# 메타버스 서비스를 위한 보안 모델 연구

[1*]조도은

# A Study on the Metaverse Framework Security Service Model

[1*]Do-Eun Cho

## 요 약

최근 메타버스에 대한 사회적 관심이 높아짐에 따라 다양한 메타버스 플랫폼 및 서비스가 등장하고 있으며, 가상 세계의 수많은 가능성과 엄청난 잠재력을 보여주고 있다. 이러한 메타버스는 하나의 유형에만 국한되는 것이 아니라 경계를 허물며 가상융복합경제 형태의 서비스로 진화하며 발전하고 있다. 이에 따라 메타버스에서의 다양한 보안에 대한 이슈가 대두되고 있다. 메타버스는 가상 공간에서 모든 활동이 이루어지므로 프라이버시 침해나 가상 자산 탈취 또는 사기 등의 다양한 문제가 발생할 수 있다. 본 논문에서는 메타버스에서 안전한 서비스를 제공하기 위한 서비스 보안 모델을 제안하였다. 이를 위해 메타버스 프레임워크에서의 보안 위협을 분석하고, 위협을 방지하기 위한 보안 서비스 모델을 제안하였다. 제안 모델의 보안성을 평가하여 효과적으로 메타버스에서 안전한 서비스가 가능함을 보였다.

## *Abstract*

*emerging. And it shows numerous possibilities and tremendous potentials in the virtual world. This metaverse is not limited to one type, but it is evolving and developing into a service in the form of a virtual convergence economy by breaking down boundaries. As a result, various security issues in metaverse are emerging. Metaverse performs all activities in the virtual space, so various problems such as privacy infringement, virtual asset theft, or fraud can occur. In this paper, a service security model is proposed to provide safe services on metaverse. To this end, we analyze security threats in the metaverse framework and propose a security service model to prevent threats. By evaluating the security of the proposed model, it was shown that safe services are effectively possible on the metaverse.*

***Keywords:*** *Metaverse, Security Mechanism, Blockchain, Metaverse Framework, Security Service Model*

[1*]*목원대학교 SW교양학부 교수 (decho@mokwon.ac.kr)*

Received: Dec. 07, 2022, Revised: Dec. 28, 2022, Accepted: Dec. 28, 2022

# I. 서론

메타버스(Metaverse)는 가상을 뜻하는 메타(Meta)와 하나의 세계를 의미하는 유니버스(universe)의 합성어로서 인터넷 공간과 물리적 공간이 공존하는 집합적 가상공존세계(virtual shared space)를 의미한다[1]. 메타버스가 활용되는 분야로는 로블록스, 마인크래프트, 포트나이트 등 게임 분야가 있고, 제페토, 위버스, 호리즌 등 쇼핑, 소통, 모임을 기반으로 한 소셜 분야가 있다. 또한 탁스의 스마트로라 인도어 사이클링, 닌텐도의 링피트 홈트레이닝, 마이크로소프트의 홀로 렌즈처럼 생활 및 산업분야에도 활용되고 있으며, 가상융합기술이 접목된 디바이스를 이용하여 운동, 교육, 시뮬레이션, 훈련 등을 목적으로 활용되기도 한다[2][3]. 이처럼 메타버스는 3 차원 공간에 구축된 가상 세계에서 사용자들이 자신의 아바타를 가지고 다양한 활동을 할 수 있도록 한다.

2022 년 시장 조사업체 가트너의 보고서에 따르면 “2026 년까지 전세계 인구 중 25%가 업무, 쇼핑, 교육, 사교 및 엔터테인먼트를 목적으로 메타버스에서 최소 1 시간을 보내게 될 것”이라고 전망했다. 또한 해당 보고서에서 2026 년까지 전 세계 기업의 30%가 메타버스에서 제품과 서비스를 보유할 것으로 예상했다. 이처럼 메타버스는 특정 분야에 국한하지 않고 산업계 전반에 두루 적용되며, 현실과 유사하게 경제, 문화활동이 가능해지면서 독창적인 형태로 발전하고 있는 추세이다.

최근 메타버스는 기술적인 발전과 더불어 다양한 기업과 비즈니스에 접목하려는 움직임이 활발하다. 또한 메타버스에서 사용자가 직접 참여해 새로운 콘텐츠와 시장을 창출하고 있다. 메타버스 내에서 사용자가 함께 콘서트를 즐기고 게임을 하기도 하며, 경제적 수익을 창출하기도 한다. 사용자가 아이템 등 콘텐츠를 직접 제작할 수 있게 하고, 제작물의 수익을 지원하는 가상화폐, NTF 등 거래 시스템 구축을 통해 비즈니스 플랫폼으로 발전하고 있다. 현재 메타버스 플랫폼은 게임, 엔터테인먼트, 생활, 소통 분야가 주를 이루고 있지만, 제조, 의료, 건축 등 다양한 분야를 전문으로 한 메타버스 플랫폼도 등장하고 있다. 이처럼 점점 진화하고 있는 메타버스는 사용자들 간의 소통, 상호 관계 활동이 큰 장점이지만, 이로 인해 프라이버시 침해나 가상 자산 탈취 또는 사기 등의 다양한 문제가 발생할 수 있다. 점차 메타버스 서비스와 생태계가 확산됨에 따라 메타버스 보안 이슈에 대한 관심도 더욱 증가하고 있다.

글로벌 로펌 퍼킨스 코이(Perkins Coie LL)에서 2020 년 3 월에 발간한 <2020 Augmented and Virtual Reality Survey Report>의 설문조사 결과에 따르면, 메타버스의 구현 기술과 관련 콘텐츠 개발자들이 가장 먼저 고려해야 할 보안 사항으로 “서비스의 이용자 프라이버시 및 데이터 보호(Consumer Privacy/ Data Security)”를 지목하고 있다[4].

따라서 본 논문에서는 메타버스 보안 위협에 대해 살펴보고, 안전한 메타버스 서비스 이용을 위한 보안 서비스 모델을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2 장은 관련연구로 메타버스 프레임워크에 대해 살펴보고, 메타버스 보안 위협에 대해 분석한다. 3 장에서는 본 논문에서 제안하는 메타버스 프레임워크의 보안 서비스 모델에 대해 기술하고, 보안성 평가에 대해 논한다. 마지막으로 4 장에서는 결론에 대해 기술하고, 본 연구가 갖는 한계점 및 향후 연구에 대하여 기술한다.

# II. 관련 연구

## 2.1 메타버스 프레임워크

2007 년 미국의 기술 연구단체인 ASF 는 메타버스를 그림 1 과 같이 증강현실(Augment Reality), 라이프로깅(Lifelogging), 거울 세계(Mirror World), 가상 세계(Virtual World)의 네 가지 유형으로 분류하였다[5]. 증강 현실(AR)은 물리적 현실환경에 2D 또는 3D 로 표현되는 가상의 사물 및 인터페이스 등을 겹쳐 놓음으로써 만들어지는 환경을 말하며, 라이프 로깅(LG)은 사용자의 신체적, 감정적, 경험적 정보들을 텍스트, 이미지, 영상 등으로 디지털 환경에 기록하는 기술이다. 거울 세계(MW)는 현실 세계의 모습, 정보, 구조 등을 가능한 사실적으로 디지털 환경에 정교하게 구현한 기술이며, 가상 세계(VR)는 사용자들이 디지털 환경에서 아바타 등을 활용하여 소통, 거래, 행동

등의 활동을 할 수 있는 환경을 말한다. 메타버스 개념이 점점 구체화되면서 각 유형들이 서로 융합되고 상호 작용을 하며 하나의 거대한 플랫폼으로 발전하게 되었다.

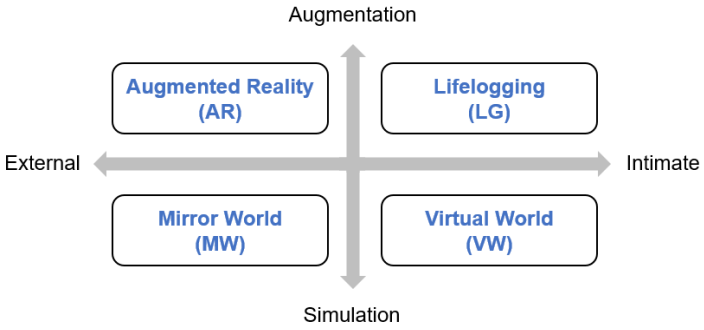


Figure 1. Four Types of Metaverse in ASF
그림 1. ASF 의 메타버스 4 가지 유형

메타버스의 대표적 사례인 네이버 Z 의 “제페토(ZEPETO)”, 로블록스의 “ROBLOX”는 이용자들에게 콘텐츠를 제공할 뿐만 아니라 콘텐츠를 직접 개발 및 제공할 수 있는 플랫폼의 역할을 수행하며 가상세계에서의 다양한 가능성을 보여주고 있다. 이처럼 메타버스는 이용자가 메타버스 구현에 직접 참여하는 플랫폼이 있는 반면, 현실 세계를 가상 공간에 그대로 반영함으로써 가상 공간에서 오프라인 활동을 대체할 수 있는 온라인 서비스를 제공하는 플랫폼들도 있다. 예를 들어 화상회의 플랫폼인 게더타운(Gather town)은 이용자들이 가상의 공간에서 현실 세계와 동일하게 교육 및 세미나, 회의를 할 수 있는 온라인 플랫폼이다.

최근 메타버스는 블록체인 기술과 융합하면서 새로운 형태의 가상현실 서비스로 거듭나고 있다. 블록체인이 뒷받침되지 않으면 메타버스 내의 통용되는 자원이나 재화가 가치를 인정받거나, 현실 경제에 준하는 경제적인 상호작용이 일어나기 어렵다[6]. 따라서 게임, 친목 도모 공간을 넘어 다양한 경제 활동까지 가능해짐에 따라 결제 수단인 암호 화폐와 대체 불가능한 토큰(Non-Fungible Token:NFT)을 활용하는 추세로 시장이 급격히 커지고 있다. 이러한 구성 요소를 토대로 메타버스의 프레임워크를 일반화하면 그림 2 과 같다.

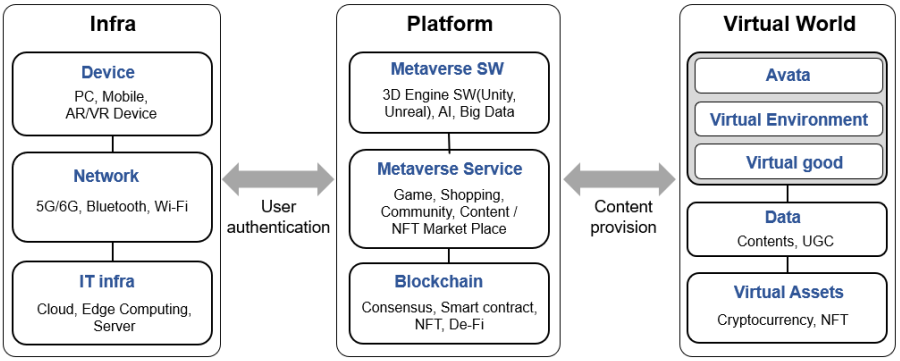


Figure 2. Metaverse Framework
그림 2. 메타버스 프레임워크

메타버스 프레임워크는 현실세계를 디지털세계와 연결하는 인프라와 이를 가상세계로 확장하는 플랫폼 그리고 아바타, 콘텐츠 · IP, 데이터들의 집합체인 가상 세계로 구성된다.

인프라(Infra)는 AR · VR 실감형 디바이스와 네트워크, 클라우드 등의 혁신적 기술을 통해 메타버스에 진입하는 진입점(Entry Point)이 되며, 메타버스에서 원활하고 타임 래그(Time Lag) 없

는 체험을 실현하는데 있어 불가결한 요소이다. 인프라의 기술혁신은 몰입적 경험을 제공하는 실감형 콘텐츠의 발전으로 메타버스 가상세계를 가속화한다.

플랫폼(Platform)은 메타버스의 기반이 되는 가상현실(VR), 증강현실(AR), 혼합현실(MR) 등의 서비스를 제공한다. 플랫폼은 3D 엔진 SW, AI, 빅데이터, 블록체인 등의 기술로 현실세계와 가상세계를 잇는 공간이며, 실감형 콘텐츠의 개발, 유통, 서비스를 경험하게 하는 운영 기반이 된다.

가상세계(Virtual World)는 대부분 디지털 환경으로 구현되어, 사용자가 창작하거나 활동하는 이력 등의 모든 행위가 디지털 데이터로 저장된다. 최근 블록체인 기술을 접목함으로써 이러한 데이터의 사용자 소유권을 보장해주기도 한다. 가상 세계는 콘텐츠 · IP 로 가상 공간을 현실과 유사하게 구현 가능하며, 사용자 기반의 콘텐츠 생산(UGC)과 가상공간의 브랜드 및 아티스트 IP 의 제휴가 활발하다. 또한 이러한 가상세계의 활동에서 생겨난 데이터는 AI, 빅데이터, 클라우드의 기술혁신을 통해 데이터를 분석하고 다양한 분야에 활용할 수 있다.

### 2.2 메타버스 보안의 중요성

메타버스 서비스와 생태계가 확산됨에 따라 메타버스 보안 이슈에 대한 관심도 증가하고 있다. 메타버스는 현실세계의 대체 공간으로서 사회적 관심을 받으며 일상에서 다양하게 적용되는 중이다. 그러나 이 같은 메타버스 활동 영역의 확장은 사이버 위협에 대한 취약성을 증대시키고 있다. 특히, 사물인터넷(IoT)이 적용된 메타버스 기반 보안 위협이 발생 시, 주요 인프라에 대한 물리적 피해와 사회적 혼란 가능성이 제기되고 있다. 메타버스는 AI, NFT 와 함께 새로운 유형의 신종 사이버위협을 초래한다. 예를 들어, 메타버스 공간 내의 개인정보 및 콘텐츠 침해사고, 가상재화 · 암호화폐와 관련된 금융범죄, 메타버스 플랫폼 환경 조작, 인프라 시스템 마비, 통신 네트워크, 데이터의 처리 · 분석 과정에서 악의적인 해킹 위협이 발생할 수 있다[7]. 현재 서비스되고 있는 메타버스 플랫폼들은 이미 몇 차례 보안 취약점이 노출되어 서비스 업체와 사용자들이 모두 피해를 입은 사건이 있었으며, 주로 공격자의 해킹, 시스템 변형 또는 사기 등에 의해 위험에 노출되었다. 메타버스 관련 실제 침해사고는 기존 정보시스템 취약점을 활용한 사례부터 최근 메타버스와 연계된 NFT 를 탈취하는 침해사고로까지 증가하고 있다. 또한 메타버스 서비스의 주고객으로 아동/청소년이 급증하고 있어 온라인상에서의 성범죄, 그루밍 범죄도 증가하고 있으며, NTF 해킹, 계정탈취, 피싱 메일 등 전통적인 보안 위협도 지속적으로 발생되고 있는 상황이다[8]. 이외에도 VR 플랫폼을 통해 가상현실로 손 동작을 통해 아바타의 표정을 제어할 수 있는 등의 제스쳐 인식 기술과 GPS 기반 위치정보, 개인 생체정보, 개인 계정정보, 주변 AP 기반 유무선 통신 등의 기술 적용으로 인해 프라이버시 침해가 매우 쉽게 일어날 수 있다. 최근 발생한 메타버스 프라이버시 침해에 대한 사례를 살펴보면 다음 표 1 과 같다[9].

Table 1. A case of privacy issues in Metaverse
표 1. 메타버스에서의 프라이버시 이슈

| Case | Privacy issues |
|---|---|
| Zepeto | Exposing a face image |
| | Leakage of personal information based on survey results for coin charging |
| Nike Run Club | Life radius and routine exposure using GPS |
| | Exposing personal health records such as heart rate |
| | Expose personal information based on physical security to tags or smartwatches attached to running shoes |
| Animal Crossing New Horizons (ACNH) | Account information registered on the game platform Nintendo can be leaked (April 2019, 160,000 accounts were leaked) |
| | Product can be purchased with leaked account information |
| | Ask a friend and steal an item from a stranger |
| Pokémon GO | GPS-based operations track user behavior and life radius |
| | Security issues with cameras equipped with smartphones can occur |

### 2.3 메타버스 보안 위협 사항

(1) 사용자 인증 문제

현재 대부분의 메타버스 플랫폼은 계정을 생성하고, 자신의 아바타를 가지고 활동하고 있기 때문에 아바타의 행동이나 대화 등 많은 정보가 무분별하게 노출되면 사용자의 신원이 노출될 가능성이 있고, 이를 이용해 신원 사칭 행위가 발생할 수 있다. 뿐만 아니라 시스템 해킹으로 사용자 계정을 탈취하여 시스템 교란이 발생할 수 있다. 일례로 로블록스가 2012 년 4 월 테스트 서버에서 관리자 계정을 해킹 당하였다. 그 결과 로블록스에서 사용되는 화폐인 '로벅스'가 플레이어들에게 공짜로 주어지고, 로벅스를 받은 사용자들은 계정이 사라져 피해를 본 사건이 발생하였다 [10].

(2) 생체정보 문제

메타버스는 XR 을 지원하는 디바이스들을 활용하는 플랫폼들이 증가하고 있어 생체정보에 대한 문제가 발생할 수 있다. XR 디바이스에 부착된 센서들로 착용자의 눈동자 움직임이나 홍채정보는 물론 사용자의 행동을 감지할 수 있고, 손가락의 미세한 움직임까지 감지하기 때문에 생체정보에 대한 유출의 위협이 있다. 또한 음성을 기반으로 한 플랫폼을 이용할 때 역시 목소리 정보 등이 유출될 수 있다는 문제점이 있다.

(3) 사용자 정보 문제

메타버스에서 서비스 중인 많은 어플리케이션들이 위치정보 수집/활용을 허용해야 사용할 수 있다. 특히 메타버스에서의 이용기기가 자체적으로 위치정보, 공간정보, 사용자 자세, 태그 인식 등 현실세계의 정보를 수집하여 증강 정보를 제공하고 있다. 사용자는 이러한 위치정보 유출의 심각성을 인지하지 못하고 있으며, 이러한 위치정보 유출 역시 프라이버시에 위협이 될 수 있다.

(4) 가상자산 보안 문제

메타버스 속에서는 다양한 경제활동이 일어나고 있고, 가상융합경제의 발전으로 가상 화폐 및 가상 자산 시장도 성장하고 있어 금융정보에 대한 보안 대책이 필요하다. 2022 년 2 월에 세계 최대의 종합 NFT 거래 플랫폼인 오픈씨(OpenSea)를 사칭한 이메일을 통해 피싱 웹 사이트에서 32 명의 사용자가 NFT 를 도난당한 사건이 발생하기도 하였다.

이 외에도 메타버스 프레임워크에서의 다양한 보안 위협을 구성요소별로 나타내면 그림 3 과 같다.

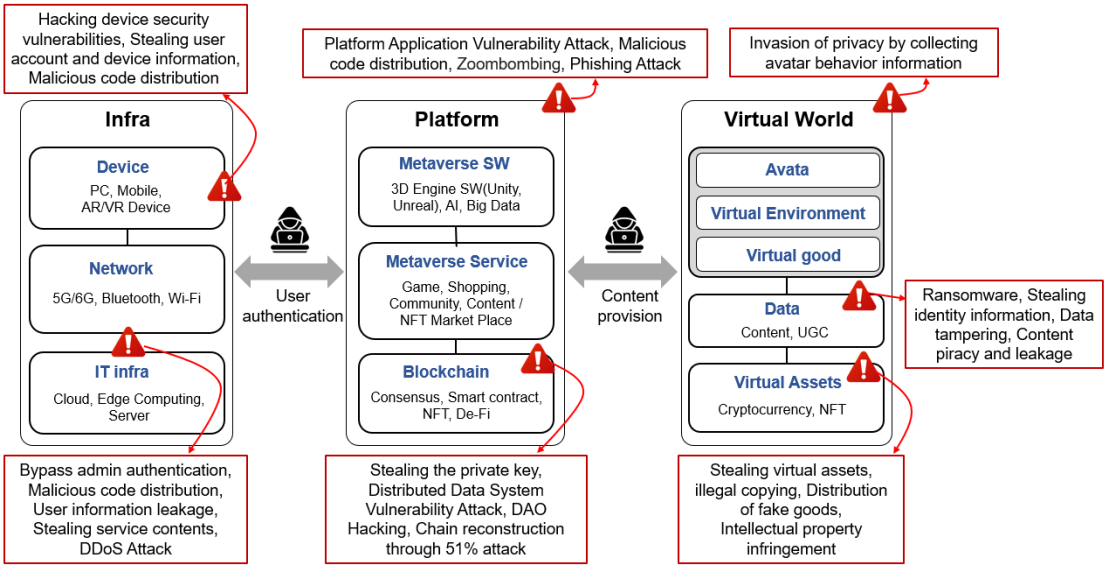


Figure 3. Security Threats in the Metaverse Framework
그림 3. 메타버스 프레임워크에서의 보안 위협

# III. 메타버스 프레임워크 보안 서비스 모델

## 3.1 보안 서비스 모델의 요구 사항

2 장에서 인프라-플랫폼-가상세계 관점에서 메타버스 보안 위협을 살펴보았듯이, 인프라에 대한 위협에는 시스템과 네트워크 통신, 메타버스 이용기기에 대한 보안 위협이 존재한다. 또한 플랫폼에 대한 보안 위협으로는 메타버스 서비스를 위한 소프트웨어를 공격대상으로 한 보안위협이 있으며, 가상세계에서의 사용자 데이터와 가상 자산에 대한 보안위협이 있다. 따라서 메타버스에서의 안전한 서비스를 위해서 메타버스내의 보안요구사항을 4 가지로 도출하여 보안 모델을 제시한다.

- **사용자 인증(User Authentication)** : 사용자 계정, 가상 공간의 신원을 확인 및 보증
- **정보 보호(Information Protection)** : 가상 세계의 데이터(사용자 정보, 콘텐츠, UGC 등) 위/변조 방지 및 개인 정보 보호
- **가상자산 보호(Virtual Assets Protection)** : 가상 자산(가상 화폐 및 NFT) 의 디지털 소유권 보장 및 사기 방지
- **프라이버시(Privacy)** : 저장된 데이터의 개인 정보 암호화, 데이터 분석 및 결합을 통한 개인정보 식별 방지

표 2 에서는 메타버스 프레임워크의 각 구성요소에 필요한 보안 요구사항과 이에 대한 대응 기술을 나열하였다.

Table 2. Security requirements and Security technology of the proposed model
표 2. 제안 모델의 보안요구 사항 및 대응 기술

| Category | Security Requirements | Security Technology | |
|---|---|---|---|
| Device | Privacy, User Authentication | Privacy | Prevention of reverse engineering, Information Encryption, |
| | | User Authentication | FIDO(Fast IDentity Online), Self-inflicted continuous authentication, Biometric Authentication |
| Network, IT Infra | User Authentication, Information Protection | Network Access Control | Role-based Dynamic Access Control, Adaptive User Authentication |
| | | Information Protection | Anti DDOS, IPS/IDS |
| Platform | User Authentication | User Authentication | Blockchain-based DID Authentication, Zero-knowledge proof, FIDO(Fast IDentity Online) |
| Data sets (Information, Contents, UGC) | Information Protection, Privacy | Privacy | Non-identification of personal information, Privacy Preserving Machine Learning(PPML), Differential Privacy(DP) |
| | | Integrity Verification | Secure coding, Bypass Root Detection |
| Virtual Assets (Cryptocurrency, NTF) | Virtual Assets Protection | Ensuring NFT Ownership | Blockchain wallet certification, Blocking the minting bot |
| | | NFT Fraud Prevention | Detect and remove malicious URLs |

• 디바이스(Device) : 디바이스에서 수집된 데이터는 저장하지 않도록 하고, AI 기술을 활용하여 과도한 개인정보 수집을 지양한다. 또한 디바이스의 역공학 방지를 통해 공격자의 해킹을 방지할 수 있다.

• 네트워크(Network, IT infra) : IT 인프라는 기존 정보시스템, IoT 보안 정책 및 보안 기술이 필수로 적용되어야 한다. 클라우드, 서버 등 IT 인프라 지속 가능한 서비스 제공을 위해 정보시스템 보안 요구사항 적용 및 준수 필요하며, 저장된 정보 보호를 위해 네트워크 사용자 접근 통제 기술을 사용할 수 있다.

• 플랫폼(Platform) : 메타버스 플랫폼에서 프라이빗과 퍼블릭 영역을 구분하여 서비스하는 경우 사용자가 인증정보 생성 시 강력한 보안 정책을 설정하여 보안성을 강화해야한다. 또한 메타

버스 서비스 프로그래밍 과정에서 SW 개발 보안 원칙을 준수해야 하며, 소스코드와 디지털 자산에 대한 취약점 점검, 오픈소스 취약점 보완, 플랫폼 관리자 접근제어와 보안정책 수립이 필요하다.

• 데이터(Data sets) : 이용자의 개인 정보, 컨텐츠, UGC 등에 대한 정보보호 수집·관리 정책 수립과 데이터 암호화 및 개인정보 비식별화 처리가 필요하다. 특히 데이터 접근을 위한 인증이 필요한 경우 이용자 계정의 이상행위 탐지 및 통보 시스템 구현, 이용자 보호를 위한 신원인증체계 강화(2 단계 인증, 생체인증, OTP 등)하는 기법을 사용할 수 있다.

• 가상자산(Virtual Assets) : 안전한 디지털 자산 거래 및 이용을 위해 이용자 인증체계를 강화해야 한다. 또한 디지털 자산 보호를 위한 저작권, 지적재산권 권리 입증 체계 마련, 가상세계의 UGC(아이템, 맵, 채팅) 등에 삽입된 QR 코드, URLs 등에 대한 모니터링을 통해 악성 URL 탐지 및 제거하는 기능을 사용할 수 있다.

### 3.2 제안하는 보안 서비스 모델

메타버스에서 안전한 서비스를 위한 보안 서비스 모델은 그림 4 와 같다. 제안한 모델은 2 장에서 설명한 메타버스 프레임워크에서 Agent Server, Authentication Server, Virtual Assets Server, Info Server 를 추가 구성하였다.

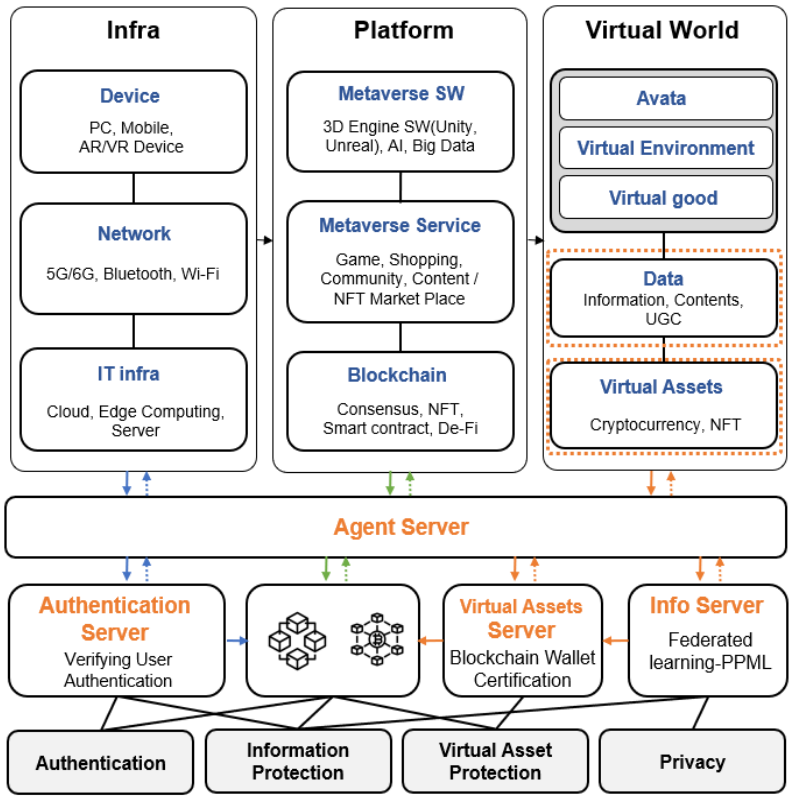


Figure 4. Suggested Metaverse Security Service Model
그림 4. 제안하는 메타버스 보안 서비스 모델

Agent Server 는 메타버스에 접속하기 위한 사용자 인증 요청을 받고, 인증서버(Authentication Server)에 해당 계정의 유효성 검사를 요청한다. 사용 디바이스에 따라 일시적 사용인증 또는 지속적 사용인증으로 구분하여 처리할 수 있다. 또한 가상 데이터를 저장하는 정보 서버(Info Server)에서 데이터 분석과 결합을 통해 개인 정보가 식별될 수 있는 프라이버시 침해에 대해 저장된 정보의 가중치(weight)값을 통해 제 2 의 데이터 모델을 생성함으로써 공개정보와 비공개 정

보를 분리하는 차등 프라이버시를 처리할 수 있다. 그리고 가상 자산 서버(Virtual Assets Server)에 저장된 가상 자산 조회와 소유권 인증 요청을 처리한다.

Authentication Server 는 블록체인의 분산된 원장의 특징은 해커가 대상으로 할 중앙 집중식 거래의 약점이 없다는 것을 의미한다. 사용자 인증 요청 시 일시적 사용자와 지속적 사용자를 구분한 적응형 인증방법을 사용한다. 지속적 사용자인 경우 디지털 식별 플랫폼을 사용하여 개인 디지털 ID 를 생성하고, 이를 블록체인을 통해 저장 및 개인의 신원을 확인함으로써 안전한 사용자 인증 서비스를 할 수 있다.

Virtual Assets Server 는 블록체인 월렛 기술을 통해 가상자산의 진본성(Authenticity)을 검증할 수 있으며, 이는 계약서, 의료 기록, 금융 문서 등 중요 데이터에 대한 보안 및 보호 수단이 될 수 있다. 아바타 및 가상 콘텐츠가 안전하게 이용 · 거래되기 위해 블록체인 기반 스마트 계약, NFT 기술 등이 활용될 수 있다.

Info Server 는 가상 세계의 다양한 정보와 안전성이 검증된 컨텐츠, UGC 를 저장하는 서버로, 블록체인 기술을 기반으로 분산된 불변의 데이터베이스에 ‘디지털 파일 지문’ 을 보관하는 방식으로 데이터를 보호할 수 있다. 또한 데이터 저장 시 차등 프라이버시를 위해 저장된 데이터에 가중치를 부여하여 데이터 보안의 단계를 설정할 수 있으며, 데이터 분석 및 데이터 결합 시 암호화된 개인정보가 식별되지 않는 개인정보 암호화 상태에서도 검색이 가능하게 하는 방법을 사용할 수 있다.

### 3.3 제안된 모델의 보안성 평가

메타버스는 블록체인 없이도 존재할 수 있는 가상현실 공간이지만, 블록체인 기술을 활용했을 때 더 나은 효용성을 제공받을 수 있다. 최근 탈중앙화된 컴퓨팅 능력과 데이터 위변조 방지 관점에서 블록체인 기술이 메타버스에서도 핵심적인 역할을 수행할 수 있을 것이라는 기대가 커지고 있는 추세이다. 블록체인은 거래 기록의 위변조를 방지할 수 있어 신뢰성과 안정성을 보장하며, 네트워크 공격에 대한 보호, 악의적인 행위자 처벌, 합의 메커니즘 및 개인 정보 보호와 같은 핵심적인 기능을 제공한다. 제안한 보안 서비스 모델은 이러한 블록체인을 메타버스에 활용하고, 안전한 사용자 인증과 정보보호, 가상자산 보호 및 프라이버시를 위하여 Agent Server 를 메타버스 프레임워크에 추가가 함으로써 안전성과 효율성을 높이고자 하였다. 또한 인증서버와 가상공간의 각종 데이터를 저장하는 정보서버, 가상 자산 서버를 추가하여 메타버스 내의 보안 및 보호 수단이 되도록 하였다. 이에 대한 보안 요구사항의 만족 여부를 분석한 결과 메타버스 프레임워크의 각 구성요소별 필요 요구사항을 만족하는 것으로 평가되었다. 제안한 메타버스 서비스를 위한 보안 모델의 보안성 분석 결과 다음 표 3 과 같다.

Table 3. Security requirements and Security technology of the proposed model
표 3. 제안 모델의 보안성 평가

| Security Requirements / Metaverse Framework | Authentication | Information Protection | Virtual Assets Protection | Privacy |
|---|---|---|---|---|
| Device | O | O | | O |
| Network, IT Infra | O | O | | O |
| Platform | O | O | O | O |
| Data sets (Information, Contents, UGC) | O | O | | O |
| Virtual Assets (Cryptocurrency, NTF) | O | | O | |

## IV. 결론 및 향후 과제

최근 메타버스에 대한 사회적 관심이 높아짐에 따라 다양한 메타버스 플랫폼 및 서비스가 등장하고 있다. 이러한 메타버스는 하나의 유형에만 국한되는 것이 아니라 경계를 허물며 가상융복합 경제 형태의 서비스로 진화하며 발전하고 있다. 이에 따라 메타버스내에서 다양한 보안에 대한

이슈가 대두되고 있다. 메타버스는 가상 공간에서 모든 활동이 이루어지고, 다양한 디바이스를 이용한 센싱 데이터를 활용하기 때문에 기존의 다른 IT 서비스들보다 많은 정보가 축적되어 정보 보안이 보장되지 않는다면 많은 피해가 발생할 수 있다. 또한 메타버스 속에서 다양한 경제활동으로 가상 화폐 및 가상 자산 시장도 성장하고 있어 금융정보에 대한 보안 대책도 필요하다. 따라서 이러한 메타버스 보안이슈에 대응하기 위해서는 메타버스 프레임워크 내의 보안 위협을 고려한 새로운 보안체계와 보안정책 수립이 요구된다.

본 논문에서는 메타버스에서 안전한 서비스를 제공하기 위한 서비스 보안 모델을 제안하였다. 이를 위해 메타버스 프레임워크에서의 보안 위협을 분석하고, 위협을 방지하기 위한 보안 서비스 모델을 제안하였다. 제안 모델의 보안성을 평가하여 효과적으로 메타버스에서 안전한 서비스가 가능함을 보였다. 본 논문은 최근 이슈가 되고 있는 메타버스의 안전한 서비스 모델 연구에 의의를 찾을 수 있다. 향후 연구에서는 메타버스 정보 보안을 위한 구체적인 기술을 다룰 필요가 있다. 또한 블록체인을 이용한 가상자산 보안 및 메타버스 정보 보안도 지속적으로 연구되어야 할 필요가 있다. 따라서 이에 대한 연구를 본 논문의 향후 과제로 한다.

## VI. 참고문헌

[1] S. H. Lee, "Metaverse begins: 5Major Issues and Forecast" SPRi Analysis Issue Report, IS-116, Apr, 2021.
[2] S. Y. Ko, H. G. Jeong, J. I. Kim, Y. T. Shin, “Metaverse Concepts and Direction of Development,” Korea information processing society review v.28 no.1, 2021, pp.7-16
[3] “Realistic Content Security Model – PART II: Metaverse, Digital Twin,” Korea Internet & Security Agency, 2021.
[4] “2020 Augmented and Virtual Reality Survey Report”, Perkins Coie LL, March, 2020.
[5] John S., Jamais C., Jerry P., Corey B., Jochen H., James H., Randal M., “Metaverse Roadmap,” ASF, 2007.
[6] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp.557-564.
[7] “Analysis of 2021 Cyber Threats and 2022 Prospects”, Ministry of Science and ICT, December, 2021, p.4.
[8] https://www.hankookilbo.com/News/Read/A20220204165600042 67
[9] “A Study on the Spread and Security Issues of the Virtual Convergence Economy,” KISA Insight Vol.04.
[10] [Security trend] In reality, and in metaverse, "Hold on tightly and secure."(2022.03). https://m.post.naver.com/viewer/postView.naver?volumeNo=33527418&memberNo=3185448&searchKeyword=it%20%EB%B8%94%EB%A1%9D&searchRank=254

## 저자소개

**조도은(*Do-Eun Cho*)**

2001 년 8 월 세명대학교 대학원 전자계산교육학과 석사
2007 년 2 월 충북대학교 대학원 컴퓨터공학과 박사
2008 년 3 월~현재 목원대학교 SW 교양학부 조교수

관심분야 : 정보보안, 센서네트워크, 공학교육