International Journal of Internet, Broadcasting and Communication Vol.15 No.1 13-22 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.1.13

IJIBC 23-1-3

Analysis of Information Security Issues and Classification through Metaverse Infringement Cases

Mi-Na Shim

Professor, Department of Computer Engineering, Sungkyul University, Korea
mnshim@sungkyul.ac.kr

Abstract

In the age of Web 3.0, the metaverse is emerging as a new innovative element to replace the Internet. Leading major ICT companies, it is striving to become a metaverse platform or infrastructure-oriented company. Along with the expansion of the VR and AR market, governments of each country are investing large budgets in this field. However, security concerns about metaverse are also growing. In addition to potential damage to infrastructure, platform and services, personal information leakage and privacy damage are expected to increase further. In this study, we investigated and closely analyzed cases of infringement on the infrastructure, platform, and service of Metaverse. We have clearly identified the current state of metaverse security and the characteristics of the risks of greatest concern. The research procedure is composed of a method of determining the metaverse security area for case analysis first and deriving the type of threat by area through the type of infringement. In particular, the results were mapped into Domain, Case, and Threat, and the implications of the results were analyzed. Through these results, researchers want to contribute to finding the right direction of research by clearly understanding the latest metaverse security status.

Keywords: *Metaverse, Information Security, Data Privacy, Infringement Case, Case Analysis, Classification*

1. Introduction

In the era of Web 3.0, the metaverse is being accepted as a new innovative element that will succeed the Internet. In 2007, the Acceleration Studies Foundation (ASF) in the US established and classified the metaverse concept through the ‘Metaverse Roadmap’. ASF defined it as “The Metaverse is the convergence of 1) virtually enhanced physical reality and 2) physically persistent virtual space,” and classified it into Augmentation and Simulation, Intimate and External. Based on this, ASF classifies the metaverse world into four major categories: Augmented Reality (AR), Life Logging, Virtual Words, and Mirror Worlds. Also, it was recognized that the metaverse will be considered as the most important part as it is a standard way of online life like the Web [1]. In the meantime, the metaverse and the virtual world have been regarded as the same concept. However, this view is generally accepted due to the influence of the ASF roadmap, which sees the metaverse not as a virtual space, but as an intersection or connection point connecting the physical and virtual worlds [2].

Manuscript Received: November. 5, 2022 / Revised: November. 8, 2022 / Accepted: November. 12, 2022
Corresponding Author: mnshim@sungkyul.ac.kr
Tel: +82-31-467-8371, Fax: +82-31-467-8371
Professor, Department of Computer Engineering, Sungkyul University, Korea

After the ASF roadmap, the world is making progress in the metaverse. Major ICT companies such as Meta, Microsoft, NVDIA, and Apple are accelerating preparations to become metaverse platforms or infrastructure-oriented companies. Domestic companies such as Naver and Kakao are also promoting the formation of their own metaverse ecosystem by converging technologies such as AI, Cloud, 5G, and Blockchain. According to Statista, a German statistics site, the market size of the metaverse, represented by Virtual Reality (VR), AR, and Mixed Reality (MR) technologies, is gradually expanding, and it is expected to grow from $ 28 billion in 2021 to $ 250 billion by 2028, nine times increase. It is expected to grow rapidly [3]. In September 2021, the government announced that it would invest about 2.6 trillion won in the Metaverse and Blockchain fields by 2025, and Ministry of Science and ICT (MSIT) also announced that it would invest 1 trillion won in fostering new digital industries such as the metaverse economy [4, 5].

However, concerns about metaverse security are also growing. Based on the “2030 Future Social Change and Cyber Threat Prospects of 8 ICT Technologies” report, the Korea Information Security Agency (KISA) predicted that metaverse security threats would increase more in the future than now [6]. From the provider side, threats to related systems, devices, infrastructure, data, and networks will increase in the future, and from the user side, threats that exploit device vulnerabilities such as AR/VR in the process of using services will increase. forecasted. Meanwhile, based on the survey results, Perkins Coie LLP selected ‘Consumer Privacy and Data Security’ as the security that metaverse-related engineers and content developers should consider first [7]. It was analyzed that the security threat of metaverse is greater than the potential damage that may occur due to system vulnerability hacking or device malfunction, etc., and that the damage caused by leakage of personal information and privacy is greater, and it will be a fearful threat to users. Igloo Security, LG CNS, MSIT also selected this issue as the most threatening metaverse security issue [8].

Looking at the above analysis, security issues related to the metaverse are divided into security threats centered on 'system, device, and infrastructure' and security threats centered on 'data and personal information'. KISA (2022) conducted a survey of related experts based on the threat classification of the cybersecurity threat of the metaverse from the provider and user sides and evaluated the current and future risks related to the metaverse. As a result of the survey, it was found that current cyber threats pose high risks to devices, infrastructure, and data, and in the future, while data risks will remain at the current level, risks to metaverse systems will increase [6]. As we have seen, the metaverse is a key factor in digital transformation, and it can be assumed that the importance of related industries and R&D is increasing. Therefore, for the successful development of the market, clear awareness, and preparation for expected metaverse security issues and threats are required above all else.

Therefore, this study aims to clearly understand the status and risks of metaverse security by analyzing cases of infringement related to metaverse. By analyzing previous studies, the metaverse security area is determined, and based on this, metaverse infringement cases are analyzed and infringement types by area are derived. By including problems that have already occurred or are expected to cause potential infringement, we have made it possible to closely grasp the current practical risks. The research results are intended to contribute to understanding the current level of metaverse security and helping researchers find the right research direction.

2. Related Research

2.1 Concept and Classification of Metaverse

■ Concept of Metaverse.

Metaverse is a compound word of ‘Meta’ meaning transcendence and ‘Universe’ meaning world. It was first used in the meaning of ‘three-dimensional virtual world’ in the American science fiction novel ‘Snow Crash’. Although no concept has been established yet, it implies a conceptual meaning as a ‘virtual shared space’ in which Internet space and physical space coexist [9]. According to researchers, ‘a virtual world where everyone uses avatars to engage in social, economic, and cultural activities’, ‘every phenomenon in which daily life moves to and expands to the digital world to fill the needs lacking in the analog world’ [10, 11].

According to ASF, which presented the basics of concept establishment, the metaverse is classified into AR, Life Logging, Virtual Worlds, and Mirror Worlds based on two criteria: Augmentation and Simulation, and Intimate and External. Augmentation and Simulation are space-oriented classifications. The former refers to the technology of accumulating information on top of the reality, and the latter to the technology of creating the virtual world. Intimate and External can be understood as content classification. The former refers to a user's identity, such as an avatar or profile, and the latter refers to a technology that provides information or control over the world. AR refers to “an environment in which virtual objects expressed in 2D or 3D are superimposed on the real space and interacted with.” Life Logging is “capturing, storing and describing everyday experiences and information about things and people”. Users can capture, store, and manage every moment of their daily life as text, video, and sound. Virtual Worlds are “an alternative world similar to or completely different from reality built with digital data” and is the most familiar type of metaverse to us. Mirror Worlds refers to “virtual worlds that reflect the real world as much as possible but are ‘informatically expanded’” [1].

■ Classification of Metaverse Security.

To analyze metaverse security issues or threats, classification methods are proposed according to various criteria. First, it is an example of the metaverse classification method. Similar to architectures such as AI, KISA (2022) says that the metaverse architecture is composed of ‘Infrastructure’ that connects the real worlds and digital worlds, ‘Interaction Platform’ that expands to VR, and ‘Eco System’ that is a set of components of VR [6, 12]. Infrastructure is a component of real worlds required to use or operate metaverse services, and includes Device, Network, and IT Infrastructure. Interaction Platform is a metaverse platform and development tools and technologies that make it, and Programming Engines, Asset Design Tool, and Metaverse Service fall under this category. Eco System is a VR component that users experience and use within the metaverse world, and includes Avatar, UGC, Digital Asset, and Marketplaces.

Next is an example of the metaverse security classification method. Trend Micro Research (2022) classified Cybersecurity Threats of Metaverse into 9 categories [13]. Namely, NFTs, Darkverse, Financial fraud, Privacy issues, Cyber-physical threats, VR/AR/MR/ Extended Reality (XR) threats, Social engineering, Traditional IT attacks, Miscellaneous threats and issues. First, NFTs regulate ownership of assets but do not provide storage for those assets. Thus, ransomware or other criminal attacks may occur. Second, the Darkverse could be the same danger as the Darkweb, existing inside the metaverse. The dark web is not searched for reasons of security, anonymity, and privacy. Therefore, criminals can exploit it. Third, financial fraud can occur in which criminals or criminal groups use users in the metaverse, steal money, and capture digital assets. Fourth, there is the privacy issue. Metaverse publishers can generate unfair revenue by controlling the metaverse space and collecting large amounts of user information. Fifth, there are Cyber-Physical Threats. VR/AR/MR/XR Interface can be a physical threat because it serves as a device connecting IoT and virtual space. Sixth, VR/AR/MR/XR Threats. The metaverse exists as a VR and MR world. User interaction in this space could pose various threats in the future. Seventh, the social engineering threat. Deep fake crimes or other crimes can occur through social engineering techniques. Eighth, Traditional IT Attacks. Current IT threat scenarios (DDoS, API Attack, ransomware, etc.) can occur in the metaverse. The ninth refers to other threats and problems related to the metaverse that may occur, such as intellectual property issues. As shown in Table 1, KISA (2022) classified Cybersecurity Threat of Metaverse into supplier and user aspects. And the threat types were subdivided [6]. Based on this, KISA surveyed related experts and attempted to evaluate the current and future risks related to the metaverse. For the analysis of this study, the classification method of KISA was considered and applied.

Table 1. Classification of metaverse security

Researcher (Year)	Classification 1	Classification 2
KISA(2022)	Provider: System	- Virtual world (AR, VR, S/W, etc.) system and platform security threats
	Device/Infrastructure	- Threats of virtual world-related construction and management devices, infrastructure vulnerabilities - Security vulnerabilities of WEB and metaverse applications, etc.
	data	- Invasion of personal information - Data forgery and stealing - Threats such as theft and illegal copying of virtual assets such as avatars, virtual money, and points
	Network	- Web vulnerability attack (ARP Spoofing, MAC Spoofing, etc.)
	User: use of service	- Security threats of AR/VR devices (mobile devices) - Threats to privacy (biometric information, behavioral information, etc.)

Akamai (2021) analyzed major metaverse security issues and trends as an American cloud and IT developer. Akamai specifically subdivided metaverse security issues based on the definition of metaverse [14]. Characteristics were selected from the metaverse definition and related issues were derived. The definition is: “The Metaverse is an expansive network of persistent, real-time rendered 3D worlds and simulations that support continuity of identity, objects, history, payments, and entitlements, and can be experienced synchronously by an effectively unlimited number of users, each with an individual sense of presence.” As a result, authentication, access policies, malware, encryption and secure traffic, DNS security, web app attacks, uptime, DDoS attacks, flash crowds, security vs. performance trade-offs, API security, stream protection, anti-piracy, fraud, physical/access security, hardware/IoT security, content integrity, secure registration, credential provisioning, authorization, PII, encryption, PCI compliance, tokenization, payment risk fraud Threats such as prevention, intellectual property rights, payment security, flash crowds, MFA, and security at scale were presented.

2.2 Information Security Problems and Protection of Metaverse

- **Metaverse Security and Threat.**

As a result of searching domestic papers related to metaverse security, 21 KCI journals and conference papers were identified. 10 papers deal with metaverse security issues and measures, and 11 papers deal with metaverse security technologies and models. Among them, the representative papers (4 of the former, 5 of the latter) present the characteristics and research results as shown in Table 2 [15-24]. Studies on the classification of metaverse security threats suggest classification methods based on the metaverse architecture, as discussed in Section 2.1. There is also platform-based research, which is expected because the current metaverse field is growing based on platforms. Security technology or model research also presents security mechanisms or models based on these issues or threat analysis results.

Table 2. Research for metaverse security problems and protection

Researcher	Subject	Type(P1:Problems, P2:Protection)
Jung et al. (2021.12)	Architecture based threat classification - Input & Output/Interaction/Device Protection	P1: Security Threat
Na, Choi (2022.08)	Architecture based threat classification - Using Environments (User/Devices), Virtual Environments (Avatar/Data/Contents and Interaction), Digital Twin Environments (Simulation)	P1: Security Threat
Lee et al. (2022.08)	Platform based threat classification - Platform (Zepeto, Roblox, Earth2), Domain (Contents, Infrastructure, Devices)	P1: Security Threat
Jung et al. (2022.08)	Analysis of threat and technology related to ID security issue. Issue Classification – Digital separation/Interaction stage, Surreal stage	P1: Security Threat
Lee (2022.09)	Attribute-level privacy protection mechanism (data classification) For protection personal information in the metaverse	P1: PI Issue P2: Mechanism
Hong, Park (2022.09)	Propose security model for security and privacy. Model – security based/privacy based/public Environment based	P1: Security Issue P2: Service Model
Lee, Park (2022.11)	Eye tracking Obfuscation method for improving metaverse security. Method – protection to estimate the gaze trajectory of the original data through bucket shuffling	P1: privacy P2: Mechanism
Kim et al. (2022.12)	Technique for proof of ownership of metaverse works without providing source data – propose to system	P1: property right P2: System Model
Cho (2022.12)	Analysis of Framework – Security threats (biometrics/PI/Cryptocurrency) Propose to security service model	P1: Security Threat, P2: Service Model

3. Research Methods

This study was conducted according to the following procedures and methods. First, previous research reviewed various security threat classification methods through literature review method, that is, analysis of research papers and reports related to metaverse security and organized general security threat types. Second, case studies were also investigated and analyzed various cases of infringement related to the metaverse through web searches such as reports and press releases. The scope of infringement cases was set for the last 10 years, centering on the period from 2020 to 2022, when the service of metaverse surged. Including problems that have already occurred or are potentially infringed at home and abroad, the actual risks at the present time can be closely identified by investigation. Third, it analyzes infringement cases through investigation of reports and press releases, classifies security threat types according to pre-determined relevant metaverse areas, and understands the meaning of data. In addition, based on the organized results, infringement cases and related threat types for each metaverse security area are mapped and the meaning of the threat is analyzed in detail. Therefore, the research results are presented in the form of D (Domain), C (Related Case), and T (Threat). Fourth, based on the derived threat results, the implications of the research results are analyzed, and through this, researchers present the latest metaverse security status and implications for setting research directions.

■ **3 Domain for Analysis of Infringement Cases related to Metaverse Security.**

The common infringement types of infringement cases were analyzed based on the three areas derived through the analysis of previous studies. Based on this, the threat type was derived. The meaning is as follows.

i. Device and Infrastructure: a) HMD device based on VR/AR technology as a tool to use metaverse service, b) Advanced infrastructure such as network or cloud service that supports metaverse environment.

ii. Interaction Platform: H/W, S/W platform to support various metaverse ecosystems or develop service.

iii. Service and Data: Services in various areas that users can experience or use, and data processed in the process (personal information and contents)

4. Results

4.1 Analysis of Infringement Cases from Information Security Perspective

Cases of security breaches in the metaverse were divided into Device and Infrastructure (D1), Interaction Platform (D2), and Service and Data (D3) areas, and various types of breaches appeared. In the case of Table 3, Device, and Infrastructure, two representative infringement cases were analyzed. Two threats were summarized as a result. There are not many cases of actual infringement related to Metaverse Device and Infrastructure yet. However, there are mainly cases of infringement using security vulnerabilities of the internal system for management, not the VR device itself or the metaverse service. It should be understood as a problem of existing general devices and systems, not a new infringement problem caused by the metaverse. However, it is expected that device and system security threats will gradually intensify and diversify according to the level of evolution of VR devices.

Table 3. Analysis of infringement cases (D1)

Case(C)	Key Point	Infringement(T)
(C1.D1) Discovery of security vulnerabilities in VALVE's VR games and Steam VR (2019.05)*	· Hackers can take advantage of security flaws in VRChat and High Fidelity to take control of chat rooms in advance, invite people to chat rooms, and manipulate what they see on their webcams, microphones, and VR headsets	(D1.T1)
(C2.D1) Leaked personal information of 100 million Roblox users, a metaverse game platform (2020.05)	· Hackers gained access to Roblox's internal system (customer support panel) and accessed about 100 million active user accounts. · Change e-mail address, password, remove 2-step security authentication, and sell user's items illegally	(D1.T2)

In the table, * indicates a threat that has not yet been breached but is likely to occur in the future because a vulnerability has been discovered. In addition, ** means a threat that has not been found to be infringed but is potentially likely to occur.

In the case of Table 4, Interaction Platform area, 8 representative infringement cases were analyzed. As a result, six threats were identified. The current level of metaverse evolution is still at an early stage. It is making a popular development centered on a platform or a game platform for the purpose of forming social relationships such as Zepeto. Therefore, it is identified that the infringement cases related to the Interaction Platform are the most common. Common security issues such as phishing, hacking using administrator account hijacking, and personal information leakage are also appearing in the metaverse. On the metaverse platform, sex crimes targeting avatars representing users of the metaverse appear like reality. This indicates that the threat of mental invasion on the Metaverse platform already occupies a significant portion. It is expected that it will become more serious with the development of VR devices in the future. In addition, on the metaverse platform, various virtual assets or virtual currencies are used and cashed as their own economic means. As a result, it is expected that more threats and violations that cause serious economic damage will appear.

Table 4. Analysis of infringement cases (D2)

Case(C)	Key Point	Infringement(T)
(C1.D2) Bot luring to Roblox phishing site (2019)	· After uploading a link that provides free Robux (Roblox Cash) to decorate Roblox's avatar to a fake phishing site, the user's account is obtained.	(D2.T1)
(C2.D2) Roblox Hacking (2012.04)	· A user who is a Roblox developer used an administrator account on the test site to copy user cookies, obtain administrator privileges, and hack. · Robux is provided for free to game players or accounts are lost	(D2.T2)
(C3.D2) Leakage of Naver Zepeto survey personal information	· When purchasing an item from Zepeto, the personal information of users who have charged insufficient coins through the Tapjoy function is used for spam calls, etc.	(D2.T3)
(C4.D2) Leakage of personal information of Nintendo game platform 'Animal Crossing' (2020.04, 2020.06)	· When accepting a friend request from an unknown person, an item theft accident occurred. Approximately 160,000 registered account information (name, date of birth, country, region, email, etc.) was leaked. · A hacker stole another person's Nintendo Network ID and hacked it, stealing 140,000 accounts	(D2.T4)
(C5.D2) Incidents of sexual crime, gambling, and violence in Second Life, an early VR game (2003)	· Incidents such as sex crimes, gambling, and violence between avatars occurred for the first time in early VR games	(D2.T5)
(C6.D2) Incident of sexual harassment from a male user to a female user in QuiVR (2016)	· In the VR game QuiVR, a male user attempted to touch the main parts of a female user character. · Female users feel unpleasant feelings like reality	
(C7.D2) Sexual harassment and sexual assault occurred in Horizon's VR game, Horizon World (2019.05)	· A user of Horizon World, Horizon's VR game, announced online that he was sexually harassed during the Beta Test. · Users said they suffered sexual assault and verbal sexual harassment and experienced pain like reality.	
(C8.D2) Sexual exploitation of children and sexual crimes within the metaverse, such as description of sexual acts and requests for undressing to Zepeto Avatar	· A Zepeto user (male in 30s) approached Kim (11), a victim child, by suggesting playing “princess, prince”. · Enticed a virtual romantic relationship or collected personal information (photo, address, phone number), and bought an item. · Continued sexual exploitation, such as gaslighting and online grooming	
No cases **	· N/A	(D2.T6)

In the case of Table 5, Service and Data area, 4 representative infringement cases were analyzed. As a result, three threats were identified. Infringement cases related to Metaverse Service and Data are not yet occurring. However, it is mainly seen as a security problem related to IoT or ICT devices used for services such as cameras and GPS and is expected to increase further as the service expands. A characteristic of this area is that avatars, which are newly regarded as key elements in the metaverse, are becoming targets of security breaches. The lifelogging service in the metaverse collects and records all records in real time and connects directly to real people. For this reason, it is expected that personal information leakage and resulting privacy problems will gradually intensify and become a serious threat in the future.

Table 5. Analysis of infringement cases (D3)

Case(C)	Key Point	Infringe ment(T)
(C1.D3) Making celebrity deepfake videos (2021)*	· A YouTuber in Taiwan uses AI to create and distribute fake videos (Deepfake)	(D3.T1)
(C2.D3) Possibility of massive personal information leakage in Pokemon GO game (2016.07)*	· In the process of applying OAuth 2.0, a problem was found in which information was exposed to hackers when accessing with a Google account on Apple iOS. · Hackers may be able to see all the contents associated with the user's Google account, such as emails and photos.	(D3.T2)
(C3.D3) Pointing out the possibility of criminal abuse such as child abduction and information leakage (2016.07)*	· Pokemon GO game uses real-time location information and smartphone cameras, so Bloomberg BNA points out privacy and security issues with the game. · There is a risk of being used for kidnapping that abuses child location information	
(C4.D3) Robbery case in Opalon, Missouri, USA where armed robbers lured others with Pokémon Go (2016.07)	· Lure potential victims by using Becons that gamers add to lure others in Pokemon GO · The police, who were dispatched through a tip-off, arrested the suspect	
No cases **	· N/A	(D3.T3)

4.2 Metaverse Security Threat and Implications

As shown in Table 6, the analysis results of the metaverse security breach cases can be summarized into 3 domains, 14 representative breach cases, and 11 security threat types. Among the three domains, D1 (Device and Infrastructure) and D3 (Service and Data) are not yet subject to substantial infringement, but the same traditional security problems are appearing in the metaverse. In addition, as the metaverse service expands and becomes popular, security threats such as VR devices and IoT devices used in the service are expected to deepen and increase. However, infringement cases related to D2 (Interaction Platform) occur more quantitatively than in other areas. It seems that the economic and psychological damage caused by it is already great. Now that social relationship formation and game platforms are leading the popular development of the metaverse, existing security problems such as phishing, hacking, and personal information leakage are appearing as they are. What is more worrisome is that on the metaverse platform, social and economic activities are possible through avatars representing me. Because of this, actual economic damage and mental and physical damage are already appearing seriously. The security problems that have appeared in healthcare services so far will evolve into lifelogging forms as they are combined with the metaverse environment, and will show more massive, continuous, and permanent characteristics. Therefore, the metaverse service will closely connect the virtual and real I, and it is expected that personal information leakage and privacy problems will gradually intensify and become a serious threat in the future.

Table 6. Metaverse security threats and risks

Classification	Security Threats and Risks	Related Cases
(D1) Device and Infrastructure	(D1.T1) Hacking using security vulnerabilities of hardware devices such as metaverse headsets and IoT: Stealing administrator authority of IoT devices, remote control of connected devices, infiltrating central management server and stealing specific device information (gaze information, metaverse activity contents, etc.)	(C1.D1)
	(D1.T2) Hacking using security vulnerabilities in the metaverse system and network : Acquisition of internal system access rights, abuse of authority, illegal item sales	(C2.D1)
(D2) Interaction Platform	(D2.T1) Cyber phishing using bot users that induce access to phishing sites within the metaverse platform: Using a bot disguised as a chat-type counseling system to lure users to phishing sites, hijack accounts, and install malicious codes to cause damage	(C1.D2)
	(D2.T2) Stealing administrator accounts and disrupting the system in the metaverse game production platform: Targeting valuable virtual assets in the metaverse, hijacking the administrator account of the metaverse platform with low security level and disrupting the system	(C2.D2)
	(D2.T3) Leakage of personal information in the process of conducting surveys or missions within the Metaverse platform: Personal information of users who completed surveys or missions to recharge insufficient coins is used for spam calls, etc.	(C3.D2)
	(D2.T4) Leakage of account information registered on the metaverse game platform : Using the leaked account information, hackers can purchase illegal products	(C4.D2)
	(D2.T5) Sex crimes against avatars on the metaverse platform: With the development of VR technology, a metaverse like reality is realized, so the real world has the same level of sex crime problems.	(C5.D2), (C6.D2), (C7.D2), (C8.D2)
	(D2.T6) By creating an avatar with a photograph of one's own face on the metaverse platform, a face image with a high degree of similarity to the actual self is exposed.	N/A
(D3) Service and Data	(D3.T1) Impersonation such as identity theft and fake news using Deepfake technology in the metaverse: Can be used for fake news such as politics and society or used to synthesize pornography	(C1.D3)
	(D3.T2) Security issues related to GPS-based user information tracking and user smartphone camera function in Pokemon GO game, which is an early form of AR metaverse service	(C2.D3), (C3.D3), (C4.D3)
	(D3.T3) Leakage of personal information of various personal health records collected for the jogging exercise management function in the lifelogging fitness service and physical security of the device	N/A

5. Conclusion

We analyzed metaverse-related infringement cases and more clearly identified the current metaverse security status and risks in this study. Based on related research, the area for analysis of infringement cases was determined, and based on infrastructure, platform, service, etc., infringement case analysis and infringement types by area were classified and specified. We analyzed the characteristics of the results and confirmed that the violations in the areas of Device and Infrastructure and Service and Data are not quantitative yet and appear in a form that reflects traditional security problems. In the field of Interaction Platform, it has been confirmed that there is already a lot of infringement in quantity, and the economic and psychological damage is great. It is predicted that security threats in all areas will continue to intensify and increase according to technological evolution and service expansion, such as VR and metaverse-related IoT devices. This result is presented by classifying the infringement types based on the currently occurring infringement cases. Considering its urgency and importance, it is expected to be helpful in selecting research topics and directions.

References

[1] ASF's Metaverse Roadmap. *https://www.metaverseroadmap.org/overview/.*

[2] Y. J. Oh, "The metaverse is coming again," AI Future Strategy Center, 2021.

[3] Statista. XR/AR/VR/MR market size 2021-2028. *https://www.statista.com/statistics/591181/global - augmented-virtual-reality-market-size/.*

[4] ZDNET Korea. *https://zdnet.co.kr/view/?no=20211217135045.*

[5] Korean Government's Brief of Policy. *https://www.korea.kr/news/policyNewsView.do? newsId=156523436.*

[6] Perkins Coie LLP, "2020 Augmented and Virtual Reality Survey Report," 2020.

[7] Ministry of Science and ICT, "'21 cyber threat analysis and '22 forecast analysis," Dec 2021.

[8] J. H. Yoon and G. E. Kim, "The Outlook and Innovation Strategy for the Metaverse Virtual World Ecosystem," STEPI Insight, No. 284, pp. 1-53, Dec 2021.

[9] K. M. Shon, "Matrix world metaverse created by web 2.0 and online games," ETRI CEO Information, No. 47, 2006.

[10] S. K. Kim, "Metaverse-Digital Earth, the world of floating things", *PlanB Design*, 2020.

[11] N. Huq, R. Reyes, and P. Lin et al., "METAVERSE OR METAWORSE? Cybersecurity Threats Against the Internet of Experiences," Trend Micro Research, 2022.

[12] S. Yoo, "A Study on AI Business Ecosystem," *The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC)*, Vol. 20, No. 2, pp. 21-27, Apr 2020.
DOI: https://doi.org/10.7236/JIIBC.2020.20.2.21

[13] K. S. Min, K. Y. Kim, and J. S. Park et al., "Forecast and analysis of cyber security threats, Metaverse, NFTs," KISA Insight, Vol. 4, 2022.

[14] Akamai, "Security Trends to Address now our way to the Metaverse," CEO Insights, Dec 2021.

[15] S. Y. Jeong, C. H. Seo, and J. M. Jo et al., "Security threat analysis in Metaverse, an extended virtual reality," *Journal of Information Security*, Vol. 31, No. 6, pp. 47-57, Dec 2021.

[16] H. S. Na and D. S. Choi, "Review of metaverse security threats and countermeasures," *Journal of Information Security,* Vol. 32, No. 4, pp. 19-32, Aug 2022.

[17] J. H. Lee, H. R. Jeong, and K. W. Park, "Derivation of metaverse platform threat vector through metaverse infringement response case analysis," *Journal of Information Security*, Vol. 32, No. 4, pp. 33-40, Aug 2022.

[18] S. Y. Jeong, C. H. Seo, and J. M. Jo et al., "Current status of ID management technology according to the evolution of the metaverse," *Journal of Information Security Society*, Vol. 32, No. 4, pp. 49-59, Aug 2022.

[19] D. H. Lee, "Attribute-level Privacy Protection Mechanism for a Secure Metaverse Environment," *Journal of the Korean Society of Information Technology (JKIIT)*, Vol. 20, No. 9, pp. 1-11, Sep 2022.
DOI: https://doi.org/10.14801/jkiit.2022.20.9.1

[20] S. W. Hong and J. P. Park, "A Security Model for information Security and Personal information Security in the metaverse environment," *Journal of the Korean Society of Industrial Science and Technology (JKAIS)*, Vol. 23, No. 9, pp. 32-38, Sep 2022.
DOI: https://doi.org/10.5762/KAIS.2022.23.9.32

[21] D. H. Lee and N. J. Park, "Eye Tracking Obfuscation Method to Improve Metaverse Security," *Journal of the Society for Next Generation Convergence Technology (JNCTA)*, Vol. 6, No. 11, pp. 2086-2095, Nov 2022.
DOI: https://doi.org/10.33097/JNCTA.2022.06.11.2086

[22] W. B. Kim, Y. J. Cho and, D. M. Shin, "A Technique for Proof of Ownership of Metaverse Works without Providing Source Data," *Journal of the Korea Software Appraisal Society*, Vol. 18, No. 2, pp. 37-46, Dec 2022.

[23] D. E. Jo, "A Study on the Metaverse Framework Security Service Model," *Journal of Platform Technology (JPT)*, Vol. 10, No. 4, pp. 82-90, Dec 2022.
DOI: https://doi.org/10.23023/JPT.2022.10.4.082

[24] Y. S. Shim, "A Study on Utilization Methods and Problems according to Metaverse Platform Analysis," *Journal of the Convergence on Culture Technology (JCCT)*, Vol. 8, No. 6, pp. 855-860, Nov 2022.
DOI: https://doi.org/ 10.17703/JCCT.2022.8.6.855