A survey on metaverse-empowered 6G wireless systems: a security perspective

Latif U. Khan 1, Mohsen Guizani 2, Ibrar Yaqoob 2, Dusit Niyato 2, Ala Al-Fuqaha 2, and Choong Seon Hong 2

1Mohamed Bin Zayed University of Artificial Intelligence
2Affiliation not available

December 7, 2023

Abstract

Recent trends in emerging applications have motivated researchers to design advanced wireless systems to meet their evolving requirements. These emerging applications include digital healthcare, intelligent transportation systems, Industry 5.0, and more. To address the evolving requirements, leveraging a metaverse to empower 6G wireless systems is a viable solution. A metaverse-empowered 6G wireless system can offer numerous benefits, but it may also be vulnerable to a wide variety of security attacks. In this survey, we discuss potential security attacks in metaverse-empowered 6G wireless systems. We introduce an architecture designed to enhance security within metaverse-empowered 6G wireless systems. This architecture comprises two key spaces: the meta space and the physical space. We present physical space attacks and outline effective solutions to secure metaverse-empowered 6G wireless systems. We provide invaluable insights and discussions on meta space attacks, along with promising solutions. Finally, we discuss open challenges and provide future recommendations.
A survey on metaverse-empowered 6G wireless systems: a security perspective

Latif U. Khan, Mohsen Guizani, Ibrar Yaqoob, Dusit Niyato, Ala Al-Fuqaha, Choon Seon Hong

Abstract—Recent trends in emerging applications have motivated researchers to design advanced wireless systems to meet their evolving requirements. These emerging applications include digital healthcare, intelligent transportation systems, Industry 5.0, and more. To address the evolving requirements, leveraging a metaverse to empower 6G wireless systems is a viable solution. A metaverse-empowered 6G wireless system can offer numerous benefits, but it may also be vulnerable to a wide variety of security attacks. In this survey, we discuss potential security attacks in metaverse-empowered 6G wireless systems. We introduce an architecture designed to enhance security within metaverse-empowered 6G wireless systems. This architecture comprises two key spaces: the meta space and the physical space. We present physical space attacks and outline effective solutions to secure metaverse-empowered 6G wireless systems. We provide invaluable insights and discussions on meta space attacks, along with promising solutions. Finally, we discuss open challenges and provide future recommendations.

Index Terms—6G, metaverse, machine learning, blockchain, eavesdropping, homomorphic encryption.

I. INTRODUCTION

Recent escalation in the development of novel applications (e.g., intelligent transportation systems and digital healthcare) has led to numerous research activities related to the sixth generation (6G) of wireless systems [1]–[3]. These applications are based on requirements of diverse natures, and as a result, existing wireless systems might not effectively fulfill them [4]. 6G is also in its infancy, and many works [1], [4]–[6] have proposed novel architectures to meet the demands of various applications. Among these works, the studies in [7] and [8] that have proposed the use of a digital twin and a metaverse to effectively enable 6G. The reasons for employing a metaverse-enabled 6G architecture are due to its promising features of self-sustainability and proactive online learning [7], [9]. These features enable 6G wireless systems to effectively fulfill the key requirements of various applications through proactive analysis before deployment and resource optimization. Proactive online learning-assisted 6G wireless systems will facilitate the analysis of various scenarios before the actual deployment of the wireless system. This will enable efficient deployment of wireless system components (e.g., edge/cloud servers and base stations). In addition to the deployment of wireless system components, there is a need for efficient resource management. For resource management, efficient resource management schemes with the least possible latency are required.

Although a metaverse-enabled 6G wireless system will offer many benefits, it will also face numerous challenges. These challenges include efficient metaverse signaling, deployment issues, and security-related concerns. A metaverse-based implementation of 6G will involve three primary spaces: (a) the services space, (b) the meta space, and (c) the physical interaction space [8], [10]. In the physical interaction space, all the physical entities required for the operation of a 6G wireless system will be present. The meta space will operate on the physical space entities (e.g., edge servers). Conversely, the services space will enable users to request 6G services. While the metaverse can be used to enable 6G wireless systems, there are several challenges that must be carefully addressed. These challenges encompass meta space design, seamless communication between the meta space and the physical space, resource management for both meta and physical spaces, and the security of metaverse-empowered 6G. In this article, our focus is on the security of metaverse-empowered 6G. Following this, we will discuss market statistics and research trends.

A. Research Trends and Statistics

According to statistics from [11], the 6G market is expected to experience a compound annual growth rate (CAGR) of 55% during the period 2031-2040, growing from USD 13,690.9 million in 2030 to USD 340,510.2 million by 2040. 6G will bring about a 100x increase in volumetric spectral efficiency and energy. The major 6G applications driving this market include the Internet of Everything (IoE), smart cities, digital twins, wireless brain-computer interaction, connected robotics and autonomous systems, and multisensory XR applications. In the realm of 6G, XR will give rise to a multitude of applications spanning the AR/MR/VR spectrum that will revolutionize the industry and give rise to new services. Future 5G systems will still fall short of offering a fully immersive XR experience that captures all sensory inputs due to their inability to achieve very low latencies for data-rate intensive XR applications. Regarding end-users, the 6G market has been categorized into government, consumers, businesses, and industries. The study divides the market into regions, including North America, Europe, Asia-Pacific, the Middle East & Africa, and South America. Based on geographic location, North America appears to have the highest level of participation in the growing 6G market.
The global cybersecurity market, as reported by [12], is expected to achieve USD 390.2 billion by 2030, with a projected CAGR of 14.50%. The most critical applications of cybersecurity in the IT world involve safeguarding networks, computers, programs, and data against illegal access and improper behavior. The demand for the Cyber Security Market Forecast has increased due to the global rise in cyber thefts and cyber-terrorism. Industries like retail, banking, and telecom, which heavily rely on procedures like absorbing and storing large amounts of data, have further propelled the growth of the cybersecurity business. Among many regions, North America appears to have the highest market share. China now holds the second-largest market revenue, with a CAGR of 13.4%, and is expected to surpass USD 70 billion by 2027, while the US market value was USD 44 billion in 2020 and is anticipated to continue rising steadily.

On the other hand, the metaverse market share is expected to reach USD 107.49 billion by 2030, up from USD 11.47 billion in 2023, with a CAGR of 45.2% during 2022-2030 [13]. Hardware and software are included in the component-based market segmentation for the metaverse. In 2021, the hardware market sector retained the largest share, accounting for around 47-49% of the total market. It is worth noting that the reason for discussing the metaverse market here is its key role in enabling a 6G wireless system. More detailed information about the metaverse-empowered 6G wireless system will be provided in Section II-B. Based on the preceding discussion, it can be concluded that security in metaverse-empowered 6G will be one of the main research areas for enabling emerging wireless applications.

B. Existing Surveys and Tutorials

Several works [8], [14]–[20] have explored the intersection of the metaverse, security, and 6G wireless systems. In [14], the focus was on surveying the role of the metaverse in enabling secure applications, without specifically concentrating on the metaverse itself. Another work, [15], delved into the security issues related to blockchain. Alladi et al. in [16] conducted a comprehensive study of how blockchain plays a role in enabling secure vehicular applications. Wang et al. in [17] conducted a survey on the metaverse and its security issues, with a primary focus on the meta space (a detailed discussion about the architecture will be provided in Section II). In [18], the survey revolved around the role of blockchain in enabling the metaverse. Khan et al. in [8] presented a vision for utilizing the metaverse to enable wireless systems. Lastly, [20] provided a survey on the edge-enabled metaverse.

C. Our Contributions

Our work is different from the existing works [8], [14]–[20], as outlined in Table I. Our specific focus lies in addressing security issues related to enabling 6G through the metaverse. The following summarizes our contributions.

- We explore the fundamental role of the metaverse in enabling 6G wireless systems. Furthermore, we introduce an architecture designed to enhance security for metaverse-enabled 6G, consisting of two phases: the meta space and the physical space.
- We discuss security attacks in both meta space and physical space, offering insight into potential security threats and corresponding guidelines.
- We present emerging security challenges in metaverse-empowered 6G and provide potential guidelines for addressing them. We also outline several future directions.

II. 6G: FUNDAMENTALS, USE CASES, AND ARCHITECTURE

A. Fundamentals and Use Cases

Typically, 6G services come with diverse requirements such as the need for sensory experiences, low latency, and high reliability. Additionally, a wide range of entities, including blockchain networks, edge/cloud servers, and various devices, are involved. Due to this diversity of entities and the novel requirements inherent to 6G, as opposed to existing wireless systems like 4G and 5G, we will encounter unique security challenges [21]–[24]. Table II provides an overview of parameters for both 6G and 5G wireless networks, clearly highlighting the novel requirements that 6G will bring. Meeting these requirements poses a significant challenge.

To address these challenges, the work in [8] has proposed a novel architecture based on the metaverse for 6G. A metaverse-empowered 6G system will primarily enable three design trends: (a) Proactive online learning, (b) Self-sustainability, and (c) Network as a black box.

- **Proactive online learning**: 6G applications such as digital healthcare and intelligent transportation systems come with latency constraints. Consequently, there is a pressing need to instantly cater to the requests of 6G end-users. Simultaneously, there arises a necessity to analyze the 6G wireless system before embarking on the actual implementation of new services. This preliminary analysis is crucial. Additionally, proactive learning is required before
TABLE I: Summary of existing surveys and tutorials and their primary focus

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Salman et al. [14]</td>
<td>✗</td>
<td>✗</td>
<td>✗ (considered generally blockchain)</td>
<td>✗</td>
<td>Surveyed the use of blockchain for enabling secure services.</td>
<td>The authors did not discuss the security issues in the blockchain itself.</td>
</tr>
<tr>
<td>Li et al. [15]</td>
<td>✗</td>
<td>✗</td>
<td>✗ (considered security in blockchain)</td>
<td>✗</td>
<td>Surveyed the security issues in blockchain.</td>
<td>The authors discussed the security issues in blockchain without focusing on the metaverse.</td>
</tr>
<tr>
<td>Alladi et al. [16]</td>
<td>✗</td>
<td>✗</td>
<td>✗ (considered blockchain for securing vehicular networks)</td>
<td>✗</td>
<td>Surveyed the role of blockchain in securing vehicular networks.</td>
<td>The authors surveyed the role of blockchain in enabling vehicular networks without focusing on the metaverse.</td>
</tr>
<tr>
<td>Wang et al. [17]</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>Surveyed concept, security, and privacy of metaverse.</td>
<td>Our work considered a secure metaverse-empowered 6G.</td>
</tr>
<tr>
<td>Gadekallu et al. [18]</td>
<td>✓</td>
<td>✗</td>
<td>✗ (considered blockchain for metaverse)</td>
<td>✗</td>
<td>Surveyed the role of blockchain in enabling metaverse.</td>
<td>N/A</td>
</tr>
<tr>
<td>Khan et al. [8]</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗ (proposed general architecture)</td>
<td>The vision of metaverse for the wireless system was presented.</td>
<td>N/A</td>
</tr>
<tr>
<td>Khan et al. [19]</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗ (presented edge-enabled metaverse architecture)</td>
<td>Focused on the role of ML in enabling metaverse.</td>
<td>N/A</td>
</tr>
<tr>
<td>Xu et al. [20]</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>Presented enablers, general architecture, and open challenges.</td>
<td>Our work presents a novel architecture for secure metaverse-enabled 6G</td>
</tr>
<tr>
<td>Our Tutorial</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>N/A</td>
</tr>
</tbody>
</table>

TABLE II: Comparison of 5G and 6G [1].

<table>
<thead>
<tr>
<th>Parameter</th>
<th>5G</th>
<th>6G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio only delay requirements</td>
<td>100ns</td>
<td>10ns</td>
</tr>
<tr>
<td>End-to-end reliability requirements</td>
<td>99.999%</td>
<td>99.99999%</td>
</tr>
<tr>
<td>Energy efficiency</td>
<td>1000x relative to 4G</td>
<td>10x relative to 5G</td>
</tr>
<tr>
<td>Processing delay</td>
<td>100ns</td>
<td>10ns</td>
</tr>
<tr>
<td>Latency</td>
<td>ms level</td>
<td>&lt; 1ms</td>
</tr>
<tr>
<td>Mobility</td>
<td>350 km/h</td>
<td>&gt; 1000km/h</td>
</tr>
<tr>
<td>Traffic density</td>
<td>10 Tb/s/km²</td>
<td>&gt; 100 Tb/s/km²</td>
</tr>
<tr>
<td>Receiver sensitivity</td>
<td>About −120dBm</td>
<td>&lt; −130dBm</td>
</tr>
<tr>
<td>Peak data rate</td>
<td>10 − 20 Gbps</td>
<td>&gt; 1Tbps</td>
</tr>
<tr>
<td>Spectrum efficiency</td>
<td>3 ~ 5x relative to 4G</td>
<td>&gt; 8x relative to 5G</td>
</tr>
</tbody>
</table>

users request services. This proactive learning aids in developing machine learning models that can be stored for future use in serving 6G users. To conduct such learning, various schemes can be employed, contingent on the chosen approach, whether centralized or distributed. In the context of centralized training, it becomes imperative to transfer device data to the cloud to facilitate the training process. This method offers several advantages, such as faster convergence and heightened context-awareness. However, centralizing the training process brings about certain disadvantages, including privacy vulnerabilities in the presence of malicious users and substantial consumption of communication resources, especially in scenarios involving frequent data generation (e.g., autonomous cars). Centralizing the training process can potentially expose device privacy to breaches in the cloud, instigated by malicious users. To address this issue, the preferable solution is to distribute the learning process among multiple devices, involving the training of local models on distributed devices and aggregating them. Nonetheless, distributing the learning process encounters certain challenges. These challenges encompass data heterogeneity, involving non-independent and non-identically distributed (non-IID) data distribution, as well as system heterogeneity, signifying varying computing capabilities among different devices, such as differences in CPU cycles per second. Consequently, it becomes essential to address and resolve these challenges when
implementing distributed learning schemes.

- **Self-sustainability:** In a typical 6G wireless system, there will be a wide array of participants and a complex architecture designed to cater to a vast number of users, as illustrated in Table II. Consequently, managing 6G wireless networks will present numerous challenges. These challenges primarily encompass intricate management functions, such as wireless resource management and computing resource management. To address these challenges, it is imperative to introduce self-sustaining 6G systems capable of operating with minimal intervention from network operators and users.

- **Network as a black box:** 6G wireless systems will involve numerous participants and a substantial user base, resulting in complex and challenging management tasks. One such challenge is the impact of the wireless channel on wireless signals, which can lead to performance degradation. To mitigate this problem, one approach is to estimate the wireless channel and then apply it to the received signal to enhance the performance. Various estimation methods are available, including those based on mathematical analytics. However, schemes relying solely on mathematical analytics may not perform optimally. To tackle this challenge, one can treat wireless channels as black boxes and train machine learning models.

To meet the aforementioned design trends, there is a requirement for an innovative approach to 6G. An implementation empowered by the metaverse can be
embraced for 6G. While metaverse-empowered 6G holds the potential for numerous benefits, it also encounters certain security challenges. Subsequently, we delve into the metaverse-empowered architecture for 6G and explore various enabling factors alongside potential security threats.

B. Architecture

Generally, we employ the Confidentiality, Integrity, and Availability (CIA) framework for discussing the security of a wireless system. Therefore, we also apply the CIA framework to a metaverse-empowered 6G wireless system, as illustrated in Fig. 1. Confidentiality pertains to safeguarding sensitive information from unauthorized users, while integrity ensures that information remains complete and accurate. Meanwhile, availability ensures that information is accessible when needed.

In Fig.2, one can observe the architecture of a metaverse-empowered 6G wireless system. The framework is divided into two spaces: the meta space and the physical space. The physical space encompasses all the physical entities, such as devices, edge servers, cloud servers, and base stations, capable of running the metaverse. The meta space, on the other hand, represents a logical space that governs the physical space through a control plane separation, akin to software-defined networking, along with other technologies. These technologies encompass blockchain, machine learning, optimization, game theory, among others. Moreover, there must be interaction between these two spaces facilitated by interfaces [25], [26]. These interfaces can take the form of wireless, wired, or touch interfaces (e.g., a mobile phone’s touch screen for interacting with applications). Fig.2 also enumerates key enablers for various layers, alongside a list of potential security threats.

III. PHYSICAL SPACE SECURITY

The physical space encompasses all the necessary entities for operating the metaverse-based 6G, as illustrated in Fig. 2. Within the physical space, our primary areas of focus are the security of access networks, the physical security of devices, network slicing security, and blockchain security attacks. It’s worth noting that we adhere to the layered architecture for networking, which comprises several layers: the physical/access layer, network/Internet layer, transport layer, and application layer. In this section, our attention will be directed toward physical layer attacks (e.g., eavesdropping) and application layer attacks (e.g., authentication attacks). We will proceed to discuss these aspects one by one.

A. Access Network Attacks

An access network facilitates interactions among various participants within a metaverse-empowered system through a wireless network. The primary sources of an attack within an access network include “Eavesdropping” attacks, jamming attacks, and pilot contamination attacks [27]. Furthermore, the presence of a malicious node capable of inserting false information can also lead to performance degradation. To mitigate these issues, employing encryption/decryption and node validation before considering the signal at the receiver becomes imperative. Beyond false information injection, there exist various other attacks, such as jamming. In this context, our focus centers on security attacks at the physical layer for emerging communication schemes, such as terahertz communication:

1) Millimeter wave and Terahertz Communication Security Attacks: Herein, we discuss the security concerns associated with millimeter-wave communications. Various studies have explored eavesdropping [28]–[31], pilot contamination [32]–[36], and jamming attacks [37]–[41] in the context of millimeter-wave communications, as depicted in Fig. 3.

In the context of eavesdropping, a third-party malicious user gains access to a wireless channel’s signal through inference and sniffing. In Fig. 3a, the transmitter (Alice) and receiver (Bob) aim to communicate with each other. An eavesdropper intercepts the communication within the beam scope, wiretapping the channel to carry out a security breach. Eavesdroppers outside the beam scope may employ intelligent reflecting surfaces to intercept the signal, as demonstrated in Fig.3b. However, positioning these intelligent reflecting surfaces poses numerous challenges that eavesdroppers must overcome.

Beyond eavesdropping, another concern is jamming attacks in wireless access networks. In such attacks, an attacking node injects a signal on the same frequency as that of “Bob,” disrupting “Bob’s” use of the channel and causing a Denial of Service (DoS) attack, as shown in Fig. 3c.

Another form of attack is pilot contamination, where the attacking node transmits identical pilot signals to degrade the receiver’s detection performance, as illustrated in Fig. 3. Similar to mmWave attacks, attacks can also occur in terahertz communication. Therefore, it becomes essential to devise novel strategies to counteract such attacks.

2) Visible Light Communication Security Attacks: In visible light communication, there can be several communication topologies defined by the IEEE 802.15.7 standard, as depicted in Fig.4. These topologies include peer-to-peer, star, and broadcast configurations. To analyze security in visible light communication, we first examine the modes of communication, as shown in Fig.4. The peer-to-peer topology is employed for communication between two devices, while the star topology can be seen as an alternative to WiFi [42]. On the other hand, the broadcast topology serves multimedia purposes.
Fig. 3: Overview of mmWave attacks: (a) Eavesdropper simply receives the signal, (b) eavesdropper receives the signal by using a reflector in the beam scope, (c) an attacker generates a signal with frequency $f_2$ to degrade the performance of the communication between transmitter and receiver, and (d) pilot contamination attacks [27].

Fig. 4: Overview of (a) VLC communication modes, (b) Eavesdropping, (c) Wiretapping channel model, and (d) Jamming attacks.

Multiple levels of security measures can be implemented in visible light communication. For layers above the MAC layer, security schemes primarily rely on encryption/decryption methods, authentication procedures, and password protection, among others. Our primary focus here is on physical layer security. The most common attack in this
context is eavesdropping, which is more prominent in broadcast and star topologies compared to the peer-to-peer topology. This discrepancy arises from the fact that the coverage area for star and broadcast topologies tends to be larger than that of the peer-to-peer topology. The wiretap channel is depicted in Fig. 4, where the channel state information for "Bob" and "Eve" differs. To safeguard the information "Alice" intends to transmit to "Bob," encryption is essential before transmission, preventing "Eve" from inferring "Alice’s" information.

In a study conducted by Blinowski et al. [43], qualitative risk analysis was performed for various communication modes in visible light communication. The highest risk was associated with fixed-to-infrastructure and mobile-to-infrastructure modes. Additionally, in the work by Classen et al. [44], various attacks on visible light communication were investigated, including eavesdropping and jamming. In friendly jamming scenarios, a jamming node emits a signal that degrades the Signal-to-Interference-plus-Noise Ratio (SINR) condition, resulting in a weaker signal received by "Bob," as shown in Fig. 4d.

Furthermore, the work by Chow et al. [45] delved into jamming attacks in visible light communication. They considered jamming and data light-emitting diodes, generating random binary signals. As a proof of concept, they utilized two LEDs connected to a pattern generator, producing 5 Mbps pseudo-random binary signals. For detection, a photodiode positioned 100 meters away from the sources was used to detect the signals. Additionally, it was assumed that ceiling lamps were not available, as illustrated in Fig. 5. Fig. 5 demonstrates the concept of a secure visible light communication zone, providing various settings to establish secure communication zones for visible light communication. Although the work by Chow et al. [45] explored secure visible light communication, there remains a need to propose novel, emerging, and effective encryption schemes (e.g., homomorphic encryption) for visible light communication.

B. Network Slicing Security Attacks

In the architecture outlined in Section II, one can employ the concept of network slicing to facilitate efficient network management through network function virtualization. Network slicing is grounded in software-defined networking (SDN) and network function virtualization (NFV) principles [46]–[48]. SDN allows the separation of the control plane from the data plane, while NFV enables the utilization of general-purpose hardware for diverse purposes.

It's worth noting that the use of slicing enables the efficient implementation of the meta space. However, even though the meta space can be efficiently utilized with SDN and NFV, it faces several challenges. These challenges encompass unauthorized access to devices/SDN switches, SDN controller spoofing, data plane attacks, control plane attacks, and man-in-the-middle attacks [49], [50]. In an SDN controller spoofing scenario, an attacker impersonates the controller to gain unauthorized access and then carries out malicious activities to disrupt the entire operation of metaverse-enabled 6G [51], [52]. To tackle this challenge, the development of novel, lightweight authentication schemes is imperative to prevent unauthorized access to SDN controllers [53].

In addition to these concerns, there must be an efficient mechanism in place to mitigate DoS attacks in metaverse-empowered 6G. Furthermore, safeguards against eavesdropping and man-in-the-middle attacks must be integrated into SDN-enabled NFV systems.

C. Blockchain Security Attacks

Blockchain can facilitate various functions within the metaverse in a transparent and immutable manner [54]–[57]. As illustrated in Fig. 2, a metaverse-empowered 6G system consists of three primary spaces: the applications space, meta space, and physical space. All network elements reside in the physical space, which bears the responsibility of running and executing all applications. The meta space, in contrast, is a logical space that operates on the actual entities, such as edge/cloud servers, within the physical space. A significant volume of data is associated with the meta space, including the need to train meta space models (pre-training prior to user requests) and subsequently store them within the blockchain.

To manage and handle such data, including data and pre-trained models, blockchain is employed to carry out these tasks in an immutable and transparent manner. Additionally, blockchain contributes to the operation and management of the metaverse-empowered 6G wireless system, allowing secure transactions to take place. Blockchain can also support digital content creation within the metaverse by effectively managing the data. However, despite its numerous advantages, blockchain faces several challenges, including high energy consumption and latency (e.g., in proof-of-work systems), management complexity due to its distributed nature, and security and privacy concerns.

Fig. 6c illustrates the security considerations related to blockchain. These security concerns can be categorized into three primary groups: (a) mining attacks, (b) networking attacks, and (c) privacy attacks. Before delving into the details of these attacks, it’s important to discuss how blockchain mining operates. Fig. 7 presents the blockchain workflow [58]. Initially, all nodes broadcast transactions to one another. Following the broadcast, each node constructs a candidate block utilizing information from the previous block (e.g., version number, block height, hash function) and the received
Blockchain for metaverse

- Scalable
- Sustainable
- Interoperable
- Secure

Digital assets

Decentralized storage of meta space models

Blockchain-enabled Distributed learning for meta space

ML

ML

ML

ML

Digital content creation

Decentralized meta space datasets

Blockchain-enabled Distributed meta space

Figure 6: Overview of (a) role of blockchain in the metaverse, (b) metaverse and blockchain design aspects, and (c) security attacks in blockchain for the metaverse.

Fig. 7: Overview of blockchain workflow.

Users broadcast the transactions to all nodes

Nodes form candidate block and run consensus algorithm over wireless network

Winner node send block to other nodes over a wireless network

Transaction is officially into the chain

The node adds the block to the blockchain that it maintains

Other nodes perform validation operation on the block

transactions. Each node employs a consensus algorithm to determine the right to account for the candidate block. For instance, the proof-of-work consensus algorithm involves mining the block to establish accounting rights for the current block. Subsequently, the node that secures the accounting rights broadcasts its candidate block to other nodes. The
recipient nodes verify the received block before adding it to the blockchain. It’s worth noting that communication occurs over a wireless channel between different nodes, rendering them susceptible to eavesdropping and other poisoning attacks.

Moreover, DoS attacks can be carried out to disrupt the entire process. To mitigate eavesdropping and poisoning, efficient encryption/decryption schemes commonly used in blockchain can be implemented. Additionally, due to its distributed nature, eavesdropping on blockchain is challenging for malicious entities. Conversely, poisoning attacks can be executed more easily within the blockchain. Man-in-the-middle attacks and replay attacks are also plausible in the blockchain context. In man-in-the-middle attacks, information can be intercepted and modified, while replay attacks involve recording a legitimate transaction and later replaying it for fraudulent purposes. To counter these attacks, novel security and verification schemes are essential.

D. Summary: Lessons Learned and Insights

The key lessons learned from this section are as follows:

- We learned that deploying efficient power control and frequency hopping is essential to avoid jamming attacks in physical space wireless access networks. In frequency hopping, one can regularly change the signal frequencies to make it difficult for attackers to jam the signal. However, designing the frequency hopping requires careful consideration, and it faces challenges such as limited frequency range and synchronization. Effective synchronization between the transmitter and receiver is necessary for seamless communication in frequency hopping scenarios [59].

- We also learned that beamforming can enhance secure communication. To prevent eavesdropping, effective beamforming techniques can be employed. However, narrowing the beam scope may reduce coverage, potentially causing signal reception issues. Although beamforming offers benefits for secure communication, it encounters challenges, including computing complexity, interference effects, and mobility issues. Narrow beam signals can experience significant degradation when obstructed, especially in high-frequency scenarios like mmWave and terahertz communication. Additionally, the mobility of receiving nodes can impact performance due to the limited coverage area of narrow beam signals.

- Finally, it is essential to develop novel security schemes to enhance the security of blockchain for its use in metaverse-empowered 6G systems. Various security threats in blockchain include malware attacks, fork attacks, and vulnerabilities in smart contracts. Novel blockchain schemes must effectively address these types of attacks.

IV. Meta Space Security

In metaverse-empowered 6G wireless systems, one can deploy the meta space either at the network edge, in the cloud, or use a hybrid approach involving both the edge and the cloud. The choice of meta space deployment depends on the nature of the 6G application. For instance, applications like digital healthcare, which require low-latency communication, should have meta space implemented at the network edge. Deploying meta space at the network edge offers low-latency communication but comes at the cost of lower computing power compared to the cloud. Therefore, for applications that require more computing power and have a delay-tolerant nature, meta space can be deployed in the cloud. Alternatively, a hybrid approach can be used to deploy meta space, taking advantage of both cloud and edge computing.

Next, let us consider how to deploy meta space for various 6G applications. Given the wide range of 6G applications, an efficient approach is needed. This approach can be based on the on-demand creation of meta space in response to user requests. Additionally, one can employ separate hardware (e.g., edge servers) for implementing meta space. However, this scheme may not be suitable for handling simultaneous requests from multiple users. Therefore, virtual machines or containers can be used to implement meta spaces for various applications, allowing the same hardware to be shared among different applications.

Since a diverse set of players and technologies will be involved in meta space implementation, there will be a variety of potential attacks. Apart from implementation considerations, there is also a need to store meta space data using blockchain in an immutable and transparent manner. Furthermore, for the efficient management of physical devices in 6G networks, there must be a clear separation between meta space and the physical space. To achieve this, the concept of network slicing, based on network function virtualization and software-defined networking, can be employed.

Broadly, the attacks on the meta space can be categorized into two main groups: DoS attacks, malware attacks, and authentication attacks:

A. DoS Attacks at Meta Space

DoS attacks refer to attacks that result in the inaccessibility of a service [60]–[62]. Since the metaverse can be implemented at the network edge, in the cloud, or both at the edge and in the cloud, the DoS attacks that occur at these locations can also affect the meta space [63]–[67].

In their work [63], the authors surveyed distributed DoS attacks on the cloud and categorized them mainly into two types: suffocative attacks and protocol attacks. Suffocative attacks involve the use of excessive traffic to saturate the target infrastructure’s bandwidth. Specifically, the attacker’s goal is to generate massive traffic, such as TCP flooding, to deny service to the actual cloud. On the other hand, protocol attacks aim to make the target inaccessible, resulting in a DoS. An example of a protocol attack in the cloud running the meta space is the smurf attack, as depicted in Fig. 8. Smurf attacks fall under the category of distributed DOS (DDoS) attacks in cloud environments. In this type of attack, a large number of Internet Control Message Protocol (ICMP) packets, using the source IP address of the victim’s machine, are sent to the network’s broadcast address. When these ICMP messages are received, the network responds by sending ICMP replies
to all, overwhelming the victim's machine with traffic and causing a DoS. The risk of Smurf attacks in meta space based on the cloud can be higher due to the shared nature of the underlying infrastructure for various meta spaces of different applications within the metaverse. In the metaverse, shared physical resources are used for different applications, making it possible for an attacker to launch a Smurf attack against one user's instance and affect the performance of the entire environment. To mitigate Smurf attacks, it is essential to ensure that the instances of all meta spaces based on the cloud are effectively secured with up-to-date patches and firewalls.

Similar to the cloud, DoS attacks can be carried out at the network edge as well. Mitigating such attacks at the network edge can be more challenging due to the geographically distributed nature of edge deployments. DDoS attacks at the network edge can take various forms, including volumetric attacks, protocol attacks, and application layer attacks. Volumetric attacks flood the network edge with a large volume of traffic, resulting in a DoS. Protocol attacks exploit vulnerabilities in network protocols to render the edge-based meta space unavailable to end-users. On the other hand, application layer attacks target application interfaces, such as web servers or APIs, attempting to exhaust their resources. To mitigate security attacks on meta space deployed at the network edge, various measures are needed, including firewalls, intrusion detection systems, and content delivery networks.

Additionally, meta space is susceptible to DoS attacks targeting virtual machines/containers because virtual machines/containers are utilized for running meta space [68]–[70]. The rationale behind employing virtual machines/containers is the presence of numerous users across various applications, all served by a limited number of edge servers or a cloud infrastructure. Consequently, virtual machines are employed to facilitate the operation of different meta spaces on the same hardware, such as an edge server or cloud server. With different virtual machines coexisting on the same cloud/edge infrastructure, a diverse range of DoS attacks may occur within these virtual machines/containers hosting the meta space. Primarily, three types of attacks can be observed, including resource depletion attacks, application-level attacks, and network attacks.

Resource depletion attacks involve overwhelming virtual machines/containers with an extensive volume of requests, often originating from malicious users. This onslaught of requests depletes the virtual machines' resources, rendering them incapable of serving end-users within the meta space. Application layer attacks within virtual machines/containers target the applications running within them. For instance, if the services layer in metaverse-based 6G is implemented using virtual machines/containers, these types of attacks can be anticipated. Conversely, network attacks focus on inundating the network, such as wireless interfaces, with a massive influx of traffic, thereby inducing a DoS.

To mitigate the aforementioned attacks, several measures can be implemented, including the use of firewalls, intrusion detection systems, and load-balancing schemes.

B. Malware Attacks at Meta Space

These attacks involve the utilization of malicious software to gain unauthorized access to a system, devices, or networks. Subsequently, the malicious software executes various undesirable actions, including ransomware, spyware, adware, trojans, and viruses. In a metaverse-based 6G wireless system, malicious software can be employed to infiltrate the meta space or services space, followed by the execution of malicious activities. These attacks can lead to an array of issues within a metaverse-based system, such as system crashes, user privacy breaches, and network disruption (either frequent or continuous). Among the most common malware attacks are viruses, capable of self-replication from one device to another (e.g., from one edge running meta space to another). Another form of attack encompasses worms, which are self-replicating programs that can result in substantial bandwidth consumption. Such viruses can induce significant delays in metaverse signaling, consequently affecting the prompt service delivery to metaverse users. Moreover, viruses have the potential to trigger complete Denial of Service (DoS) scenarios. Therefore, it is imperative to devise effective strategies for handling viruses in a metaverse-enabled 6G wireless system.

Additional forms of attacks include trojan horses, which initially appear harmless but subsequently seize control of the system and engage in malicious activities. For instance, a trojan within a metaverse can seize control of the meta space, altering pre-trained models and manipulating signaling to disrupt the overall operation. Modifying pre-trained models can result in substantial losses, given that these models are obtained through the execution of distributed learning models, which is a time-consuming process. Other malware attacks (e.g., adware, spyware, botnets, rootkits, and fileless malware) should also be prevented within the meta space.

C. Authentication Attacks

Authentication attacks involve attempts to gain unauthorized access to the metaverse-empowered 6G wireless system, typically by exploiting system vulnerabilities. Authentication specifically pertains to the process of verifying a user's identity before granting access to the system. Common authentication threats within a metaverse-enabled wireless system encompass identity theft, impersonation attacks, avatar authentication issues, and concerns regarding trusted and interoperable authentication [17].

In cases of identity theft, malicious entities steal user or mobile device identities, potentially leading to the exposure of
users’ digital assets, such as avatars and social relationships. Attackers in the meta space can take control of user accounts and engage in malicious activities within the metaverse. Furthermore, attackers with access to user credentials may employ spoofing techniques to deceive others within the system. A notable example of identity attacks is an attack in a metaverse-enabled 6G wireless system occurred on the Opensea NFT marketplace, where user accounts were compromised due to flaws in smart contracts, resulting in a loss of 1.7 million USD [17], [71].

On the other hand, an impersonation attack within the metaverse involves pretending to be the avatar of a legitimate user within the meta space. The fraudulent avatar can engage in various malicious behaviors, potentially disrupting synchronization between the physical and meta spaces. Synchronization is essential for efficient metaverse-empowered wireless system operation, and attackers may exploit vulnerabilities to disturb this synchronization, leading to performance degradation.

D. Summary: Lessons Learned and Insights

Here, we discuss several lessons learned from this section, as follows:

- We learned that it is necessary that we should carefully deal with the identity of the avatars in metaverse-empowered wireless systems. Different from the traditional schemes used for user authentication, one should propose novel schemes due to the fact that avatars are the digital counterparts of real humans/mobile devices. Therefore, we must consider various factors, such as height, 3D shape, voice, and facial features [10].

- There is a need to carefully design a metaverse-empowered 6G system against the DoS attacks as multiple meta spaces will be running on a single device (e.g., cloud or edge server). Using a single hardware for running multiple meta spaces is a feasible solution, however, DoS attacks launched for one meta space will affect another meta space as well.

- Meta space pre-trained ML models stored in a blockchain network must be carefully handled. Blockchain will enable distributed storage by avoiding a single point of failure. Additionally, blockchain will enable distributed storage in an immutable and transparent manner. Other than pre-trained models, one can store other data in the blockchain as well. Although blockchain can offer various benefits, it has a few limitations. These limitations are security and privacy issues in the blockchain itself. Additionally, running a blockchain consensus algorithm requires a significant amount of energy and time. There is a need to propose novel consensus algorithms that offer low latency and less energy consumption. Also, we must propose schemes to make blockchain secure and privacy-preserving.

- Authentication schemes for meta space can be either centralized or decentralized. In the case of centralized authentication schemes, one can have a centralized server that can manage all the authentication credentials, such as user accounts, passwords, and access rights. Centralized authentication schemes offer risk minimization of inconsistencies and errors. Although centralized authentication schemes offer benefits, it has a few downsides. The main of these downsides is the single point of failure. Moreover, an attacker can gain access to the central server and perform malicious activities. To address this issue, one can use distributed authentication schemes that rely on multiple nodes/devices for managing the authentication procedure. Emerging decentralized authentication schemes can be based on blockchain. Although blockchain offers various benefits, it has a few challenges that need to be addressed as well. These challenges are privacy leakages and the security of blockchain.

V. OPEN CHALLENGES

A. Blockchain-Empowered Secure Distributed Authentication Schemes

How can one enable distributed authentication schemes for the metaverse to avoid a single point of failure? In traditional authentication schemes, the data are stored in a centralized location (e.g., a cloud), which might be vulnerable to a single point of failure, degrading system performance. To address this issue, there is a need to propose distributed authentication schemes. One approach is to use blockchain to implement distributed authentication schemes for the metaverse, storing authentication credentials in distributed datasets. Such a distributed authentication scheme can avoid a single point of failure but may require more complex management compared to a single server-based authentication scheme. However, it is important to note that blockchain itself has privacy and security vulnerabilities.

The major privacy concern in the public blockchain is that data is visible to all nodes in a network, potentially compromising user privacy. Additionally, blockchain uses pseudonymous identities for users, which can provide a certain degree of anonymity but not complete anonymity. Therefore, we must address these issues when deploying blockchain-based authentication schemes for metaverse-empowered 6G wireless systems. These secure blockchains for metaverse-empowered 6G can be built on secure mining, secure network communication, and secure access control principles.

B. Privacy-Preserving Federated Analytics for Metaverse-Empowered 6G

In a metaverse-empowered 6G system, there will be numerous devices and entities interacting to perform various tasks. These metaverse entities will share a significant amount of data. However, some applications (e.g., healthcare and Industry 5.0) may be hesitant to share their data, while others (e.g., autonomous cars) will generate substantial amounts of data. Transmitting such a vast volume of data from one entity to another would consume a considerable amount of communication resources.

To address these challenges, federated analytics can be employed to preserve privacy and reduce communication overhead. For example, consider the scenario of autonomous cars,
where each car generates massive amounts of data. Federated analytics can be used to minimize the data that needs to be transmitted. Instead of sending the entire dataset, only a function of the data can be transmitted, significantly reducing the consumption of communication resources. Various methods, such as analytical solutions and federated learning (as discussed in [72], [73]), can be used to compute these functions. Furthermore, to enhance user privacy during wireless communication, homomorphic encryption schemes can be applied.

C. Machine Learning for Anomalies Detection in Metaverse-empowered 6G Systems

How Can Machine Learning Enhance the Security of Metaverse-empowered 6G? Machine learning can play a crucial role in enhancing the security of metaverse-empowered 6G across various layers, including meta space, application space, and physical space. For example, machine learning can be utilized to detect anomalies in the physical space, which refer to data or events deviating from the norm. Such anomalies can significantly impact the performance of the 6G wireless system, making efficient detection essential.

To detect anomalies in the physical space, a centralized machine learning can be employed. However, it is important to consider privacy concerns related to data sharing in centralized approaches. To address these concerns, federated learning can be utilized. In federated learning, multiple anomaly detection modules are trained on local devices and then share their knowledge to collectively improve performance. While federated learning offers privacy preservation, it may have slower convergence compared to centralized learning due to the non-IID (non-identically distributed) nature of the data. Therefore, the development of novel federated learning schemes that enable faster convergence is necessary. Furthermore, effective anomaly detection schemes are also needed for the meta space and the service space to ensure comprehensive security.

D. Secure Wearable Devices for Metaverse-Empowered 6G

How Can Secure Wearable Devices for Metaverse-Empowered 6G Be Enabled? In 6G wireless systems, there will be a wide variety of wearable devices, such as extended reality devices. These wearable devices will contain sensitive data, including users’ personal information, password protection, and biometric data. Consequently, these devices will be vulnerable to various types of attacks, including authentication attacks, networking attacks (e.g., eavesdropping), physical security threats, and software security vulnerabilities.

Moreover, in future 6G networks, the number of wearable devices is expected to be significantly high, potentially replacing traditional devices like smartphones. The challenge of ensuring physical security for these devices is compounded by their massive numbers and distributed nature. Therefore, it is imperative to develop efficient and lightweight authentication schemes tailored for wearable devices. In addition to authentication, wearable devices will communicate via wireless channels with the meta space. Hence, the development of efficient encryption schemes for secure communication is essential. One potential solution is the use of homomorphic encryption, which preserves the confidentiality of data during transmission. Furthermore, machine learning can be employed.

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Design aspect</th>
<th>Causes</th>
<th>Guidelines</th>
</tr>
</thead>
</table>
| Blockchain-Empowered Secure Distributed Authentication Schemes | Meta space and physical space | • Single point of failure  
• High communication overhead for management signaling  
• High latency | • Distributed authentication schemes using secure mining  
• Secure networking for blockchain nodes communication  
• Secure access control |
| Privacy Preserving Federated Analytics for Metaverse-empowered 6G | Meta space and physical space | • Privacy leakage issues  
• High communication overhead | • Homomorphic encryption-enabled analytics  
• Federated learning |
| Machine Learning for Anomalies Detection in Metaverse-empowered 6G Systems | Meta space and physical space | • Abnormal events/activities degrade the system performance  
• Abnormal twins and avatars in meta space | • Centralized machine learning based schemes  
• Federated learning based schemes |
| Secure Wearable Devices for Metaverse-Empowered 6G | Meta space and physical space | • Distributed nature of massive number of wearable devices in 6G  
• Authentication attacks  
• Networking attacks | • Homomorphic encryption  
• Lightweight authentication schemes |
| Secure Metaverse-Empowered 6G Economy | Mainly on meta space | • Repudiation and refusal-to-pay and disrespectful avatars in metaverse  
• Malicious avatars and twins | • Centralized, secure body for regulating metaverse trading |
to enhance intelligent encryption methods, as discussed in [74].

E. Secure Metaverse-Empowered 6G Economy

How can we enable a secure metaverse-empowered 6G economy that provides digital asset ownership, service trust, and economic fairness? In metaverse trading, various fraudulent activities may occur, such as repudiation, refusal to pay, and disrespectful avatars. Additionally, ensuring the trustworthiness of twins and avatars during meta space modeling is essential. It is crucial to execute precise modeling to create authentic replicas of real-world 6G devices and entities. There is a risk of illegal copies of avatars and twins (e.g., Deira Twin Towers in Dubai) being created and sold for profit. Furthermore, the absence of a centralized entity to regulate the metaverse market poses challenges. The metaverse market is overseen by various distributed bodies, making it difficult to maintain globally unique prices, digital ownership, and trading, among other aspects. To address these challenges, there is a need to propose the establishment of a centralized governing body responsible for defining rules and regulations for metaverse-empowered 6G trading.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we have conducted a survey of security attacks within metaverse-empowered 6G systems and proposed a high-level architecture for enhancing their security. Our architecture suggested two main spaces, such as meta space and physical space. Next, we provided various kinds of enabling technologies for these spaces along with possible solutions. Finally, we presented some important open challenges. In future developments, several key directions emerge. These include advancing blockchain-based authentication for metaverse-empowered 6G systems, focusing on privacy and security concerns while incorporating secure mining, network communication, and access control within blockchain. Additionally, research must continue to optimize federated analytics for privacy preservation and reduced communication overhead, especially in high-data contexts like autonomous cars, utilizing techniques like homomorphic encryption. Machine learning’s role in anomaly detection across various metaverse-empowered 6G layers must expand, with a specific emphasis on efficient federated learning schemes and enhanced anomaly detection in both meta and service spaces. Moreover, lightweight authentication for the growing number of wearable devices and advanced encryption methods, such as homomorphic encryption, for secure wearable-device communication should be explored. Finally, the establishment of a centralized governing body to regulate metaverse-empowered 6G trading, mechanisms for ensuring the trustworthiness of twins and avatars, and strategies to combat fraudulent activities in the metaverse market must be actively developed.

REFERENCES

Latif U. Khan received his Ph.D. degree in Computer Engineering at Kyung Hee University (KHU), South Korea. Prior to that, He received his MS (Electrical Engineering) degree with distinction from University of Engineering and Technology, Peshawar, Pakistan in 2017. He is the recipient of KHU Best thesis award. He is author of two books: (a) Network Slicing for 5G and Beyond and (b) Federated Learning for Wireless Networks. He has reviewed over 200 times for the top ISI-Indexed journals and conferences. He has authored many most popular articles in the leading journals (i.e., IEEE Communications Surveys and Tutorials) and magazines (IEEE Communication Magazine, IEEE Network, and IEEE Wireless Communications Magazine). His research interests include analytical techniques of optimization and game theory to edge computing, end-to-end network slicing, wireless federated learning, and digital twins.

Mohsen Guizani (S’85, M’89, SM’99, F’09) received his B.S. (with distinction) and M.S. degrees in electrical engineering, and M.S. and Ph.D. degrees in computer engineering from Syracuse University, New York, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor with the Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE. Previously, he served in different academic and administrative positions at the University of Idaho, Western Michigan University, the University of West Florida, the University of Missouri-Kansas City, the University of Colorado-Boulder, and Syracuse University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He was the Editor-in-Chief of IEEE Network. He serves on the Editorial Boards of several international technical journals, and is the Founder and Editor-in-Chief of the Wireless Communications and Mobile Computing journal (Wiley). He is the author of nine books and more than 500 publications in refereed journals and conferences. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as a IEEE Computer Society Distinguished Speaker and is currently an IEEE ComSoc Distinguished Lecturer. He is a Senior Member of ACM.

Ibrar Yaqoob (S’16–M’18–SM’19) is a Senior Lecturer/Senior Research Fellow at AI and Cyber Futures (AICF) Institute, Charles Sturt University, Australia. He is a theme lead for the Smart and Resilient Supply Chains strand at the AICF. Before joining the AICF, he worked as a Research Scientist with the Department of Electrical Engineering and Computer Science, Khalifa University, United Arab Emirates. Previously, he worked as a research professor at the Department of Computer Science and Engineering, Kyung Hee University, South Korea, where he completed his postdoctoral fellowship. He worked as a research assistant at the Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya. He received his Ph.D. (Computer Science) from the University of Malaya, Malaysia. He is working on the editorial boards of IEEE, Elsevier, and Springer journals. He has been involved in a number of conferences and workshops in various capacities, such as as Chair, Co-chair, and Track Chair. His current research focuses on leveraging blockchain, NFTs, and metaverse for healthcare, supply chain and logistics, wireless networks, IoT, and smart cities. Furthermore, he has conducted research in the areas of mobile edge-cloud computing, IoT, computer networks, and big data. He has been selected as a highly cited researcher (HCR) worldwide for multiple years, 2021 and 2022, by Clarivate (Web of Science).

Dusit Niyato (M’99–SM’15–F’17) is a professor in the School of Computer Science and Engineering, at Nanyang Technological University, Singapore. He received B.Eng. from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand in 1999 and Ph.D. in Electrical and Computer Engineering from the University of Manitoba, Canada in 2008. His research interests are in the areas of sustainability, edge intelligence, decentralized machine learning, and incentive mechanism design.

Ala Al-Fuqaha (Senior Member, IEEE) received the Ph.D. degree in computer engineering and networking from the University of Missouri-Kansas City, Kansas City, MO, USA, in 2004. He is currently a Professor at the Information and Computing Technology Division, College of Science and Engineering, Hamad Bin Khalifa University (HBKU), Doha, Qatar. His research interests include the use of machine learning in general and deep learning in particular in support of the data-driven and self-driven management of large-scale deployments of the Internet of Things (IoT) and smart city infrastructure and services, wireless vehicular networks (VANETS), cooperation and spectrum access etiquette in cognitive radio networks, and management and planning of software-defined networks (SDNs).
Choong Seon Hong (S’95-M’97-SM’11) received the B.S. and M.S. degrees in electronic engineering from Kyung Hee University, Seoul, South Korea, in 1983 and 1985, respectively, and the Ph.D. degree from Keio University, Tokyo, Japan, in 1997. In 1988, he joined KT, Gyeonggi-do, South Korea, where he was involved in broadband networks as a member of the Technical Staff. Since 1993, he has been with Keio University. He was with the Telecommunications Network Laboratory, KT, as a Senior Member of Technical Staff and as the Director of the Networking Research Team until 1999. Since 1999, he has been a Professor with the Department of Computer Science and Engineering, Kyung Hee University. His research interests include future Internet, intelligent edge computing, network management, and network security. Dr. Hong is a member of the Association for Computing Machinery (ACM), the Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), the Korean Institute of Information Scientists and Engineers (KIISE), the Korean Institute of Communications and Information Sciences (KICS), the Korean Information Processing Society (KIPS), and the Open Standards and ICT Association (OSIA). He has served as the General Chair, the TPC Chair/Member, or an Organizing Committee Member of international conferences, such as the Network Operations and Management Symposium (NOMS), International Symposium on Integrated Network Management (IM), Asia-Pacific Network Operations and Management Symposium (APNOMS), End-to-End Monitoring Techniques and Services (E2EMON), IEEE Consumer Communications and Networking Conference (CCNC), Assurance in Distributed Systems and Networks (ADSN), International Conference on Parallel Processing (ICPP), Data Integration and Mining (DIM), World Conference on Information Security Applications (WISA), Broadband Convergence Network (BcN), Telecommunication Information Networking Architecture (TINA), International Symposium on Applications and the Internet (SAIN), and International Conference on Information Networking (ICOIN). He was an Associate Editor of the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and the IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS. He currently serves as an Associate Editor for the International Journal of Network Management.