoofing and regulatory issues. Privacy and trust management challenges in 6G-enabled vehicular networks focus on industry and academies [82]. Trust management is considered a foundational principle for sharing and controlling all critical parameters of the vehicle.

However, 6G-based massive heterogeneous connectivity creates dynamic vehicle-to-infrastructure (V2I) environments through mm-Wave 3D beam tracking. It involves symmetry-based environmental encoding resulting in several vulnerabilities [83]. The conditional attributes-based balance between privacy preservation and authentication is considered an optimum potential solution in the 6G era. Physical layer attributes contain a wide spectrum of possibilities for implementation of authentication and privacy preservation based on Physical Layer Security (PLS). Reconfigurable surfaces-based multi-antenna beamforming techniques can provide proper protection against jamming and interference in a dense 6G communication environment. Seamless acceptance and commercialized expansion of 6G can only be achieved through human-centric communication with high secrecy and massive throughput. To overcome propagation and secrecy challenges in long-distance THz communication, the authors in [84] proposed antenna selection-based joint utilization of optical and RF links focusing on secrecy performance against eavesdropping attacks in 6G networks. The solution executes a probabilistic secrecy analysis of mixed RF and optical communication through secret antenna selection to avoid eavesdroppers. However, the proposed scheme has a scope limited to eavesdropping attack MIMO technology, and, currently, the increased complexity due to AI-based implementations in MIMO has increased the vulnerabilities and security implementation issues [85]. The authors in [86] proposed a Bloom filter-based private set intersection mechanism to achieve conditional privacy preservation. The scheme has been optimally designed for embedding confidentiality in a system; however, it has limitations related to scalability and high computational overhead. The study in [87] used a reconfigurable surfaces-based multi-antenna for high controller beamforming to avoid DoS attacks. However, the mechanism requires further research to cover the complete spectrum of possible attacks. Moreover, the proposed concept also has limitations related to complexity, scalability and compatibility with heterogenous networks. Table 4 provides the summary of the discussion on Entity Attribute-based countermeasures in 6G communication.

Table 4. Entity Attribute countermeasures for 6G communication.

Ref.	Threat Area	Countermeasure	Attributes	Limitations
[32]	Integrity	Context-aware security	• Physical layer security • Wireless edge awareness • Adaptive protocols	• Backward Compatibility • Physical Layer Processing • Degradation in interference/jamming
[46]	Authentication	QR code	• Secret sharing scheme • Secret image shadows based on polynomial • RS encoding for secret recovery	• QR security issues, such as Q phishing, replacement of QR code
[80]	Authentication	Quantum key distribution	• Simulation scheme for the quantum key distribution • Final length key for symmetrical encryption	• Simulation solution • Specific to MitM only • Integration with higher layer in network
[81]	Authentication	3D location	• Spectrum matching game • UAV based communication strengthening • Mixed integer nonlinear programming	• Subject to GPS spoofing • Regulatory Issues
[86]	Confidentiality	Conditional Attributes	• Bloom filter-based private set intersection • Conditional privacy preservation	• High communication overhead • Scalability issues • High computational cost
[87]	Availability	Physical layer attributes	• Reconfigurable surfaces-based multi-antenna • Beamforming	• Specific to DoS attack only • Complexity • Scalability
[84]	Confidentiality	Antenna selection	• Joint utilization of optical and RF links • Probabilistic secrecy analysis • Monte Carlo simulations	• Limited to eavesdropping attack MIMO technology • Compatibility with heterogenous networks

3.3. Intrusion Detection-Based Countermeasures

Researchers perform several solutions and evaluations to formulate mechanisms related to threat detection schemes in 6G networks. In [88], the authors presented a simplified threat matrix to define risks posed in the emerging 6G era. The threat matrix acts as a threat library for efficient detection and categorization. However, the proposed scheme requires common agreement to maintain the threat library in a distributed heterogenous network, otherwise this scheme will surface several compatibility issues. Likewise, the authors in [89] suggested a Non-Orthogonal Multiple Access (NOMA) sparse signatures matrix for the 6G network that can act as a threat detection system. However, the proposed solution covers only the wireless domain; therefore, coordination with the upper layer may become complex in multi-tier heterogeneous networks. Moreover, this solution is probable to cause compatibility issues with non-NOMA IoTs. Similarly, In [90], the authors proposed an unconventional security scheme for detecting and identifying malicious maneuvers of flooding attacks in the 6G network. The solution is based on a routing scheme to improve Low Energy Adaptive Clustering Hierarchy (LEACH) protocol performance with minimum resource utilization. The scheme detects the flow pattern to identify the least data transmissions to the flooding attacker. However, the research has focused only on flooding attacks, and further research is required to cover all possible attacks through the same approach. In [91], the authors presented a Channel State Information (CSI)-based authentication scheme for 6G security; the same can be employed for intrusion detection in a cyber-secure 6G network. However, the solution is suitable for wireless domain only. The scheme will cause backward compatibility issues and processing overheads. Moreover, the solution is susceptible to low performance due to degradation in interference/jamming. The authors in [92] present a short survey for using AI and ML to establish a secure intrusion detection system capable for use in a 6G-enabled network domain in intelligent and secure vehicular communications. The Deep Learning (DL) technique is widely researched for secure network domains with intrusion detection capabilities [93,94]. Moreover, AI/ML-enabled authentication and privacy-preserving solutions are increasingly suggested for

intelligent detection of attacks, such as jamming, malware, DoS or DDoS [95]. In [48], the authors presented a moving target defense mechanism for proactive defense against multiple attacks including MitM. However, the study has considered only the wireless domain and compatibility issues with the upper layer in a network. Similarly, in [51], the authors suggested a novel approach for IDS to counter several attacks including MitM, showing 99.99% performance of the proposed ML algorithm against various threats. However, the proposed study needs evaluation for suitability in heterogenous networks.

Cognitive radio-enabled 6G networks bring various opportunities and challenges through automated security techniques to counter malicious intrusion in communication paths [96,97]. 6G physical layer manipulation is an extreme point of interest for both attackers and security solution designers. At one end, where vast bandwidth and heterogenous connectivity create favorable grounds for the attacker, 6G spectrum monitoring provides intelligent neural network-based prediction of Secrecy Outage Probability (SOP). SOP is an important criterion for evaluating network secrecy performance [98].

An SDN-enabled blockchain-based resource allocation scheme can provide a secure ecosystem in 6G networks through smart contracts [99]. Secure resource allocation builds an intrusion-proof foundation and trusted network architecture [100]. Similarly, blockchain-based secure data aggregation enables distributed data-dependent industrial applications [101]. Moreover, blockchain-based integrated security provides reliable service delegation in the 6G columniation environment [102]. SDN-enabled fog computing provides intelligent lightweight security infrastructure and an intelligent intrusion detection system in 6G networks [103]. The virtual representation of a 6G physical network, known as a digital twin, provides analyses and optimization of various synchronization solutions for IDS implementation [104]. Table 5 provides the summarized view of our analysis on IDS-based countermeasures in 6G communication.

Table 5. IDS-based countermeasures for 6G communication.

Ref.	Threat Area	Countermeasure	Attributes	Limitations
[88]	CIA^3	Simplified threat matrix	• Attack vector-based categorization	• Common agreement required • Compatibility issues
[89]	Authentication	Sparse Signatures matrix	• NOMA • Channel state information • Linear minimum mean square error	• Covers only wireless domain • Compatibility issues with non-NOMA IoTs
[90]	Availability	Routing scheme	• Identify Malicious Maneuver • Energy based Cluster head selection	• Specific to flooding attacks
[91]	Authentication	CSI	• Channel parameters-based authentication • Secret key distillation for physical layer security • Hilbert Schmidt independence criterion	• Wireless domain only • Backward Compatibility • Physical Layer Processing • Degradation in interference/jamming
[48]	Confidentiality	Moving target defense	• Proactive defense • Standardization perspective	• Wireless domain • Compatibility with upper layer in network
[51]	CIA^3	Machine Learning	• ML-based model • Covers seven different types of new and contemporary attacks	• Scalability issues • Compatibility with heterogenous devices
[98]	Confidentiality	Neural network-based prediction	• Transmit antenna selection • Secrecy Outage Probability • Evaluation network secrecy performance	• Physical Layer Processing • Compatibility with heterogenous devices
[102]	Integrity	Blockchain	• Service delegation • Secure columniation environment	• Scalability issues • Resource constraint
[103]	Availability	SDN-enabled fog computing	• Intelligent lightweight security • Intelligent resource scheduling • Collaborative trust model	• Scalability issues • SDN-based vulnerabilities
[104]	Authentication	Digital twin	• Public key update process • Optimized synchronization • Cryptogram validation	• Processing power intensive • Quantum Computing-based Factorization

4. Authentication Techniques in 6G Communication

In this section, we will discuss the authentication techniques for 6G cellular networks. We categorized the authentication techniques into eight types, including handover authentication, mutual authentication, physical layer authentication, deniable authentication, token-based authentication, certificate-based authentication, key agreement with privacy and multi-factor authentication.

4.1. Handover Authentication

With the exponential expansion in mobile devices and advancement in network technology, cellular data traffic has increased. Secure and seamless mobility of devices in a cellular network primarily depends on authentication during the handover process. Due to limited processing power and exposed wireless links [105], it is extremely challenging to design an appropriate handover authentication protocol [106]. An efficient and dependable handover authentication scheme needs to be developed for guaranteed security in the massively mobile and integrated paradigm of next-generation networks. Handover authentication is visualized as a significant security- and mobility-related proper functionality in unconventional network implementations such as terrestrial satellites. The 6G network is envisioned as an integrated holistic network capable of handling terrestrial satellite network applications. The handover authentication is a challenging problem due to multi-domain scenarios as shown in Figure 5. The authors in [107] proposed a lightweight clustering and game-based handover decision framework with authenticated ground mobility management configurations in 6G-integrated mega satellite constellations. This provides reduced handover delays, signaling overheads and fast convergence. However, this does not cover issues such as handover in higher-layer constellations, inter-layer management and management structure optimization.

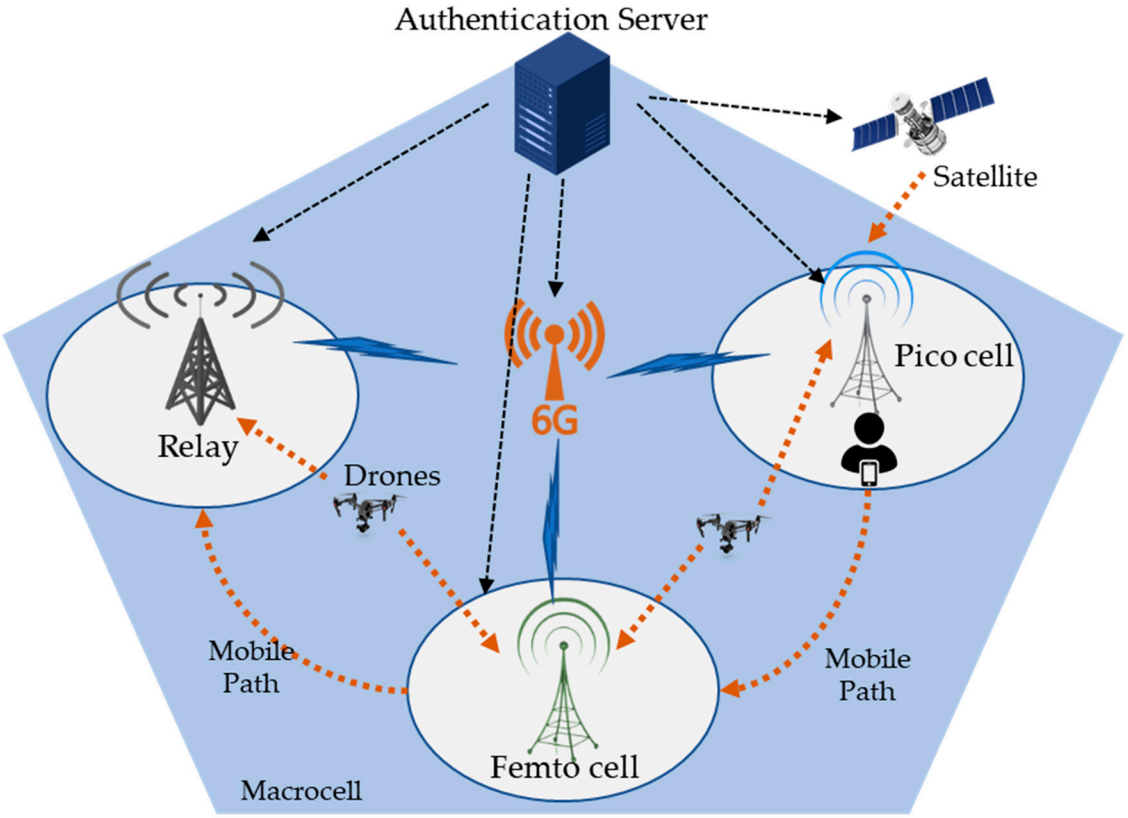

Figure 5. Handover authentication in 6G paradigm.

Similarly, the authors in [37] proposed a handover authentication scheme for 6G Cybertwin between mobile vehicles and edge nodes. This scheme uses a proxy-based ring

signature technique for handover authentication. Blockchain-based handover authentication is visualized as a potential candidate for 6G secure handover. The authors in [108] suggested an efficient, lightweight cryptography-based handover authentication scheme for the fog computing environment. Mobile edge computing reduces handover authentication latency due to mobility pattern traceable schemes [109]. In [110], the authors provide categorization on the basis of mobility pattern to reduce handover latencies and reauthentication delays. However, the scheme lacks consideration of complexity, compatibility and scalability issues. 6G networking concepts are evolving toward a heterogeneous integrated environment with massive mobile entities such as vehicles, drones, UAVs, etc. [111]. Handover management is emerging as a critical area in researching and implementing network domains. Drones and UAVs are mobile in 3D space, due to which handover authentication becomes much more challenging [112]. Poor propagation, shadowing and fading effects are seen as millimeter wave-based contributors for increased complexity in challenges related to the handover mechanism in 6G [113]. The authors in [114] proposed multi-connectivity architecture for improved handover procedural efficiency and coverage range in fading signals. Massively dynamic and multilayer architectures lead mobile devices to frequent handovers in 6G networks. Table 6 summarizes this analysis on handover authentication techniques for 6G mobile networks.

Table 6. Emerging handover authentication techniques in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[107]	Mobility in terrestrial satellites and 6G terrestrial broadband	Clustering and game-based handover decision-based lightweight authentication framework	• Low handover delays • Low signaling overheads • Fast convergence	• Higher-layer constellation design • Inter-layer management • Management structure optimization
[37]	Cybertwin edge nodes in vehicles to everything	Proxy ring signature	• Low overhead • Low processing requirements • Low transmission cost	• Secure migration of historical data
[108]	Handover in fog computing	Cooperative fog nodes	• High handover efficiency • Resist known attacks • Low computation	• Trust management in fog nodes
[110]	Mobile edge computing	Nodes categorization on mobility patterns	• Reduce latency up to 54% • Minimal re-authentication latency	• Higher complexity • Scalability issues • Historical data sharing
[114]	Handover in fading signals	Multi-connectivity architecture	• Handover procedural efficiency • Increased coverage range	• Higher increased initial access • Higher base station discovery times

4.2. Mutual Authentication

Lightweight cryptographic solutions are actively researched for mutual authentication and key agreement schemes in resource-constrained IoT devices. In [115], the authors proposed a random HMAC and ECC-based D2D mutual authentication scheme. The scheme guarantees message authorships with 7.7-times-lower delay and reduced complexity. Moreover, the scheme counters several attacks, including free-riding attack. These schemes have gained prominence due to efficient processing and resilient defense against sophisticated attacks such as free-riding attacks. Security policy management is challenging in mobile devices due to dynamic behavior and situational requirements. Therefore, mutual authentication is considered a promising approach for security policy management. In [116], the authors suggested a fingerprint and MAC address-based mutual authentication scheme for a handshake between mobile nodes. The results include strong bit level integrity and improved trust level validation through MATLAB-based simulations.

Maritime Transport Systems (MTSs) are incorporated with various mutual authentication schemes to avoid unauthorized vessel location data access. The authors in [117] proposed lightweight mutual authentication in multi-server architecture for MTSs. The scheme provides reduced latencies and shows superior performance in comparison with equivalent designs. However, this scheme is vulnerable to brute force and dictionary

attacks due to SHA-1. The IoT environment usually has device-to-device communication where the authentication server usually acts as the third party. Batch authentication in 6G-enabled vehicular networks covers wide authentication requirements such as mutual authentication and anonymity. The authors in [118] proposed a secure, anonymous mutual authentication scheme and key agreement in 6G-enabled IoTs. The scheme utilizes the bilinear paring technique to evade message modification. Although the scheme executes with low overhead and reduced computational costs, it is vulnerable to data privacy issues due to a possible compromise of Trust Authority. Key management schemes in next-generation networks largely depend on mutual authentication. The authors in [119] suggested a client–server key management scheme based on bilinear parring and ECC. The scheme resists most of the network attacks and provides low overhead with reduced computation costs. The scheme is vulnerable to brute force attacks due to a fixed curve in issues in ECC and SHA-1 weaknesses. Table 7 provides the analysis on mutual authentication techniques for 6G mobile networks.

Table 7. Emerging Mutual authentication techniques in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[115]	D2D communication	Randomly HMAC and ECC	• Counters free-riding attacks • Guarantees message authorships • Low complexity in secure key exchange • 7.7 times faster	• Brute force is possible on any singled-out device • Increase in message size • Fixed curve vulnerability in ECC
[116]	Mobile nodes communication	Fingerprint and MAC address-based mutual authentication	• Strong session tokens • Bit level information integrity • Improved trust level on password security	• Finger print hacking vulnerability
[117]	Maritime transport systems	Lightweight mutual authentication in multi-server architecture	• Reduced latency • Superior performance	• Higher bit exchange • SHA-1 Brute force and dictionary attack issues
[118]	Batch authentication in 6G vehicular networks	Bilinear pairing technique	• Evade message modification • Low computational overhead	• Trust Authority compromise vehicle registration and location data
[119]	Client–Server Key Management	Bilinear pairings and ECC	• Resist common network attacks • Low overhead • Reduced computation cost	• Increase in message size • Fixed curve vulnerability in ECC • SHA-1 Brute force and dictionary attack issues

4.3. Physical Layer Authentication

Most of the concepts related to authentication mechanisms are available in higher layers above the physical communication layer. However, it is observed that the implementation of authentication at the physical layer has evolved as an unconventional and stealthy mechanism, where the authentication process is achieved through the superimposition of a critically designed secret modulation on waveforms. Physical layer authentication has gained prominence due to robustness to interference and almost negligible bandwidth dependence [120]. The authors in [121] proposed a spread spectrum-based secret modulation for interference-resistant authentication. The scheme involves spread spectrum-enabled hardware; therefore the scheme has the limitation of compatibility with traditional modulation schemes. Performance of authentication schemes is critically dependent on channel estimation and dynamic compatibility of the protocol with variations in the communication link [122]. In [123], the authors presented an adaptive ML-based intelligent physical layer authentication technique for an improved authentication mechanism in time-varying scenarios. Here, machine learning is embedded in the physical layer through a physical attributes-based fusion model on a kernel machine. Physical layer security techniques emerge as a suitable framework for reduced complexity, low delay, and light footprint in the context-aware security paradigm. MIMO technology in 6G has potential to control physical wireless links at the individual device level as shown in Figure 6.

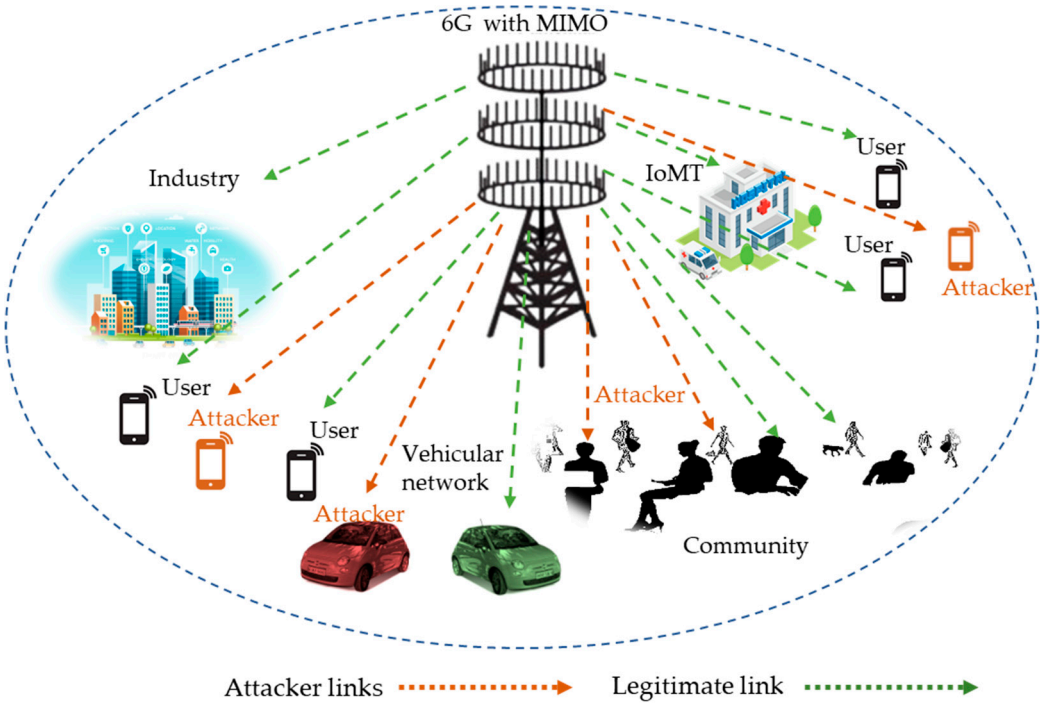

Figure 6. Physical layer authentication with MIMO technology in 6G communication.

The physical layer authentication mechanism provides exposure-free operation of higher layers in 6G-enabled networking architecture. PLS techniques result from channel characteristics' exploitation and randomness in wireless link parameters. Lightweight algorithms are considered ideal for implementation at the physical layer in resource-constrained IoTs. In [124], the authors suggested a Channel State Information (CSI)-based lightweight symmetric cipher-based authentication. It covers various attacks such as small integer stacks, spoofing and replay attacks. The scheme utilizes clustering properties instead of trusted party dependence. 6G-based physical layer security schemes are emerging as an unconventional futuristic paradigm of Human Bond Communication (HBC) and Molecular Communication, where related attributes of five human senses and biological characteristics are integrated into networks for remote analysis and medical procedures [125]. Physical layer security measures have evolved to cover all the foundational security requirements of the CIA triad in 6G networks [126]. Specifications of 6G are still in the evolution stage. 6G will be compatible with heterogeneous communication technologies, including LTE, 5G, B5G and other emerging communication technologies [127]. 6G has various challenges related to enormously high data rates reaching Tbps/THz. Physical Layer Modeling (PLM) and control of the authentication mechanism at the physical layer bring various further unknown research frameworks [128]. The authors in [129] provide a PLS based on mailbox theory with distributed learning. The scheme employs self-organization through a self-learning mechanism to reduce transmission quantity and transmission error.

Orbital Angular Momentum (OAM) modes in joint implementation with MIMO have the potential to reach up to a 100 Gbps throughput in point-to-point transmission [130]. Emerging technologies using the THz spectrum are researched for physical security through hybrid free space optical (FSO)-THz communication. The authors in [131] employed OAM modes in mutually linked FSO and THz schemes. The scheme is advocated to be a potential solution to counter bandwidth degradation issues of RF and to enhance physical layer security. Similarly, the authors in [132] suggest an OAM-based physical layer authentication to improve the bit error rate (BER). The proposed scheme has been evaluated for BER performance over Rician fading channels. However, spatial multiplexing of orthogonal waves with OAM are unable to achieve conventional efficiency. Moreover, minor misalignments in the antenna system sufficiently affect the OAM scheme [133].

Table 8 provides the analysis on physical layer authentication techniques for 6G mobile networks.

Table 8. Emerging physical layer authentication techniques in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[121]	Spread spectrum	Secret modulation	• Robustness to interference • Negligible bandwidth dependence	• Compatibility issues • Complexity
[123]	Channel estimation	ML with kernel least mean square	• Improved reliability • Robust • Compatible with time-varying environment	• Limited to low power devices • Combability issues with 3rd party devices
[124]	CSI	Clustering and lightweight symmetric cipher with channel state information	• Secure and simple • No trusted party • Resist small integer attacks • Reduced data loss • Reduced latencies	• Limited to MIMO-OFDM systems • Combability issues with 3rd party devices • Hardware complexity
[129]	6G transmission with PLS	Mailbox theory, distributed learning and blockchain	• Self-organization • Self-learning • Reduced transmissions quantity • Reduced transmission error	• High processing • Complex implementation • Backward compatibility issues

4.4. Deniable Authentication

Pre-sharing of system parameters before security verification of the communication paradigm is an essential part of the authentication process. This exposes some of the vulnerable characteristics of devices, resulting in serious security incidents, especially in wireless network communication scenarios. Therefore, Deniable Authentication (DA) protocols are designed to empower the sender with the ability to reject the authentication process to any third party. DA protocols are mostly recommended to avoid the "Encryption-then-MAC" paradigm by disallowing entities from initiation of the MAC-based authentication process [134]. In [135], the authors suggested a source-hiding scheme with projective hash functions. The scheme secures WIFi authentication by rejection to third party linkages.

Similarly, Mobile Ad hoc Network (MANET) is the foundational element in modern communication [136,137]. In [138], the authors suggested an identity-based DA protocol for MANET with formal security verification through a random oracle model. DA protocols are developed to maintain possible heterogeneity due to the highly diverse nature of the emerging communication environment in wireless networks. The authors in [139] proposed a bilinear pairing-based formal security proof of DA though identity-based cryptography. Group Key Agreement (GKA) protocols also utilize DA in fog computing-enabled vehicular networks, as this highly mobile wireless environment makes key parameters vulnerable. The authors in [140] proposed a random oracle model for authentication in social media network communication. This scheme executes through a single logical step and fairly reduces cipher text length and computational cost. It is pertinent to highlight that limited available works in the literature directly relate the implementation, solutions and challenges for deniable authentication in 6G networks. Table 9 summarizes the analysis on deniable authentication techniques for 6G mobile networks.

Table 9. Emerging deniable authentication techniques in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[135]	Wi-Fi authentication	Source hiding with projective hash functions	• Rejection to authentication process to any third party • Prevent the location leakages	• Null values problem • Hash collisions
[138]	Mobile Ad Hoc Networks	Bilinear Pairings	• Suitable for resource-limited MANET environments • Formal security model	• TA dependence • SHA-1 Brute force and dictionary attack issues
[139]	Pervasive computing	Bilinear pairings	• Formal security proof • Identity-based cryptography	• SHA-1 Brute force and dictionary attack issue • Achieves partial deniability only
[140]	Social Networks	Random oracle model	• Reduces the computational cost • Reduces the length of ciphertext • Single logical step	• Specific to awkward conversations over the internet

4.5. Token-Based Authentication

Taken-based authentication schemes emerged as a stateless, scalable, decoupled and transparent secure digital information dissemination framework in B5G as shown in Figure 7. MEC technology is widely incorporated with token-based access control management in next-generation networks. In [141], the authors proposed the JavaScript Object Notation (JSON) web token-based authentication for MEC. The scheme provides compliance with standard requirements for credentials transfer between multiple parties. Token-based authentication and authorization schemes are suitable for 6G-enabled IoTs due to the reduced energy consumption associated with token-based data transfer [142]. The authors in [143] suggested on-chip physically unclonable functions for energy-efficient token-based authentication. The scheme utilizes ECC for compatibility with low-resource IoTs. Due to ease of implementation and functioning of token-based authentication schemes, special mechanisms such as Network Repository Functions (NRF) are employed to generate access tokens for authorization servers in 6G-enabled IoTs. NRF-based authentication works in combination with TLS architecture [144]. In [145], the authors used token-based authentication along with a lightweight security module in 6G-enabled smart city infrastructure. Here, tokens are bound with timespan limits, ensuring limited vulnerability concerning mal-intentioned interference.

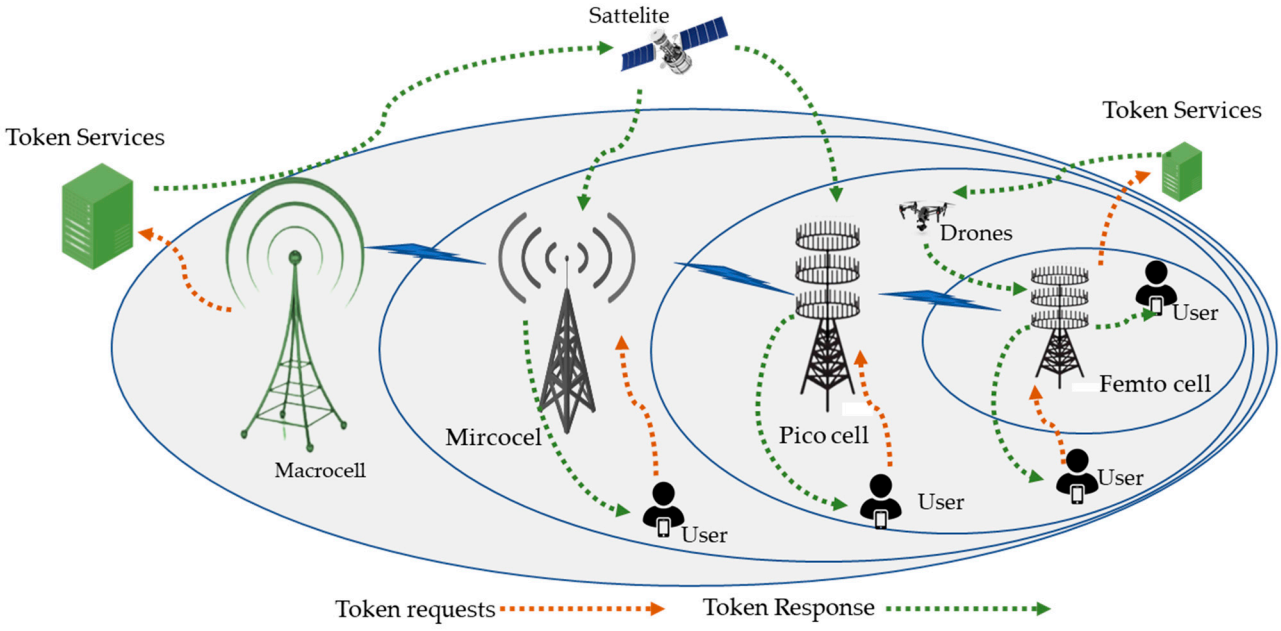

Figure 7. Token-based authentication in heterogenous 6G networks.

Token-based authentication provides implementation of QoS-aware 6G-enabled ultra-low latency services in edge communication-based drones, IoTs and health care applications [146]. In [147], the authors suggest a gait information aggregation-based high-coverage authenticated gait diagnosis scheme. However, this scheme suffers issues related to high latency and scalability with respect to mobility requirement of heterogenous IoTs in the 6G network. Token authentication is merging with blockchain and SDN-related unconventional concepts in 6G communication. Blockchain with token-based authentication provides a secure and auditable orchestration mechanism for multi-domain SDN infrastructure in 6G networks [148]. Due to token-based authentication's robust and network-friendly attitude, IEEE 802.11p-based applications are securely migrating to 6G networks [149]. The token-based implementation provides joint authentication and access control in resource-constrained blockchain-enabled IoTs in 6G networks. Token-based authentication mechanisms are vulnerable to prediction and stealing attacks; therefore, it is imperative to formally verify the security strengths of token generation and distribution mechanisms. Thus, tokens are largely blended with time and session-based attributes for dedicated gateways with exceptional security infrastructure controlling token generation and distribution. In [150], the authors suggested SHA-256-based cyclic keys for narrow-band IoTs. Nowadays, organizations deploy blockchain-based intelligent mechanisms to identify and monitor the malicious behavior of IoTs. The authors in [151] proposed the ECC-supported blockchain for efficient and trusted secure data movement among industries. The scheme is vulnerable to ECC-specific issues such as fixed curve and quantum attacks. We summarize our discussion on token-based authentication on 6G communication in Table 10.

Table 10. Emerging token-based authentication techniques in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[141]	MEC	JSON Web Token	• Compliance with the standard requirements • Credentials transfer between parties	• JSON security failures • Vulnerable to confusion attacks
[143]	Conventional client-server	On-chip physically unclonable functions	• Reduced energy consumption • Token-based data transfer • Energy-quality scaling	• IoT specific • ECC fixed curve issues
[145]	Geographically distributed networking	Lightweight security module	• Reduces delay • Avoids high power consumption	• IoT specific • Increased overhead
[147]	Edge level	Gait information aggregation	• Accurate for abnormal gait diagnosis • Latency of 335 ms • High SDN coverage Ratio	• Specific application • Scalability issues
[148]	SDN	Blockchain	• Auditable orchestration • Zero-trust security model • End-to-end encryption	• Scalability issues • Key management issues • Consensus overheads
[150]	Narrow-band internet of things	SHA-256 cyclic keys	• Dynamic key-based security • D2D communication • Machine-to-machine	• Vulnerable to • Prediction attacks • Stealing attacks • Quantum computing
[151]	Cross-domain secure data sharing	Blockchain with ECC	• Secure data movement • Trust among the industries • Collaborate on manufacturers	• Scalability issues • Fixed curve vulnerability in ECC

4.6. Certificate-Based Authentication

Foundationally, a certificate-based authentication scheme is a joint implementation of various cryptographic algorithms and handshaking protocols. Certificate-based authentication is widely used in current world applications and smart infrastructures. In [152], the authors proposed a lightweight cryptography-based certificate authentication scheme with anonymity and untraceability. The scheme provides resistance against several attacks such as MitM, DoS, impersonation and replay attacks. Although certificate-based security mechanisms are considered impracticable in resource-constrained IoTs, several overhead

reduction modifications are being performed for the suitability of certificate-based authentication in next-generation networks based on distributed IoTs. These modifications include pre-validation, session resumption and handshake delegation. Certificate-based authentication is designed with a focus on MitM attacks in wireless network communication, unlike attribute-based mechanisms such as biometric or One Time Password (OTP) mechanisms [153]. Certificate-based authentication provides many solutions with public key-based unique credentials.

6G communication is bringing huge cross-domain communication along with state legislative obligations of centralized certification authorities, which is normally an unsecured global phenomenon. Therefore, massive heterogenous communication in 6G is shifting from centralized certification to decentralized self-sovereign identity-based certification [154]. Lightweight cryptography-based certification is widely suggested for key agreement in 6G-enabled Internet of Drones (IoDs), where the edge computing environment provides processing and implementation of authentication protocols. In 6G communication security, the implementation of blockchain technology is expanding rapidly due to no dependency on a centralized Certification Authority (CA) [155]. Therefore, CA-based schemes will become outdated due to unconventional decentralized blockchain certificates (Bcert). In these schemes, devices locally generate the blockchain certificates, which are periodically updated with new certificates without changing the identifier information. Here, the originality of certificate updates is ensured through digital signatures corresponding to the previous certificate [156]. Blockchain-based certificates can provide efficient cross-domain authentication in 6G-enabled heterogeneous communication. Table 11 provides a summarized analysis of certificate authentication techniques for 6G mobile networks.

Table 11. Emerging certificate-based authentication techniques in 6G networks.

Ref.	Network Model	Technique	Features	Limitations

[152]	Smart Homes	ECC	• Lightweight authentication
			• Anonymity and intractability
			• Resistant to
			  • MitM attack
			  • DoS attack
			  • Impersonation attack
			  • Replay attack
				• Fixed curve vulnerability in ECC
				• Scalability issues

[153]	Phasor measurement unit	Explicit certificate	• Designed with a focus on MitM attacks • Real-time solution • Covers IEC 61850-90-5 communication standard	• Overheads • Certificate update issues • Vulnerable to brute force attacks
[154]	Cross-domain identity management	Self-sovereign Identity	• Self-sovereign certification • Decentralized architecture	• Scalability • Key management • Standardization issues
[155]	CyberTwin	Diffused Practical Byzantine Fault Tolerance	• Non-dependence on centralized CA • Blockchain empowered • Improved latency, overhead and storage cost	• Scalability • Standardization issues • Processing limitation in IoTs
[156]	Cross-domain authentication model	Blockchain	• Unconventional, decentralized • Blockchain certificates • Temper-resistant • Anonymous	• Scalability • Processing cost • Vulnerable to quantum computing attacks

4.7. Key Agreement with Privacy

Key agreement is considered the backbone of most of the authentication schemes. Various hierarchical key agreement frameworks have evolved for the privacy-protected authentication among gateways, sensors and users. Key agreement is also considered a primary driving factor in various cryptographic algorithm-based security protocols. Various vulnerabilities associated with the critical agreement process include protocol replay, key reuse, deniability, signature tempering, key compromise, server trust issues, identity manipulation, etc. However, a major challenge is a secret-key agreement over unauthen-

ticated public channels, where massive attacks rise exponentially, such as the health care system facing challenges in establishing a secure session key among medical servers and patients. Moreover, biometric credential misuse and privacy exploitation can result in irreparable damages. Therefore, dynamic privacy-protected key agreements are required for the intractability of biometric parameters in authentication servers [157]. Similarly, smart grids and smart cities are low processing, dynamic and massively expanded scenarios in next-generation communication. Smart grids are usually targeted by malicious entities for monetary gains related to billing manipulation; however, large-scale sophisticated attacks on smart grid systems can paralyze the whole governance and management system. In [158], the authors proposed novel privacy-aware authenticated and unclonable one-way hash-based key agreement scheme for secure communication between resource-constrained smart meters and the grid management server. Due to dense interconnectivity and massive networking in modern communication, key management is emerging as a challenge, as depicted in Figure 8.

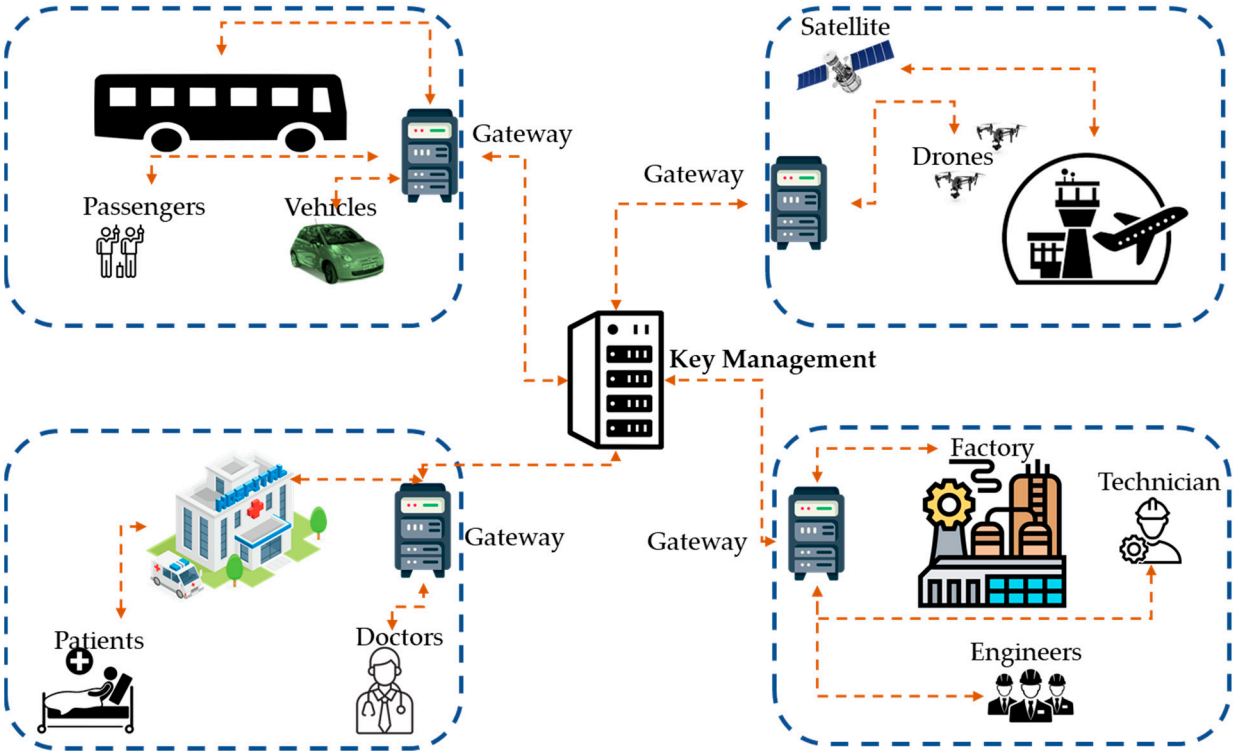

Figure 8. Key management scenarios in modern communication.

Physically Unclonable Functions (PUF) are being designed for local security to digital devices and biometric credentials are distributed 6G-enabled networks. The PUF-related security implementations are focused on low processing power scenarios such as signal processing, information theory, coding theory and hardware complexity limitations [159]. In [160], the authors suggested blockchain-based subscription authentication with characteristics such as auditability, resistance to DoS attacks, low transmission cost and low overhead. However, the scheme has limitations related to scalability and standardization issues. Emerging key agreement protocols being are designed to eliminate the requirement of a secure channel between Home Networks (HNs) and Serving Networks (SNs) in 6G-enabled smart cities. Achievement of a decentralized key agreement on the unsecure channel can be attributed to blockchain technology with provisions for auditable communication and decentralized implementation for protection against Denial of Service (DoS) attacks. The authors in [161] proposed a third-party independent decentralized blockchain-based spatial crowdsourcing scheme in a 6G-enabled Network In Box (NIB). In this scheme, the control station shares counter-based encrypted location parameters for

establishing a key agreement with sensing nodes. Table 12 summarizes our analysis of key agreement with privacy techniques in 6G mobile networks.

Table 12. Emerging key agreement with privacy for authentication in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[157]	Electronic healthcareLuo MiaoBiometric parameters	Biometric authentication	• Undisclosed and untraceable • Unclonable one-way hash • Semantic secure under the real-or-random model.	• Finger print hacking vulnerability • Vulnerable to stolen verifier attack
[158]	Smart Grid	Physically unclonable functions	• Less resource consumption • Tampering resistant • Low overhead	• Brute force and dictionary attack issues • TA dependency
[160]	Subscriber authentication	Blockchain	• Auditable • Resistant to DoS attack • Execution costs • Low overhead	• Scalability • Standardization issues
[161]	Network In Box	Spatial crowdsourcing	• Prevents leakage of sensing node location • Provides confidentiality and integrity	• Task assignment results manipulation • Data migration • Processing requirements

4.8. Multi-Factor Authentication

Multi-Factor Authentication (MFA) is considered as a core element of a foolproof Identity and Access Management (IAM) policy scheme. MFA is used for enhanced security through multitude expansion in the key spectrum against brute force attacks and stolen third-party parameters. The additional factors used for MFA include SMS-based OTP, Email-based OTP, software token, smart cellular apps, biometric parameters, third-party certificates such as GMAIL, secret question, USB-based, smart cards, PIN, RFID, physical key, location-based, etc. Specifically, MFA-based biometric credentials have achieved technological diversity by introducing retina or iris scans, voice authentication, hand geometry, facial recognition, earlobe geometry and DNA specifications. Heterogenous connectivity of modern networks has provided several possibilities for cross-verifications in MFA, as shown in Figure 9. The prominent attacks against MFA include MitM, reverse brute force, credential stuffing, key loggers, spear-phishing and phishing. MFA is increasingly recommended for 6G-enabled massive and heterogenous communication scenarios to counter quantum computing-based cryptographic attacks [162].

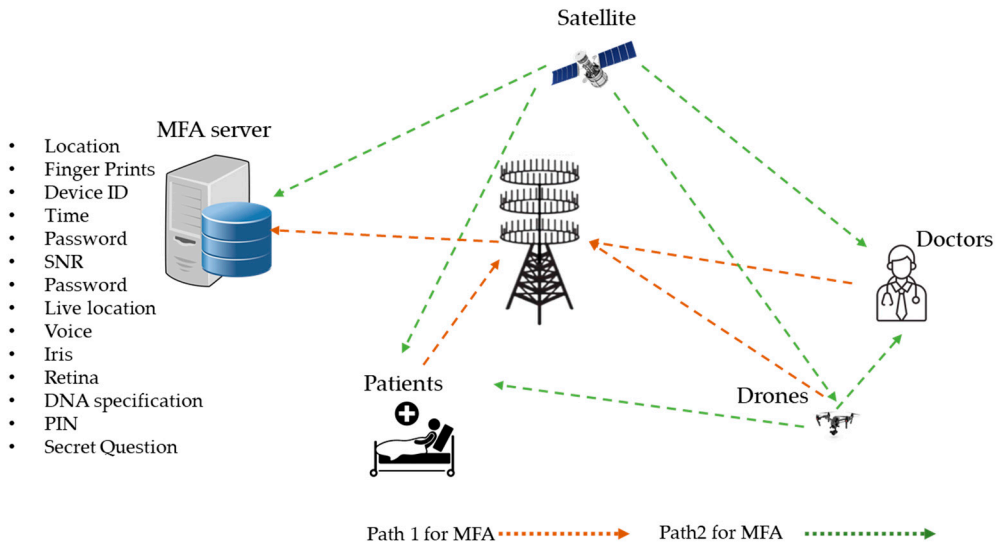

Figure 9. MFA spectrum in modern communication.

Similarly, the authors in [163] suggested a blockchain-based authentication for heterogenous devices to provide joint authentication and access control. Although this scheme provides minimum error, it has limitations in scalability, key management and consensus overhead. In [164], the authors proposed McEliece and Niederreiter crypto-code on elliptic codes for quantum-resistant authentication in a closed mobile internet channel. The scheme provides an offline mode for closing the voice channel; however, the employed algorithms are sensitive to fault injection attacks. Organized and structured CIA triad-compliant security policies are implemented through utilizing MFA in next-generation cloud computing-based architecture [165]. Due to a broad MFA spectrum, security policy management is becoming crucial and increasingly sophisticated. The authors in [166] suggested an MFA among distributed edge nodes and cloud nodes. The scheme utilizes various AI techniques for processed events-based authentication with human independence. Table 13 provides a summary of our analysis of MFA schemes in 6G mobile networks.

Table 13. Emerging MFA schemes in 6G networks.

Ref.	Network Model	Technique	Features	Limitations
[167]	Wireless Sensors	Elliptic curve cryptography with user anonymity	• Suitable for real-time application • Extendible to advanced mobile networks such as 6G.	• Vulnerable to the user collision • Desynchronization attacks are possible
[163]	Heterogeneous device	Blockchain	• Joint authentication and access control • Suitable for resource-constrained IoTs • Minimum error rate	• Scalability issues • Key management issues • Consensus overheads
[164]	Closed Mobile Internet Channel	McEliece and Niederreiter crypto-code on elliptic codes	• Suitable for quantum computing-based attacks • Provides offline mode of closing the voice channel • Secure to full-scale quantum processing	• Processing intensive • Not suitable for resource-constrained IoTs • Sensitive to fault injection attacks
[166]	Distributed edge and cloud nodes	AI-processed events	• Human independent • Suitable for IoTs • Efficient authentication	• Learning curve • Slow optimization • Vulnerable to DoS attacks

5. Research Directions

After a detailed overview of the prevailing research landscape under the scope of secure 6G networks, we critically identified potential future research areas in 6G communication that require focus from both academia and industry.

5.1. Privacy Preservation in 6G Network-Based 3D Fog Computing

The heterogeneous requirements of 6G networks will result in a wide expansion of fog computing-based implementations. In contrast, most emerging 6G applications are increasingly 3D, such as drones, UAVs, etc. Therefore, research and evaluation of existing technologies are prerequisites for the optimized integration of 6G in the emerging 3D paradigm. Similarly, 3D applications are expanding beyond UAVs in robotic solutions related to high-rise buildings in urban areas. Optimized implementation of security solutions with seamless QoS would contain several challenges associated with the 3D spatiotemporal behavior of malicious entities.

5.2. 6G-Enabled Privacy-Protected Smart Infrastructures and Augmented Reality

Augmented Reality (AR)-based solutions are receiving huge attraction from almost all sectors, including education, health reality, management, governance, industry and smart cities. 6G is emerging as a key enabler in AR integration at the heterogenous level and is fulfilling fundamental AR requirements related to latency, bandwidth and massive connectivity. Therefore, all smart infrastructures are the potential platform for AR applications. However, it is imperative to highlight that the literature lacks any holistic cyber security framework covering all emerging requirements related to AR-based smart implementation.

5.3. SDN-Based Secure Architecture in 6G Network

SDN is emerging as a potential solution to achieve optimized networking in a massive heterogeneous network environment. However, there are several challenges related to SDN functionality and security, especially in wireless cellular applications. It is deduced from this review that the literature and available solutions require further research for optimized and secure integration of SDN in all scenarios related to 6G communication. Here, challenges associated with SDN functionality are manifold when it is visualized through the lens of cyber security requirements in 6G communication.

5.4. Optimized Secure Routing in 6G Networks

Routing is considered the fundamental pulse of network implementation and optimization. Therefore, this essential characteristic is on the hit list of malicious elements in any network [168]. 6G emergence results in massive integrated network communication scenarios with manifold level diversities. Therefore, conventional routing protocol also requires compatible evolution for secure provisioning of 6G QoS. Moreover, several 6G network-based emerging technologies require routing optimization and security frameworks. These technologies include NVF, MEC, NS, etc. Currently, it is a research challenge to propose an optimized routing framework with security and backward compatibility.

5.5. 6G Physical Layer Security and THz Spectrum

Physical layer security implementations have received massive attention from researchers, especially related to mm-waves in 6G communication. However, resource-constrained 6G-enabled IoTs, heterogeneous integration of cloud computing-based emerging technologies [169] and HNV-based evolution require research to design optimum PLS security protocols. PLS protocols face significant challenges related to seamless fusion with higher layers, especially cloud infrastructures [24]. Moreover, security control and key management between higher-level network layers and massive physical communication is a major challenge in the 6G-enabled network. Similarly, in combination with 6G-enabled emerging technologies, PLS brings several challenges related to conventional cryptographic algorithms and physical layer signature-based protocols. Likewise, various material-based advancements, such as molecular communication, atomic communication, etc., are also open research areas for optimum cyber-secure 6G-enabled infrastructure at the physical layer.

5.6. 6G Security in Quantum Computing

6G BigCom is emerging as the global central backbone of tertiary communication, including satellites, UAVs, aviation, etc. Therefore, 6G communication must adapt to all emerging sister technologies such as quantum computing. It is envisaged that quantum processors will crack widely used crypto algorithms, the Rivest–Shamir–Adleman (RSA), until the 2030s [170]. Similarly, 6G communication is also considered a 2030s technology. Therefore, 6G communication requires extensive research in several related areas including post-quantum cryptography, quantum-resistant network hardware, quantum fog computing, quantum cloud computing, quantum key distribution and quantum cyber attacks.

5.7. Blockchain-Based Distributed Security in 6G

Blockchain is evolving as a prime distributed ledger technology in 6G communication. However, several challenges require in-depth research for optimum blockchain integration in future network infrastructure. The prominent challenge is the blockchain architecture design for secure integration with ultra-low latency and high-throughput in massive 6G-enabled IoTs [171]. Similarly, there are several dominating shortcomings in blockchain technology itself that need critical research to achieve an optimum distributed framework in 6G-enabled networks. The technological obstacles in blockchain include (1) scalability for block validation in massive communication, (2) privacy leakage due to public visibility

of transactions and (3) selfish mining through blockchain reversal in over 51% of processing power nodes [172].

6. Conclusions

This article surveyed the emerging state-of-the-art techniques in 6G network security. We performed a systematic review through classifications related to the overall research paradigm of security in 6G networks. After a detailed analysis, we were able to present a CIA^3-based threat model for 6G networks. Further, we discussed the latest research works related to each threat. The threat model provided the overall significance and latest trends of security solutions in 6G networks. In addition, we were able to categorize emerging security countermeasures into three types related to various vulnerabilities in 6G network security, which include cryptographic methods, entity attributes and IDS. Cryptographic methods cover PKI, RSA, DSS, ECC, AES, ESAR and NGTP. Entity attributes include QR codes, 3D location, PLS, joint optical and RF links and reconfigurable surfaces. Likewise, IDS countermeasures incorporate several interdisciplinary solutions such as threat matrix, signatures matrix, CSI, DL, ML, AI and SOP.

Hence, after a holistic overview of the security landscape in 6G communication, we categorized authentication techniques in the 6G communication into eight distinct types, including handover authentication, mutual authentication, physical layer authentication, deniable authentication, token-based authentication, certificate-based authentication, key agreement-based authentication and multi-factor authentication.

With the focus on the vision of next-generation communication, we deliberated upon seven emerging future research directions in 6G communication with a special emphasis on security. The future research directions include privacy preservation in 6G network-based 3D fog computing, 6G-enabled privacy-protected smart infrastructures and augmented reality, SDN-based secure architecture in 6G networks, optimized secure routing in 6G networks, 6G physical layer security and THz spectrum, 6G security in quantum computing and blockchain-based distributed security in 6G networks.

Author Contributions: Conceptualization, S.H.A.K. and R.H.; methodology, K.N.; formal analysis, F.Q.; writing—original draft preparation, S.H.A.K.; writing—review and editing, F.Q.; visualization, A.A.A.I.; funding acquisition, A.A.A.I. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is supported by the Universiti Kebangsaan Malaysia Geran Galakan Penyelidik Muda (GGPM) with code GGPM-2021-040 and Universiti of Malaysia Sabah: AXD353255.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would also like to acknowledge the support provided by Universiti Kebangsaan Malaysia for conducting the review.

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

References

1. Hassan, R.; Qamar, F.; Hasan, M.K.; Aman, A.H.M.; Ahmed, A.S. Internet of Things and its applications: A comprehensive survey. *Symmetry* **2020**, *12*, 1674. [CrossRef]
2. Snehi, J.; Snehi, M.; Prasad, D.; Simaiya, S.; Kansal, I.; Baggan, V. SDN-Based Cloud Combining Edge Computing for IoT Infrastructure. In *Software Defined Networks: Architecture and Applications*; Wiley-Scrivener Publishing: Beverly, MA, USA, 2022; pp. 497–540.
3. Katz, M.; Matinmikko-Blue, M.; Latva-Aho, M. 6Genesis flagship program: Building the bridges towards 6G-enabled wireless smart society and ecosystem. In Proceedings of the 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM), Guadalajara, Mexico, 14–16 November 2018; pp. 1–9.
4. Uusitalo, M.A.; Ericson, M.; Richerzhagen, B.; Soykan, E.U.; Rugeland, P.; Fettweis, G.; Sabella, D.; Wikström, G.; Boldi, M.; Hamon, M.-H. Hexa-X the European 6G flagship project. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 580–585.

5. Strinati, E.C.; Alexandropoulos, G.C.; Sciancalepore, V.; Di Renzo, M.; Wymeersch, H.; Phan-huy, D.-T.; Crozzoli, M.; D'Errico, R.; De Carvalho, E.; Popovski, P. Wireless environment as a service enabled by reconfigurable intelligent surfaces: The RISE-6G perspective. *arXiv* **2021**, arXiv:2104.06265.
6. Corici, M.; Troudt, E.; Chakraborty, P.; Magedanz, T. An Ultra-Flexible Software Architecture Concept for 6G Core Networks. In Proceedings of the 2021 IEEE 4th 5G World Forum (5GWF), Montreal, QC, Canada, 13–15 October 2021; pp. 400–405.
7. McBurnett, M.M. *Regulatory Audit Summary of South Texas Project, Units 3 and 4 Combined License Application Revision 4—American Society Of Mechanical Engineers Design Specifications and Component Classification*; Nuclear Innovation North America (NINA): Bay City, TX, USA, 2011.
8. Brito, J.M.C.; Mendes, L.L.; Gontijo, J.G.S. Brazil 6G project-an approach to build a national-wise framework for 6G networks. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
9. Dang, S.; Amin, O.; Shihada, B.; Alouini, M.-S. What should 6G be? *Nat. Electron.* **2020**, *3*, 20–29. [CrossRef]
10. Qamar, F.; Hindia, M.N.; Abbas, T.; Dimyati, K.B.; Amiri, I.S. Investigation of QoS performance evaluation over 5G network for indoor environment at millimeter wave bands. *Int. J. Electron. Telecommun.* **2019**, *65*, 95–101.
11. Nor, A.M.; Fratu, O.; Halunga, S. Quality of Service Based Radio Resources Scheduling for 5G eMBB Use Case. *Symmetry* **2022**, *14*, 2193. [CrossRef]
12. 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), Virtual, 13–15 October 2021; pp. 1–4.
13. Khan, L.U.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. 6G wireless systems: A vision, architectural elements, and future directions. *IEEE Access* **2020**, *8*, 147029–147044. [CrossRef]
14. Nayak, S.; Patgiri, R. 6g communication: Envisioning the key issues and challenges. *arXiv* **2020**, arXiv:2004.04024. [CrossRef]
15. Wang, J.; Wang, C.-X.; Huang, J.; Chen, Y. 6G THz Propagation Channel Characteristics and Modeling: Recent Developments and Future Challenges. *IEEE Commun. Mag.* 2022; *in press*.
16. Qamar, F.; Siddiqui, M.U.A.; Hindia, M.N.; Hassan, R.; Nguyen, Q.N. Issues, challenges, and research trends in spectrum management: A comprehensive overview and new vision for designing 6G networks. *Electronics* **2020**, *9*, 1416. [CrossRef]
17. Sheikholeslami, S.M.; Fazel, F.; Abouei, J.; Plataniotis, K.N. Sub-Decimeter VLC 3D Indoor Localization With Handover Probability Analysis. *IEEE Access* **2021**, *9*, 122236–122253. [CrossRef]
18. Je, D.; Jung, J.; Choi, S. Toward 6G Security: Technology Trends, Threats, and Solutions. *IEEE Commun. Stand. Mag.* **2021**, *5*, 64–71. [CrossRef]
19. Shayea, I.; Dushi, P.; Banafaa, M.; Rashid, R.A.; Ali, S.; Sarijari, M.A.; Daradkeh, Y.I.; Mohamad, H. Handover Management for Drones in Future Mobile Networks—A Survey. *Sensors* **2022**, *22*, 6424. [CrossRef]
20. Nguyen, V.-L.; Lin, P.-C.; Cheng, B.-C.; Hwang, R.-H.; Lin, Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [CrossRef]
21. 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]
22. Sun, Y.; Liu, J.; Wang, J.; Cao, Y.; Kato, N. When machine learning meets privacy in 6G: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2694–2724. [CrossRef]
23. Porambage, P.; Gur, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The Roadmap to 6G Security and Privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122. [CrossRef]
24. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Ylianttila, M. 6G security challenges and potential solutions. In Proceedings of the European Conference on Networks and Communications (EuCNC), Porto, Portugal, 8–11 June 2021; pp. 1–6.
25. Sheth, K.; Patel, K.; Shah, H.; Tanwar, S.; Gupta, R.; Kumar, N. A taxonomy of AI techniques for 6G communication networks. *Comput. Commun.* **2020**, *161*, 279–303. [CrossRef]
26. Zhao, Y.; Zhai, W.; Zhao, J.; Zhang, T.; Sun, S.; Niyato, D.; Lam, K.-Y. A comprehensive survey of 6g wireless communications. *arXiv* **2020**, arXiv:2101.03889.
27. Vaigandla, K.K.; Bolla, S.; Karne, R. A Survey on Future Generation Wireless Communications-6G: Requirements, Technologies, Challenges and Applications. *Int. J. Adv. Trends Comput. Sci. Eng.* **2021**, *10*, 3067–3076.
28. Steingartner, W.; Galinec, D.; Kozina, A. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry* **2021**, *13*, 597. [CrossRef]
29. Farooqui, M.N.I.; Arshad, J.; Khan, M.M. A Layered Approach to Threat Modeling for 5G-Based Systems. *Electronics* **2022**, *11*, 1819. [CrossRef]
30. Novokhrestov, A.; Konev, A.; Shelupanov, A.; Buymov, A. Computer network threat modelling. In Proceedings of the International Scientific Conference on Electronic Devices and Control Systems (EDCS 2019), Tomsk, Russia, 20–22 November 2019; p. 012002.
31. Rizvi, S.; Pipetti, R.; McIntyre, N.; Todd, J.; Williams, I. Threat model for securing internet of things (IoT) network at device-level. *Internet Things* **2020**, *11*, 100240. [CrossRef]
32. Chorti, A.; Barreto, A.N.; Kopsell, S.; Zoli, M.; Chafii, M.; Sehier, P.; Fettweis, G.; Poor, H.V. Context-aware security for 6G wireless the role of physical layer security. *arXiv* **2021**, arXiv:2101.01536. [CrossRef]
33. Lin, D.; Peng, T.; Zuo, P.; Wang, W. Deep-Reinforcement-Learning-Based Intelligent Routing Strategy for FANETs. *Symmetry* **2022**, *14*, 1787. [CrossRef]

34. Abdel Hakeem, S.A.; Hussein, H.H.; Kim, H. Security Requirements and Challenges of 6G Technologies and Applications. *Sensors* **2022**, *22*, 1969. [CrossRef] [PubMed]
35. Ahmed, S.; Hossain, M.; Kaiser, M.S.; Noor, M.B.T.; Mahmud, M.; Chakraborty, C. Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. In *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 23–47.
36. Sun, W.; Li, S.; Zhang, Y. Edge caching in blockchain empowered 6G. *China Commun.* **2021**, *18*, 1–17. [CrossRef]
37. Li, G.; Lai, C.; Lu, R.; Zheng, D. SecCDV: A Security Reference Architecture for Cybertwin-driven 6G V2X. *IEEE Trans. Veh. Technol.* **2021**, *71*, 4535–4550. [CrossRef]
38. Elkandoz, M.T.; Alexan, W. Image encryption based on a combination of multiple chaotic maps. *Multimed. Tools Appl.* **2022**, *81*, 25497–25518. [CrossRef]
39. Vinodha, D.; Anita, E.M.; Geetha, D.M. A novel multi functional multi parameter concealed cluster based data aggregation scheme for wireless sensor networks (NMFMP-CDA). *Wirel. Netw.* **2021**, *27*, 1111–1128. [CrossRef]
40. 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]
41. 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]
42. Zakaria, M.S.; Ghani, A.T.A.; Yahya, M.S.; Jamali, S.N. Information Technology Risk Management for Water Quality Monitoring IoT Infrastructure: A Case Study at Tasik Chini Unesco Biosphere Reserve. *Asia-Pac. J. Inf. Technol. Multimed.* **2020**, *9*, 94–102. [CrossRef]
43. Ayaz, F.; Sheng, Z.; Tian, D.; Nekovee, M.; Saeed, N. Blockchain-empowered AI for 6G-enabled Internet of Vehicles. *Electronics* **2022**, *11*, 3339. [CrossRef]
44. Hiller, J.; Henze, M.; Serror, M.; Wagner, E.; Richter, J.N.; Wehrle, K. Secure low latency communication for constrained industrial IoT scenarios. In Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN), Chicago, IL, USA, 1–4 October 2018; pp. 614–622.
45. Kumar, K.S.; Radhamani, A.; Sundaresan, S. Proficient approaches for scalability and security in IoT through edge/fog/cloud computing: A survey. *Int. J. Data Sci.* **2021**, *6*, 33–44. [CrossRef]
46. Xiong, L.; Zhong, X.; Xiong, N.N.; Liu, W. QR-3S: A High Payload QR code Secret Sharing System for Industrial Internet of Things in 6G Networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7213–7222. [CrossRef]
47. Chen, Y.-H.; Lai, Y.-C.; Zhou, K.-Z. Identifying Hybrid DDoS Attacks in Deterministic Machine-to-Machine Networks on a Per-Deterministic-Flow Basis. *Micromachines* **2021**, *12*, 1019. [CrossRef]
48. Soussi, W.; Christopoulou, M.; Xilouris, G.; Gür, G. Moving Target Defense as a Proactive Defense Element for Beyond 5G. *IEEE Commun. Stand. Mag.* **2021**, *5*, 72–79. [CrossRef]
49. Hasan, M.K.; Habib, A.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *J. Netw. Comput. Appl.* **2022**, *209*, 103540. [CrossRef]
50. Long, Q.; Chen, Y.; Zhang, H.; Lei, X. Software defined 5G and 6G networks: A survey. *Mob. Netw. Appl.* **2022**, *27*, 1792–1812. [CrossRef]
51. Shrestha, R.; Omidkar, A.; Roudi, S.A.; Abbas, R.; Kim, S. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. *Electronics* **2021**, *10*, 1549. [CrossRef]
52. Ma, X.; Zhou, Y.; Wang, L.; Miao, M. Privacy-preserving Byzantine-robust federated learning. *Comput. Stand. Interfaces* **2022**, *80*, 103561. [CrossRef]
53. Lin, J.; Du, M.; Liu, J. Free-riders in federated learning: Attacks and defenses. *arXiv* **2019**, arXiv:1911.12560.
54. Kantola, R. 6g network needs to support embedded trust. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–5.
55. Hewa, T.; Gür, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The role of blockchain in 6G: Challenges, opportunities and research directions. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
56. 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]
57. Partala, J. Post-quantum Cryptography in 6G. In *6G Mobile Wireless Networks*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 431–448.
58. Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wirel. Commun.* **2020**, *27*, 126–132. [CrossRef]
59. Catak, F.O.; Catak, E.; Kuzlu, M.; Cali, U.; Unal, D. Security Concerns on Machine Learning Solutions for 6G Networks in mmWave Beam Prediction. *arXiv* **2021**, arXiv:2105.03905. [CrossRef]
60. Jiang, H.; Zhu, X.; Han, J. Instruction-Fetching Attack and Practice in Collision Fault Attack on AES. *Symmetry* **2022**, *14*, 2201. [CrossRef]
61. Al Mousa, A.; Al Qomri, M.; Al Hajri, S.; Zagrouba, R. Utilizing the eSIM for Public Key Cryptography: A Network Security Solution for 6G. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6.
62. Yu, Q.; Ren, J.; Zhou, H.; Zhang, W. A cybertwin based network architecture for 6G. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
63. Yu, Q.; Wang, M.; Zhou, H.; Ni, J.; Chen, J.; Céspedes, S. Guest Editorial Special Issue on Cybertwin-Driven 6G: Architectures, Methods, and Applications. *IEEE Internet Things J.* **2021**, *8*, 16191–16194. [CrossRef]

64. Liu, J.; Yu, Y.; Li, K.; Gao, L. Post-Quantum Secure Ring Signatures for Security and Privacy in the Cybertwin-Driven 6G. *IEEE Internet Things J.* **2021**, *8*, 16290–16300. [CrossRef]
65. Liu, J.K. Ring signature. In *Advances in Cyber Security: Principles, Techniques, and Applications*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 93–114.
66. Somsuk, K. The Improvement of Elliptic Curve Factorization Method to Recover RSA's Prime Factors. *Symmetry* **2021**, *13*, 1314. [CrossRef]
67. 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]
68. Shankar, K.; Taniar, D.; Yang, E.; Yi, O. Secure and Optimal Secret Sharing Scheme for Color Images. *Mathematics* **2021**, *9*, 2360. [CrossRef]
69. Liao, S.; Sun, Y.; Cao, S.; Yang, L. A 23.8Tbps Random Number Generator on a Single GPU. In Proceedings of the 2020 International Conference on Space-Air-Ground Computing (SAGC), Beijing, China, 4–6 December 2020; pp. 33–37.
70. Suraci, C.; Pizzi, S.; Molinaro, A.; Araniti, G. MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System. *IEEE Internet Things J.* **2021**, *9*, 11524–11532. [CrossRef]
71. Tsavos, M.; Sklavos, N.; Alexiou, G.P. Lightweight Security Data Streaming, Based on Reconfigurable Logic, for FPGA Platform. In Proceedings of the 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 26–28 August 2020; pp. 277–280.
72. Al-Eryani, Y.; Hossain, E. The D-OMA method for massive multiple access in 6G: Performance, security, and challenges. *IEEE Veh. Technol. Mag.* **2019**, *14*, 92–99. [CrossRef]
73. Lee, Y.U. Secure visible light communication technique based on asymmetric data encryption for 6G communication service. *Electronics* **2020**, *9*, 1847. [CrossRef]
74. 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]
75. Ulitzsch, V.Q.; Park, S.; Marzougui, S.; Seifert, J.-P. A Post-Quantum Secure Subscription Concealed Identifier for 6G. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, TX, USA, 16–19 May 2022; pp. 157–168.
76. Zhang, Z.; Duan, A. An Adaptive Data Traffic Control Scheme with Load Balancing in a Wireless Network. *Symmetry* **2022**, *14*, 2164. [CrossRef]
77. Ong, A.V.; Peradilla, M. An IoT Framework Based on SDN and NFV for Context-Aware Security. In Proceedings of the 2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN), Jeju Island, Korea, 17–20 August 2021; pp. 167–172.
78. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K. Routing-based Interference Mitigation in SDN enabled Beyond 5G Communication Networks: A Comprehensive Survey. *IEEE Access* **2023**, *11*, 4023–4041. [CrossRef]
79. Zhang, X.; Zhao, J.; Xu, C.; Wang, H.; Zhang, Y. Dopiv: Post-quantum secure identity-based data outsourcing with public integrity verification in cloud storage. *IEEE Trans. Serv. Comput.* **2022**, *15*, 334–345. [CrossRef]
80. Al-Mohammed, H.A.; Yaacoub, E. On the use of quantum communications for securing IoT devices in the 6G era. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Virtual, 14–23 June 2021; pp. 1–6.
81. Qin, P.; Zhu, Y.; Zhao, X.; Feng, X.; Liu, J.; Zhou, Z. Joint 3D-location planning and resource allocation for XAPS-enabled C-NOMA in 6G heterogeneous Internet of Things. *IEEE Trans. Veh. Technol.* **2021**, *70*, 10594–10609. [CrossRef]
82. Muniyandi, R.C.; Qamar, F.; Jasim, A.N. Genetic optimized location aided routing protocol for VANET based on rectangular estimation of position. *Appl. Sci.* **2020**, *10*, 5759. [CrossRef]
83. Zhang, L.; Zhong, W.; Zhang, J.; Lin, Z.; Yang, Z.; Wang, J. mmWave Beam Tracking for V2I Communication Systems Based on Spectrum Environment Awareness. *Symmetry* **2022**, *14*, 677. [CrossRef]
84. Ibrahim, M.; Badrudduza, A.; Hossen, M.; Kundu, M.K.; Ansari, I.S. Enhancing security of TAS/MRC based mixed RF-UOWC system with induced underwater turbulence effect. *arXiv* **2021**, arXiv:2105.09088. [CrossRef]
85. Siddiqui, M.U.A.; Qamar, F.; Kazmi, S.H.A.; Hassan, R.; Arfeen, A.; Nguyen, Q.N. A Study on Multi-Antenna and Pertinent Technologies with AI/ML Approaches for B5G/6G Networks. *Electronics* **2023**, *12*, 189. [CrossRef]
86. Liu, Z.; Huang, F.; Weng, J.; Cao, K.; Miao, Y.; Guo, J.; Wu, Y. BTMPP: Balancing trust management and privacy preservation for emergency message dissemination in vehicular networks. *IEEE Internet Things J.* **2020**, *8*, 5386–5407. [CrossRef]
87. Khalid, W.; Yu, H.; Do, D.-T.; Kaleem, Z.; Noh, S. RIS-aided physical layer security with full-duplex jamming in underlay D2D networks. *IEEE Access* **2021**, *9*, 99667–99679. [CrossRef]
88. Lanoue, M.; Bollmann, C.A.; Michael, J.B.; Roth, J.; Wijesekera, D. An Attack Vector Taxonomy for Mobile Telephony Security Vulnerabilities. *Computer* **2021**, *54*, 76–84. [CrossRef]
89. Lu, K.; Yang, H. Design of NOMA Sparse Signature Matrix for 6G Integrating Sensing and Communications Networks. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 27–30 September 2021; pp. 1–5.
90. Soni, G.; Chandravanshi, K. Security Scheme to Identify Malicious Maneuver of Flooding Attack for WSN in 6G. In Proceedings of the 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 26–27 August 2021; pp. 124–129.
91. Srinivasan, M.; Skaperas, S.; Chorti, A. On the Use of CSI for the Generation of RF Fingerprints and Secret Keys. *arXiv* **2021**, arXiv:2110.15415.
92. 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]
93. Sagu, A.; Gill, N.S.; Gulia, P.; Chatterjee, J.M.; Priyadarshini, I. A Hybrid Deep Learning Model with Self-Improved Optimization Algorithm for Detection of Security Attacks in IoT Environment. *Future Internet* **2022**, *14*, 301. [CrossRef]

94. Ankita, A.; Rani, S. Machine Learning and Deep Learning for Malware and Ransomware Attacks in 6G Network. In Proceedings of the 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 3 July 2021; pp. 39–44.
95. Rekkas, V.P.; Sotiroudis, S.; Sarigiannidis, P.; Karagiannidis, G.K.; Goudos, S.K. Unsupervised Machine Learning in 6G Networks-State-of-the-art and Future Trends. In Proceedings of the 2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 5–7 July 2021; pp. 1–4.
96. Abbas, L.; Shoaib, U.; Bashir, A.K. Priority based dynamic spectrum management using Virtual Utility Functions in Cognitive Radio enabled Internet of Things. *Comput. Commun.* **2022**, *196*, 239–248. [CrossRef]
97. Aslam, M.M.; Du, L.; Zhang, X.; Chen, Y.; Ahmed, Z.; Qureshi, B. Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1331428. [CrossRef]
98. Xu, L.; Zhou, X.; Tao, Y.; Yu, X.; Yu, M.; Khan, F. AF Relaying Secrecy Performance Prediction for 6G Mobile Communication Networks in Industry 5.0. *IEEE Trans. Ind. Inform.* **2021**, *18*, 5485–5493. [CrossRef]
99. 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. *Wirel. Pers. Commun.* 2022, *in press*.
100. Shukla, A.; Gupta, R.; Tanwar, S.; Kumar, N.; Rodrigues, J.J. Block-RAS: A P2P resource allocation scheme in 6G environment with public blockchains. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 8–10 December 2020; pp. 1–6.
101. Lin, H.; Garg, S.; Hu, J.; Kaddoum, G.; Peng, M.; Hossain, M.S. A blockchain-based secure data aggregation strategy using 6g-enabled nib for industrial applications. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7204–7212. [CrossRef]
102. Manogaran, G.; Rawal, B.S.; Saravanan, V.; Kumar, P.M.; Martínez, O.S.; Crespo, R.G.; Montenegro-Marin, C.E.; Krishnamoorthy, S. Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Comput. Commun.* **2020**, *161*, 248–256. [CrossRef]
103. Wu, J. Security and Intelligent Management for Fog/Edge Computing Resources. In *Fog/Edge Computing for Security, Privacy, and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 213–234.
104. Khan, L.U.; Saad, W.; Niyato, D.; Han, Z.; Hong, C.S. Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions. *arXiv* **2021**, arXiv:2102.12169. [CrossRef]
105. Hindia, M.; Qamar, F.; Majed, M.B.; Abd Rahman, T.; Amiri, I.S. Enabling remote-control for the power sub-stations over LTE-A networks. *Telecommun. Syst.* **2019**, *70*, 37–53. [CrossRef]
106. Yap, K.Y.; Chin, H.H.; Klemeš, J.J. Future outlook on 6G technology for renewable energy sources (RES). *Renew. Sustain. Energy Rev.* **2022**, *167*, 112722. [CrossRef]
107. Ji, S.; Sheng, M.; Zhou, D.; Bai, W.; Cao, Q.; Li, J. Flexible and Distributed Mobility Management for Integrated Terrestrial-Satellite Networks: Challenges, Architectures, and Approaches. *IEEE Netw.* **2021**, *35*, 73–81. [CrossRef]
108. Guo, Y.; Guo, Y. FogHA: An efficient handover authentication for mobile devices in fog computing. *Comput. Secur.* **2021**, *108*, 102358. [CrossRef]
109. Siddiqui, M.U.A.; Qamar, F.; Tayyab, M.; Hindia, M.N.; Nguyen, Q.N.; Hassan, R. Mobility Management Issues and Solutions in 5G-and-Beyond Networks: A Comprehensive Review. *Electronics* **2022**, *11*, 1366. [CrossRef]
110. Abdullah, F.; Kimovski, D.; Prodan, R.; Munir, K. Handover authentication latency reduction using mobile edge computing and mobility patterns. *Computing* **2021**, *103*, 2667–2686. [CrossRef]
111. Khan, M.A.; Kumar, N.; Mohsan, S.A.H.; Khan, W.U.; Nasralla, M.M.; Alsharif, M.H.; Żywiołek, J.; Ullah, I. Swarm of UAVs for network management in 6G: A technical review. *arXiv* **2022**, arXiv:2210.03234. [CrossRef]
112. Angjo, J.; Shayea, I.; Ergen, M.; Mohamad, H.; Alhammadi, A.; Daradkeh, Y.I. Handover Management of Drones in Future Mobile Networks: 6G Technologies. *IEEE Access* **2021**, *9*, 12803–12823. [CrossRef]
113. Qamar, F.; Siddiqui, M.H.S.; Hindia, M.N.; Dimyati, K.; Abd Rahman, T.; Talip, M.S.A. Propagation Channel Measurement at 38 GHz for 5G mm-wave communication Network. In Proceedings of the 2018 IEEE student conference on research and development (SCOReD), Bangi, Malaysia, 26–28 November 2018; pp. 1–6.
114. Özkoç, M.F.; Koutsaftis, A.; Kumar, R.; Liu, P.; Panwar, S.S. The Impact of Multi-Connectivity and Handover Constraints on Millimeter Wave and Terahertz Cellular Networks. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 1833–1853. [CrossRef]
115. Chow, M.C.; Ma, M. A lightweight traceable D2D authentication and key agreement scheme in 5G cellular networks. *Comput. Electr. Eng.* **2021**, *95*, 107375. [CrossRef]
116. Bairwa, A.K.; Joshi, S. Mutual authentication of nodes using session token with fingerprint and MAC address validation. *Egypt. Inform. J.* **2021**, *22*, 479–491. [CrossRef]
117. 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, *in press*.
118. Vijayakumar, P.; Azees, M.; Kozlov, S.A.; Rodrigues, J.J. An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 1630–1638. [CrossRef]
119. Yang, L.; Chen, Y.-C.; Wu, T.-Y. Provably Secure Client-Server Key Management Scheme in 5G Networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 4083199. [CrossRef]
120. Hindia, M.N.; Qamar, F.; Abbas, T.; Dimyati, K.; Abu Talip, M.S.; Amiri, I.S. Interference cancelation for high-density fifth-generation relaying network using stochastic geometrical approach. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719855879. [CrossRef]

121. Paul, L.Y.; Baras, J.S.; Sadler, B.M. Physical-layer authentication. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 38–51.
122. Bahache, A.N.; Chikouche, N.; Mezrag, F. Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *SN Comput. Sci.* **2022**, *3*, 382. [CrossRef]
123. Fang, H.; Wang, X.; Hanzo, L. Learning-aided physical layer authentication as an intelligent process. *IEEE Trans. Commun.* **2018**, *67*, 2260–2273. [CrossRef]
124. Chen, Y.; Wen, H.; Wu, J.; Song, H.; Xu, A.; Jiang, Y.; Zhang, T.; Wang, Z. Clustering based physical-layer authentication in edge computing systems with asymmetric resources. *Sensors* **2019**, *19*, 1926. [CrossRef] [PubMed]
125. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.-A.; Abreu, G.; Haas, H. Physical-layer security in 6G networks. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1901–1914. [CrossRef]
126. Shakiba-Herfeh, M.; Chorti, A.; Poor, H.V. Physical layer security: Authentication, integrity, and confidentiality. In *Physical Layer Security*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 129–150.
127. Alzubaidi, O.T.H.; Hindia, M.N.; Dimyati, K.; Noordin, K.A.; Wahab, A.N.A.; Qamar, F.; Hassan, R. Interference Challenges and Management in B5G Network Design: A Comprehensive Review. *Electronics* **2022**, *11*, 2842. [CrossRef]
128. Singh, S.P. Physical Layer Design Challenges for 6G Wireless. In *6G Mobile Wireless Networks*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 43–52.
129. Hao, Y.; Miao, Y.; Chen, M.; Gharavi, H.; Leung, V. 6G cognitive information theory: A mailbox perspective. *Big Data Cogn. Comput.* **2021**, *5*, 56. [CrossRef]
130. Lee, D.; Sasaki, H.; Fukumoto, H.; Yagi, Y.; Shimizu, T. An evaluation of orbital angular momentum multiplexing technology. *Appl. Sci.* **2019**, *9*, 1729. [CrossRef]
131. Djordjevic, I.B. OAM-based hybrid free-space optical-terahertz multidimensional coded modulation and physical-layer security. *IEEE Photonics J.* **2017**, *9*, 7905812. [CrossRef]
132. Hu, T.; Zhang, B.; Zhao, K.; Wang, Y.; Zhang, J. Data BER analysis of OAM-assisted physical layer authentication system. *IEICE Electron. Express* **2022**, *19*, 20220434. [CrossRef]
133. Cagliero, A.; Gaffoglio, R. On the spectral efficiency limits of an OAM-based multiplexing scheme. *IEEE Antennas Wirel. Propag. Lett.* **2016**, *16*, 900–903. [CrossRef]
134. Hale, B.; Komlo, C. On End-to-End Encryption. *Cryptol. Eprint Arch.* 2022, *in press*.
135. Zeng, S.; Mu, Y.; Zhang, H.; He, M. A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy. *Inf. Sci.* **2020**, *516*, 331–345. [CrossRef]
136. Al-Mekhlafi, Z.G.; Hassan, R. Evaluation study on routing information protocol and dynamic source routing in Ad-Hoc network. In Proceedings of the 2011 7th International Conference on Information Technology in Asia, Sarawak, Malaysia, 12–13 July 2011; pp. 1–4.
137. Abdelhaq, M.; Serhan, S.; Alsaqour, R.; Hassan, R. A local intrusion detection routing security over MANET network. In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, Bandung, Indonesia, 17–19 July 2011; pp. 1–6.
138. Gupta, D.S.; Islam, S.H.; Obaidat, M.S.; Hsiao, K.-F. A Novel Identity-based Deniable Authentication Protocol Using Bilinear Pairings for Mobile Ad Hoc Networks. *Adhoc Sens. Wirel. Netw.* **2020**, *47*, 227–247.
139. Li, F.; Hong, J.; Omala, A.A. Practical deniable authentication for pervasive computing environments. *Wirel. Netw.* **2018**, *24*, 139–149. [CrossRef]
140. Huang, W.; Liao, Y.; Zhou, S.; Chen, H. An efficient deniable authenticated encryption scheme for privacy protection. *IEEE Access* **2019**, *7*, 43453–43461. [CrossRef]
141. Niewolski, W.; Nowak, T.W.; Sepczuk, M.; Kotulski, Z. Token-Based Authentication Framework for 5G MEC Mobile Networks. *Electronics* **2021**, *10*, 1724. [CrossRef]
142. Ibrahim, M.Z.; Hassan, R. The implementation of internet of things using test bed in the UKMnet environment. *Asia-Pac. J. Inf. Technol. Multimed.* **2019**, *8*, 1–17. [CrossRef]
143. Aman, M.N.; Taneja, S.; Sikdar, B.; Chua, K.C.; Alioto, M. Token-based security for the Internet of Things with dynamic energy-quality tradeoff. *IEEE Internet Things J.* **2018**, *6*, 2843–2859. [CrossRef]
144. Soldani, D. 6G Fundamentals: Vision and Enabling Technologies. *J. Telecommun. Digit. Econ.* **2021**, *9*, 58–86. [CrossRef]
145. Kamruzzaman, M. 6G-Enabled Smart City Networking Model Using Lightweight Security Module. *Res. Sq.* 2021, *in press*.
146. Sadeq, A.S.; Hassan, R.; Al-rawi, S.S.; Jubair, A.M.; Aman, A.H.M. A qos approach for Internet of Things (Iot) environment using mqtt protocol. In Proceedings of the 2019 International Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, 25–26 September 2019; pp. 59–63.
147. Mukherjee, A.; Mukherjee, P.; De, D.; Dey, N. QoS-aware 6G-enabled ultra low latency edge-assisted Internet of Drone Things for real-time stride analysis. *Comput. Electr. Eng.* **2021**, *95*, 107438. [CrossRef]
148. Balachandran, C.; Ramachandran, G.; Krishnamachari, B. EDISON: A Blockchain-based Secure and Auditable Orchestration Framework for Multi-domain Software Defined Networks. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhode Island, Greece, 2–6 November 2020; pp. 144–153.
149. Munasinghe, G.K.; Murtaza, M. Analyzing Vehicle-to-Everything Communication for Intelligent Transportation System: Journey from IEEE 802.11p to 5G and Finally Towards 6G. In Proceedings of the 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia, 25–27 November 2020; pp. 1–7.
150. Pothumarti, R.; Jain, K.; Krishnan, P. A lightweight authentication scheme for 5G mobile communications: A dynamic key approach. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 1–19. [CrossRef]

151. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT. *J. Parallel Distrib. Comput.* **2021**, *156*, 176–184. [CrossRef]
152. Nyangaresi, V.O.; Ogundoyin, S.O. Certificate Based Authentication Scheme for Smart Homes. In Proceedings of the 2021 3rd Global Power, Energy and Communication Conference (GPECOM), Virtual, 5–8 October 2021; pp. 202–207.
153. Farooq, S.M.; Hussain, S.; Kiran, S.; Ustun, T.S. Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5. *Electronics* **2018**, *7*, 370. [CrossRef]
154. Garzon, S.R.; Yildiz, H.; Küpper, A. Decentralized Identifiers and Self-sovereign Identity in 6G. *arXiv* **2021**, arXiv:2112.09450. [CrossRef]
155. 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]
156. Wang, W.; Hu, N.; Liu, X. BlockCAM: A blockchain-based cross-domain authentication model. In Proceedings of the 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018; pp. 896–901.
157. Zhang, L.; Zhang, Y.; Tang, S.; Luo, H. Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. *IEEE Trans. Ind. Electron.* **2017**, *65*, 2795–2805. [CrossRef]
158. Gope, P.; Sikdar, B. Privacy-aware authenticated key agreement scheme for secure smart grid communication. *IEEE Trans. Smart Grid* **2018**, *10*, 3953–3962. [CrossRef]
159. Günlü, O.; Schaefer, R.F. An optimality summary: Secret key agreement with physical unclonable functions. *Entropy* **2021**, *23*, 16. [CrossRef]
160. Hojjati, M.; Shafieinejad, A.; Yanikomeroglu, H. A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks. *IEEE Access* **2020**, *8*, 216461–216476. [CrossRef]
161. Zhang, J.; Wang, Z.; Wang, D.; Zhang, X.; Gupta, B.; Liu, X.; Ma, J. A Secure Decentralized Spatial Crowdsourcing Scheme for 6G-Enabled Network in Box. *IEEE Trans. Ind. Inform.* **2021**, *18*, 6160–6170. [CrossRef]
162. 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]
163. Joshi, S.; Stalin, S.; Shukla, P.K.; Shukla, P.K.; Bhatt, R.; Bhadoria, R.S.; Tiwari, B. Unified Authentication and Access Control for Future Mobile Communication-Based Lightweight IoT Systems Using Blockchain. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 8621230. [CrossRef]
164. Євсєєв, С.; Погасій, С.; Хвостенко, В. Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. *Системи обробки інформації* **2021**, 35–40. [CrossRef]
165. Gonzalez, A.J.; Grønsund, P.; Dimitriadis, A.; Reshytnik, D. Information Security in a 5G Facility: An Implementation Experience. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 425–430.
166. Rahman, M.A.; Hossain, M.S.; Showail, A.J.; Alrajeh, N.A.; Ghoneim, A. AI-Enabled IIoT for Live Smart City Event Monitoring. *IEEE Internet Things J.* 2021, *in press*.
167. Shin, S.; Kwon, T. A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things. *IEEE Access* **2020**, *8*, 67555–67571. [CrossRef]
168. Sen, J.; Haas, Z. Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparison. In Proceedings of the 2011 Wireless Advanced, London, UK, 20–22 June 2011.
169. Zhang, X.; Zhao, J.; Xu, C.; Li, H.; Wang, H.; Zhang, Y. CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors. *IEEE Trans. Cloud Comput.* **2019**, *9*, 1362–1375. [CrossRef]
170. Sevilla, J.; Riedel, C.J. Forecasting timelines of quantum computing. *arXiv* **2020**, arXiv:2009.05045.
171. Shah, K.; Chadotra, S.; Tanwar, S.; Gupta, R.; Kumar, N. Blockchain for IoV in 6G environment: Review solutions and challenges. *Clust. Comput.* **2022**, *25*, 1927–1955. [CrossRef]
172. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]