*International Journal of Internet, Broadcasting and Communication Vol.15 No.1 23-32 (2023)*
*http://dx.doi.org/10.7236/IJIBC.2023.15.1.23*

**IJIBC 23-1-4**

# Classification of NFT Security Issues and Threats through Case Analysis

Mi-Na Shim

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

***Abstract***

*Since NFTs can be used like certificates due to the nature of blockchain, their use in various digital asset trading markets is expanding. This is because NFTs are expected to be actively used as a core technology of the metaverse virtual economy as non-transferable NFTs are developed. However, concerns about NFT security threats are also growing. Therefore, the purpose of this study is to investigate and analyze NFT-related infringement cases and to clearly understand the current security status and risks. As a research method, we determined NFT security areas based on previous studies and analyzed infringement cases and threat types for each area. The analysis results were systematically mapped in the form of domain, case, and threat, and the meaning of the comprehensive results was presented. As a result of the research, we want to help researchers clearly understand the current state of NFT security and seek the right research direction.*

***Keywords:*** *NFT (Non-fungible token), Metaverse, Information Security, Intellectual Property Rights, Case Analysis*

## 1. Introduction

In October 2015, Non-fungible token (NFT) started as 'Etheria Project' and was first introduced at 'DevCon', an Ethereum developer conference held in London in November. Due to the characteristics of blockchain, once issued, it cannot be duplicated or counterfeited by third parties or transaction parties, and the transaction information, ownership, and copyright of the block are stored together and can be used as a 'certificate'. Because of these characteristics, its use has been expanded to the trading market of various digital assets, and the NFT market has begun to form since 2017. 'Crypto Punks', an NFT issued by Larva Labs, was the first start. Recently, NFTs are being actively traded in the form of various projects such as games, arts, and real assets. In addition, with the tokenization of various certificates based on ERC-1238 and the development of 'NFTs that cannot be traded or transferred', a complex economic system like reality operates in the metaverse. Therefore, it is expected that the use of NFT as a core technology will become active [1, 2].

In April 2021, at Christie's New York auction, Mike Winkelmann's JPEG work 'Everydays: The First 5000 Days' was sold for $69.3 million, and Twitter CEO Jack Dorsey's first tweet broke the auction for $2.5 million [3]. According to the 'NFT Market Forecast Report by 2027' by MarketsandMarkets, the global market size of NFT is expected to grow by about 35% from $3 billion in 2022 to $13.6 billion in 2027 [4]. In September

Manuscript Received: November. 10, 2022 / Revised: November. 12, 2022 / Accepted: November. 16, 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

2021, the Korean government announced that it would invest about 2.6 trillion won in the Metaverse and Blockchain (NFT) fields by 2025. MICT also announced that it would invest 1 trillion won to foster new digital industries [5].

However, concerns about NFTs are also growing. MIT Tech. The Review mentioned concerns in terms of speculation frenzy, environmental issues, legal issues, safety, and permanence [3]. The Korea Information Security Agency (KISA) predicted that NFT security threats will continue to increase in the future. In particular, security threats occur in the process of building blockchain systems and platforms on the provider side, and continuous security threats occur during the process of using blockchain-based services on the user side. As NFT security threats increase, it is predicted that it will become a threat to the virtual economy combined with the metaverse. Looking at the cases of security incidents in the last two years, hacking of NFT-based service platforms or users is increasing, and financial damage is already serious [1].

As described above, NFTs will gradually expand their use along with the metaverse, which is a key element of digital transformation. Therefore, it is necessary to clearly understand and prepare for security issues and threats for the successful development of related industries and markets. Therefore, this study aims to analyze NFT-related infringement cases and clearly identify the risks. The research results will serve as a milestone in the right direction for relevant researchers and policy makers.

## 2. Research Methods

This study was conducted through literature review and case analysis according to the following four steps. That is, related research, case study, data analysis, and implication analysis. In the first procedure (preceding research), papers and reports on NFT security were analyzed. The threat classification method related to NFT security was reviewed and the types of threats were summarized. In the second procedure (case study), a report or web search was performed. NFT-related infringement cases were investigated, and the contents analyzed. The scope of analysis was investigated throughout the period, but the cases of the last two years, when NFTs were actively traded, were concentrated. We have made it possible to know the current practical risks, including problems that have already occurred or are expected to be potentially violated. In the third procedure (data analysis), cases were analyzed. Security threat types were classified according to NFT areas, and their meanings were identified. Based on the results, infringement cases and related threat types for each NFT security area were mapped and their meaning analyzed. Therefore, the research results are presented in the form of D (Domain), C (Related Case), and T (Threat). In the fourth procedure (semantic analysis), based on the derived threat results, the implications of the results were analyzed, and perspective points were provided to researchers or policy makers.

■ **2 Domain for analysis of Infringement Cases related to NFT Security.** NFT Marketplace, Virtual Economical World

Infringement cases are analyzed based on the following two areas derived from the review of related studies. Derive threat types based on the analysis results.

(a) NFT Marketplace: An area related to the NFT trading market consisting of data storage, system, platform, etc. It is about security threats such as hacking and transaction fraud using phishing and smishing attacks, vulnerabilities of the original data storage system and NFT-based service platform, which are targets of NFT.

(b) Virtual Economical World: A virtual economy-related area that combines the metaverse environment and NFT. When trading tokens (contents or items, etc.) used in transactions between users in the metabus

service, NFT is a means of guaranteeing the copyright of content and the core of the virtual economy. Attacks targeting them are on the rise.

## 3. Related Research

### 3.1 Overviews of NFT

■ **Concept and Characteristic of NFT.**

NFT is an abbreviation for Non-Fungible Token, which means 'a token that is unique and non-interchangeable as a unit of data stored on a blockchain'. While fungible tokens have the same value and can be exchanged with each other, NFTs each have their own uniqueness. Therefore, NFTs can permanently remain on the blockchain and ensure their uniqueness [6]. NFT consists of four elements: Blockchain, Smart Contract, Address and Transaction, and Data Encoding. Based on these factors, it can be understood that it is more like a certificate than the content itself by giving a unique recognition value to digital assets using blockchain technology. Since the NFT method is essentially a decentralized application, it basically follows the advantages and characteristics of public ledgers. Accordingly, the key properties of NFT can be called Verifiability, Transparent Execution, Availability, Tamper-resistance, Usability, Atomicity, and Tradability [7]. On the other hand, NFT is evolving to the stage of 1.0 and 2.0. If the initial NFT 1.0 is a 'blockchain asset with unique metadata', the upgraded NFT 2.0 is characterized by 'providing usability to users based on NFT 1.0'. NFT 2.0 utilizes the existing NFT infrastructure to provide users with more usability (Smart Contract and Interaction, Algorithm Randomness and Personalization) [8]. Therefore, NFTs are currently being used in various fields such as entertainment, video, automobiles, and real estate, changing the Internet environment.

■ **Classification of NFT and Metaverse Security.**

NFT security is often comprehensively covered in metaverse or blockchain security. Therefore, to analyze NFT security threats, we looked at various classification methods presented in studies related to metaverse and blockchain security.

Trend Micro Research (2022) classifies metaverse security threats into nine categories: NFTs, Darkverse, Financial fraud, Privacy issues, Cyber-physical threats, Virtual Reality (VR)/ Augmented Reality (AR)/ Mixed Reality (MX)/ Extended Reality (XR) threats, social engineering, Traditional IT attacks, Miscellaneous It was classified into threats and issues [9]. NFT was presented as one of the threat types. NFTs regulate ownership of assets. However, because it does not provide storage for assets, ransomware or other criminal attacks may occur. No details are given in this classification.

KISA (2022) consists of the metaverse architecture as Infrastructure, Interaction Platform, and Eco System. Infrastructure is a real worlds component for using and operating metaverse services, and includes Device, Network, and IT Infrastructure. Interaction Platform is a development tool and technology for the metaverse platform and production, and includes Programming Engines, Asset Design Tool, and Metaverse Service. Eco System is a VR component that includes Avatar, UGC, Digital Asset, and Marketplaces. In addition, KISA classified the Cybersecurity Threat of NFT blockchain into supplier and user aspects and subdivided the threat classification for detailed analysis. The following as shown in Table 1 and Table 2 is a metaverse and block chain security threat classification covering NFT security threats [1]. Since NFT is based on blockchain,

various threats can occur not only in IT infrastructure but also in service areas. Therefore, in Table 1, data threats (virtual asset threats) can be seen as NFT threats.

**Table 1. Classification of metaverse and NFT security**

| Researcher | Classification 1 | Classification 2 |
|---|---|---|
| KISA(2022) Metaverse | Provider: | |
| | System | - Virtual world (AR, VR, etc.) system and platform security threats |
| | Device/ Infrastructure | - Threats of virtual world-related construction and management devices, infrastructure vulnerabilities<br>- Security vulnerabilities of WEB and metaverse applications, etc. |
| | **data** | - Invasion of personal information<br>- Data forgery and stealing<br>- **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)<br>- Threats to privacy (biometric information, behavioral information, etc.) |

**Table 2. Classification of blockchain and NFT security**

| Researcher | Classification 1 | Classification 2 |
|---|---|---|
| KISA(2022) Blockchain | Provider: | |
| | System | - Code vulnerability (System), Smart contract security risk, Threats of hot wallet (Security threats to hot wallets (malicious code, ransomware, virtual asset theft, etc.), APT attacks, etc. |
| | Device/ Infrastructure | - (Public Blockchain) Distributed node hacking risk, Distribution of malware/ransomware to systems such as blockchain creation nodes or cryptocurrency mining, etc. |
| | data | - (private key, public key) privilege stealing, Seizing 51% consensus (hijacking), etc. |
| | Network | - Distributed Denial of Service attack, Agreed Time Lag Attack (Flash Loan Attack), DNS, Border Gateway Protocol (BGP) Hijacking, etc. |
| | User: | |
| | use of service | - private key leak, E-wallet security issues, Personal information leakage and easy decryption problems, etc. |

### 3.2 Research for NFT Security

As a result of searching domestic and foreign papers related to NFT security, 12 papers were identified. The characteristics and research results of 7 papers, excluding 5 conference papers, are summarized in Table 3 [7, 10, 11, 12, 13, 14, 15, 16]. From a technical point of view, NFT security threat research is comprehensively dealt with in the blockchain or metaverse rather than alone. There are papers that classify some security threats, but most of them are limited to issues of security or privacy.

**Table 3. Research for NFT security problems and protection**

| Researcher | Subject | Type |
|---|---|---|
| Jung, Lee (2022.04) | Security threat analysis of NFT transaction in NFT Marketplace<br>Method: STRIDE Threat Modeling Techniques and Case Studies | P1: Security Threat |
| Bhujel, Rahulamathavan (2022.11) | Research on the market dynamics of the NFT ecosystem with a focus on technology components<br>Analysis of problems and solutions in terms of security, transparency, and scalability | P1: Security Issues |
| Gupta, Kumar (2022.03) | Derive a set of major risks and damages related to the NFT ecosystem and classify them into a simple taxonomy<br>Method: Compare and analyze Web 2.0 and Web 3.0 | P1: Security Threat |
| Rehman et al. (2021) | Provides a comprehensive overview of NFTs, Ethereum, and blockchains and presents security challenges<br>: Intellectual Property Right, Cyber Security, Security and Privacy etc. | P1: Security Issues |
| Wang et al. (2021) | Inform the technical components of NFT solutions and present various challenges<br>Security and Privacy Issues: NFT Data Inaccessibility, Anonymity/Privacy | P1: Security and Privacy Issue |
| Das et al. (2021.11) | NFT Ecosystem Target, Marketplaces Issues Analysis (User Auth., Token Minting/Listing/Trading Perspective)<br>Security Issues: Issues of External Entities, Fraudulent user behaviors | P1: Security Issue |
| Kim, Kim (2022.11) | Based on metaverse anonymity, interactions that exclude negative true self are strengthened, and problems that cause trust are pointed out.<br>Implementation of NFT-based avatar generation methodology: Creation of user identification means that combines user appearance/personal information to create reliability and positive response formation | P2: Methodology |

* Type (P1: Problems, P2: Protection)

## 4. Results

### ■ Analysis of Infringement Cases from Information Security Perspective.

Cases of NFT security breaches appear in various types, as shown in Table 4 and Table 5, when divided into NTF Marketplace (D1) and Virtual Economical World (D2). In the former, 9 representative cases were analyzed, and 3 threats were summarized. Infringement cases related to the NFT Marketplace are like existing security problems in that they use security vulnerabilities in the storage of NFT original data and legacy systems. Authentication settings or security vulnerabilities in web pages are the same. In addition, phishing and smishing attacks on NFT services are frequently occurring, and security threats such as stealing wallet privileges or cryptocurrency by using discord or smart contract for phishing appear as representative types. These threats are predicted to continue to appear as the service expands in the future and cause serious financial damage.

For the latter, four representative cases were analyzed, and three threats were identified. Infringement cases related to the Virtual Economical World can be viewed as security threats from the legal and policy aspects rather than from the technical aspects. In this area, it appears as a problem due to unauthorized person minting NFT or stealing and selling it on the platform. Most of these problems can be seen as problems in terms of copyright. As a liability issue of some Online Service Providers (OSPs), discussion is needed as it should be dealt with similarly to the issue dealt with in the Information and Communications Network Act. As for the types of copyright infringement, there are no relevant laws yet. Therefore, it is necessary to urgently prepare legal and institutional preparations in anticipation of the activation of NFT transactions in the future.

**Table 4. Analysis of infringement cases (D1)**

| Case(C) | Key Point | Infringement(T) |
|---|---|---|
| (C1.D1) Banksy homepage hacking and NFT sales/ issuance fraud (2021.08) | · Fraudulent crime of hacking the Banksy website, issuing, and selling NFTs<br>· Using the method of creating arbitrary files by using security vulnerabilities of the homepage and posting one's own pages and contents | (D1.T1) |
| (C2.D1) Hacking Nifty Gateway's security-vulnerable accounts, stealing NFTs and cryptocurrencies (2021.03) | · Among Nifty Gateway NFT wallet accounts, account hijacking by hacking passwords targeting accounts that do not have two-factor authentication set up<br>· Transfer NFTs and cryptocurrencies of the target account to the hacker's wallet | (D1.T2) |
| (C3.D1) Vulnerability found in OpenSea to steal wallet privileges through malicious NFT issuance and phishing (2021.09)* | · Issue and sell malicious NFTs by deceiving them as being sent from OpenSea<br>· A vulnerability was found in which wallet privileges were granted to hackers when users received purchased NFTs and transferred them to their wallets | |
| (C4.D1) Hacking and NFT transaction fraud using security vulnerabilities in OpenSea webpage (2022.01) | · Hacking using front-end security vulnerabilities of pages that disclose NFT information and market prices of OpenSea web pages<br>· Changed NFT price to sell at less than 1%, causing financial damage to NFT owners | |
| (C5.D1) Cryptocurrency and coin stealing through Axie Infinity hacking (2022.03) | · Vulnerability attack on Axie Infinity's Sidechain, Ronin<br>· Steals Ethereum and Circle Stable Coin (USDC) managed by Ronin | |
| (C6.D1) Stealing cryptocurrency through hacking and phishing in Monkey Kingdom (2021.12) | · Phishing hacking using vulnerability of discode page in Monkey Kingdom, a Solana (SOL) based NFT project<br>· Attack the vulnerability of Grape, an authentication solution, acquire an administrator account in Discord, and send a URL for phishing to the Discord user<br>· Obtain SOL tokens by requiring users to authenticate with a cryptocurrency wallet when accessing the website | (D1.T3) |
| (C7.D1) Hacking using security vulnerabilities in OpenSea webpage to steal cryptocurrency (2022.02) | · Hacker pretends to be an administrator and sends e-mails to users through phishing websites<br>· When the user signs the migration smart contract included in the email, the user's cryptocurrency is actually signed for the NFT sale, and the user's cryptocurrency is sent to the hacker | |
| (C8.D1) Hyundai Motor Company's official NFT Discord target, stolen wallet by bot hacking attack (2022.05) | · Hacker hacked MEE Bot targeting Hyundai Motor vehicle company's NFT Discord, acquired posting rights on notice board, and uploaded notice with phishing link<br>· Steals the user's wallet by tricking the user into clicking on the link and entering the wallet address | |
| (C9.D1) Stealing NFTs and cryptocurrency by hacking and phishing the BAYC Discord server (2022.06) | · Hacking the Discord server by stealing BAYC's administrator account<br>· Post a phishing link on the Discord channel and induce users to click on it to steal cryptocurrency | |

**Table 5. Analysis of infringement cases (D2)**

| Case(C) | Key Point | Infringement(T) |
|---|---|---|
| (C1.D2) NFT auction of works by Jung-seop Lee, Whan-ki Kim, and Soo-geun Park (2022.06) | · Wannab Corp made NFTs of the works of artists Jung-seop Lee, Whan-ki Kim, and Soo-geun Park and conducted an online auction, but the auction was suspended due to concerns about forgery and lack of copyright agreement<br>· A contract was signed with the owner of the work, but there is no copyright or permission other than the exhibition of the work | (D2.T1) |
| (C2.D2) Issuance of NFTs of virtual items created by avatar characters (2021) | · When an avatar with AI function creates a virtual item by combining the platform's pixels, copyright issues occur<br>· Recognition of copyright, whether copyright infringement on other people's works, etc. | |
| (C3.D2) Publication of NFTs that transform the works of Jae-beom Joo (2021) | · Open Sea's anonymous account (Monas) obtained unfair profits by making many works that transformed the Pixel Art of artist Jae-beom Joo into NFTs<br>· Digital works that recreate the Pixel Art of famous paintings (the copyright period has expired) are secondary works, and copyright issues arise because the original artist owns the copyright | |
| (C4.D2) CROSS platform's NFT issuance (2021) | · Unauthorized copying of NFT works registered on BCAEX, an NFT platform, to another platform, CROSS, and selling them as plagiarism works<br>· Reproduction of illegal works, neglect of transmission, and liability issues of OSP have occurred | (D2.T2) |
| No Cases** | · N/A | (D2.T3) |

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.

## ■ NFT Security Threat and Risks

As a result of the analysis, security infringement cases related to NFTs can be organized into 2 domains, 13 representative cases, and 6 security threat types as shown in Table 6. First, D1 (NTF Marketplace) is not a traditional security problem, but security threats arising from NFT-related data storage or systems as well as new security threats from NFT services and platforms. Traditional security threats are problems that need to be quickly dealt with by applying existing countermeasures. New security threats continue to occur as services expand in the future and may cause financial damage. Therefore, it is necessary to prepare new countermeasures through active research. Security threats in NFT platforms or services have already been identified quantitatively in various cases, so it is necessary to deal with them more urgently.

D2 (Virtual Economical World) is not a security problem from a technical aspect, but a security threat from a policy aspect. Most of them appear as copyright infringement issues in NFT Minting, and several cases have already been confirmed quantitatively. There are many problems with NFTs of famous works with high monetary value, and they are transformed or appear as new types of security threats to NFTs created by AI. There is no legal or institutional mechanism yet for this problem of copyright infringement. Considering the lack of understanding of new technologies or services by legislative or policy makers, it is urgently necessary to revise laws and systems that are in line with reality through continuous discussions by experts in each field. After preparing such a foundation, technological devices should be combined to respond organically.

**Table 6. NFT security threats and risks**

| Classification | Security Threats and Risks | Cases |
|---|---|---|
| (D1) NFT Marketplace | (D1.T1) Cyberattack using security vulnerabilities in NFT original data storage: Security threats using vulnerabilities of external storage systems that store and manage original data subject to NFT issuance (art works digital contents, etc.)<br>(a) Creation of arbitrary files and posting of contents by exploiting security vulnerabilities of the homepage | (C1.D1) |
| | (D1.T2) Security threats using vulnerabilities of legacy systems related to NFT service platforms: Security threats using security vulnerabilities of legacy systems connected for NFT-based service platform providers' wallets, marketplaces, and user management<br>(a) Stealing an account by hacking the password of an NFT wallet account without two-factor authentication<br>(b) Exploitation of security vulnerabilities to steal wallet privileges when malicious NFTs are transferred to user wallets<br>(c) Modify the NFT market by using the front-end security vulnerability of the web page<br>(d) Hacking by obtaining the validator's node key using Ronin's vulnerability and creating a backdoor in the gas free RPC node | (C2.D1), (C3.D1), (C4.D1), (C5.D1) |
| | (D1.T3) NFT and virtual asset theft of NFT service users through phishing and smishing attacks: Stealing NFTs and virtual assets through phishing and smishing attacks that send false messages, notices, and notifications about NFT services, platforms, and marketplaces to service users<br>(a) Acquisition of administrator account using vulnerability of authentication solution and acquisition of user token through phishing<br>(b) Impersonating an administrator to send a phishing email to sign a smart contract to the user and obtain the user's cryptocurrency<br>(c) Obtaining the right to post on the bulletin board by hacking the MEE Bot and stealing the user's wallet through the phishing link<br>(d) Steal cryptocurrencies by posting phishing links on Discord Channels | (C6.D1), (C7.D1), (C8.D1), (C9.D1) |
| (D2) Virtual Economical World | (D2.T1) Problems with non-right holders' NFT minting: If a person who is not the copyright holder mints and sells digital images, a buyer's copyright dispute may arise<br>(a) NFT minting under the contract with the owner of the work has no copyright or permission other than the exhibition of the work<br>(b) Copyright infringement issues of NFTs created by Avatar on the Metaverse platform<br>(c) Copyright infringement issues regarding the act of transforming and selling digital works that recreate famous pixel art | (C1.D2), (C2.D2), (C3.D2) |
| | (D2.T2) Registration and sale of unauthorized stolen NFTs on the NFT platform: Liability issues such as OSP's neglect of copying and transmission of NFT illegal works | (C4.D2) |
| | (D2.T3) Copyright infringement in NFT transaction process: When uploading someone else's work to be minted, it may constitute an infringement of the transmission right (or reproduction right) | N/A |

## 5. Conclusion

Recently, as NFT has rapidly emerged as a core technology of the virtual economy, its use in the trading market of various digital assets is expanding. Therefore, concerns about security threats surrounding NFTs are gradually growing. The purpose of this study is to investigate and analyze NFT-related infringement cases and to clearly understand the current security status and risks. In this study, we analyzed NFT infringement cases and tried to understand the current NFT security situation, especially security issues and risks, more clearly. To successfully carry out the research, we systematically classified the type of infringement by area by defining the security area of NFT and analyzing infringement cases. The analysis results were systematically mapped

in the form of domain, case, and threat, and the meaning of the comprehensive results was presented.

As a result of the study, the following important characteristics were identified. Based on the case analysis, we have confirmed that existing security threats are applied to the NTF Marketplace area or new threats appearing in NFT platforms or services, and that various infringements have already occurred in quantity and serious financial damages have occurred. Violations in the Virtual Economical World area are less damaging than the former. However, it was confirmed that serious disputes could be created in the future because legal and institutional mechanisms to respond to security issues from a policy perspective were not prepared. NFT is a key element needed to form a virtual economy by being combined with the metaverse. Therefore, security threats in the two areas related to NFTs will cause very serious problems in the future when the metaverse virtual economy is expanded and activated. Therefore, technical and policy research on these security threats is urgently needed. As a result of this study, we presented practical infringement types based on the currently occurring infringement cases. In particular, the analysis results are organized in the form of domain, case, and threat so that NFT security threats can be clearly understood and utilized. Therefore, it will be an important milestone for researchers to set the direction of their research and utilize the results of this study.

## References


[1] 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.

[2] Metaverse Korea. "What's the Metaverse?", *https://metaverse-korea.net/coin/nft%EB%9E%80-%EB%AC%B4%EC%97%87%EC%9D%BC% EA%B9%8C-non-fungible-tocken%EA%B3%BC-%EB%A9%94%ED%83%80%EB%B2%84%EC%8A%A4/.*

[3] MIT Technology Review, "What's the Metaverse?" *https://www.technologyreview.kr/what-is-nft/?gclid=EAIaIQobChMIgMP1u6Tn_AIV9Z7CCh1n0AyYEAMYASAAEgJ5ofD_BwE.*

[4] CIO Korea. "NFT market to grow 35% annually by 2027… Estimated market size of $13.6 billion in 2027", *https://www.ciokorea.com/tags/87955/%EB%A7%88%EC%BC%93%EC%95%A4%EB%A7%88%EC%BC%93/249538.*

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

[6] Wikipedia. Non-fungible token, *https://ko.wikipedia.org/wiki/%EB%8C%80%EC%B2%B4_%EB%B6%88%EA%B0%80%EB%8A%A5_%ED%86%A0%ED%81%B0.*

[7] Q. Wang, R. Li, and Q. Wang et al., "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," Oct 2021.

[8] Metaverse Korea. "NFT 2.0", *https://metaverse-korea.net/meataverse/nft-20-%EC%A0%95%EC%9D%98-%ED%8A%B9%EC%A7%95-%EC%82%AC%EB%A1%80-nft-0%EA%B3%BC%EC%9D%98-%EC% B0%A8%EC%9D% B4%EC%A0%90/.*

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

[10] S. H. Jung and C. M. Lee, "A Study on the Analysis of Security Threats of NFT Transaction in Korea," *Korean Journal of Industry Security* (KAIS), Apr 2022.
DOI: https://doi.org/10.33388/kais.2022.12.1.293

[11] S. Bhujel and Y. Rahulamathavan, "A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces," *Journal of Sensors*, Vol. 22, No. 8833, Nov 2022.
DOI: https://doi.org/10.3390/s22228833

[12] Y. Gupta and J. Kumar, "Identifying Security Risks in NFT Platforms," Mar 2022.
DOI: https://doi.org/10.48550/arXiv.2204.01487

[13] W. Rehman, H. E Zainab, and J. Imran et al., "NFTs: Applications and challenges," *IEEE 22nd International Arab Conference on Information Technology (ACIT)*, pp. 1-7, Dec 2021.

DOI: https://doi.org/10.1109/ACIT53391.2021.9677260
[14] D. Das, P. Bose, and N. Ruaro et al., "Understanding Security Issues in the NFT Ecosystem," *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Nov 2021.
DOI: https://doi.org/10.1145/3548606.3559342
[15] J. Kim and K. U. Kim, "Non-Fungible Token-based Virtual Avatar for User Identification in the Metaverse," *Journal of KIISE (JOK)*, Vol. 49, No. 11, pp. 1032-1042, Nov 2022.
DOI: https://doi.org/10.5626/JOK.2022.49.11.1032
[16] 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