Human-centric Computing and Information Sciences

December 2022 | Volume 12

www.hcisjournal.com

KIPS Korea Information Processing Society

KIPS CSWRG Korea Information Processing Society Computer Software Research Group

HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2022) 12:60
DOI: https://doi.org/10.22967/HCIS.2022.12.060
Received: August 31, 2022; Accepted: November 5, 2022; Published: December 30, 2022

The Future of Metaverse: Security Issues, Requirements, and Solutions

Min Choi[1], Abir EL Azzaoui[2], Sushil Kumar Singh[2], Mikail Mohammed Salim[2], Sekione Reward Jeremiah[2], and Jong Hyuk Park[2,*]

Abstract

Recently, the term “Metaverse” gained more interest from both industry and academia, especially after major companies announced metaverse as a novel billion-dollar industry. Metaverse is built upon various existing technologies such as virtual reality (VR), augmented reality (AR), the latest network generation (5G), blockchain, and so on. These technologies are highly developed, yet they are prone to multiple security issues. While the industry is working to develop the metaverse for average users, academia is still lacking related research, notably in the security area. However, only a few of research papers addressed the security and privacy issues related to these applications. Metaverse requires real-time and continuous data collection from users including private data such as location, identification, and biometric data. Before any further development of metaverse applications, the possible security threats must be mitigated. To this end, in this paper, we conduct a comprehensive survey on metaverse. The main contribution of this research is to give a comprehensive insight for future researchers regarding the current metaverse projects around the world and their security issues, along with some of the recent solutions and technologies used to improve metaverse quality of experience and security.

Keywords

Metaverse, Security, Privacy, Virtual Reality

1. Introduction

With the development of artificial intelligence (AI), digital twin, virtual reality (VR), augmented reality (AR), and many other technologies, the concept of the metaverse was proposed [1]. The metaverse is a virtual 3D world with an immersive experience, and the virtual world and the physical world are interconnected and can influence each other [2]. In addition, the Metaverse is unified and permanent, and the change in a user's operation on the metaverse is irreversible and will affect the whole virtual world and even the real world [3]. Although the metaverse is just a concept at the present stage, many industries, such as e-commerce, education, medical care, media entertainment, and real estate, which are important components of the metaverse, are making revolutionary innovations and development. They are investing

***Corresponding Author:** Jong Hyuk Park (jhpark1@seoultech.ac.kr)
[1]Department of Information and Communication Engineering, Chungbuk National University, Cheongju, South Korea
[2]Department of Computer Science and Engineering, Seoul National University of Science & Technology (SeoulTech), Seoul, Korea

in and studying the Internet economy across digital and physical worlds based on the metaverse [4]. In Web 2.0, users lose control over content ownership, and their creations belong to centralized service providers, who provide them with ample incentives to create. In Web 3.0, power shifted from centralized platforms like Google and Microsoft to networks controlled by multiple stakeholders who used the platforms and were financially rewarded for their content. The metaverse is the ultimate theme that can merge the physical world with the digital world, based on Web 3.0 and using various technologies such as VR, AR, and blockchain. Metaverses are different from immersive VR games, and while the two concepts are very similar in the general public's perception, there are many more possibilities in metaverse. Metaverses have more freedom than company-run games or social platforms [5]. Currency in the metaverse has real value, rather than being worthless once off the platform. Behavior in the metaverse can affect the real world and not only the real world affects the virtual world. Everything in the metaverse will be explored, and there will be new opportunities and challenges in metaverse, such as social and economic issues that will be reflected directly in the metaverse. Facebook's CEO said the metaverse will be a "generational leap" in physical and digital networks, and that society will evolve along with it. In order to achieve such a huge leap, very large financial support and solid technical support are needed [6].

The creation of a sustainably maintained metaverse requires the support of almost all current technology domains [7]. Creating immersive virtual Spaces requires the support of VR and creating connections between VR and the real world requires the support of AR. Bringing and sharing real-world objects into Metaverse and maximizing privacy in metaverse requires digital twins. If metaverse is to provide additional real-world data, it requires sensors from smart devices. The application of smart sensors and related technologies makes data collection and processing more efficient and enhances the stability and diversity of the connection between the real world and the virtual world. Metaverse will also offer a rich marketplace for physical and virtual goods [8]. Transactions in metaverse will be bound to and owned by the characters themselves, implemented as non-replaceable tokens (non-fungible tokens [NFTs]), and transactions between them will be more secure and non-repudiation. Next-generation web technologies and algorithms (6G and quantum algorithms) will make metaverse more ubiquitous than current social media and social networking platforms. Blockchain-based NFT makes transactions in virtual worlds more secure and open; digital creation and digital authorization based on AI is a necessary foundation for the benign evolution of the metaverse ecosystem. The integration of AI and blockchain can build an intelligent, open, and fair metaverse ecosystem [9]. All in all, the existing techniques of classical computer science have great potential for future metaverse, where in order to efficiently and safely create and manage the metaverse, human posture and eye tracking, sustainable management technology, privacy security, and real-time data processing are important challenges in the sustainable development of the metaverse. Non-vertical industries such as the culture industry, tourism industry, and news media will also better export their content on a complete platform, providing a completer and more immersive environment for experience, thus promoting the understanding of the whole human society [10].

The metaverse market is a competitive and fragmented one. New communities in emerging regions are entering more and more, and there is a growing demand for services such as education, knowledge sharing, and networking. Countries around the world have carried out lively research on this new concept. Tencent Ltd., Facebook, NetEase, Bytedance Ltd., Epic Games, NVIDIA Corporation, Unity Technologies, Roblox Corporation, Lilith Games, Roblox Corporation, NetEase, and ZQGame are currently the major holding companies in the metaverse market. Each company has its own specialty, and they are more inclined to use its cutting-edge technology and large-scale market to create competitive advantages in the metaverse. For example, Tencent plays the role of the world's largest video game provider and has absolute dominance of social networks in China. Therefore, Tencent pays less attention to the importance of VR hardware and prefers to use video games as its niche market in the metaverse. At the other end of the spectrum is Google, where CEO Sundar Pichai explained his vision of the metaverse as "computing evolving in an immersive way with augmented reality." In fact, Google already has extensive experience in augmented reality with its Google Glass product. In November 2021, Google also reorganized its VR and AR divisions with a new Google Labs team that included Project Starline, a

holographic video conferencing tool. Google's current focus is on connecting us through enhanced avatars that combine the digital and physical worlds. While we have not seen a solid metaverse solution from Google yet, the foundations are there [11].

No matter what technology is used in the Web 3.0 era, there are various security risks: evasion attacks, poison attacks, backdoors for AI technology, 51% attacks on blockchain, terminal security, and key management issues [12]. The metaverse is a virtual world that integrates the technology and cultural features of various fields, so the combination of single technologies may produce more and more serious security risks and vulnerabilities. In addition, the contradictory and diversified data of different cultures, religious beliefs, and political opinions in Metaverse will cause an unexpected cognitive impact on users' ontology, thus increasing the possibility of ordinary users being subjected to network fraud and high-tech fraud. Therefore, the security needs of Metaverse are becoming more and more important as its popularity increases. There is an increasingly strong demand for a comprehensive investigation of Metaverse security-related fields, and vulnerability repair and prevention of technical security are imminent.

In this paper, we conduct a comprehensive and systematic survey of the security problems, security requirements, and related solutions in the Metaverse. Based on the existing research and projects related to the Metaverse, we summarize the applied technologies of the Metaverse and propose an architecture of the Metaverse. This architecture divides the Metaverse into several levels and provides a detailed description of the interactions between each level. Finally, a use-case scenario for a secure and private Metaverse environment is created and discussed, and the future development direction and research motivation of the Metaverse are discussed from this scenario.

The main contribution of this paper is summarized as follows:

- We present a comprehensive and detailed summary of the concept of the Metaverse while underlying the major required technologies.
- A detailed summary of the recent developments in the research of the Metaverse is presented, and the recent related projects and research achievements are discussed.
- We explain the characteristics of the Metaverse and proposed the structural framework of the Metaverse with a detailed description of the technologies that can be applied in the Metaverse. On the premise of diversity technology fusion, it lays the technological foundation for the ecological environment of the Metaverse.
- This paper delves into security issues in Metaverse and explores existing solutions to them. From the aspects of privacy security, malicious attacks, decentralized systems, real-time communication with the real world, and so on, we sort out the frequent problems and summarize the security requirements of the Metaverse.
- Finally, we propose a comprehensive definition of a secure and private Metaverse environment and provide a use case scenario. According to this scenario, the future research direction is discussed, and then the related research in the field of Metaverse security is planned and guided.

The rest of the paper is organized as follows: Section 2 discusses the recent state-of-the-art related works regarding Metaverse market and use cases along with the technologies deployed in Metaverse. Section 3 depicts the architecture of Metaverse with all the required elements and technologies. In Section 4, we discuss the security and privacy issues of Metaverse and some of the recent and feasible solutions.

2. Related Work

Nearly 30 years ago, Neal Stephenson's science fiction novel *Snow Crash* introduced the idea of the Metaverse [13]. However, Metaverse has recently sparked a lot of interest in the tech industry and academia. In academia, several survey articles considering various aspects of the Metaverse have been published up to this point. Metaverse has also gained attention in the tech industry mainly due to recent advancements in VR/AR, Internet of Things (IoT), AI, blockchain technology, and cloud computing. This section provides the existing cutting-edge metaverse studies (Section 2.1). From the tech industry, we highlight the most significant metaverse projects (specific metaverse products) and their representative

companies alongside their countries of origin (Section 2.2). In Section 2.3, we point out the key considerations of our work.

2.1 Existing Survey Papers

Metaverse has sparked a lot of interest for researchers. Several survey papers considering several aspects of the metaverse have been published up to this point. For example, eight essential technologies that make up the metaverse are reviewed and examined by Lee et al. [1], together with the prospects it presents from six user-centric aspects. Yang et al. [9] look into the possibilities of fusing blockchain and AI technology to create future metaverses. In terms of national policies, industrial initiatives, infrastructures, supporting technologies, VR, and social metaverse, Ning et al. [4] assess the development state of the metaverse. Dionisio et al. [14] outline four qualities of successful 3D virtual worlds (or metaverses), including ubiquity, realism, scalability, and interoperability, and they also address continuous advancements in the underlying virtual world technology. Park and Kim [15] evaluated the user interaction, implementation, and typical applications in the metaverse environment and described three components of the metaverse (i.e., content, software, and hardware). From a sociological and legal standpoint, Leenes [16] examines potential privacy problems in online games.

This paper thoroughly analyzes the metaverse's foundational concepts and the major problems and potential solutions for creating a safe and private metaverse. In contrast to the previous surveys on the general metaverse or the potential for service provisioning in social VR/AR games [17], hybrid education [18], metaverse retailing [19], computational arts [20], and metaverse for social good [24], we concentrate on the perspective of metaverse security and privacy issues, such as potential security/privacy threats, critical security/privacy challenges, and state-of-the-art solutions. Table 1 summarizes our key contribution in relation to other relevant works to understand better the key difference between our work and relevant existing ones [1, 4, 9, 15–17, 19, 20].

Table 1. Comparison between our work and existing ones

Study	Year	Main contribution
Falchuk et al. [17]	2018	A survey on security and privacy concerns and solutions pertaining to digital footprints in social metaverse games.
Leenes [16]	2020	This article covers a survey on designing, creating, and implementing a virtual or metaverse world in a learning environment (for hybrid education).
Bourlakis et al. [19]	2021	Survey and proposal for a 3-layered architecture for metaverse applications intended to be used for social goods.
Lee et al. [1]	2021	The study explored six user-centric factors (i.e., Avatar, Content Creation, Virtual Economy, Social Acceptability, Security and Privacy, and Trust and Accountability. Then the study suggests a specific research plan for the growth of the metaverse.
Ning et al. [4]	2021	This article describes the technological architecture of the metaverse. It discusses the development status from five viewpoints, i.e., network infrastructure, management technology, fundamental standard technology, VR object connection, and VR convergence. The study also covers the metaverse's social and hyper spatiotemporal aspects and examines its initial application domains as well as some potential issues and difficulties.
Lee et al. [20]	2021	This article provides an in-depth analysis of computational arts, focusing on seven crucial areas pertinent to the metaverse and describing cutting-edge works in hybrid virtual-physical worlds.
Yang et al. [9]	2022	The study explores the metaverse and discusses how blockchain and AI interact with it. It examines the most recent studies on its elements, digital currencies, virtual world AI applications, and blockchain-enabled technology.
Park and Kim [15]	2022	The study reviews user interaction, implementation, and representative applications in the metaverse and the hardware, software, and content components that make up the metaverse.
This work	2022	A comprehensive survey of the metaverse's general architecture, requirements, security, and privacy concerns, discussions of its most pressing challenges, current state-of-the-art solutions, open issues, and future research directions to secure metaverse.

Table 2. Representative metaverse projects

Company	Country	Project description
Amazon	USA	Amazon has been attempting to enhance the VR shopping experience since 2018. While that shows its market dominance, it also aims to develop a virtual store and improve user experience.
Roblox	USA	With Roblox, the only limitation is one's creativity because Roblox allows users to create virtual worlds or other games. Roblox is compatible with iOS, Android, PC, and Mac, enabling VR equipment to enhance user experience.
Facebook	USA	It was announced in July 2021 that Facebook would change its name to Meta in November 2021 and become a metaverse corporation within five years. For that goal, the company invested over $10 billion in its Reality Labs initiative [22].
Disney	USA	In November 2020, Tilak Mandadi, Disney parks experience and products' executive vice president, said in an attempt to transform Storytelling and bring it to life, building a "theme park metaverse" was the next step [23].
NVIDIA	USA	Nvidia unveiled the Nvidia Omniverse project on August 11, 2021, intending to develop the first virtual simulation and collaboration platform [24].
Microsoft	USA	In 2021, Microsoft revealed that Mesh for Microsoft Teams, said to be Microsoft's version of the metaverse, would be available early in 2022 [25].
Tencent	China	To rank among the top players in the metaverse business, Tencent has made several investments in the ecosystem of the metaverse, including the AR development platform.
Alibaba	China	The E-commerce giant Alibaba had recently applied for the registration of trademarks such as "Ali Metaverse" and "Taobao Metaverse." Alibaba has the potential to recreate itself in the metaverse, moving away from the oversaturated e-commerce sector [26].
ByteDance	China	By purchasing a Chinese VR startup PoliQ, ByteDance increases its investment in the metaverse. PoliQ will be integrated into the VR headset company PICO which is also owned by ByteDance [27].
NetEase	China	The design of metaverse by NetEase is centered on the gaming industry and offers simple tools for game creation. The corporation invested in both the IMVU virtual character platform and IMPROBABLE's meta-computing platform, enabling others to create virtual worlds.
Sony	Japan	The first Japanese metaverse platform, Mechaverse, allows businesses to swiftly introduce new products and provide users access to video introductions and 3D model trials.
Avex Business	Japan	The "Virtual Avex Group," founded by Avex Business Development and Digital Motion, intends to promote animated video game characters, host virtual events, and virtualize live performances.
Samsung	South Korea	The largest asset manager in South Korea, Samsung Asset Management, has introduced a fund linked to the metaverse, a virtual environment.
SK Telecom	South Korea	To begin its 5G virtual service business, South Korean mobile carrier SK Telecom in July 2021unveiled a brand-new metaverse platform named "Ifland." The term alludes to a virtual environment where users may adopt any identity they like, interact with anybody they choose, and realize a vast array of possibilities [28].
Maze Theory	UK	A "fan metaverse" will be built on well-known IPs and fan worlds by the well-known British VR firm Maze Theory [29].
Stage11	France	Stage11 was founded in 2020 and has already started on its quest to reimagine music for the metaverse. It will utilize the €5 million funding to bring on crucial recruits, sign influential artists and brand relationships, and develop its infrastructure [29].
RIMOWA	Germany	RIMOWA, a German luxury luggage company, announced in May 2021 that it would collaborate with NUOVA to release 4 NFT artworks for their metaverse project [30].
Gucci	Italy	Gucci's most recent metaverse collaboration is with 10KTF, an NFT project that features a virtual floating "New Tokyo" world, fashionable items NFT owners can buy for their profile pictures [31].

2.2 Metaverse Projects

Metaverse combines cutting-edge technologies such as 5G, cloud computing, computer vision, blockchain, artificial intelligence, and more, finding its applications mostly in video games, art, and

business. From Section 2.1, we had a preliminary overview and understanding of the diverse research and publications in the area of metaverse. In this section, we'll discuss the significant representative metaverse projects alongside their companies and the countries in which they originated. Table 2 summarizes these projects and their representative companies.

2.3 Key Consideration

The primary consideration of our paper is as follows:

Metaverse architecture: in our work, we discuss the metaverse fundamentals, including its general design architecture, enabling technologies, and critical characteristics.

Projects and applications: Our work also closely examines some state-of-the-art metaverse projects and applications alongside their related companies and countries of origin.

Security and privacy: We examine security and privacy issues in the metaverse environment from several perspectives, the significant difficulties in addressing them, the state-of-the-art measures and solutions, and their feasibility in securing the metaverse environment.

Open issues: we highlight the present and future open research directions for developing the metaverse realm that is efficient, secure, and with privacy-preserving capabilities.

3. Overview of Metaverse Architecture

In this section, the relationship between the physical and virtual dimensions is investigated, forming the foundation of the metaverse environment. A layered architecture highlights the key infrastructure components and technologies required to connect the user with the 3D virtual world, including spatial computing, a decentralized platform, and the human interface. Furthermore, we discuss the types of data collected from user interaction with the metaverse using devices and sensors. Finally, we present the different types of existing metaverse applications and potential future application prototypes.

3.1 Metaverse Architecture

The virtual 3D world is built on the foundation of fusing multiple technologies such as 6G, edge computing, digital twins, blockchain, and AI, enabling an immersive, low latency, and secure environment-based user experience. As illustrated in Fig. 1, the foundational technologies of the metaverse environments are as follows.

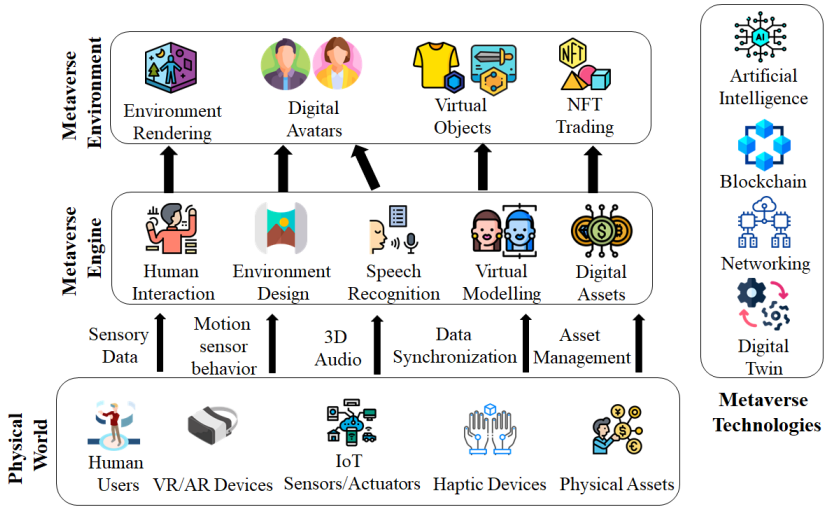

Fig. 1. Metaverse architecture.

3.1.1 Artificial Intelligence

AI-empowered decision-making systems supported by big data and deep learning models provide intelligent and autonomous systems for various digital infrastructures. The convergence of AI with the metaverse enables the designing of immersive environments by populating them with human-like non-playable characters (NPC). Popularized in video games, NPCs in the metaverse use natural language processing to support users with digital assistants for voice analysis, text-to-speech conversion, and cognitive behavior generation. Computer vision is another application of AI in the metaverse for generating human-like models with realistic facial expressions and emotions in response to human interaction. Convolutional neural network (CNN) models deep scan visual models such as facial expressions and eye gaze tracking to inhabit realistic models in the metaverse. Furthermore, the infusion of computer vision and natural language processing populates the virtual environment with life-like digital humans, animals, and birds mimicking natural movement patterns and responses to user interaction. Reinforcement learning is implemented for building computer agents with decision-making protocols in response to the surrounding environment. NPCs learn using trial and error methods and create an improved response behavioral model with each consecutive user interaction.

3.1.2 Blockchain

Decentralized networks prevent a single authority such as a metaverse service provider from controlling all aspects of user data. Blockchain technology provides secure data storage by storing data in blocks and linking each block with its predecessor using a consensus model. Each block holds the hash value of each previous block, thus preventing data modification attempts. Metaverse relies on the decentralized architecture to avoid single point of failure vulnerabilities prevalent in centralized databases. Moreover, the decentralized architecture's secure and non-repudiation characteristics provide a record of each data shared with other entities using smart contracts. Data requests using smart contracts are recorded and stored in blocks, thus creating irrefutable proof of transfer of data ownership. The metaverse environment protects data ownership rights for all user-generated data using NFT. Metaverse users, designers, and creators monetize their digital assets by tokenizing them as NFTs and maintaining a private key granting them ownership. An Ethereum-based blockchain network secures all digital content as each NFT is unique and is assigned a unique ID and metadata. Transfer of ownership is tracked and recorded, representing the original owners of the content and the chain of ownership till the current owner.

3.1.3 Digital twin

Digital twins are virtual reproductions of real-world physical objects and serve as the foundational blocks of the metaverse environment. Physical objects are mirrored in the virtual world using IoT sensors connected and streaming data in real time. Object mapping for the metaverse extends to human beings, neighborhoods, hospitals, and entire city infrastructure. Furthermore, data modeling and data analysis of digital twins using AI algorithms enable prediction analysis of the physical object behavior and replicate in the metaverse. AI further enables the construction and design of large-scale and complex rendering of physical entities for precise model creation in the metaverse resulting in increased user immersiveness.

3.1.4 Extended reality (VR/AR/mixed reality)

Embedded sensors in user hardware extend to head mounted displays (HMD), brain-computer interface, and VR devices that serve as input to the user experience in the metaverse environment. Physical sensors models user behavior based on recognition of physical motion, hand gestures, and brain wave signals. VR devices serve as gateways to the immersive environments for users to experience the virtual world, whereas sensors connected to users, mimic their physical behavior and project them on the virtual environment.

3.1.5 Networking

Metaverse requires and relies on low latency solutions to bridge the physical and virtual world and guarantee an immersive experience similar to reality. A lag in response between an action initiated by the user wearing the HMD and its reaction in the virtual world produces a dizziness effect. Metaverse worlds for healthcare education and driving schools require real-time responses, and as such, edge computing plays an essential role in executing computation near the device layer. Current 5G networks support near-zero latency for the transmission of graphics of the virtual world to display hardware. As realism takes precedence for increased immersion and the amount of social data grows, faster network communication technologies are required. The future of telecommunication technology focuses on the next generation of 6G networks with higher bandwidth and increased mobility support, fusing AI to push computing operations from the network core to near devices on edge.

4. Security Issues of Metaverse and Existing Solutions

In this section, we discussed security issues and existing solutions in metaverse applications. It utilized various advanced technology such as AR, VR, mixed reality (MR), and others for the development of smart applications. However, it offered an interactive, advanced environment in the current social media platform. Still, there are many security and privacy challenges and threats, such as identity-related threats, data-related threats, network-related threats, and many more, according to the advanced version requirements of daily life in metaverse applications.

4.1 Security and Privacy Issues of Metaverse

Security and privacy issues in metaverse applications are discussed in this subsection. So, we categorized these issues into eight categories based on various threats such as identity, data, network, and many more, which are the following.

4.1.1 AR-based security and privacy issues

AR is essential pillar technology of metaverse, which provides virtual content as a real environment in advanced applications. With the utilization of AR advancement, it uses advanced approaches, mechanisms, and tools for collecting IoT and sensor data. On the other hand, AR provides new possibilities for linking real and virtual worlds. Still, there are many security and privacy issues available in AR-based applications, which are directly connected to the metaverse applications. For example, if malicious users compromise AR devices, then generate a user privacy issue. In addition, social engineering attacks, user network credential theft, and distributed denial of service (DDoS) attacks are part of AR-based security and privacy issue [32].

Social engineering attacks: User identification is an essential task for security and privacy in every metaverse application. Thus, anyone can show their identity with relevant ID documents in a real-world application. But the user must need a face, voice, and video identification in the metaverse environment; Avatar completes it with the help of AR and VR devices [33]. Thus, an unauthorized user can hack the user's personal information through social engineering techniques if he compromises AR or VR devices. So, it is called social engineering attack.

User's network credential theft: User's network credential theft is a metaverse application security and privacy issue because anyone can access the network credentials easily, then user identity can be accessed easily [34]. Thus, malicious users compromise the network credential of the users via advanced devices, which is based on AR and VR.

DDoS attack: We know that metaverse gaming application is dependent on AR and VR because these games need interactive environments with high-definition connectivity of networks. For this purpose, advanced AR and VR devices provide high-definition connectivity to the network. But, in the pipeline of

network resource requests, malicious users can send requests for network resources, then generate privacy issues in the metaverse gaming applications [35]. This attack is related to the DDoS attacks.

4.1.2 VR-based security and privacy issues

VR is the technology that offers an automatic and artificial environment with automation software to the user worldwide in the metaverse applications and shows the real infrastructure. Various games and applications such as Tilt Brush, virtual Rick-ality, Cloudlands VR Minigolf, Moss, Wipeout Omega Collection, Catan VR, Astro Bot Rescue Mission, and many more are available, dependent on VR [36]. Like AR, VR is also responsible for security and privacy issues in metaverse applications, such as biometric data in fingerprints, retina scans, voice prints, and facial recognition. Ransomware and identity theft attacks are the major privacy issues in the metaverse with VR.

Ransomware attacks: It is like a social engineering attack, but it is generated due to the VR in the metaverse applications. For example, the malicious user can easily insert the basic functionality in the VR platform or VR devices and change the original information or hack the user's personal information, then call ransom to the actual user in the form of digital currency [37].

Identity theft attacks: We know that VR is the essential technology for advanced metaverse applications because it provides a better virtual environment with the help of digital avatar. Still, various machine learning-based algorithms and applications are available to modify the audio and videos of the actual user; it seems like actual user sounds and images. Thus, a malicious user easily hacks the motion-tracking data of a VR headset as an actual user [38]. So, we can say that identity theft attack is generated in the metaverse with VR.

4.1.3 Impersonation attack

In the metaverse applications, we use a digital avatar for functioning as an actual user in the real world to the virtual world. Unauthorized users can change their form as impersonation and access the metaverse system services. For example, an unauthorized user uses the same helmet or device on the digital avatar with the help of AR and VR devices and gets up the impersonate user and access the metaverse services of the advanced applications. Another example is that the hacker can exploit Bluetooth impersonation threats to the network's actual Bluetooth endpoint, and illegally access metaverse services [39].

4.1.4 Avatar verification and validation issue

In the virtual world as a metaverse, user authentication and verification are typical tasks compared to the real world because face, video, audio authentication, and validation are used as digital avatars in the virtual world [4]. With advanced AR and VR devices or tools, and AI bots, an attacker can easily create the same sounds and videos by imitating the actual user's appearance. Thus, we can say that the security and privacy of the digital avatar are primary issues of the metaverse applications.

4.1.5 Managing issue of new types of data

According to the metaverse requirements, various new types of data such as head and hand movement, facial recognition, data storage, and hardware devices such as AR and VR for more interactive environments. For this purpose, metaverse applications need high-definition connectivity also more advanced security and privacy techniques needs for the metaverse. Managing these data and devices is the challenge of metaverse applications; also advanced security and privacy techniques are also challenging issues for metaverse applications nowadays.

4.1.6 Privacy leakage in data communication and processing

In metaverse applications, data collection task is completed from advanced sensors or augmented intelligence of things and wearable devices such as HMDs [1]. Then, data are communicated by guided or unguided media. Currently, existing encryption and decryption techniques are not feasible for secure data transmission and processing. Thus, we can say that privacy leakage is also challenging security and

privacy issues in the metaverse application because advanced attacks are also available at the present time.

4.1.7 Misuse of digital avatar

According to the metaverse applications, all works are completed by the digital avatar. Suppose a hacker hacks the activity of the actual digital avatar via AR and VR tools and devices. In that case, the hacker creates a malicious avatar and misuses the metaverse applications such as gaming, banking, and others. Then, generate security and privacy issues in the applications.

4.1.8 Wearable devises key management as security

For security purposes, key management (Generation, Distribution, Updating, Recovery, and all) of the wearable devices are the primary task in the metaverse. Existing key management techniques are based on cryptographic systems such as public key infrastructure, Diffie-Hellman, and others. However, in the metaverse, key management of wearable devices needs more computation power, memory size, and latency which is not available in existing encryption and decryption key management technique [40].

4.2 Existing Solutions

Many researchers provide solutions for security and privacy issues in metaverse applications. These solutions are based on various advanced technologies, including blockchain, digital twin, federated learning, avatar confusion, and private copy, cloud forensic, image fingerprints, AR, VR, and others for the development of secure metaverse applications. Security and privacy issues in metaverse are based on various attacks such as data-related attacks, identity-related attacks, network-based attacks, transaction-based attacks, and many more.

Shen et al. [41] used blockchain technology to create a decentralized cross-domain authentication scheme. The proposed method used anonymous authentication protocols and offers a trust environment and identity-based encryption via consortium blockchain, and it was proved to be safe in multiple attack types such as identity theft, privacy attacks, man-in-the-middle attacks, and so on. On the other hand, in order to secure metaverse environment from digital footprints and privacy threats, Falchuk et al. [17] proposed a novel technique using avatar confusion and private copies. The adapted method provides complete confusion and private copy to the avatar via privacy preservation tools for digital footprints in metaverse applications and it is suitable for digital footprints attack and other privacy threats. Zhu et al. [42] used a heuristic greedy method for dynamic node blocking against physical, social, and information spreading threats in metaverse applications. The proposed method deploys dynamic node blocking technique to minimize misinformation spreading influence in online social networks such as metaverse. Krishnan et al. [43] tried to solve intrusion-based network attacks in metaverse environment using digital twins and SDN. The proposed method constructs a behavior monitoring and profiling approach where security procedures are evaluated on digital twins, then deployed in a real network as a metaverse environment.

Another approach to solve privacy violations and governance-based threats was proposed by Zoo et al. [44] using cloud-based privacy leakage forensics scheme. In their paper, a privacy leakage forensics scheme is proposed to get digital proof without touching users' private data in a simulated virtual domain with taint investigation and RAM mirroring. Identity, data, and network related attacks are a critical problem in metaverse era, to this end, Sayegh [45] tried to solve this dilemma using advanced threat detection methods based in multi-factor authentication and strong password techniques. The proposed scheme implemented visibility and analysis throughout the fabric of the metaverse to detect anomalies, uncover activities, and maintain experiences. Another problem in metaverse is the transaction data-based attacks that was approached by the author of [46] using hash-chain-based aggregate digital signature technique. The proposed solution provides the guarantee of the reliability, authenticity, and traceability of transactions and digital data in metaverse applications. Ruth et al. [47] took under consideration the

unsecure AR content sharing attack and tried to solve it using content sharing control mechanism. The proposed solution implements a prototype as a content sharing mechanism on HoloLens to permit AR content sharing among remote users with inbound and outbound control. Transaction and economy-based attacks in another critical issue with metaverse security that was approached by Guan et al. [48]. In their paper, authors deployed blockchain technology and proposed a zero-knowledge proof-based blockchain scheme with privacy preservation for secreting sender-recipient linkage, account balances, and transaction amounts in metaverse. Han et al. [49] deployed hierarchical game for dynamic and optimized digital twins synchronization in metaverse environment. In metaverse applications, end devices collect the status information of physical entities, and virtual service providers determine the proper synchronization intensities. Li et al. [50] tried to solve privacy and network security issues using blockchain as well to create a decentralized forensics method. The proposed method deploys smart contracts to implement automated forensics systems among multiple entities and platforms with enhanced convenience and mitigated costs in the metaverse. While Kwon et al. [51] proposed a novel way to enhance metaverse's quality of service and its security. The authors investigated the convergence of quantum techniques with metaverse in four main points including security, randomness, computation, and communication. The authors proposed the usability of both quantum random number generation (QRNG) and quantum key distribution (QKD) to enhance the security of metaverse against current and future cyber-attacks. Quantum algorithms can be used also for complex optimization problems in metaverse as mentioned in paper [52].

Based on the aforementioned survey on security and privacy issues, we strongly believe that security measurements shall be enhanced and improved before any further development in metaverse applications. Metaverse is a merge of multiple technologies that are prone to various security threats, thus, mitigating those issues is a pillar phase that both academia and industry are required to solve it.

5. Conclusion

Metaverse is built upon various existing technologies such as VR, AR, extended reality (XR), AI, the latest network generation (5G), blockchain, and so on. These technologies are highly developed, yet they are prone to multiple security and privacy issues. Merging all of the aforementioned technologies and more into one application would create a complex system with more censorious security dilemmas. While the industry is working to develop and improve the metaverse for average users, academia is still lacking related research, notably in the security area. Most of the currently published research papers discuss the potential of metaverse in various industries such as military, education, real estate, and so on. However, only a few of them addressed the security and privacy issues related to these applications. Metaverse requires real-time and continuous data collection from users including private data such as location, identification, and biometric data. This information urges high-security levels as they are critical to the user. Before any further development of metaverse applications and expansions in use cases, the possible security threats must be mitigated. In this paper, we conduct a comprehensive survey on metaverse and its related security and privacy issues while discussing some of the possible mitigations.

Author's Contributions

Conceptualization, MC. Data curation, MC, AEA. Formal analysis, MC, AEA, SKS, MMS, JHP. Funding acquisition, MC. Investigation, MC, AEA, SKS, MMS, JHP. Methodology, MC, AEA. Project administration, JHP. Resources, MC, JHP. Software, MC, AEA. Supervision, JHP. Visualization, MC. Writing–original draft, MC, AEA, SKS, MMS, JHP. Writing–review & editing, MC, AEA, SKS, MMS, JHP.

Funding

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Strategic Research Program (No. NRF-2017R1E1A1A01075128) supervised by the National Research Foundation of Korea (NRF) and under the Grand Information Technology Research Center support program (No. IITP-2022-2020-0-01462) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

Competing Interests

The authors declare that they have no competing interests.

References

[1] L. H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, "All one needs to know about metaverse: a complete survey on technological singularity, virtual ecosystem, and research agenda," 2021 [Online]. Available: https://arxiv.org/abs/2110.05352.

[2] M. Sparkes, "What is a metaverse," *NewScientist*, vol. 251, no. 3348, pp. 1-18, 2021. https://doi.org/10.1016/S0262-4079(21)01450-0

[3] S. Mystakidis, "Metaverse," *Encyclopedia*, vol. 2, no. 1, pp. 486-497, 2022.

[4] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, "A survey on metaverse: the state-of-the-art, technologies, applications, and challenges," 2021 [Online]. Available: https://arxiv.org/abs/2111.09673.

[5] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: a university campus prototype," in *Proceedings of the 29th ACM International Conference on Multimedia*, Virtual Event, 2021, pp. 153-161.

[6] G. Bedi, G. K. Venayagamoorthy, and R. Singh, "Development of an IoT-driven building environment for prediction of electric energy consumption," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4912-4921, 2020.

[7] J. Kim, "Advertising in the Metaverse: research agenda," *Journal of Interactive Advertising*, vol. 21, no. 3, pp. 141-144, 2021.

[8] F. Y. Wang, R. Qin, X. Wang, and B. Hu, "Metasocieties in metaverse: metaeconomics and metamanagement for metaenterprises and metacities," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 2-7, 2022.

[9] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: a survey," 2022 [Online]. Available: https://arxiv.org/abs/2201.03201.

[10] S. V. Rehm, L. Goel, and M. Crespi, "The metaverse as mediator between technology, trends, and the digital transformation of society and business," *Journal of Virtual Worlds Research*, vol. 8, no. 2, pp. 1-6, 2015.

[11] D. Van der Merwe, "The metaverse as virtual heterotopia," in *Proceedings of the 3rd World Conference on Research in Social Sciences*, Vienna, Austria, 2021.

[12] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q. V. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the Metaverse: a review," 2022 [Online]. Available: https://arxiv.org/abs/2203.09738.

[13] J. Joshua, "Information bodies: computational anxiety in Neal Stephenson's Snow Crash," *Interdisciplinary Literary Studies*, vol. 19, no. 1, pp. 17-47, 2017.

[14] J. D. N. Dionisio, W. G. Burns, and R. Gilbert, "3D virtual worlds and the metaverse: current status and future possibilities," *ACM Computing Surveys*, vol. 45, no. 3, pp. 1-38, 2013.

[15] S. M. Park and Y. G. Kim, "A Metaverse: taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 10, pp. 4209-4251, 2022.

[16] R. Leenes, "Privacy in the Metaverse," in *The Future of Identity in the Information Society*. Boston, MA: Springer, 2007, pp. 95-112.

[17] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: battle for privacy," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 52-61, 2018.

[18] J. Diaz, C. Saldana, and C. Avila, "Virtual world as a resource for hybrid education," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 15, pp. 94-109, 2020.

[19] M. Bourlakis, S. Papagiannidis, and F. Li, "Retail spatial evolution: paving the way from traditional to metaverse retailing," *Electronic Commerce Research*, vol. 9, no. 1, pp. 135-148, 2009.

[20] L. H. Lee, Z. Lin, R. Hu, Z. Gong, A. Kumar, T. Li, S. Li, and P. Hui, "When creators meet the metaverse: a survey on computational arts," 2021 [Online]. Available: https://arxiv.org/abs/2111.13486.

[21] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: a university campus prototype," in *Proceedings of the 29th ACM International Conference on Multimedia*, Virtual Event, 2021, pp. 153-161.

[22] Meta, "The Facebook company is now Meta," 2021 [Online]. Available: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

[23] K. Miller, "Disney's Tilak Mandadi: using technology to transform storytelling in the Disney Metaverse," 2020 [Online]. Available: https://www.iaapa.org/news/funworld/disneys-tilak-mandadi-using-technology-transform-storytelling-disney-metaverse.

[24] NVIDIA, "NVIDIA launches omniverse design collaboration and simulation platform for enterprises," 2021 [Online]. Available: https://nvidianews.nvidia.com/news/nvidia-launches-omniverse-design-collaboration-and-simulation-platform-for-enterprises.

[25] S. Takle, "Microsoft's Mesh metaverse launches early 2022," 2021 [Online]. Available: https://www.beyondgames.biz/17102/microsofts-mesh-metaverse-launches-early-2022/.

[26] N. Cheredeka, "Alibaba recently applied for a number of trademarks including "Ali Metaverse" & "TaoBao Metaverse"," 2022 [Online]. Available: https://member.unitedglobalasset.com/blog/market-news/16209/alibaba-recently-applied-for-a-number-of-trademarks-including-ali-metaverse-taobao-metaverse.

[27] A. Chen, "ByteDance expands metaverse investment with acquisition of Chinese virtual reality (VR) startup PoliQ," 2022 [Online]. Available: https://en.pingwest.com/a/10417.

[28] S. H. Song, "SKT unveils new metaverse platform Ifland," 2021 [Online]. Available: http://www.koreaherald.com/view.php?ud=20210714000750.

[29] P. Graham, "Maze theory envisions fan metaverses for IP's like peaky blinders," 2021 [Online]. Available: https://zephyrnet.com/maze-theory-envisions-fan-metaverses-for-ips-like-peaky-blinders/.

[30] D. Kelly, "RIMOWA releases first-ever NFT collection," 2021 [Online]. Available: https://hypebeast.com/2021/5/rimowa-nft-collection-metaverse-auction-new-release-info.

[31] M. McDowell, "Gucci goes deeper into the Metaverse for next NFT project," 2022 [Online]. Available: https://www.voguebusiness.com/technology/gucci-goes-deeper-into-the-metaverse-for-next-nft-project.

[32] N. Xi, J. Chen, F. Gama, M. Riar, and J. Hamari, "The challenges of entering the metaverse: an experiment on the effect of extended reality on workload," *Information Systems Frontiers*, 2022. https://doi.org/10.1007/s10796-022-10244-x

[33] T. A. Jaber, "Security risks of the metaverse world," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 13, pp. 4-14, 2022.

[34] K. Nath, "Evolution of the Internet from Web 1.0 to Metaverse: the good, the bad and the ugly," 2022 [Online]. Available: https://www.techrxiv.org/articles/preprint/Evolution_of_the_Internet_from_Web_1_0_to_Metaverse_The_Good_The_Bad_and_The_Ugly/19743676.

[35] S. B. Far and A. I. Rad, "Applying digital twins in metaverse: user interface, security and privacy challenges," *Journal of Metaverse*, vol. 2, no. 1, pp. 8-16, 2022.

[36] E. Dincelli and A. Yayla, "Immersive virtual reality in the age of the Metaverse: a hybrid-narrative review based on the technology affordance perspective," *The Journal of Strategic Information Systems*, vol. 31, no. 2, article no. 101717, 2022. https://doi.org/10.1016/j.jsis.2022.101717

[37] F. Y. Wang, R. Qin, X. Wang, and B. Hu, "Metasocieties in metaverse: metaeconomics and metamanagement for metaenterprises and metacities," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 2-7, 2022.

[38] J. N. Njoku, C. I. Nwakanma, G. C. Amaizu, and D. S. Kim, "Prospects and challenges of Metaverse application in data-driven intelligent transportation systems," *IET Intelligent Transport Systems*, 2022. https://doi.org/10.1049/itr2.12252

[39] R. Cheng, N. Wu, S. Chen, and B. Han, "Will metaverse be nextg internet? vision, hype, and reality," 2022 [Online]. Available: https://arxiv.org/abs/2201.12894.

[40] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6G for the Metaverse," *IEEE Wireless Communications*, 2022. https://doi.org/10.1109/MWC.019.2100721

[41] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942-954, 2020.

[42] J. Zhu, P. Ni, and G. Wang, "Activity minimization of misinformation influence in online social networks," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 4, pp. 897-906, 2020.

[43] P. Krishnan, K. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal, and H. Song, "MUD-based behavioral profiling security framework for software-defined IoT networks," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6611-6622, 2021.

[44] D. Zou, J. Zhao, W. Li, Y. Wu, W. Qiang, H. Jin, Y. Wu, and Y. Yang, "A multigranularity forensics and analysis method on privacy leakage in cloud environment. *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1484-1494, 2019.

[45] E. Sayegh, "How to secure a Metaverse," 2022 [Online]. Available: https://www.forbes.com/sites/emilsayegh/2022/04/28/how-to-secure-a-metaverse/?sh=720d8eab26c3.

[46] The Paypers, "Fujitsu to offer digital security solution in metaverse," 2022 [Online]. Available: https://thepaypers.com/digital-identity-security-online-fraud/fujitsu-to-offer-digital-security-solution-in-metaverse--1258072.

[47] K. Ruth, T. Kohno, and F. Roesner, "Secure {Multi-User} content sharing for augmented reality applications," in *Proceedings of the 28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA, 2019, pp. 141-158.

[48] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang, "BlockMaze: an efficient privacy-preserving account-model blockchain based on zk-SNARKs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1446-1463, 2022.

[49] Y. Han, D. Niyato, C. Leung, D. I. Kim, K. Zhu, S. Feng, and C. Miao, "A dynamic hierarchical framework for iot-assisted metaverse synchronization," 2022 [Online]. Available: https://arxiv.org/abs/2203.03969.

[50] M. Li, J. Weng, J. N. Liu, X. Lin, and C. Obimbo, "Toward vehicular digital forensics from decentralized trust: an accountable, privacy-preserving, and secure realization," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 7009-7024, 2022.

[51] H. J. Kwon, A. El Azzaoui, and J. H. Park, "MetaQ: a quantum approach for secure and optimized metaverse environment," *Human-centric Computing and Information Sciences*, vol. 12, article no. 42, 2022. https://doi.org/10.22967/HCIS.2022.12.042

[52] A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A quantum approximate optimization algorithm based on blockchain heuristic approach for scalable and secure smart logistics systems," *Human-centric Computing and Information Sciences*, vol. 11, article no. 46, 2021. https://doi.org/10.22967/HCIS.2021.11.046