Computer Science and Information Systems 21(3):851–897 https://doi.org/10.2298/CSIS230804016L

The Security and Privacy Challenges Toward Cybersecurity of 6G Networks: A Comprehensive Review

Yanlu Li[1,2], Yufeng Xiao[1,2], Wei Liang[1,2⋆], Jiahong Cai[1,2], Ronglin Zhang[1,2], Kuan-Ching Li[3,⋆] and Muhammad Khurram Khan[4]

[1] School of Computer Science and Engineering, Hunan University of Science and Technology, China
[2] Hunan Key Laboratory for Service Computing and Novel Software Technology, China
yanluli@mail.hnust.edu.cn, hnxiaoyf@hnust.edu.cn, wliang@hnust.edu.cn, jiahongcai@mail.hnust.edu.cn, ronglin@mail.hnust.edu.cn
[3] Dept. of Computer Science and Information Engineering (CSIE), Providence University, Taiwan
kuancli@pu.edu.tw
[4] Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
mkhurram@ksu.edu.sa

Abstract. The integration of 6G networks with emerging key technologies such as blockchain, artificial intelligence, and digital twins continues to improve. However, it carries many issues with security threats and challenges of 6G networks. In this article, we analyzed the security issues of 6G networks and presented some possible solutions. First, we discussed the developments of mobile communication technology, the research motivation of 6G networks, the comparison of Key Performance Indicators (KPIs) between 5G/6G networks, and the key technologies of 6G networks. Next, security threats in the 6G network were analyzed concerning architecture, major visions and related applications. This was followed by solutions to security issues in applying key technologies for 6G networks. We also presented the application of AI in solving 6G network security problems. Firstly, we illustrated the impact of AI on 6G networks from two aspects: AI promotes the construction of 6G networks, and AI brings security threats to 6G networks. Then, we demonstrated that AI can assist 6G networks in solving security problems in many ways. Lastly, the is summarized, and the future directions in this area are proposed.

Keywords: 6G security, privacy protection, AI, VLC security, THz security, blockchain security.

1. Introduction

Mobile communication technologies have evolved from 1G to 5G, and the development of 6G is underway [1]. The first generation of communication technology (1G) utilizes analog technology and Frequency Division Multiple Access (FDMA), such as the Advanced Mobile Phone (AMPS) in the United States, which is a typical representative of 1G networks [2]. However, 1G is limited by distance and network capacity during transmission and also has disadvantages such as low spectrum utilization, limited service variety, and poor confidentiality performance. The second-generation communication technology

⋆ Corresponding authors

(2G) uses digital technologies such as Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) to provide better voice quality and data transmission rates. Later, the third-generation communication technology (3G) was based on broadband wireless connectivity technologies such as TD-SCDMA in China, CD-MA2000 in the United States, and WCDMA in Europe. 3G networks connect the international Internet and wireless communication, providing better voice quality and data transmission rates [3]. The fourth generation communication technology (4G) combines 3G communication technology and WLAN technology, abandoning CDMA, with Orthogonal Frequency Division Multiple Access (OFDM) and Multiple-In Multiple-Out antenna (MIMO) technology as core technologies [4]. 4G has higher data transmission rates and much lower network latency than 3G. The fifth generation communication technology (5G) uses the millimeter wave band and MIMO technology [5]. Compared with 4G networks, it has lower energy consumption, lower latency, and faster speed, with the characteristics of ubiquitous networks and interconnection of all things [6].

In March 2019, the first 6G summit was held in Finland [7], where communication research experts worldwide worked together to draft the first 6G white paper [8]. Subsequently, governments and regional organizations began to research next-generation mobile communication technologies. China established a national 6G technology R&D promotion working group and expert group in November 2019, Huawei also launched a 6G R&D lab in Canada. China Mobile and Tsinghua University established a strategic partnership to collaborate in scientific research on 6G networks. The Korea Institute of Communication and Information Science held a 6G forum in April 2019 to officially announce the start of research on 6G networks. At the Mobile World Congress America (MWCA 2018) in September 2018 [9], US Federal Communications Commission (FCC) officials looked ahead to 6G technology for the first time in a public forum. The New York University Wireless Center (NYU Wireless) is working on wireless technology using terahertz frequency channels with transmission rates of up to 100 Gbps, and the University of California's ComsenTer Research Center has been awarded a $27.5 million grant to research the fusion of terahertz communication and sensor.

6G will outperform 5G in many aspects, such as latency, peak rate, connection density, traffic density, mobility, and spectral efficiency [10]. Regarding data transmission rate, 6G is expected to reach 50 times that of 5G, with peak transmission speeds of 100Gbps-1Tbps compared to 10Gbps for 5G. Regarding network latency, 6G networks will be reduced to one-tenth of 5G networks. Regarding connection number density, indoor positioning accuracy reaches 10 cm and outdoor is 1 m, which is 10 times higher compared to 5G and the density of connected devices reaches more than 100 per cubic meter. 6G networks use Terahertz (THz) band communication, and network capacity will be significantly increased [11]. Along with the rapid development of advanced technologies such as digital twins, blockchain technology, artificial intelligence, and space communication, the 6G network will realize the vision of a "smart connection of everything".

However, as network coverage expands and network heterogeneity increases, the security and privacy of 6G networks will be worse than in previous generations of mobile communication networks. Notably, 6G networks will face more severe security challenges, since (1) 6G networks use AI algorithms to train data, and service providers will collect a large amount of user data for model training to improve the model. These data will cover a large amount of user privacy. Once the data are leaked or attacked, the conse-

quences will be severe [12], (2) 6G network combined with the Internet of Things (IoT), the access and management of large-scale, low-power IoT devices can easily cause signaling storms. Moreover, the direct interaction of IoT devices is more frequent, as many IoT devices have higher requirements and security for group communication [13]. Thereafter, if the nodes are the wrong ones, it may bring out large-scale security problems [14], and (3) 6G is a crucial way to achieve air-space-ground-sea integration, this will expose it to more complex security issues. For example, at the UAV network level, UAVs are more susceptible to malicious attacks than ground-based stations because they cannot support complex encryption algorithms [15].

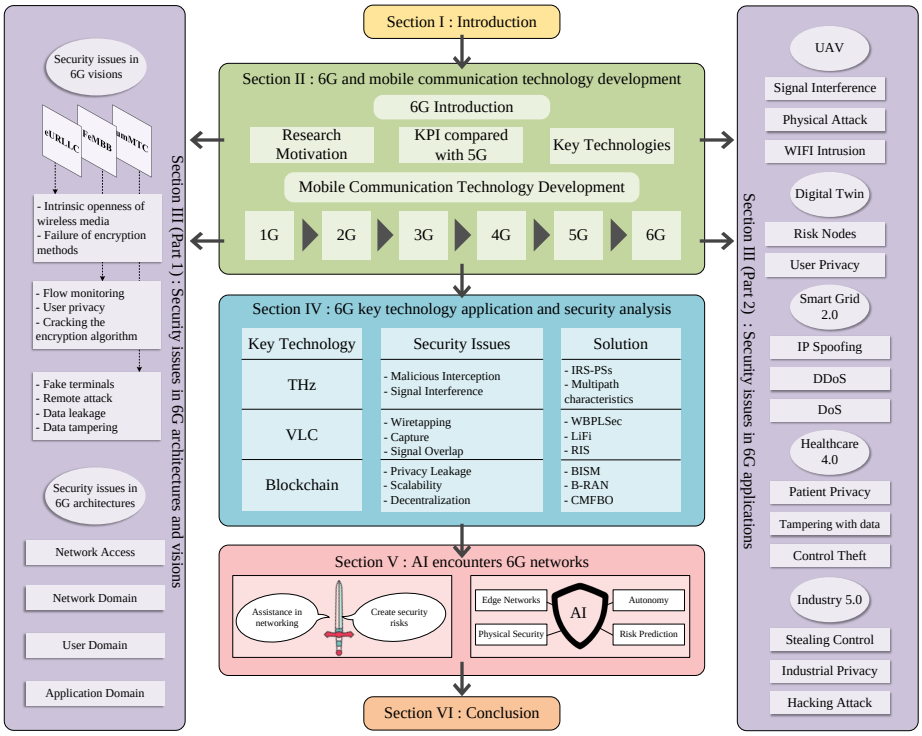

Fig. 1. The overall idea of this article

This work addressed the security issues in 6G networks, the structure and ideas of this work are shown in Figure 1. The remainder of this article is distributed as follows: In section 2, the development process of mobile communication technology from 1G to 6G is briefly introduced, and the research motivation of 6G networks is discussed. In addition, the KPIs of 6G networks are compared with 5G networks, and some key technologies of 6G networks are listed. Section 3 starts with the security issues of 6G in the network architecture, then compares the three main visions of 5G and 6G networks and lists the security issues. Also, in this section, we analyze the security issues of 6G networks in UAV mobile communication, digital twin, smart grid 2.0, healthcare 4.0, and

industrial 5.0. In section 4, we list the key technologies of 6G networks, such as terahertz communication, visible light communication, and blockchain technology, which are listed to analyze the security problems of using these technologies in 6G networks. We also offer some possible solutions to these problems. In section 5 of this work, we first mention that the application of AI in 6G networks is a double-edged sword and illustrate this point in terms of AI driving the construction of 6G networks while AI creates cyber risks for 6G networks. Next, four perspectives are presented to demonstrate that AI can assist 6G networks in addressing security threats. Finally, the work is summarized, and the future research directions are prospected.

2. Development of the Mobile Communication Technology and 6G

The second part introduces the development of mobile communication technology, summarizing the characteristics of each generation of communication networks from 1G to 5G and the enhancements over previous generations of each communication technology. Later, we introduced 6G networks in detail to raise the issue of security threats in 6G networks.

2.1. Development and Security Analysis of Mobile Communication Technology

Since the 1980s, mobile communication has produced a new generation of revolutionary technologies in a ten-year cycle. It continues to accelerate the iterative upgrade of the information industry and continuously promotes the prosperity of the economy and society. Today, it has become an indispensable primary information network to connect human society. However, the exploration of communication mobile networks is endless, communication technologies have evolved from 1G communication networks to 5G communication networks, and 5G networks are now being deployed on a large scale worldwide. At the same time, research on 6G communication networks is underway [16]. This part is a general overview of the development of the first five generations of communication networks. We briefly introduce the evolution of mobile communication technology in Figure 2.

The First Generation (1G) In 1974, Bell Labs developed the world's first mobile cellular telephone system, the Advanced Mobile Phone System (AMPS). 1G is developed to simulate information through electrical signals or electromagnetic waves directly. In the early stages, it was developed mainly to enable cell phone communication through distributed transceivers and networks.

As mentioned in [17], 1G networks can provide data rates of 1kbps to 2.8kbps and use circuit switches. It uses a bandwidth of 40 MHz, and its frequency range is between 800 and 900 MHz. The underlying technologies used in 1G networks are Advanced Mobile Phone Services (AMPS), Nordic Mobile Talk (NMT), and Cellular Digital Packet Data (CDPD).

Since the 1G network is an analog technology, call information must be transmitted through open-air electromagnetic waves. Therefore, lawbreakers can use technical means to intercept and decrypt this information, thus eavesdropping on the content of the call. It shows that the security of the communication network at that time was a matter of concern.

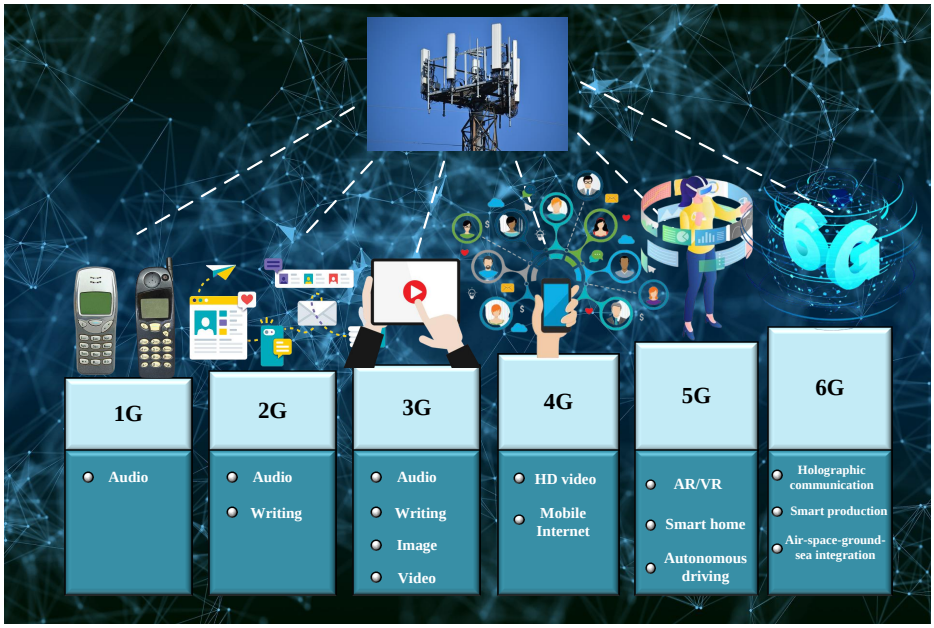

Fig. 2. History of mobile communication technology development

The Second Generation (2G) The second-generation mobile communication technology (2G) is based on digital language transmission technology as the core. In addition to the call function, some systems also introduce SMS functions and support data transmission and simulation. But the user experience rate is 10 kbps, and the peak rate is only 100 kbps, so it is only suitable for transmitting low volume of information such as e-mail, software, and others. 2G technology is divided into two types: one is based on TDMA, represented by GSM, and the other is CDMA, a form of multiplexing [18].

The 2G networks have the disadvantages of low transmission rate, unstable network, and high maintenance cost. The confidentiality of communication in 2G networks is also poor, which can easily cause security problems such as privacy leakage.

The 2G networks use weak encryption between the base station and the device, an encryption that can be easily cracked by an attacker in real time to intercept a call or text message. There is also no base station authentication technology in 2G networks, so anyone can seamlessly impersonate a 2G base station, and cell phones using the 2G protocol cannot recognize the authenticity. Fake BTSs sometimes capitalize on 2G's security vulnerabilities in order to intercept users' communications messages.

The Third Generation (3G) 3G mobile communication network is a cellular mobile communication technology supporting high-speed data transmission. Its rate is generally above several hundred kbps, it can transfer sound and data information. The main difference between 3G and 2G is the transmission rate. 3G can provide 144kbps transmission speed, which is faster compared to 2G. 3G has higher transmission rates, supports more advanced multimedia, and supports access and global roaming. It also allows you

to connect your phone to the Internet or other IP networks for voice calls, video calls, downloads, and data uploads [19].

Although 3G has a higher transmission rate, larger system capacity, and better communication quality than the previous two generations of communication networks, it has disadvantages such as limited capacity, incompatibility, inability to provide automatic roaming, and difficulty in achieving call confidentiality.

The 3G networks do not introduce public key cryptosystems in their security design, which makes it challenging to implement user digital signatures, thus reducing the security of the network. Although advanced cryptographic algorithms such as AES were used in the 3G network, the latest cryptographic achievements of the time, such as the ECC elliptic curve cryptographic algorithm, were not introduced. These pose security threats to 3G networks.

The Forth Generation (4G) The fourth-generation mobile network technology (4G) combines 3G and WLAN in one, it can download at speeds of over 100 Mbps, which is 25 times faster than home broadband ADSL. It meets many requirements of users for wireless services. In addition, 4G can be deployed in areas not covered by DSL and cable modems and then expanded throughout the area [20].

The core technologies of 4G are access methods, multiple access schemes, modulation technologies, coding technologies, high-performance receivers, smart antenna technologies, MIMO technologies, software radio technologies, etc. 4G networks provide mobile network access, IP telephony, gaming services, HD mobile TV, and video conferences.

The communication speed of 4G can be limited by the capacity of the communication system. As a result, if the amount of users is large, the communication speed will become slow. Moreover, due to the limited research conditions at that time, many difficulties were encountered during its construction and development.

4G networks may face the threat of Distributed Denial-of-Service (DDoS) attacks. This refers to an attacker sending a large number of invalid or high-traffic network requests to a target server by controlling a large number of botnet hosts, causing the server to run out of resources and not be able to respond appropriately to legitimate user requests.

The Fifth Generation (5G) The fifth generation mobile communication technology (5G) is a new communication technology with high speed, low latency, and ample connectivity, it is a network that enables the interconnection of people and machines [21]. 5G has a peak data download speed of up to 10 Gbps, nearly 100 times higher than 4G networks. It also has a significant increase in capacity compared to 4G networks due to the construction of many base stations. At the same time, 5G networks also have lower latency, higher bandwidth, and more excellent connectivity [22]. 5G networks are combined with technologies such as digital twin, blockchain, and IoT. And 5G is applied in various fields such as healthcare, education, logistics, and travel. It brings great convenience to our life [20,23]. Nevertheless, as the 5G networks are used in a broader range of scenarios, this makes it trickier to deal with a wide variety of security threats.

2.2. 6G Communication Network Introduction

In this section, we will introduce 6G networks from three aspects: research motivation, key performance indicators, and key technologies.

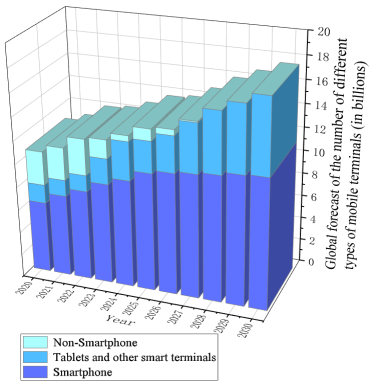

Fig. 3. Global forecast of the numberof different types of mobile terminals

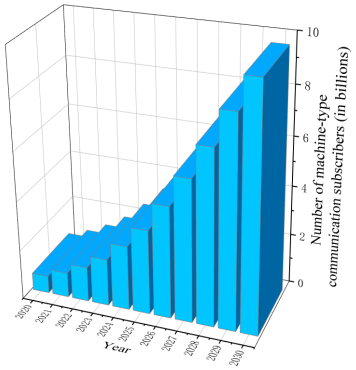

Fig. 4. Global forecast of the number of machine-based communication subscribers

6G Research Motivation With the rapid development of communication technology, 5G communication technology was born. It has the characteristics of low latency, high speed, ubiquitous network, and low power consumption. The International Telecommunication Union (ITU) defines three major types of 5G application scenarios [24], namely ultra-reliable low-latency communications (uRLLC), enhanced mobile broadband (eMBB), and massive machine-type-communications (mMTC).

5G networks have a massive impact on society. As a significant technology in digital transformation, 5G networks are changing how people live and work. Technologies such as smart cities, automated driving, and remote surgery are becoming a reality, promoting innovation in healthcare, logistics, agriculture, education, and other fields. Also, 5G is rapidly boosting the development of the world economy, with literature [25] indicating that 5G is expected to achieve approximately $12.3 trillion in global economic output in 2035, exceeding the total consumer spending of China, Germany, France, UK, and Japan in 2016.

Although 5G technology brings excellent convenience to society, as 5G is commercialized, many demands are raised that cannot be realized by 5G. Figure 3 and Figure 4

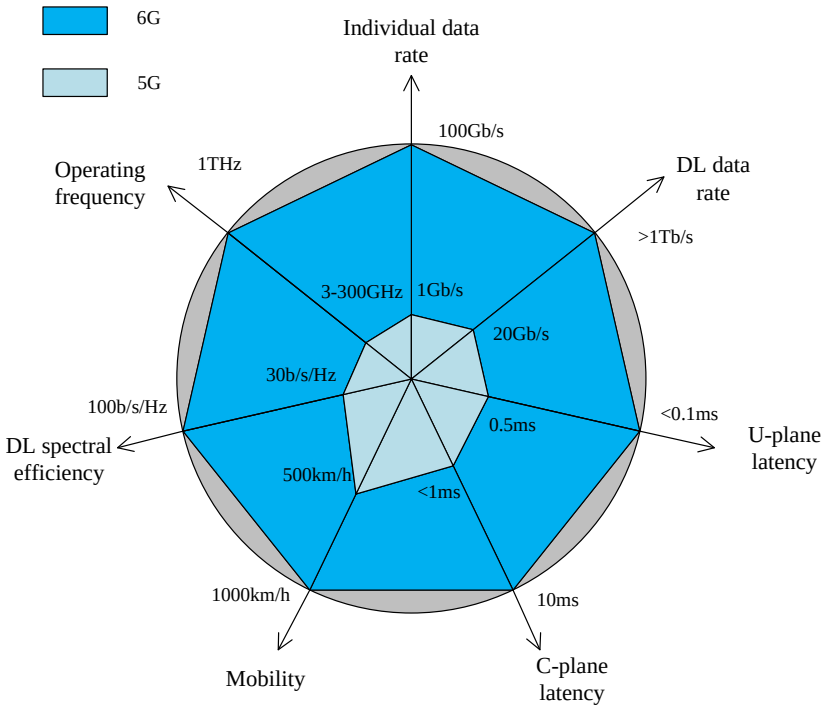

Fig. 5. Comparison of KPIs between 5G and 6G networks

show the bar graphs of future global mobile services and the number of terminal devices forecast in the Global Mobile Services Forecast 2020-2030 report [26] published by the International Telecommunication Union (ITU). Research on 6G wireless communication networks has been initiated in this context.

Comparisons of KPIs between 5G and 6G networks Compared with 5G networks, 6G networks will usher in more significant improvements in various aspects, such as transmission rate, traffic density, positioning accuracy, connection number density, mobility, etc. Due to the improved performance, 6G networks will also see an inevitable increase in energy consumption.

In March 2019, Bell Labs, USA, proposed some key performance indicators for 6G networks. In December 2020, the Chinese Communications Standardization Association also presented key indicators for 6G networks and compared 5G network indicators with 6G. Jiang *et al.* estimated the requirements and characteristics of 6G in [27]. The comparison of the key performance indicators between 5G and 6G networks is shown in Figure 5.

Key Technologies in 6G The widespread use of advanced technologies such as digital twins and blockchain for digital transactions, privacy protection, and others, accelerating the research of 6G communication networks and promoting the development of next-generation communication technologies [28,29,30]. Some key technologies for 6G

networks are listed here: terahertz communication technology, air-space-ground-sea integrated communication technology, and visible light communication technology. The concepts of these four key technologies will be described, and how the technology can be applied in 6G networks will be shown in this part.

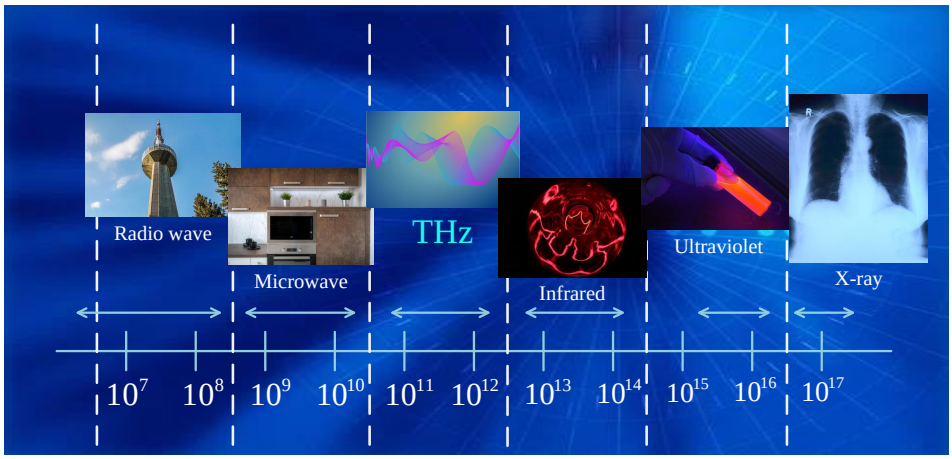

Fig. 6. The applications of electromagnetic waves in different frequency bands

A. Terahertz Communication Technology

As shown in Figure 6, terahertz waves have a frequency between 0.1 and 10 THz. In terms of frequency, terahertz waves are located between millimeter waves and infrared waves. In terms of energy, it is located between electrons and photons. The high frequency of terahertz waves can solve the problem of large-scale data information limited by bandwidth, and it can meet the future requirements of mass data transmission as well as high transmission rate communication. Terahertz waves are characterized by abundant spectrum resources, strong anti-interference capability, high transmission rate, and high penetration. Therefore, it can effectively complement today's null-port transmissions [31,32].

B. Air-space-ground-sea Integrated Communication Technology

Air-space-ground-sea integration means that the 6G network will cover the sky, space, ground as well as the sea, connecting all parts of the network to form an integrated communication network, which is shown in Figure 7. Air-space-ground-sea integrated communication technology takes ground-based networks as the basis, while space-based, air-based, and sea-based networks are considered as expansion and extension. The ground-based networks are composed of local area networks and cellular mobile networks, and the network service area in this area is relatively dense. The space-based networks are composed of various satellite networks, which can be classified into low-orbit satellites, medium-orbit satellites and high-orbit satellites. The air-based networks are composed of

Fig. 7. Air-space-ground-sea integrated communication

planes, airships, drones, and other flying communication equipment networks. The sea-based networks are composed of ocean underwater communication [33], ship communication and island communication networks, etc. [34]. We can connect the communication networks in each area of the integrated air-space-sea network and fully use the various resources in them to meet a wide range of requirements in the future [35].

C. Visible Light Communication (VLC) Technology

VLC is a communication method that uses light in the visible wavelength band as a message carrier to transmit optical signals directly in the air. The number and density of communication devices will multiply in the future. If traditional radio communication continues to be used, this will lead to a shortage of communication bands. And because of its unique information carrier, visible light communication technology provides a new choice for short-range wireless communication [36]. The applications of VLC are shown in Figure 8:

The RF signal of traditional radio communication will not only cause harm to the human body, but also cause interference to other devices. At the same time, visible light transmission will not produce radiation to the human body and will not be affected by external electromagnetic interference. It has a more enormous scope of application than radio communication [36]. From the perspective of environmental protection, visible light communication is green and low-carbon. Then, from the aspect of privacy protection, radio electromagnetic signals will have the problem of electromagnetic leakage, which will not be conducive to privacy protection. But visible light communication rarely appears to be eavesdropped and illegally appropriated.

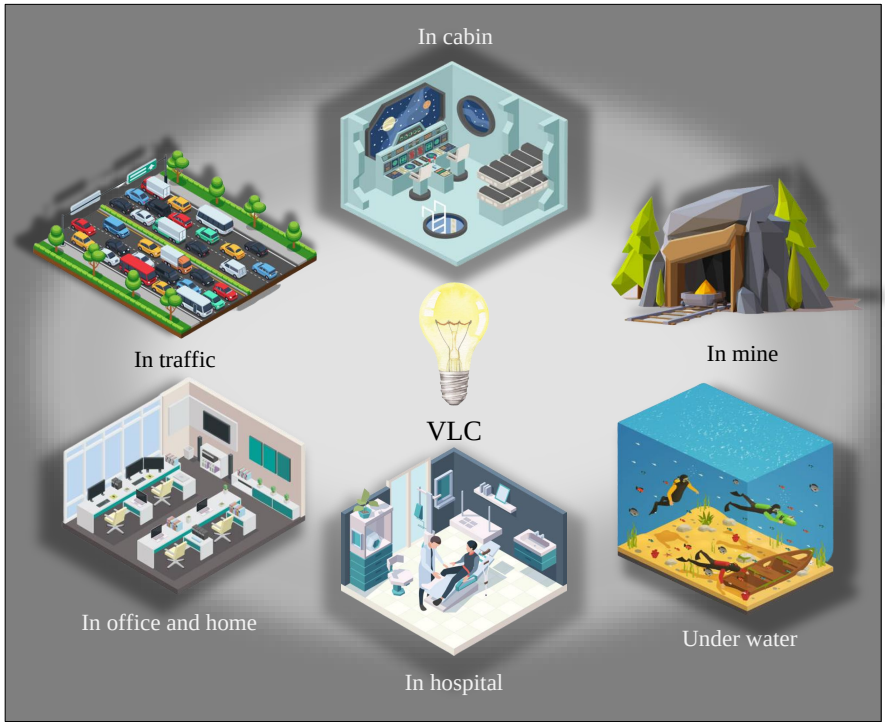

Fig. 8. Applications of the visible light communication technology in different scenarios

From the exposition in this section, we can see that people have great confidence and motivation in developing 6G communication technology, and all countries strongly support the research of 6G technology and invest a lot of time and money to promote the development of 6G. 6G has a vast improvement compared with previous generations of mobile communication technology. With the application of 6G technology in many fields, it will bring great convenience to people and change the face of society. However, some security issues in 6G networks will also arise. In the following parts of this article, we will analyze some security issues in 6G networks.

3. Security Challenges of 6G Networks in Architecture, Visions and Applications

After the introduction of the development of mobile communication networks and 6G networks in the previous section, this section will discuss some security issues existing in 6G networks. Here, we mainly introduce the security threats of 6G in network architecture, visions, and related applications, and we also list some related countermeasure strategies.

3.1. Security Issues in Architecture

The network architecture of 6G can be divided into network access, network domain, user domain, and application domain. This section will summarize the security issues in the 6G architecture and possible solutions, as shown in Table 1.

Table 1. Security issues and solutions in 6G architecture

Security Issues	New Requirements	Possible Solution	References
Network Access Security	• New authentication model and password system	• 6G-AKA • Quantum security codes • Physical layer security • A design of SD-WAN-oriented wide area	• Wang *et al.* [37] • Liang *et al.* [38] • Sun *et al.* [39] • Tanveer *et al.* [40] • Wang *et al.* [41] • Mine *et al.* [42]
Network Domain Security	• New open authentication method • Authentication methods during network domain switching	• Lightweight encryption methods • New authentication technology • Blockchain technology	• Khashan *et al.* [43] • Alresheedi *et al.* [44] • Arfaoui *et al.* [45] • Yazdinejad *et al.* [46]
User Domain Security	• New authentication method • New user experience	• Biometric-based authentication technology, smart cards, etc. • Multi-party information sharing and cooperation • Blockchain technology	• Liu *et al.* [47] • Liang *et al.* [48] • Sengupta *et al.* [49] • Cao *et al.* [50] • Lu *et al.* [51] • Long *et al.* [52]
Application Domain Security	• Solutions for different security needs in different areas	• Customized security solutions • Network security regulation and management • Data encryption and privacy protection	• Abdel *et al.* [53] • Akbar *et al.* [54] • Ramezanpour *et al.* [55] • Khan *et al.* [56] • Zhang *et al.* [57]

Network Access Security The 6G network will access a large number of devices, including IoT devices, sensors, smart terminals, and so on. The security of these devices is one of the core issues when 6G network devices access the network. Devices may have security vulnerabilities, such as hardware vulnerabilities, software vulnerabilities, communication protocol vulnerabilities, etc., which can be exploited by attackers to gain control of the device, steal data, or perform malicious operations. For example, the era of 6G networks will usher in immersive cloud XR, and multisensory XR applications will apply molecular communication technologies, THz technologies, and quantum communication technologies [41]. However, combining XR with uRLLC and eMBB has many outstanding security issues, such as malicious behavior, access control, internal communication,

and so on. Therefore, 6G networks require new authentication models and cryptographic systems, such as 6G-AKA and quantum security cryptography.

6G network design will gradually shift to a cloud-based and open programmable network platform, leading to changes in the authentication architecture. 6G networks may inherit the security model of 5G networks, such as providing a unified authentication platform for open and access network irrelevant individuals and flexible scheduling and dispatching of resources through network slicing mechanisms. However, the inherited security model is far from solving the network access security problems that 6G networks will face. Consequently, some solutions need to be adopted, such as the 6G-AKA protocol proposed by Nguyen *et al.* in [58]; this method needs to prove which component will determine authentication in cross-slice communication. 6G-AKA needs to be able to verify endpoint identity even in deeply sliced and open programmable network platforms.

Network Domain Security The 6G air-space-ground-sea integrated network architecture will be based on terrestrial cellular mobile networks. It can combine the broad coverage, flexible deployment, and efficient broadcasting features of broadband satellite communications and achieve full coverage of sea, land, space, and air through the deep integration of multiple heterogeneous networks, which will bring new opportunities for the markets of marine, airborne, cross-border and the fusion of heaven and earth. As the 6G networks will cover various network domains, security issues must be considered when switching between different network domains. To solve this problem, authentication methods can be designed during the switching process to ensure security. It is also important to note that the 6G coverage network domain includes non-terrestrial networks such as satellite and maritime communications, which will require new open authentication methods.

User Domain Security Nowadays, authentication is valued, and various researches have been carried out in this direction [59,60]. Nevertheless, most applications have been using password-based authentication, which not only makes it easy for hackers to crack passwords but also it is not excluded that users may forget their passwords, which does not guarantee user account security, and users will have a poor experience. 6G networks can use biometric-based authentication encryption methods [61] or provide password-free services, such as retina-based or brainwave-based authentication [47]-[52]. It may provide users with a more secure and better user experience in the future.

Application Domain Security 6G is expected to be commercially available in 2030, when it will become the key communication infrastructure for us to meet many requirements. People will apply 6G to Unmanned Aerial Vehicle(UAV), autonomous driving, Smart Grid 2.0, Industrial 5.0, super smart healthcare, digital twin, extended reality, collaborative robotics and many other areas. The application domain of 6G communication networks will continue to expand.

However, as 6G communication technology is applied to more and more fields, some security issues will continue to emerge. For example, different application domains have different usage scenarios and different levels of security requirements. Moreover, many domains are new, and people have little research on them. As a result, safety will be difficult to guarantee. People need to take corresponding solutions for different security

requirements in different domains. For instance, in identity verification, even though symmetric key mutual authentication is still used in 5G, it may benefit more from blockchain technology and distributed ledger technology in a 6G network environment. This means that there is still a great deal of work to be done in application domain security for 6G networks.

3.2. Security Issues in Visions

The three significant visions of 5G networks are uRLLC, eMBB, and mMTC. In contrast, the visions in 6G networks have further enhancements based on the visions of 5G networks, which are enhanced Ultra-Reliable Low-Latency Communication (eURLLC), Further enhanced Mobile Broadband (FeMBB), and ultra massive Machine-Type Communications (umMTC) [62]. In this section, some security issues of 6G networks in these three visions are analyzed. We summarize the contents, as shown in Table 2.

eURLLC The goal of uRLLC is to enable network characteristics and functions to manifest under extreme conditions [62]. To keep round-trip latency between critical infrastructure and computers within 1ms, techniques such as network slicing, beam forming, and packet re-transmission protocols are used to improve reliability and reduce latency. And the network reliability will be required to exceed 99.999%. The eURLLC proposed by 3GPP introduces enhanced ultra-reliable, low-latency communications, and the network's reliability will increase to 99.99999% [72]. Service applications for eURLLC include latency-sensitive services that require high reliability, such as autonomous driving, tactile Internet, telemedicine, and industrial automation. The end-to-end packet transmission delay for mission-critical applications should be between 10-100ms.

The security threats faced in eURLLC are as follows:

1. Intrinsic Openness of the Wireless Medium

   eURLLC should consider the impact of security workflow delays to ensure the quality of service [63]. At the same time, the ultra-high reliability of 6G networks will imply the need for more efficient security protection schemes to meet the high requirements they impose, so as to protect the availability of services and resources. As also mentioned in the literature [65], the security issues of eURLLC are raised due to the inherent openness of the wireless medium. Traditional cryptography-based approaches are able to solve the security problem of high-level information transmission under the assumption that the eavesdroppers (Eves) have limited computational ability. However, once the above assumptions fail, traditional cryptography will not be able to solve the security problem. Therefore, more sophisticated and innovative encryption methods are needed to solve the security problems of information transmission in eURLLC.
2. Multi-level Architecture Security

   Many agents and virtual spaces are generated with the continuous innovation of information technology [66]. Object communication (OCC) exhibits the multi-flow concurrency characteristics of multi-dimensional, heterogeneous, and multi Quality of Service (QoS) requirements. Data computing transitions from cloud computing

Table 2. Comparisons of 5G, 6G visions and security issues in 6G application scenarios

5G	6G	Differences	Security Issues	Possible Solutions	Applications
uRLLC	eURLLC	• Lower latency • Higher reliability • More device connections are supported • More technologies are adopted	• Intrinsic openness of wireless media [63,64] • Failure of encryption methods [65] • Multi-level architecture security [66] • Malicious software	• Secure network architecture design • Secure communication protocols • Security authentication and authorization • Safety monitoring and management	• UAV-based Mobility • IoT Healthcare • Drone-based systems
eMBB	FeMBB	• Higher bandwidth • Lower latency • Greater throughput • Faster transmission speed • Wider network coverage • Greater network capacity	• Flow monitoring [67] • User privacy [68] • DoS and resource attacks • Crack of the encryption algorithm	• Data encryption • Authentication and access control • Installation of firewall and intrusion detection system • Establishing an effective security monitoring and management mechanism • Lightweight authentication • Techniques for keys management	• UAV-based Mobility • Holographic Telepresence • Super-Fast Hotspot • IoT Healthcare • Industrial Internet of Smart Things • Ultra-dense cellular IoT networks
mMTC	umMTC	• More device connections are supported • Application to larger scale IoT communications	• Fake terminals [69] • Remote attack [70] • Device forgery and illegal access • Hacking and malware intrusion • Data leakage • Data tampering	• MTC endpoint embedded device security [71] • Implement authentication and data encryption for devices and users in umMTC • Risk assessment and management • Enhance physical equipment security management	• Holographic Telepresence • Super-Fast Hotspot • IoT supply chain • IoT Healthcare • Drone-based systems

to edge computing, then gradually convert from edge computing to distributed computing and heterogeneous computing. Therefore, the security of centralized and distributed multi-level architectures will also become a factor affecting the security of eURLLC requirements for 6G networks.

FeMBB eMBB is one of the three main 3G New Radio (NR) use cases defined by 5GPP. eMBB is defined by Dakhaz *et al.* in the literature [73] as follows: eMBB communication is intended to meet high throughput requirements and is used for several high-priority services. eMBB is proposed to meet the latest applications due to the rapidly increasing use of broadband data. In the era of 6G networks, a range of immersive applications, including 3D extended reality capabilities, 3D multimedia, and IoE are predicted to emerge [74], which will need to be achieved with high-quality services at tens of times the peak Gbps rate. Therefore, the 6G network mobile broadband speed must be further improved to provide a Tbps level mobile broadband data rate peak to meet the higher requirements, thus proposing FeMBB. Business applications for FeMBB include high-resolution video streaming and expanded reality with large data packets. This creates high bandwidth requirements for 6G networks.

The security threats of 6G networks in FeMBB are shown in the following points:

1. Flow Monitoring

   In the future, FeMBB will be applied to 4K/8K HD video and mobile roaming immersive services based on Virtual Reality (VR) and Augmented reality (AR), generating a large amount of data consumption. Existing network firewalls and security devices such as intrusion detection systems will not be able to ensure adequate security protection when large amounts of data monitoring and storage are involved [67].
2. User Privacy

   Extreme data rates in FeMBB will pose challenges for secure traffic processing, such as attack detection, AI/ML pipelines, traffic analysis, and universal encryption [63]. In FeMBB, a large amount of user data needs to be processed, including identity information, location information, communication information, and so on. Therefore, if the work related to secure traffic processing is not done correctly, then it can cause serious privacy leakage problems [68].

umMTC One of the key communication scenarios envisaged to be supported by 6G is the umMTC [75]. Its main feature is the large number of low-power devices to be connected, with up to 1 million sensors per square kilometer. IoT devices and their connectivity in the IoE world will dramatically change the scale of machine-type communication in the IoE revolution [76]. In IoE architectures, there may be a trillion brakes and sensors automatically transferring data back and forth. With such massive machine communication, current machine-type communication architectures will not be able to meet effective and efficient connectivity, thus requiring umMTC architectures to support reliable connectivity for large-scale networks.

The security issues in umMTC are as follows:

1. Fake Terminals

Since the IoT terminal is weak in resource processing and computation, this leads to a situation where authentication may not be achievable. Even if authentication is possible, the restricted computing power can only be used in simple authentication methods that are not effective. This situation leads to forged, counterfeit terminals that cannot be identified, which in turn creates security problems [69].

2. Remote Attack

   Intruders may take the shortcomings of the simplicity and weak protection of IoT terminals and then remotely attack the IoT terminals through software and hardware interfaces and then use the compromised terminals to launch cyber attacks [70].

3.3. Security Issues in Applications

6G networks will be used in the future in many fields, such as healthcare, transportation [77,78], logistics [79], and production, but applications in every field will face some security issues [63]. For the application of technology, we have selected UAV technology, which is the key technology to realize the concept of the air-space-ground-sea integration of the 6G network. As well as digital twin technology, a popular technology for applications in the future society. We have also selected people's visions of Smart Grid 2.0 and Healthcare 4.0 arising from the future 6G era as application examples. As well as Industry 5.0, an upcoming application domain, is also presented in this section. Figure 9 summarizes the security issues in applying 6G networks in different fields.

UAV based Mobility UAVs are mainly used in 6G networks for communication at the air-based network level. UAVs can be deployed in various scenarios, and the essential communication of ground-based networks can be expanded to air-based networks and connected with the satellite equipment of space-based networks and the communication equipment of sea-based networks, thus realizing the whole area coverage of 6G networks. In [80], Shrestha *et al.* proposed an advanced and fully autonomous 6G-based UTM system by applying UAVs.

Some security issues will also arise in the autonomous UAV system. For example, an attacker could gain control of a UAV by jamming the control signals or capturing it physically and then hacking inside it to obtain critical data. An attacker could also combine UAVs with other smart devices and thus convert from a cyber attack to a physical attack, which could lead to even more damage. Hooper *et al.* [81] predicted that an attacker could also gain remote control of a UAV by hacking into it through WiFi.

Smart Grid 2.0 The smart grid is the intellectualized grid, also known as "Smart Grid 2.0", based on integrated, high-speed two-way communication networks. Advanced sensing and measurement technologies, equipment technologies, control methods and decision support system technologies are applied to make the grid reliable, secure, economical, efficient, environmental-friendly and safe to use [82]. Its main features include (1) self-healing, (2) stimulating and protecting customers, (3) resisting attacks, (4) providing power quality that meets customer needs, (5) allowing access to different forms of generation, (6) initiating power markets, (7) optimizing the efficient operation of assets [83].

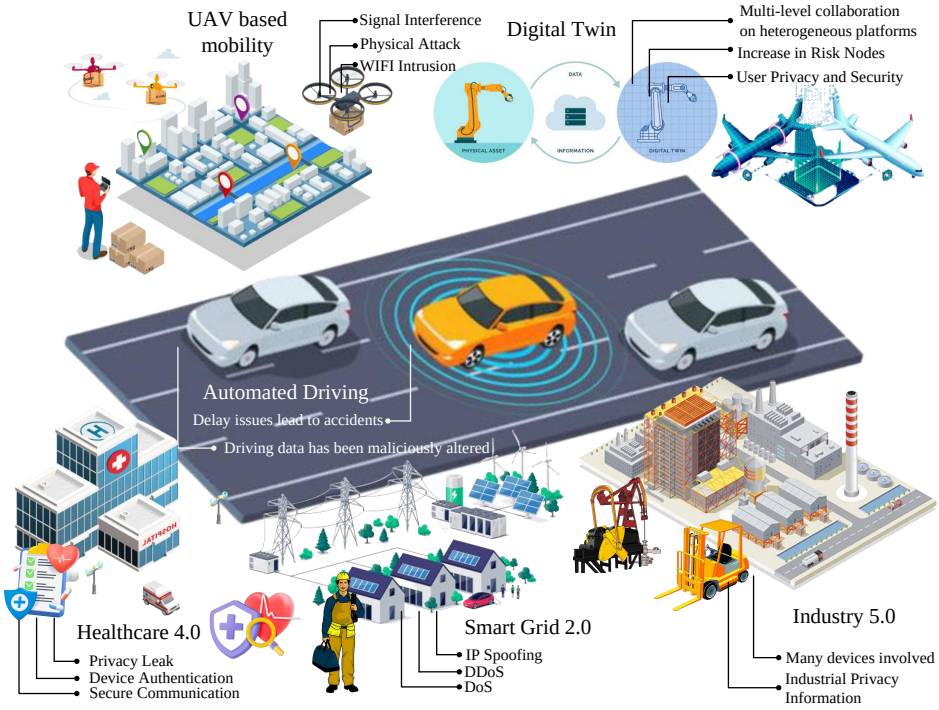

Fig. 9. Summary of security issues of 6G network applications in different fields

Smart grids improve network reliability by combining advanced sensing, communication, and control infrastructure. In the context of Smart Grid 2.0, the performance of the grid is affected by cyber-attacks and physical disturbances (e.g., symmetric and asymmetric faults), which can lead to power system instability. An attacker may analyze traffic data to gather helpful information or eavesdrop on smart grid entities(i.e., smart meters and control centers) [84]. Intruders or eavesdroppers can impact the security of smart grid network entities through component, DoS, DDoS, IP spoofing, and MitM attacks. From a cybersecurity perspective, a reliable and secure information system is required for the effective operation of a smart grid [85]. Especially when the smart grid is subjected to cyber-attacks, its physical layer performance is also affected, which may lead to decreased system reliability. In addition, improvements in trust management of transaction mechanisms are also critical to maintaining the security of the smart grid.

Healthcare 4.0 In the era of 6G networks, many smart medical devices applying communication technologies, sensors, vehicle technologies, and artificial intelligence will be deployed into the medical industry in large numbers [86]. 6G networks will facilitate the improvement of reliable remote monitoring systems in medical systems so that remote surgery, diagnosis, monitoring, and emergency care will become a reality in the 6G era. The 6G networks with high-speed rates, low latency, and ultra-reliable features will fa-

cilitate the fast and efficient transmission of data between many medical devices, thus improving the efficiency and quality of medical services.

Smart medical devices will collect large amounts of data, such as Body Area Networks (BANs) equipped with intelligent embedded systems to facilitate personalized management and health detection [87], and these BANs can collect human health data from various parts of sensors, dynamically share and interact with network services. 6G is likely to become the central communication platform for smart medical platforms, and there will be a large amount of private information involving patients transmitted in the network, which will have unimaginable consequences in case of security issues leading to information leakage. Healthcare monitoring frameworks are also increasing in their requirements for network performance as well as privacy-preserving means [88]. The vulnerable healthcare supply chain in networks is also risky [89]. This is because it may reduce the quality of some healthcare services, thereby threatening the privacy and security of patients as well as test results. In summary, device authentication, secure communication and access control for billions of micro medical devices will be the issues that need to be addressed for 6G network security.

Industry 5.0 Since mid-2010, the world has been in the fourth industrial revolution, also known as ”Industry 4.0”. The World Economic Forum defines this revolution as a combination of AI, advanced robotics, 3D printing, and IoT [90]. Recently, the automation level in the manufacturing industry has increased significantly [91], various smart devices are gradually appearing, and the way machines are connected by the Internet is fundamentally transformed. Some people describe this shift as ”Industry 5.0”, and the collaboration between humans, robots, and smart technologies will become the next industrial revolution breakthrough in the ”Industry 5.0” era [92].

The ”Industry 5.0” era involves many industrial privacy issues, such as the intellectual property rights of industries, production information of factories and the identity of employees. In an industrial Internet system, a company can collect raw data from its devices and sensors. These raw data allow the company to deliver scalable and reliable applications faster to meet the changing needs of the customers. Nevertheless, this raw information may contain the kind of private information mentioned above, and if this information is hacked illegally, it can lead to a serious privacy leakage problem. Therefore, in the ”Industry 5.0” era, applications must meet basic security requirements such as integrity, availability, authentication, and auditing.

Digital Twins The coming of the 6G era heralds the coming of the digital twin era. With the development of communication and artificial intelligence technologies, objects and processes will be able to produce a replica in digital form, and intelligent mapping of human-human and object-object interactions in digital environments will occur [93]. Through various complex algorithmic models, people can predict, plan and simulate the real world through the digital world. In this way, the optimal solution to solve some practical problems is thus obtained. In the field of industrial manufacturing, the digital twin can virtually construct a digital model of a product to simulate it for testing and verification. In the healthcare assurance industry, the same type of sensor data system can be used to track various health metrics and generate significant insight results [94].

Currently, technologies such as artificial intelligence, big data, and industrial Internet are developing rapidly. The connection between the virtual space of intelligent manufacturing based on the digital twin and the physical world is built on the basis of network information flow transmission. With the accelerated integration of digital twins and smart manufacturing, there will be a great possibility of transforming from a closed system to an open system in the future, and systemic security issues will be concentrated. With the integration of smart manufacturing with big data and cloud computing, as well as the deep involvement of third-party collaboration services and multi-level collaboration of a large number of heterogeneous platforms, the number of network security risk nodes will rapidly increase. It also brings more ways of intrusion, and many security issues are required to be solved [95].

4. 6G Key Technology and Security Analysis

There are many key technologies in 6G communication networks, the classic technologies are selected, such as THz communication, VLC, and blockchain. In this section, we analyze some security issues of the application of these key technologies in 6G and list some countermeasure strategies as references.

4.1. Terahertz Communication Technology

In recent years, the communications industry has developed rapidly. Due to the large number of people using wireless TV, mobile communication, amplitude modulation (AM), FM radio (FM), and other communication devices, the RF band has been almost wholly occupied. It is challenging to meet the massive demand for 6G networks, people need to explore higher-frequency electromagnetic waves to meet the new demand. Therefore, people focus on the THz electromagnetic waves. Terahertz, which ranges from 0.1 THz to 10 THz, will provide more bandwidth, greater capacity, and higher data transmission rates for 6G networks [96,97].

Security Threats Although the use of terahertz electromagnetic waves will facilitate the rapid development of 6G networks, there are many security issues in their application. For example, the high directionality of transmissions in narrow beams makes them robust to interception attacks, but there is still the possibility that malicious nodes can successfully intercept the signals. As a result, they can compromise access control, steal user information and essential data, and gain access to unauthorized resources. Singh *et al.* [98] confirmed that an unauthorized attacker could maliciously place some obstacles in the transmission path and thus make the attacker capture the communication through radiation scattering. The principle of this method is schematically shown in Figure 10. The attacker can also set the target of the jamming beam as the receiver of the signal and then jam the signal by electronic methods.

Possible solutions As 6G networks will use a higher frequency range, fine-grained frequency management, and coordination will be required to ensure that signals from different users do not interfere with each other. This can be achieved through techniques such as

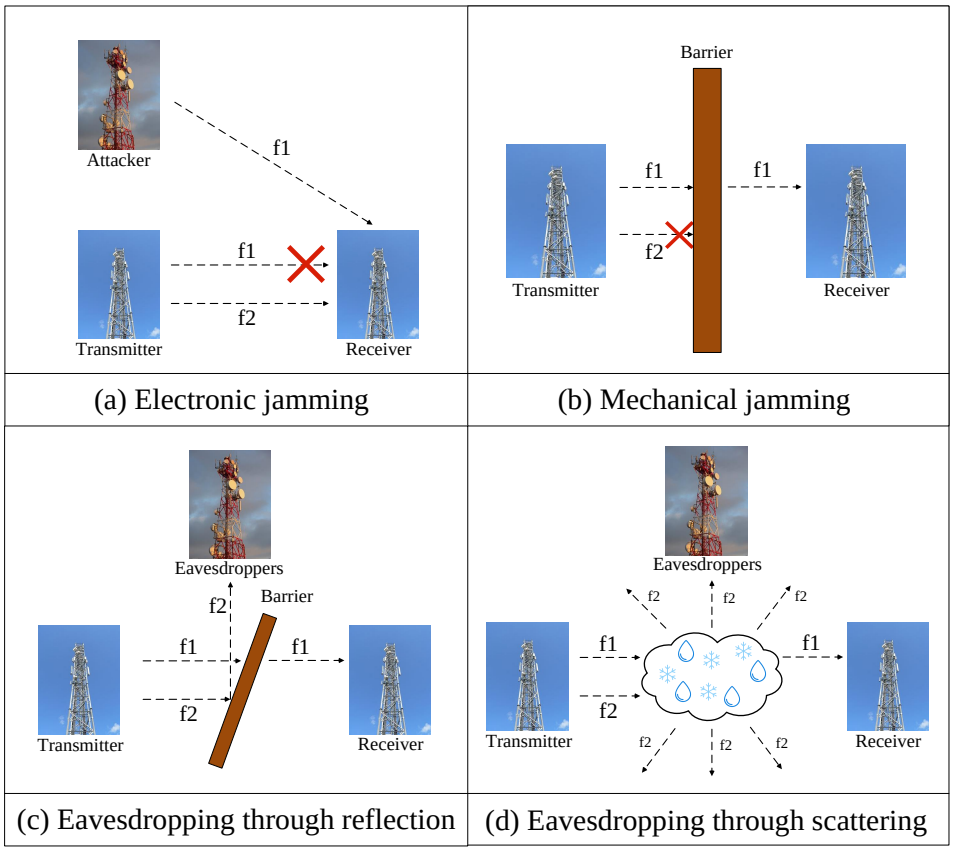

Fig. 10. Schematic of the principle of signal capture by radiation scattering

dynamic frequency allocation, coordinated spectrum sharing, and interference cancellation. Interference between different users can also be reduced by spatially isolating them through the use of massive antenna techniques. At the same time, beamforming techniques can concentrate signal energy in specific directions, improving signal quality and reducing interference to other users. Furthermore, Ning *et al.* [99] propose to maximize the secrecy rate by designing active beamformers at the base station (BS) and deploying passive reflective phase shifters (PSs) at the Intelligent Reflective Surface (IRS). To cope with the mixed integer nonconvex optimization problem involved, the authors propose a joint design with high-security performance and a low computational complexity design in the article. Apart from this, Li *et al.* applied IRS to wireless secure communication to study how to make the secure rate reach the optimal secure capacity from the perspective of optimization technique [100]. Petrov *et al.* in the literature [101] propose to exploit the inherent multi-path property of terahertz communication to reduce the probability of messages being eavesdropped. The authors suggest the ability to share data between communicating entities over the multiple terahertz propagation paths that are available. In this

way, even if eavesdroppers cooperate, this could have a significant effect in addressing the risk of eavesdropping. But at the same time, it will lead to a reduction in link capacity.

4.2. Visible Light Communication

VLC is a communication method that uses light in the visible wavelength band as an information carrier to transmit optical signals directly in the air [102]. VLC is considered a technology that supports 6G networks because of its huge bandwidth and terahertz frequency. The concepts related to VLC have been mentioned earlier in Section 2.2.3 and will not be elaborated on here. Possible security threats and their countermeasures are shown below:

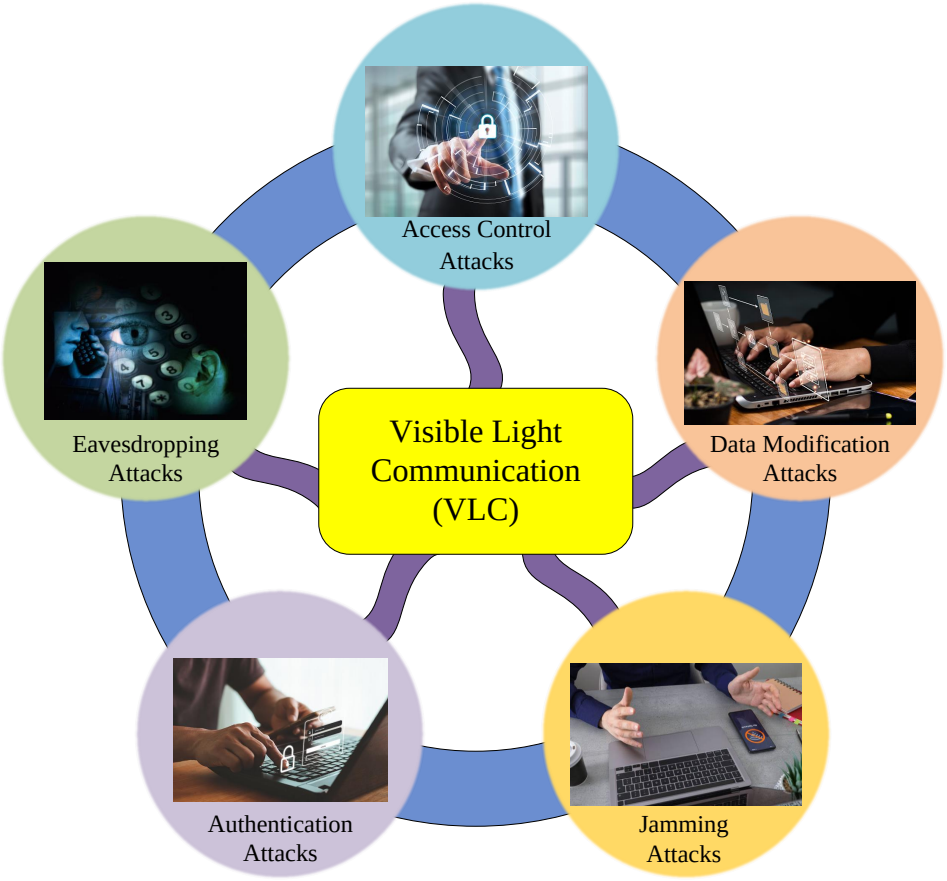

Fig. 11. Security issues in VLC

Security Threats Due to the open and broadcast characteristics of VLC, when the nodes of a VLC system are deployed in areas with large coverage, it may result in the overlap-

ping of signals from different transmitters, which makes VLC systems potentially exposed to some security issues [103]. At the physical level, attackers may attack the physical layer by eavesdropping, jamming, and capturing signals. Other access control attacks are carried out by illegally gaining access to the wireless medium. The security threats to the application of VLC technology in 6G networks are shown in Figure 11.

Possible solutions To address the security problems of VLC technology in 6G, it is necessary to strengthen technological innovation and establish a mature security system. For example, coding and modulation techniques with higher security can be developed to improve the reliability of data transmission. In [104], Soderi *et al.* propose a Watermark-Blind Physical Layer Security algorithm (WBPLSec) that combines watermarking and interference primitives to protect visible optical communications at the physical layer. They also use Intelligent Supersurface (RIS) techniques to improve the security performance of communications. In the literature [103], the authors enhance the confidentiality performance of MIMO VLC systems by linear pre-coding. Chen *et al.* proposed a visible light communication system of LiFi (light fidelity) network in the literature [105], which can provide high-speed broadband services to users with multiple addresses and mobile support. The authors also propose a transmitter and receiver design with omnidirectional characteristics in order to improve the channel quality and robustness of the uplink in LiFi systems.

4.3. Blockchain

Blockchain is a naturally distributed trust mechanism that is maintained by multiple parties collaboratively. It has the characteristics of openness and transparency, immutability, full trace, intelligent execution, etc. It can provide effective ideas for operation management, security trustworthiness enhancement and multi-party trust model of 6G networks [106]. The nature of blockchain distributed bookkeeping and its immutability provides a fair and open operating environment for every operator involved in the shared construction of the 6G network [107]. The smart contract in blockchain has the characteristics of value transfer, resource share, and enabling intelligent settlement [108,109]. Therefore, blockchain is applicable to resource sharing and settlement in the integrated air-space-ground-sea network [110], which makes the sharing of the infrastructure resources and the process of value transfer in the integrated network transparent, reliable, and real [111]. Blockchain can also be applied in the Internet of Vehicles (IoV) to prevent malicious participants from modifying the transmitted information and ensure the security of in-vehicle information transmission [112].

Security Threats The application of blockchain is exposed to a number of risks, and if it is deployed in a 6G network, these security threats will be manifested in the 6G network, as shown in Figure 12 [113]:

- 51% attack: Blockchain can build trust without the involvement of third-party institutions, when malicious people occupy 51% or more of the blockchain nodes, attackers may succeed in taking control of the network and thus tamper with information or affect transactions [114].

- Scalability: Blockchain-enabled systems present a number of challenges in terms of scalability in terms of throughput and storage [115,116]. Throughput depends on various factors such as hardware capacity, network latency, size of the P2P blockchain network, and others. The 6G network will have a very high data rate and connection density, coupled with the fact that many heterogeneous devices in the network will exist as nodes in the blockchain, which has a very high requirement for the throughput and storage capacity of the blockchain network.
- Privacy leakage: Since blockchain relies on transparent transactions to a certain extent, the process may cause problems such as the leakage of smart contract logic, transaction information [109], and user privacy during the execution of smart contracts.
- Decentralization: Blockchain is a decentralized network, and for untrusted nodes, blockchain needs to provide them with decentralized means of trust to prevent them from gaining more significant influence [117,118]. Whereas in a 6G network, there may be a large number of nodes with fake identities, which pose a security risk to the network as untrusted nodes. This poses a great challenge to the blockchain, and if these nodes are not handled well, the decentralization of the blockchain network will be compromised and will pose certain security threats.
- Consensus Algorithms: Consensus algorithms play a vital role in the operation of blockchain systems [119], and different types of consensus algorithms are developed and used for different applications [120]. With the development of quantum computing, there is a high possibility that 6G networks will also be integrated with quantum computing in the future. The current consensus algorithms existing in encryption mechanisms [121,122] are easily cracked by quantum computing, so we must propose new consensus algorithms encryption mechanisms for emerging technologies.

Possible solutions In order to cope with the above security issues of blockchain applications in 6G networks. We can adopt the techniques of sharding as well as a Directed Acyclic Graph (DAG) to cope with the high throughput requirements. Increase flexibility in network management and operation by decoupling the data plane and control plane in Software-Defined Networking (SDN) [123]. Quantify the degree of decentralization of blockchain by entropy method based on information theory. It is also vital to design cryptographic mechanisms with consensus algorithms against various attacks. New smart contract mechanisms can also be designed to protect private information on the blockchain.

A number of articles have proposed solutions to the security problems associated with the application of blockchain in 6G networks. In literature [124], Manogaran *et al.* introduce a blockchain-based integrated security measure (BISM) to provide secure access control and privacy protection to users. In this method, the access control process depends on the state of virtualized resources at different time instances, and the privacy protection depends on the corresponding duration of the service. Wang *et al.* propose a unified framework of Blockchain Radio Access Network (B-RAN) to improve the efficiency and security of 6G networks using blockchain technology [125]. Shahzad *et al.* [126] makes two contributions to address the security issues of blockchain applications in 6G networks. Firstly, at the process level, the authors propose a new smart contract mechanism. The specific process is done by embedding a hashed image into a message and then dividing the image into small blocks of pixels, all of which can be shuffled by

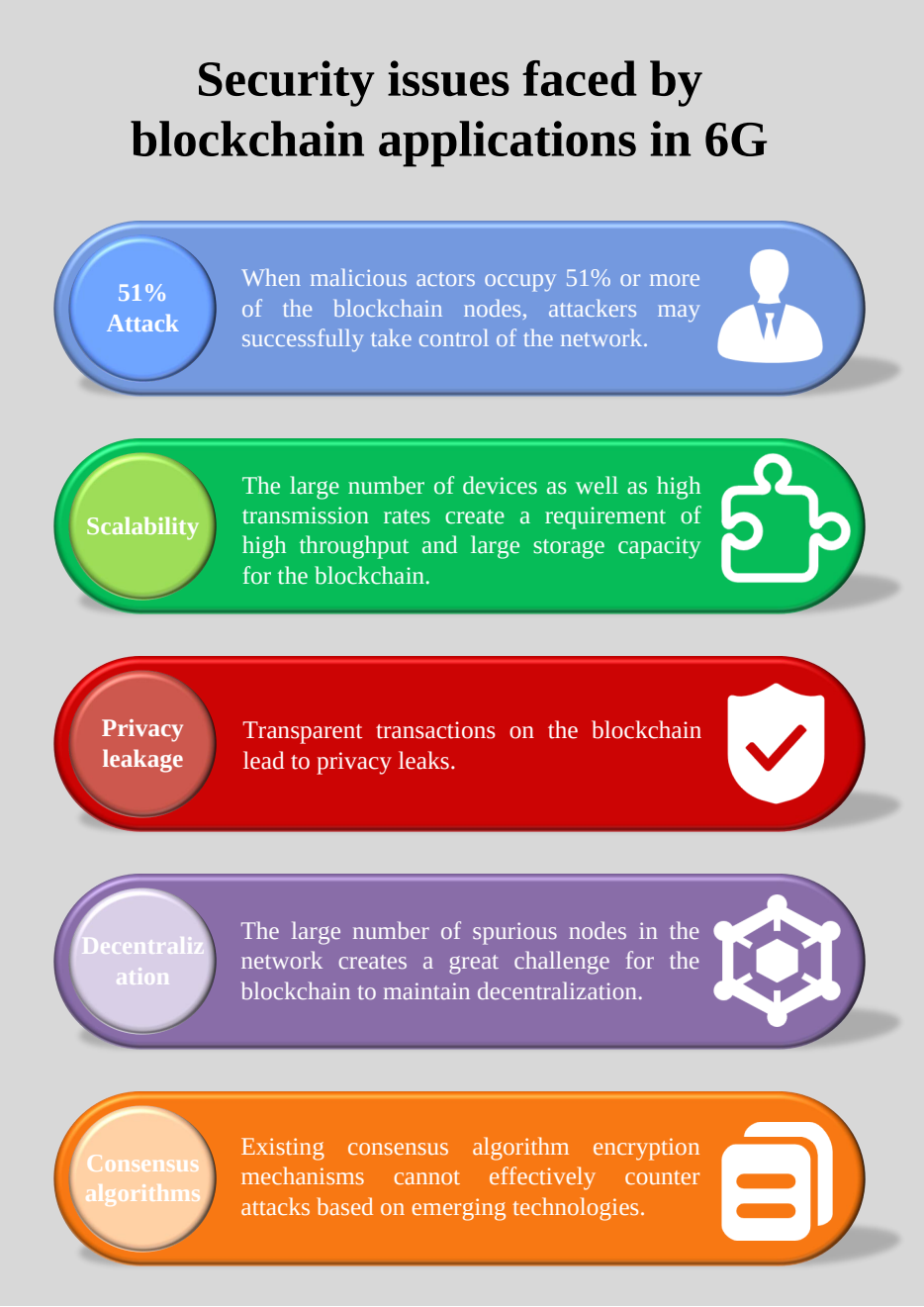

Fig. 12. Security issues in the application of blockchain technology in 6G networks

any matrix or algorithm to create a hash of that image. The receiver then restores the image to its initial state by means of the same matrix or algorithm. In this way, the record is guaranteed not to be tampered with. At the data level, the authors use a digital signature method that allows anonymization to verify and protect the blockchain without encrypting it. Abdulqadder *et al.* [127] has proposed a context-based authentication and security switching scheme using Markov Decision Method (MDM) and weighted product models to address the security issues that exist in network slicing in 6G environments. In terms of identity verification, the authors propose a context-based multi-factor biometric authentication (CMFBO) algorithm. A large number of IoT devices in 6G networks are working on insecure networks. However, the existing centralized signature schemes cannot address the challenges of security and efficiency in IoT identification. Liu *et al.* proposed a decentralized multi-signature protocol, IdenMultiSig [128], that combines Identity-Based Signature (IBS) with a Schnorr scheme under discrete logarithms on elliptic curves.

5. AI encounters 6G networks

6G networks will have greater flexibility and interoperability than 5G networks, intelligent network orchestration will be part of 6G networks, and 6G networks will move beyond the new Open Radio Access Network (O-RAN) [129]. O-RAN networks enable network flexibility by supporting techniques such as deep learning, machine learning, and reinforcement learning in AI. Applying AI algorithms to communication technologies is a way to improve spectrum utilization efficiency, reduce communication latency, and enhance security. Thus, the 6G paradigm is viewed as AI-based trust management, which is a promising one capable of delivering trusted and reliable services.

5.1. AI deployment in 6G networks is a double-edged sword

By applying AI to 6G networks, AI can help 6G networks build a flexible, intelligent, and dynamic network architecture. It assists 6G networks in building a secure and stable network environment regarding threat detection, resource allocation, and attack defense. However, while AI benefits 6G networks, some security vulnerabilities in AI will also be reflected in 6G networks with the deployment of AI in 6G networks. Therefore, AI will also bring some security threats to 6G networks, so it is said that the deployment of AI in 6G networks is a double-edged sword [130]. In this section, we will illustrate the application of AI in 6G networks from the aspects of AI facilitating network construction and the security risks brought by AI.

AI facilitates 6G network construction AI can provide a lot of convenience for the construction of 6G networks, which will help us quickly deploy 6G networks and put them into commercial use. AI can assist 6G networks in dynamically allocating network resources, so that limited resources can be reasonably allocated to different network devices. At the same time, AI can also provide personalized services according to user needs, providing users with a better experience. At the same time, AI can also realize the concept of distributed independence, autonomous management, and green communication in the 6G networks and provide a more secure and reliable authentication method for the 6G

networks. We list the contributions made by AI in driving 6G network construction and summarize some related papers in Table 3.

1. Dynamic management

   AI is expected to provide deep-learning-based security function virtualization (SFV) for 6G networks, so as to support the dynamic defense mechanism of Software Defined Security (SDS) architecture using SFV [131]. The mechanism enables intelligent monitoring of network traffic conditions at different network endpoints and segments, timely detection of anomalies and dynamic countermeasures to build an intelligent network management system.
2. Personalized service

   AI can also leverage heterogeneous network resources to provide intelligent personal customization to users by collecting their service needs and preferences. Yang *et al.* [132] proposed the concept of a Service Requirement Zone (SRZ), which is deployed at the users' end to describe and visualize the integrated service requirements and preferences for a single user's specific task. On the system side, the concept of User Satisfaction Rating (USR) is introduced to evaluate the overall service capability of the system to accomplish tasks in various SRZs [133]. We have also proposed a network AI architecture with integrated network resources and leveraging AI capabilities to guarantee the Quality of Experience (QoE) for each user based on the above. It also effectively meets diverse user needs and provides them with customized services.
3. Realization of a distributed independent autonomous system

   Deploying AI's intelligent agents to Base Stations (BSs), makes it possible for AI technology to not only optimize the network but also provide service and application intelligence to users. This means that AI will change the standards for future 6G networks. For example, future 6G networks will need to have self-aggregating capabilities for functional, situational, and location networks. Enhanced context-awareness capabilities, as well as contextual self-reconfiguration of networks and nodes, are also needed [134]. These make AI the driving force of 6G networks, enabling the proliferation of large-scale fog computing clusters driven by distributed independent autonomous systems and related common goals.
4. Authentication

   AI can automatically combine multiple non-cryptographic attributes related to users, resources and environments for determining the identity of a given entity and authorizing it after confirming successful authentication. In this way, continuous authentication and dynamic enforcement of fine-grained access policies are provided. Peng *et al.* in [135] proposed a framework for suspicious person re-recognition based on end-to-end edge devices in real public scenes. Firstly, the image information intercepted from the video is fed into the detector to obtain the pedestrian location information, and then the pedestrian attributes are recognized and re-recognized using Omni-Scale Network (OSNet). Generalized learning systems (BLSs) as well as Cycle-consistent Adversarial Networks (CycleGAN) are also utilized to remove the noisy data and unify the data style. This improves the performance of the identification model.
5. Green communications

   In the future 6G era, the number of basic communication equipment will increase dramatically, and the communication between equipment and the maintenance

Table 3. Summary of papers related to 6G network construction driven by AI

Authors&Years	Ref	Assistance in the management	Enhance network security	Green communications	Improve network architecture	Optimize user experience	Remarks
Rahman *et al.* 2022	[131]	H	M	×	L	×	By studying the security challenges posed by the convergence of operational and information technologies for 6G networks, they proposed a distributed DL-assisted SDS for 6G vertical networks, which will autonomously detect, localize and isolate security threats through SFV.
Yang *et al.* 2022	[132]	M	L	×	H	H	The authors propose SRZ to collect user requirements and preferences and introduce USR to assess the system service capability strength. Finally, a network AI architecture with the ability to integrate network resources and the capability to popularize AI is proposed.
Stoica *et al.* 2019	[134]	H	L	×	M	×	They propose to deploy intelligent agents of AI to base stations, which makes it possible for AI technology to not only optimize the network but also provide service and application intelligence to users.
Peng *et al.* 2023	[135]	×	H	×	×	L	They propose an end-to-end edge device suspicious person re-identification framework based on real public scenarios.
Mao *et al.* 2021	[136]	H	L	H	L	×	They propose to combine DL algorithms or ML algorithms for AI with traditional AI algorithms and mathematical models to reduce the complexity of the algorithms and increase the efficiency of network resource management.
Wu *et al.* 2022	[137]	H	L	×	H	×	This paper presents an AI-native network slicing architecture for 6G networks to enable synergy between AI and network slicing to facilitate intelligent network management and support emerging AI services.
Shafin *et al.* 2020	[138]	H	×	L	M	×	In this work, the authors present a vision of AI cellular networks for 6G networks, which reduces the operational costs as well as the overhead in management and planning for mobile network operators.
Yang *et al.* 2020	[139]	M	L	×	H	L	In this paper, the authors propose an AI-based intelligent architecture for 6G networks, which can realize intelligent resource management, automatic network adjustment and intelligent service issuance.
Letaief *et al.* 2021	[140]	H	M	×	M	L	In this paper, the authors present their vision for scalable and trustworthy edge AI systems through the integrated design of wireless communication strategies and decentralized machine learning models.
Xiao *et al.* 2020	[141]	M	×	×	H	L	The authors present a self-learning architecture based on self-supervised Generative Adversarial Networks (GANs) to demonstrate the potential performance improvements that can be realized through automated data learning at the edge of the network.

H :High Coverage M :Medium Coverage L :Low Coverage × :Not Mentioned

of enormous communication networks will lead to a large amount of energy consumption. It will become an urgent task to promote the research of green communication networks. However, the requirements of 6G on QoS, security, flexibility, and intelligence will become increasingly strict and diversified, which will bring significant challenges to the development of green communication. Today's research in green communication is based on two main ideas: using energy harvesting techniques and combining artificial intelligence algorithms and traditional network management models. Energy harvesting technology refers to the rapid and wide-scale deployment of energy harvesting units such as solar panels and wind turbines to collect and convert various sustainable energy sources into electrical energy for Information and Communication Technology (ICT) devices [142]. Another idea is to combine AI's DL algorithm or ML algorithm with traditional AI algorithms and mathematical models, applying them in the management of 6G networks to reduce the complexity of the algorithms and improve the efficiency of network resource management [136].

Security Issues in the Combination of AI and 6G Artificial intelligence refers to systems and machines that can mimic humans to perform tasks and iteratively improve themselves based on the information collected. Today, AI has become a ubiquitous term, many applications that can automatically perform complex tasks can be called AI. The application of AI in 6G networks will contribute to the optimization and design of architectures, protocols, and operations. Therefore, AI is of great interest in the development of 6G networks [143]. AI can adaptively adjust some models and architectures through a large amount of data training. Since 6G networks will face a large amount of data transmission and various architectural models, it is unrealistic to configure, monitor, and repair them manually. Therefore, 6G is in need of AI, which can help it achieve "intelligent endogenous" [144]. The application of AI in 6G networks will face many security issues [145]. We list some cybersecurity issues AI brings to 6G networks in Table 4 and provide some possible solutions.

1. Malicious samples

   Just because AI needs to collect a large amount of data for training, many attackers will attack 6G networks from this point. For example, an attacker may lure the AI to obtain malicious samples that are deliberately prepared(e.g., manipulating labeled data and weak labeling) for training. Then, the training data can then be tampered with to affect the learning results, leading to wrong classification and regression results. The attacker focuses on interfering with the learning algorithm and the learning logic. They can attack the agent model in the distributed learning model, manipulate the partial model parameters through malicious agents, and thus corrupt the global model. The principle of this attack method is shown in Figure 13:

   Barreno *et al.* [146] proposed a Rejection Of Negative Impact (RONI) method, which is used to detect whether the training samples are malicious. They first trained a classifier on a base training set, then added the training samples to be detected to the training set, and subsequently trained a second classifier on the training set used for comparison. They apply both classifiers to the same set of instances with known labels and compare the accuracy difference between them. The samples can be considered harmful if the first classifier produces more classification errors. Li *et*

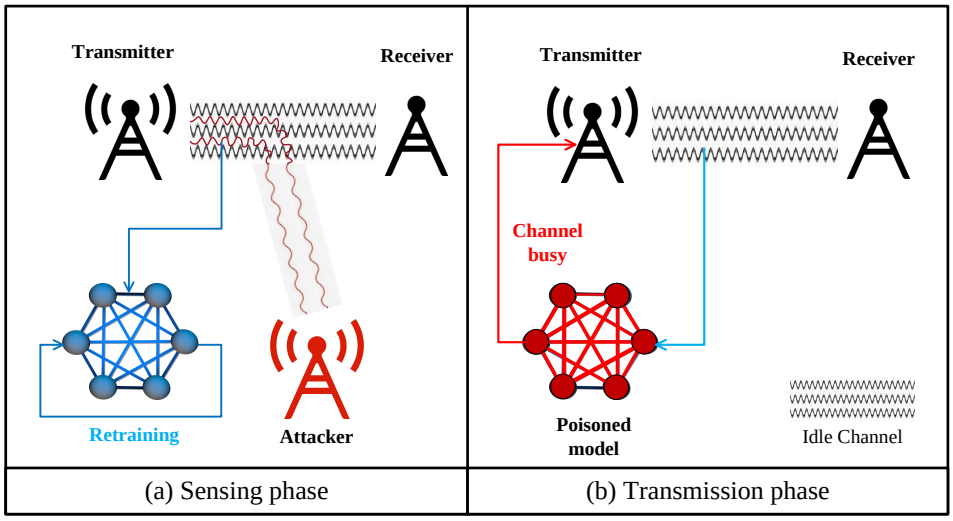

Fig. 13. The principle of malicious samples attack

al. [147] proposed a homomorphic encryption scheme with ciphertext comparison to secure machine learning training and classification.

2. Attacks based on AI

   AI can have the ability to make network-wide intelligent decisions with a distributed edge-based architecture. Attackers can discover vulnerabilities in the network by revealing patterns in large amounts of data at different levels (smart radio, edge, cloud) through an artificial intelligence-based approach. For example, AI can learn the vulnerable IoT device, compromise it, gain control of it, and subsequently launch a DDoS attack on a critical node [148].

   The solution to this AI-based attack is to use AI to train a more complete and more secure defense system by distributed intelligence. The moving target defense technique proposed by Cho *et al.* [149] is a proactive measure. It is an approach that invokes dynamism for 6G networks, thus weakening the learning speed and the learning level of AI attackers. Biamonte *et al.* [150] proposes that quantum machine learning can also design advanced defense techniques to defend against AI attacks.

3. Backdoor attack

   This type of attack generally does not affect the accuracy of the main task. A backdoor is first inserted into the AI model, or a malicious task is injected. The backdoor attack is triggered once a set event or a specific condition is triggered during the normal training process. These attacks are difficult to detect and can spoof ML models with high confidence [151].

   Aramoon *et al.* [152] introduced the concept of meta-federated learning, a new federated learning framework that facilitates the defense against backdoor attacks and the protection of user privacy. They also showed that shifting the defense execution point from a single update level to an aggregation level can effectively mitigate the impact of backdoor attacks without violating user privacy. A previous study by Liu *et al.* [153] showed that pruning and fine-tuning are two effective ways to defend

against backdoor attacks, while in later research, the combination of pruning and fine-tuning was evaluated and shown experimentally to be effective in removing or even eliminating backdoor attacks.

Table 4. Security threats raised by AI in 6G networks and possible solutions

Security threats	Possible solutions		
	Authors&Year	**Ref**	**Remarks**
Malicious samples	Barreno *et al.* 2010	[146]	The authors propose a Rejection of Negative Influence (RONI) method, which is used to detect whether a training sample is malicious or not.
	Li *et al.* 2020	[147]	The authors propose a homomorphic encryption scheme with ciphertext comparison to secure machine learning training and classification.
AI based attacks	Cho *et al.* 2020	[149]	In this paper, the authors propose a moving target defense technique to cripple the learning speed as well as the learning level of an AI attacker.
	Biamonte *et al.* 2017	[150]	The authors propose to design advanced defense techniques through quantum machine learning to defend against AI attacks.
Backdoor attacks	Aramoon *et al.* 2021	[152]	The authors propose a meta-federation learning framework that facilitates defense against backdoor attacks.
	Liu *et al.* 2018	[153]	The combination of pruning and fine-tuning is evaluated and experimentally shown to remove or eliminate backdoor attacks effectively.
Attacks against AI algorithms	Karimireddy *et al.* 2020	[154]	A SCAFFOLD algorithm is proposed, which utilizes the similarity of client data to enable the model to converge faster.
	Babaeer *et al.* 2020	[155]	The authors propose a lightweight security approach based on threshold-sensitive energy-efficient sensor network protocols and watermarking techniques to ensure the integrity and authenticity of sensed data.
	Fang *et al.* 2020	[156]	A lightweight encryption protocol is designed, and a new efficient federated learning scheme with strong privacy protection in cloud computing is proposed.

4. Attacks against AI algorithms

Aggregation algorithms orchestrate AI training models in a centralized or peer-to-peer setup. Attacks against these algorithms are typically carried out either through the aggregator or by altering the algorithmic parameters. And the system's integrity will be compromised in the event of a successful attack [151]. First, in terms of aggregators, when suffering from attacks such as data poisoning or model poisoning, non-

robust aggregators will produce compromised models. As a result, the training results will be affected. In terms of parameters, the attacker may manipulate parameters such as learning rate, batch size, among others, through some compromised clients, thus forcing the global model convergence to fail or the model's training process to be terminated.

For the problem of malicious parameter modification leading to non-convergence or slow convergence of the global model, Karimireddy *et al.* [154] proposed a SCAFFOLD algorithm that utilizes the similarity of the client's data to enable the model to converge faster. As for how to solve the problem of tampering with algorithm parameters, Babaeer *et al.* [155] proposed a lightweight security method based on threshold-sensitive energy-efficient sensor network protocols and watermarking techniques, which employs Homomorphic Encryption (HE) to ensure the integrity and authenticity of the sensed data sent from the sensor nodes to the base station. Moreover, this method also detects if the data has been tampered with. Fang *et al.* also designed a lightweight encryption protocol and proposed a new efficient federated learning scheme with solid privacy preservation in cloud computing [156], which is used to prevent the risk of model parameters shared directly between cloud servers and clients from being used for model inversion attacks. The scheme also employs an efficient optimization strategy to improve training efficiency.

5.2. AI assists 6G networks in addressing security threats

In the third part of this work, we analyze the security issues of 6G networks in terms of network architecture, network requirements, and different application areas. Meanwhile, in the fourth part, we analyze the security issues and corresponding solutions of other technologies applied in 6G networks. These two sections give us a preliminary understanding of the security threats in 6G networks. In this section, we analyze the perspectives from which AI assists 6G networks in addressing security threats. As depicted in Table 5, We list examples of AI assisting 6G networks to address security threats.

Security issues on edge networks The development of IoT, 6G networks, and autonomous driving is driving the emergence of more and more connected end devices. However, due to these devices' limited communication and computing resources, they are vulnerable to malicious attacks by intruders. Thereby gaining control of these end devices, leading to DDoS attacks on the devices. This, in turn, generates a large number of computation and processing tasks, exhausting the resources of edge servers [157]. With location-based services becoming more common, the risk of location privacy breaches is increasing [57]. Emerging network services such as telemedicine, teleconferencing, and remote construction realize real-time, remote, and convenient control and management. However, these remote control operations are susceptible to malware attacks. Once the manipulation right is intercepted by malware, it will not only lead to the leakage of a large amount of private information, but also the deprivation of the control of the computation part of the terminal devices and edge servers [158]. This leads to unauthorized computing tasks, resulting in the loss of many resources. Some hackers also provide spurious data to edge servers. As the AI model collects data for training, it enters inside the model and disrupts the AI training process [159]. This leads to a reduction in the accuracy of the training or makes

the training proceed in the wrong direction. It even leads to the failure of the entire training process, ultimately leading to the degradation of the network performance of the edge server [160].

For the above scenario of 6G networks subject to malicious attacks on edge servers, Lovén *et al.* [161] proposed that AI can be used to build machine learning models at the edge based on large amounts of real-time data on system control and application execution. Service deployment for IoT applications in Mobile Edge Computing (MEC) environments is a key problem to be solved. Considering the knowledge of mobile users' service requests and the processing power of edge servers, the microservice deployment problem in the MEC environment can be modeled as a nonlinear optimization problem. Tang *et al.* proposed an adaptive dynamic deployment optimization method, Adapt-SD [162], based on Adam and weighted round-robin scheduling algorithms, to solve the microservice deployment problem. The edge-native AI approach provides ideas for solving security problems on 6G edge networks and optimizes the execution of edge applications. It also improves the network's connectivity, reactivity, adaptability, and proactivity.

Physical security protection Physical security in 6G networks mainly reflects security issues on IoT, since the commissioning of the future 6G network requires many IoT devices as support. The security problem of communication between these devices becomes an essential threat to constructing a secure and stable network environment. There are many kinds of common physical attacks, such as the capture of sensor devices mentioned in [172,173]. The attacker obtains access to the sensor device and then uses the captured device to attack the whole network and cause significant damage. Another example is the physical attacks on network devices mentioned in [93,174], where the attacker damages the network devices by artificial physical means, thus affecting the normal operation of the communication network. There are also attacks that obtain control of devices by forging identities, which threaten network security [175].

For the abovementioned attacks against IoT physical devices, one can first consider deploying symmetric encryption systems [163,164] or asymmetric encryption systems [165] in IoT environments to prevent devices from being intruded or data from being tampered with. Communication between two IoT devices or nodes via key and encryption/decryption mechanisms can also be considered, thus avoiding eavesdropping on the communication or interruption of the communication process. Based on the above ideas, AI can provide better learning and adaptive capabilities for these safeguards and integrate new technologies to enhance the security-based of these technologies.

Autonomous mechanisms for addressing security risks For 6G networks, which are substantial communication networks, it is unrealistic to manually monitor each device's status in real-time, detect anomalies, and make timely responses. However, we can use AI to monitor device status and detect security threats and then adaptively take countermeasures, such as dynamically adjusting the network configuration or security authentication model to defend against security threats.

Shen *et al.* proposed an AI-based 6G network architecture whose core network consists of SDN [166]. Operational data is collected by emulating the virtualized network infrastructure. The AI learns from the collected data and determines appropriate network

Table 5. AI's contribution to solving 6G cybersecurity problems

Contributions	Examples		
	Authors&Year	**Ref**	**Remarks**
Assist 6G in solving security problems on edge networks	Lovén *et al.* 2019	[161]	The authors propose that AI can build machine learning models on edge networks based on large amounts of real-time system control and application execution data.
Assistance in responding to physical attacks	Jawad *et al.* 2019	[163]	Deploying symmetric encryption systems in IoT environments to prevent device intrusion or data tampering.
	Alotaibi *et al.* 2018	[164]	
	Alaya *et al.* 2021	[165]	The authors propose to deploy asymmetric encryption systems on physical devices to prevent devices from being compromised.
Provide autonomous mechanism to address security risks	Shen *et al.* 2021	[166]	An AI-based 6G network architecture is proposed, where the AI learns from the simulation data to realize intelligent resource scheduling and security configuration management and then realizes dynamic adjustment to external influences.
	Fang *et al.* 2022	[167]	This article introduces autonomous collaborative authentication and proposes a collaborative authentication scheme with privacy preservation based on federated learning.
	Xiao *et al.* 2019	[168]	The authors propose RL-based intelligent beamforming techniques to provide optimal beamforming strategies against eavesdropper attacks in VLC systems.
Future security risk forecasting	Husák *et al.* 2018	[169]	The authors propose that deep learning-based attack prediction methods are promising for malicious behavior detection.
	Tariq *et al.* 2020	[170]	The authors propose that the combination of future 6G networks with AI has the potential to realize the concept of cognitive radio. And by storing behavioral data about the environment, AI can be used to predict suspicious activities of malicious nodes.
	Zhang *et al.* 2021	[171]	This paper proposes the need to investigate intelligent and flexible security mechanisms to deal with different forms of security threats.

management policies for intelligent resource scheduling and security configuration management. In turn, it realizes dynamic adjustment to external influences. Due to the complex heterogeneous networks in 6G and the distributed nature of the devices and information involved, entities in 6G networks are susceptible to privacy leakage. Fang *et al.* [167] introduced autonomous collaborative authentication and proposed a federated learning-

based collaborative authentication scheme with privacy-preserving features. The scheme analyzes the heterogeneous information of the authenticated devices and then updates the respective authentication models locally. Then, the corresponding authentication model is used to realize privacy protection. In VLC systems for 6G networks, intelligent beamforming techniques based on Reinforcement Learning (RL) provide optimal beamforming strategies against eavesdropper attacks [168].

Future security risk projections In the future, we may face various cyber attacks in 6G networks, and they may use different methods to launch attacks from different angles. We need to detect these attacks in advance to address these security threats better and minimize the loss of benefits. We must also anticipate future security risks as attackers may change their attack methods. By detecting security threats and predicting security risks in advance, we can take countermeasures to increase the success rate of defending against cyberattacks.

In complex 6G network environments, many network parameters and states are in constant flux, which increases the difficulty of predicting risks. However, deep learning-based attack prediction methods in this changing environment are promising for malicious behavior detection [169]. Tariq *et al.* [170] also suggested that the combination of future 6G networks with AI has the potential to realize the concept of cognitive radio proposed by Mitola *et al.* in 1999. It is also argued that 6G Mitola radios will also store behavioral data of the environment so that suspicious activities of malicious nodes can be predicted through AI. We must study intelligent and flexible security mechanisms to predict, detect, mitigate, and prevent security attacks to cope with different security threats. Thus, the propagation of such vulnerabilities in 6G networks can be limited [171].

6. Concluding Remarks and Outlook

As a next-generation mobile communication technology, 6G network, based on 5G communication technology, will span the connection between people and people and the connection between people and things and eventually move towards the smart relationship of everything, allowing intelligence to be reflected in all areas of society and bringing a new face to human society. However, the large-scale use of 6G networks and their application in new fields will also make their safety challenging.

This work analyzed and discussed the security issues surrounding 6G networks and their applications. By reviewing relevant research articles, this paper introduced the development process of mobile communication technology and discussed the research motivation of 6G networks. This paper also compared the key performance index differences between 5G networks and 6G networks and analyzed the key technologies of 6G networks. This work examined the security of 6G architecture regarding network access, network domain, user domain, and application domain. Thus, this work also compared the three significant visions of 5G and 6G and summarized the security threats in the 6G visions. Security issues of 6G applications in areas such as UAV mobile communication, Smart Grid 2.0, and Industrial 5.0 were also analyzed, listing the applications of terahertz communication, visible light communication, and blockchain technology in 6G. For the above applications, we analyzed some security issues and selected the corresponding solutions proposed in recent research articles. The RONI method for detecting malicious samples,

the WBPLSec method for protecting visible light communication, and the context-based multi-factor biometric authentication algorithm mentioned in this paper all provided effective ideas for solving the security problems of 6G networks. We also introduced the application of AI to the issue of 6G network security. Firstly, we illustrated the impact of AI on 6G networks from two aspects: AI promotes the construction of 6G networks, and AI brings cyber risks to 6G networks, and we demonstrated that AI can assist 6G networks in solving security threats from four perspectives.

Because 6G networks cover a wide range of areas and have a complex architecture, much work remains to be done on 6G network security. Network attacks in the future will become increasingly sophisticated, such as the one mentioned in this work, which uses AI to carry out attacks. This requires defenders to research more comprehensive and complete solutions to address such security threats. In terms of artificial intelligence, we hope to propose more effective detection methods for malicious sample detection. In terms of terahertz technology, we hope to take measures to deal with the problem of signal interference. In blockchain technology, we hope to use the distributed ledger mechanism and smart contracts to make corresponding improvements in privacy and security protection measures. In future directions, we will conduct more in-depth research on the security problems of 6G networks in blockchain and AI, and we expect to contribute to the research of 6G network security by collecting information and conducting simulation experiments by profoundly analyzing the security risks and proposing the corresponding countermeasures.

Acknowledgment

This work was partially supported by the National Key Research and Development Program of China under Grant 2021YFA1000600, the National Natural Science Foundation of China under Grant 62072170, the Science and Technology Project of the Department of Communications of Hunan Provincial under Grant 202101, the Key Research and Development Program of Hunan Province under Grant 2022GK2015, and the Hunan Provincial Natural Science Foundation of China under Grant 2021JJ30141. The co-author Muhammad Khurram Khan is supported by King Saud University, Riyadh, Saudi Arabia, under project number (RSP2024R12).

References

1. Qi Bi. Ten trends in the cellular industry and an outlook on 6g. *IEEE Communications Magazine*, 57(12):31–36, 2019.
2. Reeya Agrawal. Comparison of different mobile wireless technology (from 0g to 6g). *ECS Transactions*, 107(1):4799, 2022.
3. AFM Shahen Shah, Ahmed Nidham Qasim, Muhammet Ali Karabulut, Haci Ilhan, and Md Baharul Islam. Survey and performance evaluation of multiple access schemes for next-generation wireless communication systems. *IEEE Access*, 9:113428–113442, 2021.
4. Jessica Moysen and Lorenza Giupponi. From 4g to 5g: Self-organized network management meets machine learning. *Computer Communications*, 129:248–268, 2018.
5. Joyce Ayoola Adebusola, Adebiyi Ayodele Ariyo, Okeyinka Aderemi Elisha, Adebiyi Marion Olubunmi, and Okesola Olatunji Julius. An overview of 5g technology. In *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, pages 1–4. IEEE, 2020.

6. Klaus David and Hendrik Berndt. 6g vision and requirements: Is there any need for beyond 5g? *IEEE vehicular technology magazine*, 13(3):72–80, 2018.
7. Karthik Kumar Vaigandla, Nilofar Azmi, Ramya Podila, and Radha Krishna Karne. A survey on wireless communications: 6g and 7g. *International Journal Of Science, Technology & Management*, 2(6):2018–2025, 2021.
8. Matti Latva-aho, Kari Leppänen, Federico Clazzer, and Andrea Munari. Key drivers and research challenges for 6g ubiquitous wireless intelligence. 2020.
9. Zihang Song, Yue Gao, and Rahim Tafazolli. A survey on spectrum sensing and learning technologies for 6g. *IEICE Transactions on Communications*, 104(10):1207–1216, 2021.
10. Choongil Yeh, Gweon Do Jo, Young-Jo Ko, and Hyun Kyu Chung. Perspectives on 6g wireless communications. *ICT Express*, 9(1):82–91, 2023.
11. Muhammad Waseem Akhtar, Syed Ali Hassan, Rizwan Ghaffar, Haejoon Jung, Sahil Garg, and M Shamim Hossain. The shift to 6g communications: vision and requirements. *Human-centric Computing and Information Sciences*, 10:1–27, 2020.
12. Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila. Ai and 6g security: Opportunities and challenges. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pages 616–621. IEEE, 2021.
13. Zisang Xu, Wei Liang, Kuan-Ching Li, Jianbo Xu, Albert Y Zomaya, and Jixin Zhang. A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0. *IEEE Transactions on Industrial Informatics*, 18(10):7118–7127, 2021.
14. Dinh C Nguyen, Ming Ding, Pubudu N Pathirana, Aruna Seneviratne, Jun Li, Dusit Niyato, Octavia Dobre, and H Vincent Poor. 6g internet of things: A comprehensive survey. *IEEE Internet of Things Journal*, 9(1):359–383, 2021.
15. Chengxiao Liu, Wei Feng, Yunfei Chen, Cheng-Xiang Wang, and Ning Ge. Cell-free satellite-uav networks for 6g wide-area internet of things. *IEEE Journal on Selected Areas in Communications*, 39(4):1116–1131, 2020.
16. Y Li, Wei Liang, K Xie, D Zhang, S Xie, and KC Li. Lightnestle: quick and accurate neural sequential tensor completion via meta learning. In *IEEE Infocom*, 2023.
17. José A del Peral-Rosado, Ronald Raulefs, José A López-Salcedo, and Gonzalo Seco-Granados. Survey of cellular mobile radio localization methods: From 1g to 5g. *IEEE Communications Surveys & Tutorials*, 20(2):1124–1148, 2017.
18. Rani P Tidke, Pritee S Uttarwar, Deepak S Dandwate, and Umesh J Tupe. A literature review on: Wireless technologies from 0g to 7g. *IRE Journals*, 4(6):59–64, 2020.
19. AFM Shahen Shah. A survey from 1g to 5g including the advent of 6g: Architectures, multiple access techniques, and emerging technologies. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1117–1123. IEEE, 2022.
20. Mamta Agiwal, Hyeyeon Kwon, Seungkeun Park, and Hu Jin. A survey on 4g-5g dual connectivity: road to 5g implementation. *Ieee Access*, 9:16193–16210, 2021.
21. Wan Siti Halimatul Munirah Wan Ahmad, Nurul Asyikin Mohamed Radzi, FS Samidi, Aiman Ismail, Fairuz Abdullah, Md Zaini Jamaludin, and MohdNasim Zakaria. 5g technology: Towards dynamic spectrum sharing using cognitive radio networks. *IEEE access*, 8:14460–14488, 2020.
22. Peter Backeman, Ashalatha Kunnappilly, and Cristina Seceleanu. Supporting 5g service orchestration with formal verification. *Computer Science and Information Systems*, 20(1):329–357, 2023.
23. Anutusha Dogra, Rakesh Kumar Jha, and Shubha Jain. A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies. *IEEE Access*, 9:67512–67547, 2020.
24. Samer Henry, Ahmed Alsohaily, and Elvino S Sousa. 5g is real: Evaluating the compliance of the 3gpp 5g new radio system with the itu imt-2020 requirements. *IEEE Access*, 8:42828–42840, 2020.

25. Karen Campbell, Jim Diffley, Bob Flanagan, Bill Morelli, Brendan O'Neil, Francis Sideco, et al. The 5g economy: How 5g technology will contribute to the global economy. *IHS economics and IHS technology*, 4(16):1, 2017.
26. IIMT Union. Imt traffic estimates for the years 2020 to 2030. *Report ITU*, 2370, 2015.
27. Wei Jiang, Bin Han, Mohammad Asif Habibi, and Hans Dieter Schotten. The road towards 6g: A comprehensive survey. *IEEE Open Journal of the Communications Society*, 2:334–366, 2021.
28. Wei Liang, Yang Yang, Ce Yang, Yonghua Hu, Songyou Xie, Kuan-Ching Li, and Jiannong Cao. Pdpchain: A consortium blockchain-based privacy protection scheme for personal data. *IEEE Transactions on Reliability*, 2022.
29. Wei Liang, Dafang Zhang, Xia Lei, Mingdong Tang, Kuan-Ching Li, and Albert Y Zomaya. Circuit copyright blockchain: blockchain-based homomorphic encryption for ip circuit protection. *IEEE Transactions on Emerging Topics in Computing*, 9(3):1410–1420, 2020.
30. Ying Long, Yinyan Gong, Weihong Huang, Jiahong Cai, Nengxiang Xu, and Kuan-ching Li. Cryptography of blockchain. In *Smart Computing and Communication: 7th International Conference, SmartCom 2022, New York City, NY, USA, November 18–20, 2022, Proceedings*, pages 340–349. Springer, 2023.
31. Hui Chen, Hadi Sarieddeen, Tarig Ballal, Henk Wymeersch, Mohamed-Slim Alouini, and Tareq Y Al-Naffouri. A tutorial on terahertz-band localization for 6g communication systems. *IEEE Communications Surveys & Tutorials*, 2022.
32. Wei Liang, Yuhui Li, Jianlong Xu, Zheng Qin, Dafang Zhang, and Kuan-Ching Li. Qos prediction and adversarial attack protection for distributed services under dlaas. *IEEE Transactions on Computers*, 2023.
33. Qiannan Zhang, Huafeng Wu, Xiaojun Mei, Dezhi Han, Mario Donato Marino, Kuan-Ching Li, and Song Guo. A sparse sensor placement strategy based on information entropy and data reconstruction for ocean monitoring. *IEEE Internet of Things Journal*, 2023.
34. Gang Dong, Lin Pan, Yi Zhang, and Yanan Liu. Air-space-ground integrated information network: Technology, development and prospect. In *Signal and Information Processing, Networking and Computers: Proceedings of the 8th International Conference on Signal and Information Processing, Networking and Computers (ICSINC)*, pages 883–891. Springer, 2022.
35. Wei Liang, Zuoting Ning, Songyou Xie, Yupeng Hu, Shaofei Lu, and Dafang Zhang. Secure fusion approach for the internet of things in smart autonomous multi-robot systems. *Information Sciences*, 579:468–482, 2021.
36. Nan Chi, Yingjun Zhou, Yiran Wei, and Fangchen Hu. Visible light communication in 6g: Advances, challenges, and prospects. *IEEE Vehicular Technology Magazine*, 15(4):93–102, 2020.
37. Yiying Wang, Xin Kang, Tieyan Li, Haiguang Wang, Cheng-Kang Chu, and Zhongding Lei. Six-trust for 6g: Towards a secure and trustworthy 6g network. *arXiv preprint arXiv:2210.17291*, 2022.
38. Wei Liang, Songyou Xie, Dafang Zhang, Xiong Li, and Kuan-ching Li. A mutual security authentication method for rfid-puf circuit based on deep learning. *ACM Transactions on Internet Technology (TOIT)*, 22(2):1–20, 2021.
39. Zhen Sun, Liyuan Song, Qin Huang, Liuguo Yin, Guilu Long, Jianhua Lu, and Lajos Hanzo. Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design. *IEEE Transactions on Communications*, 68(9):5778–5792, 2020.
40. Jawad Tanveer, Amir Haider, Rashid Ali, and Ajung Kim. Machine learning for physical layer in 5g and beyond wireless networks: A survey. *Electronics*, 11(1):121, 2022.
41. Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, and Wanlei Zhou. Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, 6(3):281–291, 2020.

42. Gao Mine, Jiao Hai, Luo Jin, and Zhou Huiying. A design of sd-wan-oriented wide area network access. In *2020 International Conference on Computer Communication and Network Security (CCNS)*, pages 174–177. IEEE, 2020.
43. Osama A Khashan, Rami Ahmad, and Nour M Khafajah. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, 115:102448, 2021.
44. Yahya M Al-Moliki, Mohammed T Alresheedi, Yahya Al-Harthi, and Ali H Alqahtani. Robust lightweight-channel-independent ofdm-based encryption method for vlc-iot networks. *IEEE Internet of Things Journal*, 9(6):4661–4676, 2021.
45. Ghada Arfaoui, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, Håkan Englund, Edith Félix, Felix Klaedtke, Prajwol Kumar Nakarmi, Mats Näslund, Piers O'Hanlon, et al. A security architecture for 5g networks. *IEEE access*, 6:22466–22479, 2018.
46. Abbas Yazdinejad, Reza M Parizi, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo. An energy-efficient sdn controller architecture for iot networks with blockchain-based security. *IEEE Transactions on Services Computing*, 13(4):625–638, 2020.
47. Chun-Yu Liu, Shanq-Jang Ruan, Yu-Ren Lai, and Chih-Yuan Yao. Finger-vein as a biometric-based authentication. *IEEE Consumer Electronics Magazine*, 8(6):29–34, 2019.
48. Wei Liang, Yuhui Li, Kun Xie, Dafang Zhang, Kuan-Ching Li, Alireza Souri, and Keqin Li. Spatial-temporal aware inductive graph neural network for c-its data recovery. *IEEE Transactions on Intelligent Transportation Systems*, 2022.
49. Sushanta Sengupta. A secured biometric-based authentication scheme in iot-based patient monitoring system. In *Emerging Technology in Modelling and Graphics: Proceedings of IEM Graph 2018*, pages 501–518. Springer, 2020.
50. Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong. A survey on security aspects for 3gpp 5g networks. *IEEE communications surveys & tutorials*, 22(1):170–195, 2019.
51. Yanrong Lu and Dawei Zhao. Providing impersonation resistance for biometric-based authentication scheme in mobile cloud computing service. *Computer Communications*, 182:22–30, 2022.
52. Jing Long, Wei Liang, Kuan-Ching Li, Yehua Wei, and Mario Donato Marino. A regularized cross-layer ladder network for intrusion detection in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 19(2):1747–1755, 2022.
53. Shimaa A Abdel Hakeem, Hanan H Hussein, and HyungWon Kim. Security requirements and challenges of 6g technologies and applications. *Sensors*, 22(5):1969, 2022.
54. Muhammad Sajjad Akbar, Zawar Hussain, Quan Z Sheng, and Subhas Mukhopadhyay. 6g survey on challenges, requirements, applications, key enabling technologies, use cases, ai integration issues and security aspects. *arXiv preprint arXiv:2206.00868*, 2022.
55. Keyvan Ramezanpour and Jithin Jagannath. Intelligent zero trust architecture for 5g/6g networks: Principles, challenges, and the role of machine learning in the context of o-ran. *Computer Networks*, page 109358, 2022.
56. Sulaiman Khan, Anwar Hussain, Shah Nazir, Fazlullah Khan, Ammar Oad, and Mohammad Dahman Alshehri. Efficient and reliable hybrid deep learning-enabled model for congestion control in 5g/6g networks. *Computer Communications*, 182:31–40, 2022.
57. Shiwen Zhang, Biao Hu, Wei Liang, Kuan-Ching Li, and Brij B Gupta. A caching-based dual k-anonymous location privacy-preserving scheme for edge computing. *IEEE Internet of Things Journal*, 2023.
58. Van-Linh Nguyen, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Ying-Dar Lin. Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, 23(4):2384–2428, 2021.
59. Zisang Xu, Wei Liang, Kuan-Ching Li, Jianbo Xu, and Hai Jin. A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. *Journal of Parallel and Distributed Computing*, 149:29–39, 2021.

60. Wei Liang, Songyou Xie, Jing Long, Kuan-Ching Li, Dafang Zhang, and Keqin Li. A double puf-based rfid identity authentication protocol in service-centric internet of things environments. *Information Sciences*, 503:129–147, 2019.
61. Shiwen Zhang, Ziwei Yan, Wei Liang, Kuan-Ching Li, and Ciprian Dobre. Baka: Biometric authentication and key agreement scheme based on fuzzy extractor for wireless body area networks. *IEEE Internet of Things Journal*, 2023.
62. Mehdi Rasti, Shiva Kazemi Taskou, Hina Tabassum, and Ekram Hossain. Evolution toward 6g multi-band wireless networks: A resource management perspective. *IEEE Wireless Communications*, 29(4):118–125, 2022.
63. Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Livanage, and Mika Ylianttila. 6g security challenges and potential solutions. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pages 622–627. IEEE, 2021.
64. Naijian Zhang, Qi Jiang, Long Li, Xindi Ma, and Jianfeng Ma. An efficient three-factor remote user authentication protocol based on bpv-fourq for internet of drones. *Peer-to-Peer Networking and Applications*, 14:3319–3332, 2021.
65. Kan Yu, Jiguo Yu, and Anming Dong. Cooperative communication and mobility for securing urllc of future wireless networks. *IEEE Transactions on Vehicular Technology*, 71(5):5331–5342, 2022.
66. Zhengyu Zhu, Gengwang Hou, Zheng Chu, Xingwang Li, Gangcan Sun, Wanming Hao, and Paramjit S Sehdev. Research and analysis of urllc technology based on artificial intelligence. *IEEE Communications Standards Magazine*, 5(2):37–43, 2021.
67. IMT CAICT. Promotion group, 5g security report. *The China Academy of Information and Communications Technology (CAICT) and IMT*, 2020.
68. Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101:55–82, 2018.
69. Ding Wang and Ping Wang. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE transactions on dependable and secure computing*, 15(4):708–722, 2016.
70. Marco Lourenco, Louis Marinos, and Lampros Patseas. Enisa threat landscape for 5g networks. In *Proc. Eur. Union Agency Cybersecurity (ENISA)*, page 87, 2019.
71. Najib Ahmed Mohammed, Ali Mohammed Mansoor, and Rodina Binti Ahmad. Mission-critical machine-type communication: An overview and perspectives towards 5g. *IEEE Access*, 7:127198–127216, 2019.
72. Cosmas Ifeanyi Nwakanma, Alifia Putri Anantha, Fabliha Bushra Islam, Jae-Min Lee, and Dong-Seong Kim. 3gpp release-16 for industrial internet of things and mission critical communications. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 403–406. IEEE, 2020.
73. Dakhaz Mustafa Abdullah and Siddeeq Y Ameen. Enhanced mobile broadband (embb): A review. *Journal of Information Technology and Informatics*, 1(1):13–19, 2021.
74. Zhenyu Na, Yue Liu, Jingcheng Shi, Chungang Liu, and Zihe Gao. Uav-supported clustered noma for 6g-enabled internet of things: Trajectory planning and resource allocation. *IEEE Internet of Things Journal*, 8(20):15041–15048, 2020.
75. Xiaohu You, Cheng-Xiang Wang, Jie Huang, Xiqi Gao, Zaichen Zhang, Mao Wang, Yongming Huang, Chuan Zhang, Yanxiang Jiang, Jiaheng Wang, et al. Towards 6g wireless communication networks: Vision, enabling technologies, and new paradigm shifts. *Science China Information Sciences*, 64:1–74, 2021.
76. Helga E Melcherts. The internet of everything and beyond: the interplay between things and humans. *Human bond communication: the holy grail of holistic communication and immersive experience*, pages 173–185, 2017.

77. Lijun Xiao, Wei Liang, Jiahong Cai, Ming Wang, Jiahong Xiao, Yinyan Gong, and Weigang Zhang. An efficiency control strategy of dual-motor multi-gear drive algorithm. *Connection Science*, 35(1):2249264, 2023.
78. Chunyan Diao, Dafang Zhang, Wei Liang, Kuan-Ching Li, Yujie Hong, and Jean-Luc Gaudiot. A novel spatial-temporal multi-scale alignment graph neural network security model for vehicles prediction. *IEEE Transactions on Intelligent Transportation Systems*, 24(1):904–914, 2022.
79. Yinyan Gong, Kuanching Li, Lijun Xiao, Jiahong Cai, Jiahong Xiao, Wei Liang, and Muhammad Khurram Khan. Vaserp: an adaptive, lightweight, secure, and efficient rfid-based authentication scheme for iov. *Sensors*, 23(11):5198, 2023.
80. Rakesh Shrestha, Rojeena Bajracharya, and Shiho Kim. 6g enabled unmanned aerial vehicle traffic management: A perspective. *IEEE Access*, 9:91119–91136, 2021.
81. Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P Lauf, Lanier Watkins, William H Robinson, and Wlajimir Alexis. Securing commercial wifi-based uavs from common security attacks. In *MILCOM 2016-2016 IEEE Military Communications Conference*, pages 1213–1218. IEEE, 2016.
82. Shurui Wang, Aifeng Song, and Yufeng Qian. Predicting smart cities' electricity demands using k-means clustering algorithm in smart grid. *Computer Science and Information Systems*, (00):13–13, 2023.
83. Foysal Ilahi, Shaswata Dutta, Md Mehedi Hasan, Sadia Afrin Rumpa, and AKM Baki. Development of a novel uwb antenna for 6g-iot based smart grid device monitoring system. In *2021 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, pages 1–5. IEEE, 2021.
84. Muhammad Tariq, Mansoor Ali, Faisal Naeem, and H Vincent Poor. Vulnerability assessment of 6g-enabled smart grid cyber–physical systems. *IEEE internet of things journal*, 8(7):5468–5475, 2020.
85. Xin Xu, Guangli Zhu, Houyue Wu, Shunxiang Zhang, and Kuan-Ching Li. See-3d: Sentiment-driven emotion-cause pair extraction based on 3d-cnn. *Computer Science and Information Systems*, 20(1):77–93, 2023.
86. Sabuzima Nayak and Ripon Patgiri. A vision on intelligent medical service for emergency on 5g and 6g communication era. *EAI Endorsed Transactions on Internet of Things*, 6(22), 2020.
87. Wenkang Liu, Yuxuan He, Xiaoliang Wang, Ziming Duan, Wei Liang, and Yuzhen Liu. Bfg: privacy protection framework for internet of medical things based on blockchain and federated learning. *Connection Science*, 35(1):2199951, 2023.
88. Jianqiang Hu, Wei Liang, Osama Hosam, Meng-Yen Hsieh, and Xin Su. 5gss: a framework for 5g-secure-smart healthcare monitoring. *Connection Science*, 34(1):139–161, 2022.
89. Jiatao Li, Dezhi Han, Zhongdai Wu, Junxiang Wang, Kuan-Ching Li, and Arcangelo Castiglione. A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control. *Future Generation Computer Systems*, 142:195–211, 2023.
90. Lingwei Xu, Xinpeng Zhou, Ye Tao, Xu Yu, Miao Yu, and Fazlullah Khan. Af relaying secrecy performance prediction for 6g mobile communication networks in industry 5.0. *IEEE Transactions on Industrial Informatics*, 18(8):5485–5493, 2021.
91. Lijun Xiao, Dezhi Han, Ce Yang, Jiahong Cai, Wei Liang, and Kuan-Ching Li. Ts-dp:an efficient data processing algorithm for distribution digital twin grid for industry 5.0. *IEEE Transactions on Consumer Electronics*, pages 1–1, 2023.
92. Jamie Snudden. Progression to the next industrial revolution: Industry 4.0 for composites. *Reinforced Plastics*, 63(3):136–142, 2019.
93. Latif U Khan, Walid Saad, Dusit Niyato, Zhu Han, and Choong Seon Hong. Digital-twin-enabled 6g: Vision, architectural trends, and future directions. *IEEE Communications Magazine*, 60(1):74–80, 2022.

94. Michael Batty. Digital twins, 2018.
95. David Holmes, Maria Papathanasaki, Leandros Maglaras, Mohamed Amine Ferrag, Surya Nepal, and Helge Janicke. Digital twins and cyber security–solution or challenge? In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, pages 1–8. IEEE, 2021.
96. Kari Rikkinen, Pekka Kyosti, Marko E Leinonen, Markus Berg, and Aarno Parssinen. Thz radio communication: Link budget analysis toward 6g. *IEEE Communications Magazine*, 58(11):22–27, 2020.
97. Chong Han, Yongzhi Wu, Zhi Chen, and Xudong Wang. Terahertz communications (teracom): Challenges and impact on 6g wireless systems. *arXiv preprint arXiv:1912.06040*, 2019.
98. Rohit Singh and Douglas Sicker. Thz communications-a boon and/or bane for security, privacy, and national security. In *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, 2020.
99. Boyu Ning, Zhi Chen, Wenjie Chen, and Lingxiang Li. Improving security of thz communication with intelligent reflecting surface. In *2019 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2019.
100. Yiming Li, Xitao Liang, Wenwu Xie, and Juan Zhu. Security performance analysis of active intelligent reflective surface assisted wireless communication. *Computer Science and Information Systems*, (00):11–11, 2023.
101. Vitaly Petrov, Dmitri Moltchanov, Josep Miquel Jornet, and Yevgeni Koucheryavy. Exploiting multipath terahertz communications for physical layer security in beyond 5g networks. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 865–872. IEEE, 2019.
102. Marcos Katz and Iqrar Ahmed. Opportunities and challenges for visible light communications in 6g. *2020 2nd 6G wireless summit (6G SUMMIT)*, pages 1–5, 2020.
103. Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Majid Safari, Chadi M Assi, and Harald Haas. Physical layer security for visible light communication systems: A survey. *IEEE Communications Surveys & Tutorials*, 22(3):1887–1908, 2020.
104. Simone Soderi, Alessandro Brighente, Federico Turrin, and Mauro Conti. Vlc physical layer security through ris-aided jamming receiver for 6g wireless networks. In *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 370–378. IEEE, 2022.
105. Cheng Chen, Rui Bian, and Harald Haas. Omnidirectional transmitter and receiver design for wireless infrared uplink transmission in lifi. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2018.
106. Ali Hussain Khan, Naveed UL Hassan, Chau Yuen, Jun Zhao, Dusit Niyato, Yan Zhang, and H Vincent Poor. Blockchain and 6g: the future of secure and ubiquitous communication. *IEEE Wireless Communications*, 29(1):194–201, 2021.
107. Jelena Marjanović, Nikola Dalčeković, and Goran Sladić. Blockchain-based model for tracking compliance with security requirements. *Computer Science and Information Systems*, 20(1):359–380, 2023.
108. Wei Liang, Lijun Xiao, Ke Zhang, Mingdong Tang, Dacheng He, and Kuan-Ching Li. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. *IEEE Internet of Things Journal*, 9(16):14741–14751, 2021.
109. Wei Liang, Yongkai Fan, Kuan-Ching Li, Dafang Zhang, and Jean-Luc Gaudiot. Secure data storage and recovery in industrial blockchain network environments. *IEEE Transactions on Industrial Informatics*, 16(10):6543–6552, 2020.
110. Sisi Zhou, Kuanching Li, Lijun Xiao, Jiahong Cai, Wei Liang, and Arcangelo Castiglione. A systematic review of consensus mechanisms in blockchain. *Mathematics*, 11(10):2248, 2023.

111. Tharaka Hewa, Gürkan Gür, Anshuman Kalla, Mika Ylianttila, An Bracken, and Madhusanka Liyanage. The role of blockchain in 6g: Challenges, opportunities and research directions. *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pages 1–5, 2020.
112. Hua-Yi Lin. Secure cloud internet of vehicles based on blockchain and data transmission scheme of map/reduce. *Computer Science and Information Systems*, 20(1):137–156, 2023.
113. Hao Xu, Paulo Valente Klaine, Oluwakayode Onireti, Bin Cao, Muhammad Imran, and Lei Zhang. Blockchain-enabled resource management and sharing for 6g communications. *Digital Communications and Networks*, 6(3):261–269, 2020.
114. Fredy Andres Aponte-Novoa, Ana Lucila Sandoval Orozco, Ricardo Villanueva-Polanco, and Pedro Wightman. The 51% attack on blockchains: A mining behavior study. *IEEE Access*, 9:140549–140564, 2021.
115. Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to scalability of blockchain: A survey. *Ieee Access*, 8:16440–16455, 2020.
116. Songyou Xie, Lijun Xiao, Dezhi Han, Kun Xie, Xiong Li, and Wei Liang. Hcvc: A high-capacity off-chain virtual channel scheme based on bidirectional locking mechanism. *IEEE Transactions on Network Science and Engineering*, 2023.
117. Javad Zarrin, Hao Wen Phang, Lakshmi Babu Saheer, and Bahram Zarrin. Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*, 24(4):2841–2866, 2021.
118. Yaqin Liu, Wei Liang, Kun Xie, Songyou Xie, Kuanching Li, and Weizhi Meng. Lightpay: A lightweight and secure off-chain multi-path payment scheme based on adapter signatures. *IEEE Transactions on Services Computing*, 2023.
119. Weiyu Zhong, Ce Yang, Wei Liang, Jiahong Cai, Lin Chen, Jing Liao, and Naixue Xiong. Byzantine fault-tolerant consensus algorithms: A survey. *Electronics*, 12(18):3801, 2023.
120. Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, and Alireza Babaei Bondarti. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, 154:113385, 2020.
121. Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A Hoque, and Alan Colman. Blockchain consensus algorithms: A survey. *arXiv preprint arXiv:2001.07091*, 2020.
122. Xiang Fu, Huaimin Wang, and Peichang Shi. A survey of blockchain consensus algorithms: mechanism, design and applications. *Science China Information Sciences*, 64:1–15, 2021.
123. Xian Guo, Chen Wang, Laicheng Cao, Yongbo Jiang, and Yan Yan. A novel security mechanism for software defined network based on blockchain. *Computer Science and Information Systems*, 19(2):523–545, 2022.
124. Gunasekaran Manogaran, Bharat S Rawal, Vijayalakshmi Saravanan, Priyan Malarvizhi Kumar, Oscar Sanjuán Martínez, Rubén González Crespo, Carlos Enrique Montenegro-Marin, and Sujatha Krishnamoorthy. Blockchain based integrated security measure for reliable service delegation in 6g communication environment. *Computer Communications*, 161:248–256, 2020.
125. Jiaheng Wang, Xintong Ling, Yuwei Le, Yongming Huang, and Xiaohu You. Blockchain-enabled wireless communications: a new paradigm towards 6g. *National science review*, 8(9):nwab069, 2021.
126. Khurram Shahzad, Ahmad O Aseeri, and Munam Ali Shah. A blockchain-based authentication solution for 6g communication security in tactile networks. *Electronics*, 11(9):1374, 2022.
127. Ihsan H Abdulqadder and Shijie Zhou. Sliceblock: context-aware authentication handover and secure network slicing using dag-blockchain in edge-assisted sdn/nfv-6g environment. *IEEE Internet of Things Journal*, 9(18):18079–18097, 2022.
128. Han Liu, Dezhi Han, Mingming Cui, Kuan-Ching Li, Alireza Souri, and Mohammad Shojafar. Idenmultisig: identity-based decentralized multi-signature in internet of things. *IEEE Transactions on Computational Social Systems*, 2023.

129. Wei Liang, Songyou Xie, Jiahong Cai, Jianbo Xu, Yupeng Hu, Yang Xu, and Meikang Qiu. Deep neural network security collaborative filtering scheme for service recommendation in intelligent cyber–physical systems. *IEEE Internet of Things Journal*, 9(22):22123–22132, 2021.
130. Wei Liang, Songyou Xie, Jiahong Cai, Chong Wang, Yujie Hong, and Xiaoyan Kui. Novel private data access control scheme suitable for mobile edge computing. *China Communications*, 18(11):92–103, 2021.
131. Md Abdur Rahman and M Shamim Hossain. A deep learning assisted software defined security architecture for 6g wireless networks: Iiot perspective. *IEEE Wireless Communications*, 29(2):52–59, 2022.
132. Yang Yang, Mulei Ma, Hequan Wu, Quan Yu, Ping Zhang, Xiaohu You, Jianjun Wu, Chenghui Peng, Tak-Shing Peter Yum, Sherman Shen, et al. 6g network ai architecture for everyone-centric customized services. *arXiv preprint arXiv:2205.09944*, 2022.
133. Jiahong Cai, Wei Liang, Xiong Li, Kuanching Li, Zhenwen Gui, and Muhammad Khurram Khan. Gtxchain: A secure iot smart blockchain architecture based on graph neural network. *IEEE Internet of Things Journal*, 2023.
134. Razvan-Andrei Stoica and Giuseppe Thadeu Freitas de Abreu. 6g: the wireless communications network for collaborative and ai applications. *arXiv preprint arXiv:1904.03413*, 2019.
135. Xiting Peng, Yichao Wang, Xiaoyu Zhang, Haibo Yang, Xiongyan Tang, and Shi Bai. A 6g-enabled lightweight framework for person re-identification on distributed edges. *Electronics*, 12(10):2266, 2023.
136. Bomin Mao, Fengxiao Tang, Zubair Md Fadlullah, and Nei Kato. An intelligent route computation approach based on real-time deep learning strategy for software defined communication systems. *IEEE Transactions on Emerging Topics in Computing*, 9(3):1554–1565, 2021.
137. Wen Wu, Conghao Zhou, Mushu Li, Huaqing Wu, Haibo Zhou, Ning Zhang, Xuemin Sherman Shen, and Weihua Zhuang. Ai-native network slicing for 6g networks. *IEEE Wireless Communications*, 29(1):96–103, 2022.
138. Rubayet Shafin, Lingjia Liu, Vikram Chandrasekhar, Hao Chen, Jeffrey Reed, and Jianzhong Charlie Zhang. Artificial intelligence-enabled cellular networks: A critical path to beyond-5g and 6g. *IEEE Wireless Communications*, 27(2):212–217, 2020.
139. Helin Yang, Arokiaswami Alphones, Zehui Xiong, Dusit Niyato, Jun Zhao, and Kaishun Wu. Artificial-intelligence-enabled intelligent 6g networks. *IEEE Network*, 34(6):272–280, 2020.
140. Khaled B Letaief, Yuanming Shi, Jianmin Lu, and Jianhua Lu. Edge artificial intelligence for 6g: Vision, enabling technologies, and applications. *IEEE Journal on Selected Areas in Communications*, 40(1):5–36, 2021.
141. Yong Xiao, Guangming Shi, Yingyu Li, Walid Saad, and H Vincent Poor. Toward self-learning edge intelligence in 6g. *IEEE Communications Magazine*, 58(12):34–40, 2020.
142. Man Chu, Hang Li, Xuewen Liao, and Shuguang Cui. Reinforcement learning-based multi-access control and battery prediction with energy harvesting in iot systems. *IEEE Internet of Things Journal*, 6(2):2009–2020, 2019.
143. Khaled B Letaief, Wei Chen, Yuanming Shi, Jun Zhang, and Ying-Jun Angela Zhang. The roadmap to 6g: Ai empowered wireless networks. *IEEE communications magazine*, 57(8):84–90, 2019.
144. Shunliang Zhang and Dali Zhu. Towards artificial intelligence enabled 6g: State of the art, challenges, and opportunities. *Computer Networks*, 183:107556, 2020.
145. Mulumba Banza Gracia, Vusumuzi Malele, Sphiwe Promise Ndlovu, Topside Ehleketani Mathonsi, Lebogang Maaka, and Tonderai Muchenje. 6g security challenges and opportunities. In *2022 IEEE 13th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT)*, pages 339–343. IEEE, 2022.
146. Marco Barreno, Blaine Nelson, Anthony D Joseph, and J Doug Tygar. The security of machine learning. *Machine Learning*, 81:121–148, 2010.

147. Jing Li, Xiaohui Kuang, Shujie Lin, Xu Ma, and Yi Tang. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. *Information Sciences*, 526:166–179, 2020.
148. Chafika Benzaid and Tarik Taleb. Ai for beyond 5g networks: a cyber-security defense or offense enabler? *IEEE network*, 34(6):140–147, 2020.
149. Jin-Hee Cho, Dilli P Sharma, Hooman Alavizadeh, Seunghyun Yoon, Noam Ben-Asher, Terrence J Moore, Dong Seong Kim, Hyuk Lim, and Frederica F Nelson. Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys & Tutorials*, 22(1):709–745, 2020.
150. Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.
151. Deepika Sirohi, Neeraj Kumar, Prashant Singh Rana, Sudeep Tanwar, Rahat Iqbal, and Mohammad Hijjii. Federated learning for 6g-enabled secure communication systems: a comprehensive survey. *Artificial Intelligence Review*, pages 1–93, 2023.
152. Omid Aramoon, Pin-Yu Chen, Gang Qu, and Yuan Tian. Meta federated learning. *arXiv preprint arXiv:2102.05561*, 2021.
153. Kang Liu, Brendan Dolan-Gavitt, and Siddharth Garg. Fine-pruning: Defending against backdooring attacks on deep neural networks. In *International symposium on research in attacks, intrusions, and defenses*, pages 273–294. Springer, 2018.
154. Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. Scaffold: Stochastic controlled averaging for federated learning. In *International conference on machine learning*, pages 5132–5143. PMLR, 2020.
155. Huda A Babaeer and Saad A Al-Ahmadi. Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. *IEEE Access*, 8:92098–92109, 2020.
156. Chen Fang, Yuanbo Guo, Na Wang, and Ankang Ju. Highly efficient federated learning with strong privacy preservation in cloud computing. *Computers & Security*, 96:101889, 2020.
157. Zubair Md Fadlullah, Bomin Mao, and Nei Kato. Balancing qos and security in the edge: Existing practices, challenges, and 6g opportunities with machine learning. *IEEE Communications Surveys & Tutorials*, 2022.
158. Hamed Haddadpajouh, Alireza Mohtadi, Ali Dehghantanaha, Hadis Karimipour, Xiaodong Lin, and Kim-Kwang Raymond Choo. A multikernel and metaheuristic feature selection approach for iot malware threat hunting in the edge layer. *IEEE Internet of Things Journal*, 8(6):4540–4547, 2020.
159. Jiawen Kang, Zehui Xiong, Dusit Niyato, Yuze Zou, Yang Zhang, and Mohsen Guizani. Reliable federated learning for mobile networks. *IEEE Wireless Communications*, 27(2):72–80, 2020.
160. Pawani Porambage, Tanesh Kumar, Madhusanka Liyanage, Juha Partala, Lauri Lovén, Mika Ylianttila, and Tapio Seppänen. Sec-edgeai: Ai for edge security vs security for edge ai. *The 1st 6G Wireless Summit,(Levi, Finland)*, 2019.
161. Lauri Lovén, Teemu Leppänen, Ella Peltonen, Juha Partala, Erkki Harjula, Pawani Porambage, Mika Ylianttila, and Jukka Riekki. Edgeai: A vision for distributed, edge-native artificial intelligence in future 6g networks. *6G Wireless Summit, March 24-26, 2019 Levi, Finland*, 2019.
162. Bing Tang, Feiyan Guo, Buqing Cao, Mingdong Tang, and Kuanching Li. Cost-aware deployment of microservices for iot applications in mobile edge computing environment. *IEEE Transactions on Network and Service Management*, 2022.
163. Khwaja Jawad, Khwaja Mansoor, Ahmed Fraz Baig, Anwar Ghani, and Azmat Naseem. An improved three-factor anonymous authentication protocol for wsn s based iot system using symmetric cryptography. In *2019 International Conference on Communication Technologies (ComTech)*, pages 53–59. IEEE, 2019.

164. Majid Alotaibi. An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for wsn. *IEEE Access*, 6:70072–70087, 2018.
165. Bechir Alaya and Lamaa Sellami. Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban vanet networks. *Journal of Information Security and Applications*, 58:102779, 2021.
166. Shuaiqi Shen, Chong Yu, Kuan Zhang, Jianbing Ni, and Song Ci. Adaptive and dynamic security in ai-empowered 6g: From an energy efficiency perspective. *IEEE Communications Standards Magazine*, 5(3):80–88, 2021.
167. He Fang, Xianbin Wang, Zhenlong Xiao, and Lajos Hanzo. Autonomous collaborative authentication with privacy preservation in 6g: From homogeneity to heterogeneity. *IEEE Network*, 36(6):28–36, 2022.
168. Liang Xiao, Geyi Sheng, Sicong Liu, Huaiyu Dai, Mugen Peng, and Jian Song. Deep reinforcement learning-enabled secure visible light communication against eavesdropping. *IEEE transactions on communications*, 67(10):6994–7005, 2019.
169. Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda. Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, 21(1):640–660, 2018.
170. Faisal Tariq, Muhammad RA Khandaker, Kai-Kit Wong, Muhammad A Imran, Mehdi Bennis, and Merouane Debbah. A speculative study on 6g. *IEEE Wireless Communications*, 27(4):118–125, 2020.
171. CL Zhang, YL Fu, H Li, et al. Research on security scenarios and security models for 6g networking. *Chinese Journal of Network and Information Security*, 7(1):28–45, 2021.
172. Shehzad Ashraf Chaudhry, Azeem Irshad, Muhammad Asghar Khan, Sajjad Ahmad Khan, Summera Nosheen, Ahmad Ali AlZubi, and Yousaf Bin Zikria. A lightweight authentication scheme for 6g-iot enabled maritime transport system. *IEEE Transactions on Intelligent Transportation Systems*, 2021.
173. Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and Mamoun Alazab. Designing authenticated key management scheme in 6g-enabled network in a box deployed for industrial applications. *IEEE Transactions on Industrial Informatics*, 17(10):7174–7184, 2020.
174. Sabuzima Nayak and Ripon Patgiri. 6g communication: Envisioning the key issues and challenges. *arXiv preprint arXiv:2004.04024*, 2020.
175. Poonam Yadav, Angelo Feraudo, Budi Arief, Siamak F Shahandashti, and Vassilios G Vassilakis. Position paper: A systematic framework for categorising iot device fingerprinting mechanisms. In *Proceedings of the 2nd international workshop on challenges in artificial intelligence and machine learning for internet of things*, pages 62–68, 2020.

Yanlu Li is an undergraduate student at Hunan University of Science and Technology. His research interests include network measurements, network security, deep learning and blockchain.

Yufeng Xiao received the Ph.D. degree from Hunan University in 2020. He is currently an Assistant Professor at the School of Computer Science and Engineering, Hunan University of Science and Technology. His research interests include machine learning, network measurements, network security and speech signal processing.

Wei Liang received a Ph.D. degree from Hunan University in 2013. He is the Dean and Professor at the School of Computer Science and Engineering, Hunan University of Science and Technology. He has authored or co-authored more than 110 papers in top-ranked

journals/conferences. Dr. Liang's research interests include blockchain security technology, network security protection, embedded system and hardware IP protection, fog computing, and security management in wireless sensor networks (WSN).

Jiahong Cai is a Ph.D. candidate at Hunan University of Science and Technology. He has published several high-quality peer-reviewed papers in journals and conferences. His research interests include network measurements, deep reinforcement learning, network security, and blockchain.

Ronglin Zhang is a graduate student at Hunan University of Science and Technology. His research interests include network measurements, service computing, network security, deep learning and blockchain.

Kuan-Ching Li is a Life Distinguished Professor at Providence University, Taiwan. Besides publications in high-quality conferences and journals, he is a co-author or co-editor of more than 40 books published by Taylor & Francis, Springer, Elsevier, and McGraw-Hill. His research interests include Big Data, parallel and distributed computing, and emerging technologies.

Muhammad Khurram Khan is currently working as a Professor of Cybersecurity at the Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia. His research areas of interest are Cybersecurity, digital authentication, IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management.

Received: August 04, 2023; Accepted: February 07, 2024.