정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

메타버스 보안 위협 요소 및 대응 방안 검토

나 현 식*, 최 대 선**

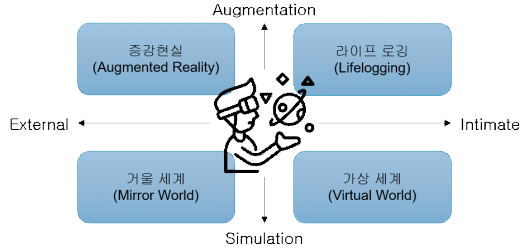
요 약

메타버스는 인공지능, 블록체인, 네트워크, 가상 현실, 착용 가능한 기기 등 수많은 현대 기술들이 발전하면서 서로 융합되어 생성된 대규모 디지털 가상화 세계이다. 현재 메타버스 기반 다양한 플랫폼들이 대중화되면서 산업계 및 연구계에서는 메타버스의 발전에 주목하고 있으며, 긍정적인 시장 전망을 예상하고 있다. 하지만, 아직까지 메타버스 세계에서 발생할 수 있는 보안 위협 요소 및 대책에 관한 연구는 상대적으로 부족하다. 메타버스는 새로운 패러다임의 컨텐츠 및 서비스를 제공하고, 기존 IT 환경에서보다 방대하고 예민할 수 있는 사용자의 데이터를 요구하며, 여러 IT 기술들이 결합된 시스템인 만큼 고려해야 할 보안 위협 요소들이 많다. 본 논문에서는 메타버스 아키텍처를 소개하고, 사용자의 이용 환경, 가상 환경 및 디지털 트윈 환경에서 발생할 수 있는 보안 위협 요소들에 대해 제시하면서, 이에 대해 메타버스 서비스 제공자, 사용자 및 관련 제도 관리자들이 고려할 수 있는 대책들에 대해 소개한다.

Ⅰ. 서 론

지난 2020년 발생한 코로나 19 대유행 이후로 게임, 소셜, 스포츠, 사회, 교육 등 다양한 분야에서 가상의 공간을 통해 다양한 사람들과 비대면 커뮤니케이션을 할 수 있는 환경이 크게 활성화되었다[1]. 재택 근무, 원격 수업, 소셜 네트워크 서비스, 온라인 쇼핑 등과 같이 기존 오프라인 환경에서의 다양한 활동은 메타버스(Metaverse)라는 3차원 온라인 환경에서 경험할 수 있게 되었다.

메타버스는 1992년 Neil Stephenson의 공상 과학 소설 Snow Crash에서 유래된 용어로, Meta(초월성)와 Universe(세계)의 합성어이다. 즉, 현실 세계의 차원을 뛰어넘은 초월 세계를 의미한다. 2007년 미국 미래가속화연구재단에서는 그림 1과 같이 메타버스를 증강현실, 라이프 로깅, 거울 세계, 가상 세계의 네 가지 개념으로 구성하였다[2]. 먼저, 증강 현실은 물리적 현실 환경에 가상의 사물 또는 데이터를 합성하여 표현할 수 있는 가상 현실을 의미하며, 라이프 로깅은 사용자의 신체적, 감정적, 경험적 정보들을 디지털 환경에 기록하는 기술이다. 또한, 거울 세계는 디지털 트윈 기술을 통해 구현될 수 있는 물리적 현실에서의 모습, 정보



〔그림 1〕 미국 미래가속화연구재단(Acceleration Studies Foundation)에서 정의한 메타버스의 네 가지 요소〔2〕.

등을 디지털 환경에 정교하게 구현한 미러링 기술이며, 가상 세계는 수많은 사용자들이 디지털 환경에서 아바타 등을 활용하여 소통, 거래, 행동 등의 활동을 할 수 있는 환경을 의미한다. 메타버스 개념이 점점 구체화되면서 각 구성 요소들이 서로 융합되고 상호 작용을 하며 하나의 거대한 플랫폼으로 발전하게 되었다.

기존 IT(Information Technology) 서비스와 비교하여 메타버스 서비스는 몇 가지 차이점이 존재한다. 먼저, 메타버스는 빅데이터, 인공지능, 블록체인, 가상 현실(VR), 디지털 트윈, 착용 가능한 기기(Wearable device) 및 뇌-컴퓨터 인터페이스(Brain-Computer Interface) 등 수많은 현대 기술들이 결합되어 있는 복

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2021-0-00511, 엣지 AI 보안을 위한 Robust AI 및 분산 공격탐지기술 개발)
* 숭실대학교 소프트웨어학과 (대학원생, rnrud7932@soongsil.ac.kr)
** 숭실대학교 소프트웨어학과 (교수, sunchoi@ssu.ac.kr)

합적인 서비스다. 예를 들어, 디지털 트윈 기술을 통해 생성된 가상 스마트 공장 시설에서 인공지능 기반 예측 모델을 점검하고 실행할 수 있다. 또한, 뇌-컴퓨터 인터페이스 기반 착용 가능한 기기를 통해 뇌파 관련 데이터를 수집하여 인공지능 기반 신원 인증 모델을 통해 메타버스 세계에 진입할 수 있다. 따라서, 메타버스 환경에서는 각 기술별 다양한 보안 위협 요소들(데이터 관리, 사용자 활동 노출 및 추적, 인공지능 보안, 물리적 인프라 안전성 등)을 모두 고려할 필요가 있다.

다음으로, 사용자는 메타버스 플랫폼과 컨텐츠에 참여하기 위해 인적 데이터, 행위 데이터, 감정 데이터, 환경 데이터 등 기존 IT 서비스에서 요구하는 데이터 종류 이외에 새로운 형태의 데이터를 제공하는 것을 허가할 필요가 있다. 예를 들어, 메타버스 서비스 제공자는 카메라를 통해 사용자의 행동 특징을 수집할 수 있으며, VR 기기를 통해 손짓, 홍채, 걸음걸이 등에 대한 정보를 획득할 수 있다. 또한, GPS(Global Positioning System) 장치를 통해 사용자의 현재 위치 정보를 얻을 수 있으며, 카메라에 비추는 배경을 통해 사용자가 거주하고 있는 장소에 대한 정보를 유추할 수 있다. 즉, 새로운 형태의 데이터(아바타 행위 정보, 사용자 환경 정보 등)에 대한 보호 대책이 마련될 필요가 있으며, 가상 공간에서 발생할 수 있는 데이터 노출 문제도 고려해야 한다.

마지막으로, 사용자들은 데이터 전송, 상호 작용, 컨텐츠 경험 등 메타버스 환경의 다양한 상황에서 동일하지 않은(heterogeneous) 장치, 컴퓨팅, 또는 네트워크를 사용하게 된다. 예를 들어, IoT 장치를 통해 사용자의 행위 데이터 또는 특정 동작 요청에 대해 수집하는 경우, 일부 WiFi 기반 장치는 라우터를 통해 직접 연결이 가능한 반면, 일부 non-IP 기반 장치는 hub를 통해 IP 기반 페이로드로 변형되어 데이터가 전송된다. 더 나아가 사용자는 동일한 플랫폼의 장치를 사용하는 것이 아닌 다양한 플랫폼의 장치를 통해 메타버스 환경에 접근할 수 있다. 즉, 기존 IT 서비스보다 메타버스 서비스는 보다 다양한 접근 경로로부터 데이터를 수집하게 된다. 이러한 환경은 보안에 더욱 취약할 수 있으며, CRI(Cross-Rule Interference)[3] 등과 같이 데이터 전송 과정에서 문제가 발생할 수 있다.

향후 메타버스 서비스는 소비자들의 관심과 수요가 급증하고, 투자자들의 지원과 시장 규모가 크게 증가할 것이라는 많은 분석이 존재하지만, 메타버스의 보안성 및 안전성에 대한 우려 또한 증가하고 있으며[4], 충분한 보안 대책이 마련되어 있지 않다. 또한, 2020년 Perkins Coie LLP에서 실시한 몰입형 기술 및 컨텐츠의 법적 리스크 우려에 대한 설문조사[5]에서는 제품 문제 및 건강과 안전 문제(48%)보다 소비자의 개인 정보 및 데이터 보안에 대한 문제(49%)에 대해 더 큰 우려를 드러냈다. 즉, 원활한 메타버스 서비스를 위해서는 충분한 보안성 및 안전성의 검증이 필요하며 철저한 대응책이 필요하다는 것을 알 수 있다.

본 논문에서는 메타버스의 다양한 환경에 따른 보안 위협 요소와 그에 대한 대책에 대해 서술한다. 기존 IT 환경에서 존재하였던 보안 침해 기술들뿐만 아니라 메타버스 환경에서 발생할 수 있는 새로운 형태의 보안 침해 기술들에 대해 소개하면서, 향후 메타버스 서비스 제공자 및 소비자, 그리고 메타버스의 보안 침해 방지를 위해 기준을 마련하는 기관들이 고려해야 할 사항들에 제시한다.

Ⅱ. 메타버스

2.1. 메타버스 주목 요인

메타버스는 스마트폰 중심의 플랫폼 시대 이후 새로운 형태의 플랫폼 및 서비스를 제공할 수 있는 차세대 사이버 공간으로 떠오르고 있다. 많은 전문가 및 매체에서 메타버스를 이와 같이 주목하고 있는 요인은 다음과 같다[6].

- IT 기술의 발전
- 새로운 차세대 플랫폼 창출
- 비대면 상호 작용의 확산
- 디지털 네이티브 세대의 등장

첫 번째로, XR(eXtended Reality), 빅데이터, 네트워크, 인공지능, 블록체인, 디지털 트윈, 클라우드 등 정보 기술의 발달로 인해 다양한 기술들이 융합되어 시너지 효과를 일으키면서 발전한 점이다. 이를 통해 더 나은 성능과 효율성을 가진 서비스들의 생산과 소비가 급증하였고, 관련 산업의 R&D가 크게 확대되면서 발전에 대한 더 큰 기대를 얻게 되었다. 두 번째로, 스마트폰 기반 플랫폼의 성장 이후 새로운 영역에서의 플랫폼이 개발된다는 기대로 인해 수많은 국내외 기업들의 적극적인 관심 및 투자를 받고 있다. 메타버스는

시간적, 공간적 제약을 최소화하는 초월적 영역에서의 서비스 제공 기능을 갖추고 있으며, 사용자가 직접 컨텐츠 및 아이템을 제작, 판매 및 소유할 수 있는 자유로운 시스템이 존재하기 때문에 새로운 형태의 플랫폼에 대한 기대를 받을 수 있게 되었다. 세 번째로, 뉴노멀 시대가 도래하면서 사회 및 경제적 참여자들의 디지털화(재택 근무, 온라인 미팅)가 가속화되고 있다. 메타버스 환경은 물리적 공간이 요구되지 않고, 제약이 적은 가상 공간에서 현실과 유사한 사회 활동이 가능하기 때문에 많은 참여자들의 기대를 받고 있다. 네 번째로, PC(Personal Computer), 스마트폰 등 디지털 환경이 익숙한 Z세대 및 알파세대들의 니즈를 충족할 수 있다는 점이다. 이들은 어린 시절부터 스마트 기기를 접해 인터넷 문화에 익숙하고, SNS를 통한 사회 활동에 많은 흥미를 느낀다. 또한, 개인의 다양성 및 개성에 중점을 두며, 개인의 가치를 중요시하는 경향이 존재한다. 이러한 성향은 메타버스에서 제공하는 자율적인 서비스와 긍정적으로 융합되고 있다.

2.2. 메타버스에 대한 국내 기관들의 발전 방향

전 세계에서 메타버스를 주목하고, 새로운 패러다임의 글로벌 트렌드로 자리잡게 되면서 국내 역시 메타버스 관련 기술과 산업에 관심을 갖고 있다.

먼저, 메타버스 세계는 디지털 가상화를 통해 구현될 수 있다. 즉, 현실 세계와 가상 세계 간 정보 디지털 신호를 통해 동기화하여 표현할 수 있으며, 이를 위해 디지털 가상화 기술의 표준 기술이 개발될 필요가 있다. 이에 따라 2019년 국내 산학계가 주도하여 참여하는 IEEE 2888 WG(Interfacing Cyber and Physical World Working Group)[7]가 신설되었으며, 이들은 물리 객체와 가상 객체 간 응용 프로그래밍 인터페이스 및 센서 기반 정보 교환을 위한 요소들(센서, 작동기, 상호 연동, 응용 기술)에 대한 표준을 정립하였다.

다음으로, 2020년 정부는 가상융합경제 발전 전략을 제시하였고[8], 특히 XR 기반 산업 및 사회 활동의 확산과 XR 기술력 고도화 및 세계적 경쟁력 확보를 위한 전략을 발표하였다. 이들은 현재 다양한 산업(제조, 건설, 교육, 의료 등)에서 XR 기술 활용 효과를 향상시키기 위해 다양한 프로젝트를 추진 중이다.

또한, 2022년 정부는 메타버스 신산업 선도전략을 소개하면서[6] 메타버스 세계로 인한 사회 및 경제적 변화에 대응하고 미래를 준비하기 위한 전략을 발표하였다. 이들은 메타버스 플랫폼의 주요 유형을 크게 사회 관계 형성, 디지털 자산 거래, 그리고 원격 협업 지원으로 분류하였다. 먼저, 사회 관계 형성은 SNS(Social Network Service), 게임 등 사용자 간 커뮤니케이션 기능을 하고, 디지털 자산 거래는 가상 부동산, 가상 상품(컨텐츠, 작품, 소비재 등)의 직거래 기능을 하며, 원격 협업 지원은 가상 공간에서의 원격 의사소통 및 다중 협업 지원 기능을 제공한다.

2.3. 메타버스 서비스 사례

현재, 이미 많은 기업들이 메타버스 플랫폼을 구축하여 다양한 서비스를 제공하고 있으며, 소비자들은 게임, 소셜 서비스, 경제 활동, 비대면 업무 수행 등 여러 컨텐츠를 소비하고 있다[9].

대중적으로 많이 알려진 메타버스 플랫폼으로는 포트나이트, 로블록스, 동물의 숲, 제페토 등이 있다. 각 플랫폼에서는 게임, 패션 브랜드 전시회, 연예인 팬 사인회, 콘서트, 커뮤니티 형성, 신제품 광고 등 광범위한 사회 및 문화 활동이 이루어지고 있다.

또한, 더 샌드박스, 디센트럴랜드, 액시 인피니티 등은 디지털 가상 세계의 토지를 가상 화폐를 통해 매매하여 해당 영역에서 건물 건축, 광고 등을 통해 실제 수익 활동을 할 수 있는 부동산 형태의 메타버스 플랫폼이다. 비록 가상의 세계에 존재하는 영역이지만 토지 주변에 큰 도시가 존재하거나 인기 있는 기업 건물이 있는 경우 토지 가격이 크게 증가하는 등 현실 세계와 매우 유사한 부동산 형태를 띠고 있다.

추가적으로, 최근 금융업 분야에서도 메타버스 플랫폼에 대한 투자를 지속적으로 하고 있음을 확인할 수 있다[10]. 예를 들어, 신한은행의 쏠버스, NH농협은행의 독도버스 등은 은행사에서 제작한 자체 플랫폼으로, 소비자들은 해당 플랫폼 내에서 예·적금 가입, 대출 상담 등 금융 거래를 할 수 있다. 또한, 신한카드와 하나카드는 제페토 플랫폼 내에서 각각 선불카드 출시와 전용 월드 개장 등의 시도를 한 경험이 있으며, 삼성화재는 자체 플랫폼 내에서 신규 브랜드를 출시한 적이 있다.

이 밖에도, 디지털 트윈 기술을 기반으로 스마트 공장 및 스마트 시티를 구현하여 제품 설계 및 진단, 공장 관리, 제조 과정 분석 및 최적화, 시설 모니터링, 시

뮬레이션, 대민 서비스 지원 등 다양한 기능을 수행하고 있다.

2.4. 메타버스 보안 침해 사례

현재 서비스되고 있는 메타버스 플랫폼들은 이미 몇 차례 보안의 취약점이 노출되어 서비스 업체와 소비자들이 모두 피해를 입은 사건이 있었으며, 주로 공격자의 해킹, 시스템 변형, 또는 사기 등에 의해 위험에 노출되었다[9].

먼저, 플레이어 참여형 글로벌 게임 제작 플랫폼 로블록스에서는 2012년 일반 사용자로부터 로블록스 테스트 사이트에서 관리자 권한을 해킹당해 통화 시스템, 아이템, 물리적 객체 등 플랫폼의 중요한 요소들이 상당히 훼손되어 사용자들과 관리자들이 큰 피해를 입은 사건이 발생하였다. 또한, 2020년 한 로블록스 관리자가 공격자로부터 매수되어 플랫폼의 백엔드 패널에 접근해 사용자들의 개인 정보가 조회되고, 통화 부여 권한이 허용되는 사건이 발생하였다.

다음으로, 2021년 익명의 미술가 뱅크시의 작품을 사칭한 가짜 NFT(Non Fungible Token)이 약 25만 파운드에 거래되는 사건이 발생하였다. 이는 한 해커가 뱅크시의 웹사이트를 해킹하여 가짜 NFT 작품을 생성한 후 경매 링크를 통해 사기 범죄를 일으킨 것으로 알려져 있다. 또한, 사용자 행동 데이터 기반 블록체인 플랫폼 림포(Lympo)에서는 한 해커가 림포의 핫월렛에 접근해 약 1억 6,500만 달러의 가치를 가진 LMT(Lympo Market Token)을 도난 하였으며, 암호화폐 거래소 LCX에서는 2022년에 핫월렛이 유출되어 약 700만 달러의 규모가 도난당한 사건이 발생하였다. 이와 같이, 만일 블록체인 기반 암호화폐의 보안이 취약한 경우, 소비자와 서비스 업체는 막대한 규모의 피해를 입을 수 있다.

한편, 스마트 도시 및 공장 서비스가 악성 코드에 감염되어 피해를 입은 사례들도 존재한다. 먼저, 2017년에 캘리포니아 스마트 도시 시스템이 랜섬웨어에 감염되어 해당 지역 버스와 경전철을 운행하는 시스템을 통해 약 3,000만 개의 파일이 손상되는 피해가 있었다. 또한, 2018년 싱가포르에서는 한 의료그룹의 데이터베이스가 악성 코드에 감염되어 약 16,000명의 처방전이 유출되는 사건이 발생하였다. 그리고, 2014년 일본의 몬주 원자력 발전소에서는 내부 작업자가 애플리케이션 업데이트 도중 악성 코드에 감염되어 발전소의 내부 정보가 유출된 사례도 존재한다.

이 밖에도, 네이버Z에서 출시한 아바타 기반 소셜 서비스 플랫폼 제페토에서는 2022년 한 30대 남성이 아동 청소년들을 대상으로 스토킹 및 성희롱을 한 사건이 발생하였다. 메타버스의 주요 소비층이 미성년자인 점(제페토 가입자 중 10대 이용자 비중이 80%에 달함[11]을 고려했을 때, 온라인 그루밍을 통한 범죄에 노출될 가능성이 높으며, 이러한 문제를 방지하기 위해 서비스 제공자는 이에 대한 대책을 마련할 필요가 있다.

Ⅲ. 메타버스 아키텍처

본 논문에서는 메타버스의 보안 위협 요소들을 분류하기 위해 그림 2와 같이 아키텍처를 구성하였다. 메타버스 아키텍처는 크게 이용 환경, 네트워크, 가상 환경, 디지털 트윈 환경, 그리고 인프라로 구성된다.

3.1. 이용 환경(물리적 세계)

이용 환경은 사용자가 메타버스 서비스를 경험할 때 실제로 존재하는 물리적 세계를 의미한다. 사용자들은 PC, 스마트폰, 태블릿 기기, IoT 기기, 또는 AR(Augmented Reality) 및 VR 기기와 같이 착용 가능한 기기 등을 통해 메타버스 환경에 진입할 수 있다.

먼저, PC는 현재 서비스되고 있는 메타버스 플랫폼에 진입하기 위해 가장 많이 사용되고 있는 방식이며, 오늘날 기술의 발전으로 인해 고사양의 메타버스 시스템에서 원활한 컨텐츠 소비가 가능해졌다. 소비자들은 집, 회사 등 PC가 구동될 수 있는 장소에서 접근할 수 있으며, 기존 2D 형식의 모니터와 같은 평면 디스플레이는 3D 환경의 공간감을 느끼기 어렵기 때문에, 소비자들은 3D TV 또는 3D 모니터와 같은 장치를 통해 한계를 극복할 수 있다. 하지만, 이러한 장치들은 공간감을 충분히 느낄 수 있지만, 공간적 자유도가 떨어진다는 문제가 있다. 이에 따라 현재 많은 사용자들은 가상 환경에 최적화된 HMD(Head Mounted Display)와 같이 착용 가능한 기기를 결합하여 이전의 문제들을 극복할 수 있다.

다음으로, 스마트폰 및 태블릿 기기는 자유로운 응용 소프트웨어 설치를 통해 다양한 컴퓨터 지원 기능을 제공하는 단말기이다. 이들은 공간적 제약이 매우

적으며, 신체적으로 자유롭게 활용 가능하다. 현재 스마트폰은 전화 통화, SNS, 지도, 문화 생활, 금융 생활 등 사용자의 전반적인 일상 생활에 큰 도움을 주고 있지만, PC와 같이 메타버스만의 3D 공간감을 완벽하게 체험하는 데 한계가 있다. 이에 따라 PC와 같이 착용 가능한 기기들과 호환을 통해 메타버스 환경에 진입할 수 있다.

한편, IoT 기기는 주로 메타버스 기반 스마트 홈 또는 스마트 도시 서비스를 구현하고 체험할 때 활용할 수 있는 방식이다. 주로 센서, 소프트웨어 등을 통해 네트워킹, 정보 처리, 감지 등의 작업을 수행하는 인터넷에 연결된 사물을 의미하며, 이들은 움직임 감지, 환경 정보 감지, 사물 감지, 위치 탐색, 음성 인식 등의 기능을 수행할 수 있다. 대표적으로, AI 스피커, 지능형 CCTV, 온도 측정 센서 등이 있다.

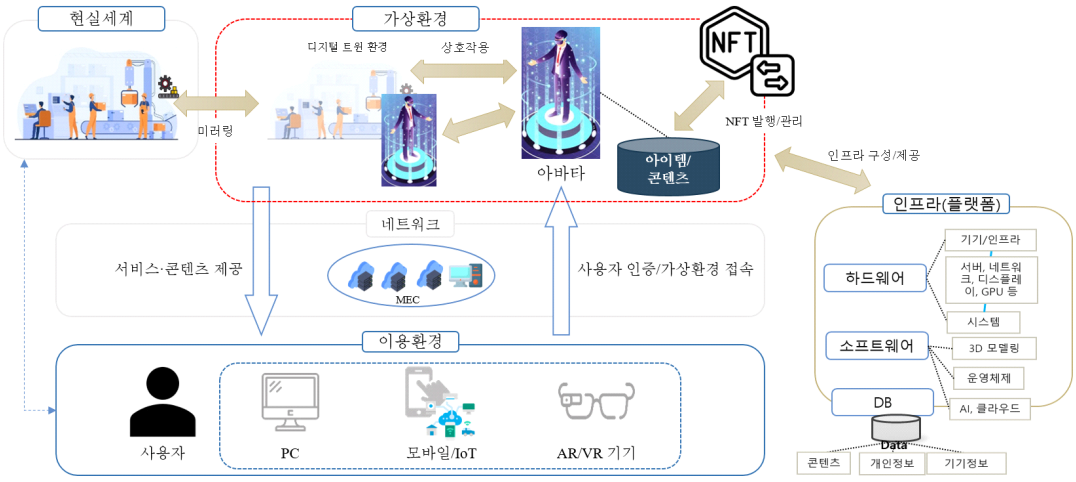
마지막으로, HMD 디스플레이와 같은 착용 가능한 기기는 사용자의 몰입감을 극대화할 수 있는 접근 방식이다. 이들은 장소의 제약이 적고, 쉽게 디스플레이를 확장할 수 있으며, 3D 환경을 구현할 수 있다는 장점이 있다. 현재까지 아직 성장 중인 분야이고, 제품의 보급 및 소비가 대중적이지는 않지만 향후 XR 시장이 크게 성장할 것으로 기대되며, 메타버스 서비스 확산을 위해 핵심적인 역할을 할 수 있는 산업이다. 대표적으로 스마트 글래스, VR 헤드셋 등이 있으며, 한 연구[12]는 VR 헤드셋과 키보드를 활용해 VR 환경에서 업무를 수행하고 이에 대한 사용자들의 평가에 대해 분석하는 실험을 시도했다.

3.2. 네트워크

네트워크는 사용자와 디지털 환경을 연결하는 영역을 의미한다. 5G 및 6G 네트워크 통신 기술의 꾸준한 발전은 메타버스가 지속적으로 성장하는 데 중요한 요소가 될 수 있었다. 특히, 5G는 기존 네트워크보다 데이터 전송 속도가 크게 향상(초고속성)되었고, 전송 대기 시간이 대폭 단축(초저지연성)되었으며, 정보 송수신 범위가 크게 확장(초연결성)되었다. 메타버스의 지속성 유지는 중요한 요소이다. 즉, 소비자가 실시간으로 컨텐츠에 지속적 몰입이 가능해야 하며, 이를 위해 대규모 메타버스 네트워크의 유연하고 확장 가능한 관리가 요구된다. 뿐만 아니라, 메타버스 플랫폼의 실시간 요구에 따라 가상화된 컴퓨팅, 스토리지, 대역폭 리소스를 동적으로 할당해야 하며, 대규모 데이터 전송에 대한 제약이 없어야 한다.

3.3. 가상 환경

가상 환경은 메타버스 세계 내에서 사용자가 주된 활동을 하는 디지털 영역이다. 이 영역은 디지털 세계, 디지털 아바타, 그리고 디지털 아이템 및 컨텐츠 등으로 구성되어 있다. 먼저, 디지털 세계는 아바타가 주된 활동을 하는 공간을 의미하며, 일부 플랫폼에서는 토지의 일부를 소비자가 소유할 수 있는 형태로 존재하고 있다. 다음으로, 디지털 아바타는 메타버스 세계에서 활동하기 위해 사용자가 생성한 가상의 캐릭터이



〔그림 2〕 메타버스 아키텍처.

다. 사용자는 아바타를 본인이 의도한 모습 또는 본인의 실제 외모와 유사한 모습으로 생성할 수 있다. 마지막으로, 디지털 아이템 및 컨텐츠는 메타버스 플랫폼에서 제공하거나 사용자들이 직접 제작한 다양한 유형의 상품(게임, 미술품, 의류, 이벤트, 서비스 등)을 의미한다. 플랫폼 내 사용자들은 아이템 및 컨텐츠를 서로 교류하며 수익을 창출할 수 있으며, NFT 기술을 활용하여 아이템에 대한 고유 권한을 획득할 수 있다. 가상 환경에 존재하는 주요 애플리케이션으로는 게임, 소셜 서비스, 온라인 협업 플랫폼, 시뮬레이션, 디자인, 그리고 경제 및 거래 시스템 등이 있다.

3.4. 현실 세계(디지털 트윈 세계)

디지털 트윈 세계는 현실 세계의 다양한 객체(토지, 건물, 기계, 운송 수단 등)들뿐 아니라 현실적 요인(경제, 기후, 인간 등)을 가상 세계에 미러링 기술을 통해 구현한 디지털 세계이다. 해당 공간에서 사용자는 아바타를 활용해 시뮬레이션, 경험, 교육 등 다양한 활동을 수행할 수 있다.

3.5. 인프라(플랫폼)

인프라는 데이터 인식, 전송, 처리 및 제어 등과 같이 메타버스 환경을 운영하고 관리하기 위해 필요한 구성 요소를 의미한다. 이는 크게 하드웨어, 소프트웨어, 그리고 데이터베이스로 구성되어 있으며, 먼저 하드웨어에는 서버, 네트워크, 디스플레이, GPU, 기타 장비가 포함된다. 또한, 기기는 PC, 스마트폰, VR/AR 장치, 뇌파 측정 장치 등이 포함되며, 추가적으로 데이터베이스를 관리하고 전송하는 데 필요한 동력을 제공하는 자원들도 포함될 수 있다.

다음으로, 소프트웨어에는 웹, 컨텐츠 관리 시스템, 운영체제 등이 포함되어 있다. 이들은 시스템과 하드웨어를 관리하고, 애플리케이션과 하드웨어 간 교류를 위해 수행되는 작업들도 포함될 수 있다. 또한, 메타버스 환경에서는 인공지능 플랫폼, 클라우드 서비스 등도 중요한 요소로서 포함된다.

마지막으로, 데이터베이스란 메타버스 환경에서 가능한 모든 활동을 위해 필요한 정보들의 집합을 의미한다. 이것은 인적, 행위, 감정, 환경 정보 등으로 구성된 사용자의 개인 정보와, 컨텐츠 사양, 장르, 크기, 가격 등으로 구성된 컨텐츠 정보와, 기기 사양, 통신 방법, 센서, 작동기 등으로 구성된 기기 정보 등으로 분류할 수 있다.

Ⅳ. 메타버스 보안 위협 요소 및 보안 대책

본 논문은 메타버스 세계를 구축하는데 필요한 선제적 위협 대응 방법과 보안 대책 및 기준을 마련하기 위해 필요하다. 또한, 향후 메타버스 보안 관련 가이드라인 제시 및 안전한 서비스를 위한 참고 자료로써 활용하기 위해 환경별 보안 위협 요소 및 대책을 강조한다.

본 논문의 목표는 메타버스 서비스의 보안 수준 제고, 사용자의 프라이버시 보호, 그리고 견고하고 안전한 메타버스 환경 구축을 위한 기반 제시이다. 또한, 메타버스 내 환경 요인 중 이용 환경 및 가상 환경에서의 보안 문제에 초점을 두고 있다. 네트워크 및 인프라 환경에서의 보안 문제는 기존 IT 환경에서의 보안 위협 사항 및 취약점 문제와 유사하며, 이용 환경 및 가상 환경의 경우, 다른 환경들보다 고려해야 할 요소들이 많다. 추가적으로, 메타버스 환경에서 새로운 형태의 데이터 및 인프라가 구축됨으로써 새롭게 발견할 수 있는 보안 이슈들에 대해 나열하는 것에 초점을 둔다. 본 논문에서 언급하지 않는 네트워크 및 인프라 환경에서의 보안 이슈들에 대한 내용은 한 연구[13]를 통해 확인할 수 있다.

해당 장에서 적용하는 보안 범위는 메타버스의 네 가지 개념, 즉, 가상 세계와 거울 세계를 중심으로 증강 현실과 라이프 로깅을 포괄한다. 적용 대상은 메타버스 서비스 제공자를 포함하여 사용자, 관련 제도 관리자를 포함한다. 아래 각 절은 각 메타버스 환경 내에 존재하는 보안 위협 대상에 따라 분류되었다. 추가로, 본 논문에서는 사용자 및 플랫폼 제공 업체에 피해를 가할 수 있는 대상을 '공격자'로 지칭하여 설명하였다.

4.1. 이용 환경 – 사용자

4.1.1. 신원정보 탈취

공격자는 메타버스 서비스 사용자의 주민등록번호, 신용 카드, 이름 등 개인 정보를 서비스 인터페이스를 통해 탈취하여 해당 사용자의 신분을 통해 범죄에 악

용할 수 있다. 주로 메신저, 전화 등을 통해 피싱 공격을 시도하며, 사용자는 주변 인물 또는 서비스 제공자로부터 수신된 요청으로 착각하여 개인 정보를 제공하게 된다.

이러한 위협에 대응하기 위해 서비스 제공자는 안티 피싱(Anti-phishing) 기술을 제공할 수 있다. 이것은 피싱 이메일을 탐지 및 차단하거나, 브랜드 사칭 메시지를 탐지하는 방식으로 공격을 방지한다[14]. 또 다른 방법으로는 안티 파밍(Anti-pharming) 기술이 있다. 이것은 신뢰할 수 있는 DNS 정보를 활용하거나 DNS 프로토콜에 보안 기능을 추가하는 방법을 통해 위협에 대응할 수 있다[15]. 추가적으로, 메타버스 플랫폼이 사용자 개인 정보를 저장하지 않고, 인증 과정에서 피어 투 피어 네트워크(Peer-to-peer network)를 구축하여 사용자들이 중개 기관을 거치지 않고 직접 본인 인증을 하는 시스템을 구축하는 방법이 있다[16]. 한편, 사용자들은 피싱 방지를 위해 이메일 인증, 스푸핑 방지 프로토콜 설치 등을 통해 공격자의 침입이 어려운 환경을 조성할 필요가 있다.

4.1.2. 인증 도용(가장)

인증 도용은 공격자가 특정 사용자로 가장하여 사용자의 정보를 획득하기 위해 SNS 등을 탐색한 후, 해당 사용자인 척 여러 공간에서 악의적 행동을 하는 것을 의미한다[17]. 이것은 실제 인물이 아닌 아바타 간 커뮤니케이션이 활성화된 메타버스 환경에서 큰 위협이 될 수 있다. 다른 사용자들은 해당 아바타가 실제 주인인지 또는 공격자인지 판단하기 어려울 수 있기 때문이다.

서비스 제공자는 이를 방지하기 위해 먼저, 멀티 팩터 인증(Multi-factor authentication) 제도를 도입할 수 있다[18]. 이것은 사용자가 접근 권한을 얻기 위해 ID 및 비밀번호 이외에 추가 확인 요소를 제공하도록 요청하는 방식으로, 생체 정보(지문), PIN, 위치 정보(GPS) 등을 활용한다. 또 다른 방법으로는 기존 비밀번호 기반 인증 절차보다 개선된 강화 인증 제도를 도입할 수 있다.

4.1.3. Identity 관리 복잡성

사용자들은 다양한 플랫폼에서 제공하는 애플리케이션 및 서비스에 접근하기 위해 각각에 대한 자격 증명 요소(ID, 개인 정보 등)를 제공해야 한다. 이에 따라, 사용자들이 사용하게 되는 ID 및 비밀번호의 수가 매우 많아지며, 서로 다른 애플리케이션에서 같은 ID 및 비밀번호를 사용하는 경우가 많아진다. 이 때, 만일 공격자가 하나의 애플리케이션에서 비밀번호를 추출한 경우 사용자는 여러 애플리케이션에서 피해를 입을 수 있다. 따라서, 메타버스 사용자들은 여러 가상 세계에 분산된 자신의 신원정보 및 자산을 편리하고 안전하게 관리할 수 있는 환경, 즉, Identity 관리의 복잡성을 완화하는 기술이 요구된다.

신원 관리(Identity management) 모델은 사용자가 애플리케이션, 시스템 및 네트워크에 대해 적절한 접근 권한을 갖도록 보장하기 위한 조직화된 프로세스이다. 또한, 공격자로부터의 해킹, 랜섬웨어, 피싱 등 기타 악성 프로그램 공격을 포함한 다양한 위협으로부터 개인 및 기업의 자산을 보호할 수 있다. 메타버스 환경과 같이 여러 플랫폼에 편리하게 접근할 수 있는 신원 관리 모델은 대표적으로 연합 신원 관리(Federated identity management)와 자기 주도형 신원 관리 모델(User-centric identity management)이 있다.

먼저, 연합 신원 관리[19]는 사용자가 동일한 신원 정보를 사용해 다양한 애플리케이션에 접근할 수 있도록 구현된 모델이다. 다시 말해, 하나의 애플리케이션에 로그인한 경우, 다른 애플리케이션에 접근할 때 다시 로그인할 필요가 없는 특징을 갖고 있다. 이것은 기업의 관점에서 Single Sign-On 기법 등 자격 증명 기술을 별개로 개발할 필요가 없어 비용 절감의 효과가 있으며, 사용자의 관점에서 반복적으로 로그인할 필요가 없어 시간 효율성이 향상되며, 로그인 프로세스가 단축되어 해킹 위험이 줄기 때문에 개인 정보 보호의 효과를 얻을 수 있다.

다음으로, 자기 주도형 신원 관리[20, 21]는 사용자에 의해 완전히 제어될 수 있는 디지털 신원 관리 모델을 의미한다. 여러 애플리케이션에 접근할 때 사용자가 자유롭게 서로 다른 개인 정보를 공유 및 연결하여 신원 정보를 상호 운용할 수 있도록 제공하며, 사용자는 디지털 지갑 등을 통해 본인의 신원 정보를 직접 관리하면서 애플리케이션 및 서비스에 해당 지갑을 활용해 접근할 수 있다.

4.1.4. 감각 왜곡 공격 및 위험 행동 유발

공격자는 디지털 환경에서뿐만 아니라 현실 환경에서 사용자에게 위협을 가할 수 있다. 예를 들어, VR 및 AR 제품과 같이 착용 가능한 기기를 조작하여 플레이 도중 갑자기 강력한 빛을 노출하거나 불쾌한 사운드를 주입하여 사용자가 어지러움, 광과민 발작 등의 감각 착각, 자극을 느끼도록 유도할 수 있다. 또한, GPU 또는 네트워크를 대상으로 공격자가 침입하여 사용자 이동, 상호 작용, 오디오 및 비디오 중단을 통해 시각적 불편함을 유발할 수 있다[22].

이와 유사하게, 디지털 컨텐츠 또는 기기를 통해 사용자가 위험한 행동을 하도록 유도하는 공격을 시도할 수 있다. 예를 들어, 실제 계단의 위치를 약간 조작하거나 계단이 존재하지 않는 것처럼 보이도록 조작하여 사용자가 계단에서 떨어지도록 유도할 수 있다. VR 헤드셋 등 착용 가능한 기기들은 실제 사용자의 주변 시야를 완전히 차단하는 특징을 갖고 있기 때문에, 기기 사용 시 사용자의 안전에 대한 위험이 항상 존재[23]하며, 만일 공격자가 만일 컨텐츠 또는 기기를 변조하여 이러한 사고를 유발한다면 큰 위험이 따를 수 있다.

이를 방지하기 위해, 서비스 제공자는 컨텐츠 및 기기 변조 방지 기술을 도입하여 공격자의 조작을 예방할 수 있다. 반면, 이와 같은 피해 사례에 대한 조치를 위해 제도적으로 금지 기준 및 처벌 정책을 마련하는 것이 필요하며, 기기를 통한 시험, 평가, 인증의 절차를 거쳐 악의적인 컨텐츠 및 기기를 필터링하도록 하는 제도가 요구된다.

4.1.5. 위험 컨텐츠

공격자는 VR 또는 AR 기반 컨텐츠를 악의적으로 제작 또는 조작하여 사용자가 공포나 충격을 느끼도록 유도할 수 있다. 예를 들어, 공격자가 사용자의 아바타 앞에 가상 환경에서 유령 사진 등 유해하고 무서운 컨텐츠를 표시해 해당 사용자가 불쾌한 자극을 느낄 수 있다. 메타버스는 몰입형 리얼리즘을 추구하기 때문에 이러한 위협 요소가 사용자에게 큰 피해를 입힐 수 있다.

서비스 제공자는 이를 방지하기 위해 위험 컨텐츠 탐지 기술을 도입할 수 있다. 사용자에게 불쾌감을 줄 수 있는 컨텐츠를 사전에 탐지하여 필터링하는 인공지능 기반 기술을 도입하면 이러한 위협을 어느 정도 방지할 수 있을 것이다. 또한, 감각 왜곡 공격과 마찬가지로 금지 기준 및 처벌 제도를 제정하여 적절한 조치를 취할 수 있도록 하는 대책도 마련할 필요가 있다.

4.2. 이용 환경 - 기기

4.2.1. 생체 정보 유출

메타버스 플랫폼에서는 주민등록번호 등 개인 정보 대신 얼굴, 지문, 홍채, 뇌파, 안전도 등 생체 정보를 통해 사용자의 접근을 허용하는 방법을 사용할 수 있다. 이 때, 공격자는 사용자의 기기를 통해 생체 정보를 유출하거나 악용할 위험이 있으며, 생체 정보 역시 사용자의 고유한 인증 정보로써 활용될 수 있기 때문에 보안성이 중요하다.

서비스 제공자는 기기의 보안을 개선하기 위해 생체 정보 전송 시 암호화 기술을 통해 비식별화[24,25]할 수 있으며, 생체 정보를 안전하게 저장하는 기술[26]을 도입할 필요가 있다.

4.2.2. 사용자 프로파일링

기기는 사용자의 다양한 센서, 표정, 시선, 제스쳐 등을 모두 인식할 수 있으며, 더 나아가 말하고, 행동하고, 느끼는 감정까지 인식할 수 있다. 이러한 행위 및 감정 정보들은 사용자의 동적 개인정보에 포함되며, 이것을 통해 공격자는 사용자를 유추할 수 있다. 사용자는 메타버스 환경 내 아바타를 통해 상호 작용을 하면서 자신의 익명성이 보장된다고 판단하지만, 기기에서 수집된 정보들이 사용자의 신원을 파악하는 데 악용이 된다면 큰 위협 요소가 될 것이다.

서비스 제공자는 기기로부터 플랫폼으로 향하는 데이터 전송 과정에서의 유출을 방지하기 위해 엣지 컴퓨팅(Edge-computing)[27] 구조를 적용할 수 있다. 즉, 사용자의 정보를 서버로 전송하지 않고, 로컬 기기에서 신원 인증을 수행하여 인식 결과만 서버에 전송하는 방식으로 구현한다면 동적 개인정보의 유출을 방지할 수 있다.

4.2.3. 주변 환경 정보 유출

앞서 언급한 생체, 행위, 감정 정보들과 같이 사용자의 환경 정보 또한 보안성이 확보되어야 한다. 사용자의 기기 내 위치 정보 또는 카메라를 통해 확인되는 영상 정보를 통해 사용자의 프라이버시가 유출될 수 있으며, 사용자의 실제 위치는 공격자가 충분히 악용할 수 있는 요소가 된다.

이를 방지하기 위해 서비스 제공자는 생체 정보 유출과 유사하게 차분 프라이버시 등 비식별화 기술을 카메라에 도입하거나, 암호화를 통해 위치 정보를 숨길 수 있다[28].

4.2.4. 전송 데이터 탈취 공격

일반적으로 사용자는 다양한 기기를 서로 연결해서 공간감을 충족시켜 서비스를 이용한다. 이러한 경우, 기기 간 데이터 전송 및 공유가 활발하게 이루어지며, 만일 특정 기기 또는 공유 네트워크에 취약점이 존재하는 경우 공격자에 의해 전송 데이터가 탈취될 우려가 존재한다[24, 29].

서비스 제공자는 이를 방지하기 위해 먼저, 채널 암호화 기법을 적용할 수 있다. 이것은 네트워크에서 전송되는 데이터 및 패킷을 암호화하여, 공격자가 데이터를 탈취하더라도 내용을 쉽게 파악하지 못하게 하는 기술이며, 채널 암호화를 지원하는 가상 시설망 등을 적용하여 구현할 수 있다. 한편, 기기 간 상호 인증[30] 제도를 도입하는 방법이 있다. 두 기기의 검증된 안전성 및 보안성에 대해 고유 특성 기반 인증 토큰을 통해 검증한 후 견고한 환경에서 연결 및 전송 절차를 진행할 수 있는 인증 방법이다.

4.2.5. 기기 정보 탈취

공격자는 의도적으로 사용자 기기에 대한 정보를 획득하기 위해 침입할 수 있다. PC, 스마트폰, IoT 기기, HMD 기기 등의 모델 일련 번호, 플랫폼 및 펌웨어 버전, MAC(Media Access Control) 주소, 연결된 주변 기기 등 정보를 불법적으로 수집 및 외부 유출을 시도하며, 악성 애플리케이션 등의 경로로 접근할 수 있다.

기기 정보에 대한 악의적 접근을 방지하기 위해, 서비스 제공자는 신뢰 실행 환경(Trusted execution environment)[31]을 구축할 필요가 있다. 이것은 민감한 데이터 및 중요한 로직을 보호하기 위해 사용되며, 메인 프로세서 내 별도의 보안 영역으로부터 실행되는 안전한 환경이다.

4.2.6. 기기 가용성 위협

기기는 사용자가 필요로 하는 경우 언제든 사용할 수 있어야 한다. 하지만 DoS(Denial of Service) 등 공격으로 인해 사용자가 정상적인 기기 및 서비스 이용을 하지 못한다면 많은 손실이 생길 수 있다. 기기 업체는 외부 공격 대응, 보안 관리와 같은 기능을 제품에 구현하여 보안성을 개선할 필요가 있다[32]. 또한, 새로운 형태의 공격에 대응하기 위해 주기적인 기기 패치가 필요하며, 기기에 대한 시험, 평가 및 인증 절차를 철저히 할 수 있는 제도가 마련되어야 한다.

4.2.7. 기기 인증 공격 및 기기 착용 인증

이 밖에도, 블루투스 등 네트워크를 통한 서로 다른 기기의 페어링을 안전하고 편리하게 관리함으로써 기기 인증 공격을 대비하고, VR 기기 또는 스마트 글래스 등을 착용한 상태에서 쉽고 빠르면서 안전하게 신원 인증을 할 수 있도록 행위 기반 인증 기술을 개발 및 보완할 필요가 있다.

4.3. 가상 환경 - 아바타

4.3.1. 아바타 추적

공격자는 메타버스 환경 내에서 사용자 아바타의 습관 또는 이동 경로 등 행적을 모니터링하고, 직접 아바타를 추적하면서 스토킹 행위를 할 수 있다. 이것은 사용자에 대한 정보를 획득할 수 있을 뿐 아니라, 메타버스 내에서의 다양한 범죄로 이어질 수 있기 때문에 예방이 반드시 필요하다.

서비스 제공자는 이러한 범죄를 예방하기 위해 메타버스 공간 내에 사용자와 유사하게 생긴 가상 아바타 클론을 생성하여 공격자의 시선을 분산시키거나, 사용자에게 온오프 기능을 제공하여 아바타 위장, 아바타 투명화 등의 예방책을 제공할 수 있으며, 2022년

메타(Meta)에서 운영하는 소셜 메타버스 플랫폼 호라이즌 월드에서는 디지털 성범죄를 예방하기 위해 아바타 간 거리두기 기능을 도입한 사례가 있다. 이 밖에도, 아바타의 개인 공간을 제공하여, 다른 아바타가 접근하지 못하는 영역을 생성하는 대책도 고려할 수 있다.

4.3.2. ID 추적 및 연결 공격

만일 특정 메타버스 플랫폼에서 사용하는 아바타와 또 다른 메타버스 플랫폼에서 사용하는 아바타의 외모와 습관 등이 유사한 경우, 공격자는 하나의 플랫폼 내 아바타를 통해 다른 플랫폼의 아바타의 소유자를 유추할 수 있다. 또한, 아바타의 외모가 실제 소유자와 유사한 경우, 공격자는 해당 인물을 추측 및 추적할 수 있으며, 이러한 linkability 속성으로 인해 익명성이 보장된 메타버스 환경의 취약점으로 연결될 수 있다.

서비스 제공자는 linkability 문제를 보완하기 위해 아바타 위장 기능을 제공할 수 있으며, 사용자는 메타버스 플랫폼마다 다른 ID(아바타)를 생성함으로써 추적을 회피할 수 있다.

4.3.3. 아바타 도용 및 복제

메타버스 플랫폼 내에서 특정 서비스 및 애플리케이션에 접근하기 위해 아바타 얼굴 인증 기술을 적용할 수 있다. 이 때, 공격자는 특정 사용자의 아바타와 동일한 외모를 띄거나 해당 사용자로 인증될 수 있는 아바타를 생성 및 사용하는 인증 도용 위협을 시도할 수 있다. 메타버스 세계에서 아바타의 외모가 인증 수단으로 활용될 수 있는 만큼, 이에 대한 대책이 필요하다.

서비스 제공자는 이를 방어하기 위해 워터마킹과 같은 복제 아바타 탐지 기술을 사용자에게 제공할 수 있다. 워터마킹은 사용자가 아바타를 생성할 때 주입할 수 있으며, 아바타의 외형을 훼손하지 않는 동시에 본인의 소유권을 인증할 수 있는 고유한 패턴 및 객체를 의미한다. 다른 방법으로는 사용자가 아바타를 생성할 때, 얼굴 인식 기반 본인 인증 또는 중복 확인 기능을 도입할 수 있다. 이를 통해 공격자가 동일한 외모를 가진 아바타를 생성하는 데 제약을 줄 수 있다.

4.4. 가상 환경 – 데이터 및 컨텐츠

4.4.1. 소유권 탈취 및 저작권 침해

저작권은 창작자의 권리를 보호하고 해당 분야의 발전을 위해 존재하는 중요한 법적 요소이다. 이것은 물리적 매체뿐 아니라 디지털 컨텐츠 및 아이템에도 적용될 수 있으며, 메타버스 세계에서의 저작권 보호 역시 중요하게 고려되어야 한다. 공격자는 특정 컨텐츠에 대한 소유권을 탈취하거나 유사한 컨텐츠를 만들어 원작의 저작권을 침해할 수 있으며, 이를 보호할 수 있는 법적 제도와 기준이 반드시 마련되어야 한다.

서비스 제공자는 게임, 아이템, 음성, 영상 등 컨텐츠 소유자의 소유권 및 저작권을 인증하기 위해 디지털 워터마킹, 고유 링크 지문(Fingerprinting)[33], 또는 유사도 인증[34]과 같은 증명 수단을 사용자에게 제공할 수 있다.

4.4.2. 아바타 초상권 침해 및 유명인 얼굴 도용

초상권은 개인의 초상에 대한 독점 권리를 의미하며, 헌법상 인정되는 인격권의 하나이다. 이것 또한 저작권과 동일하게 사용자가 보유할 수 있는 중요한 권리이며, 메타버스 세계에서는 아바타의 초상권 역시 고려할 요소가 될 수 있다. 사용자가 직접 창작한 아바타의 얼굴, 몸체 등 외형은 하나의 저작물로써 판단할 수 있기 때문이다. 추가적으로, 실존 유명인의 외모 등을 모델로 하여 유사한 캐릭터를 생성하는 것은 해당 인물의 초상권을 침해하는 사례가 될 수 있기 때문에, 이를 방지하기 위한 디지털 초상권 침해 관련 제도가 강화될 필요가 있다. 또한, 서비스 제공자는 아바타 생성 시 본인 인증 및 중복 확인 기술 도입을 통해 다른 인물의 얼굴을 도용하는 행위를 방지할 필요가 있다.

4.4.3. 허위 컨텐츠

현재 많은 디지털 플랫폼, 특히, Facebook, Youtube 등 정보 교류가 잦은 플랫폼에서 수많은 허위 정보와 허위 컨텐츠가 생산되면서 많은 피해 사례가 보도되고 있다. 메타버스 세계 또한 이러한 허위 컨텐츠가 충분히 생산될 수 있는 환경이 조성되어 있으며, 사실과는 다른 허위 정보를 컨텐츠에 포함하여 사용자가 잘못된

상식을 갖도록 유도하거나 특정 인물에 대한 잘못된 부정적인 정보를 컨텐츠에 포함시켜 피해를 입힐 수 있다.

서비스 제공자는 허위 컨텐츠를 통제하기 위해 허니팟(Honeypot)[35,36], 필터링(Filtering) 및 탐지(Detection)[37]를 활용하여 공격자의 행동을 제한할 수 있다.

4.5. 가상 환경 – 상호 작용 (아바타 ↔ 아바타 및 아바타 ↔ 서비스)

4.5.1. 상호 작용 모니터링

서비스 제공자는 보안성이 요구되는 메타버스 환경에서의 사용자 간 커뮤니케이션 내용이나 특정 서비스를 이용 중인 사용자의 행동을 접근 권한이 없는 공격자가 무단으로 도청 또는 모니터링하는 위협 행위를 예방할 필요가 있다. 예를 들어, 가상 사무실 또는 회의실에서의 대화 내용과 메시지가 유출된다면 큰 문제가 발생할 수 있다. 이를 방지하기 위해, 플랫폼의 특정 공간에 접근하는 대상의 권한을 파악한 후 입장시키면서 해당 공간에 대한 기밀성, 무결성 및 가용성을 보장하는 접근 통제 기술을 적용할 수 있다[38]. 다른 방법으로는 플랫폼 내 일반적인 활동 영역과 떨어진 영역에 환경을 구성한 가상 보안 회의 환경과, 대화 내용 및 행동에 대한 일부 모자이크 기술을 적용할 수 있다.

4.5.2. 사기 및 신뢰 관리

일부 이기적인 사용자는 메타버스 시장에 기여하지 않고 부당한 방법으로 수익을 창출(Free-riding)하여 해당 세계의 경제 지속성을 훼손하는 행위를 할 수 있다. 예를 들어, 분산 AI 모델훈련 과정에서 의미 없는 로컬 업데이트를 제출하여 훈련된 모델의 이점을 부당하게 획득하거나, 여러 사용자들이 공모하여 메타버스 시장 또는 경매를 조작할 수 있다. 이것은 메타버스 세계의 경제적 공정성을 파괴하기 때문에 적절한 대응책이 반드시 필요하다.

서비스 제공자는 플랫폼과 사용자들에 대한 신뢰성을 높이기 위해 신뢰 가능한 거래 모델, 지능형 신뢰 및 평판 관리 기술, 또는 기여 인증 시스템을 구축할 수 있다. 즉, 사기 또는 Free-riding 행위를 하는 사용자에게 페널티 점수를 부여하고, 다른 사용자들에게 해당 점수를 공개함으로써 사기 등의 사고를 예방할 수 있다.

4.5.3. 시빌 공격

시빌 공격(Sybil attack)은 악의적 목적을 가진 한 명의 공격자가 마치 여러 명인 것처럼 행동을 하는 위협이다. 이것은 보통 네트워크 해킹을 위해 사용되는 공격이지만, 메타버스 환경에서는 다수의 가짜 아바타 생성을 통해 공격자의 목표 달성을 위해 행동할 수 있다. 추가로, 분산 학습 및 연합 학습 등 인공지능 모델의 훈련 과정에 개입하여 중독 공격(Poisoning attack) 등을 시도할 수 있기 때문에, 적절한 대비책이 요구된다.

서비스 제공자는 시빌 공격을 목적으로 생성된 가짜 아바타들을 탐지하기 위해 작업 증명(Proof of Work), 지분 증명(Proof of Stake)을 요구할 수 있다. 이것들은 각각 사용자에게 작업 중 상태 인증과 데이터 또는 자산의 소유량 인증을 요구한다. 또한, CAPTCHA 방법을 통해, 아바타가 실제 사용자가 제어하고 있는 지에 대한 확인을 수행할 수 있으며, 연합 AI 모델 학습 중 탐지 방법[39]을 통해 가짜 클라이언트를 찾아낼 수 있다.

4.5.4. 어뷰징

어뷰징은 현실 환경에서는 욕설, 남용, 학대 등, 한편 디지털 환경에서는 불법 프로그램, 버그, 핵, 계정 도용 등을 포괄하는 부당한 행위를 의미한다. 사용자들이 불편이나 피해를 보지 않고 쾌적한 환경에서 메타버스 서비스를 이용하기 위해서는 어뷰징에 대한 대책을 수립해야 한다.

서비스 제공자는 각 아바타에게 개인형 블랙박스를 제공하여 공격자의 행동을 기록하거나, 공격자의 블랙박스를 통해 어뷰징 행위를 증명할 수 있다. 또한, 포렌식 기반 증거물 수집 방법을 통해 공격자의 악의적 행동을 정밀하게 수사하는 기술을 도입할 필요가 있다. 반면, 사용자들은 특정 인물의 어뷰징 행위를 적극적으로 신고하여 그들의 행동을 통제할 필요가 있으며, 법적 금지 및 처벌 제도를 명확하게 수립하여 대응

해야 한다.

4.6. 디지털 트윈 환경 – 시뮬레이션

4.6.1. 가상 환경 악용

디지털 트윈 기술을 통해 구현된 가상 환경은 공장 관리, 도시 관리 등 긍정적인 서비스를 제공할 수 있지만, 동시에 악의적 공격자들은 해당 공간에서 테러 훈련, 기계 고장 유도 시뮬레이션 등 현실에 막대한 피해를 주기 위한 준비를 수행할 수 있다.

서비스 제공자의 관점에서는 이러한 행동을 방지하기 위해 행동 모니터링 또는 프로파일링 등을 통해 사용자의 악의적 행동을 탐지해야 하며, 공장, 회사 등의 가상 환경에서는 비인가 사용자에 대해 접근 통제를 할 필요가 있다.

4.6.2. Man in the Mirroring 공격

일반적으로, 가상 환경에서 특정 행위를 시뮬레이션하는 경우, 현실과 유사한 결과를 보여야 한다. 하지만, 특정 공격자가 가상 환경에 침입하여 의도적으로 잘못된 결과를 유도하고, 이러한 결과를 기반으로 현실에서 동일하게 수행했을 때, 큰 사고로 번질 위험이 있다. 이를 방지하기 위해, 서비스 제공자는 무결성을 보장하고, 상호 인증 시스템을 도입하여 공격자의 접근을 제한할 필요가 있다.

4.6.3. 현실 정보 노출

디지털 트윈 기술을 통해 생성된 가상 환경은 현실의 정보를 그대로 가져오기 때문에, 개인 정보 또는 중요한 기밀 정보들이 유출될 위험이 있다. 서비스 제공자는 사용자에게 민감 정보를 보호할 수 있는 필터링 기술을 제공할 필요가 있다.

Ⅴ. 결 론

본 논문은 메타버스 세계를 구축하는 데 고려해야 할 다양한 위협 요소와 그에 대한 대책을 메타버스 내 환경에 따라 분류하여 소개하였다. 기존 IT 환경에서 빈번히 발생하고, 동시에 많은 전문가들이 고려했던 위협 요소들을 포함하여, 기존 환경과 다른 새로운 패러다임을 가진 메타버스 환경에서 발생할 수 있는 새로운 보안 위협 요소들에 대해 나열하였다. 본 논문의 목표는 메타버스 서비스 제공자들이 각 환경에서 발생할 수 있는 보안 위협 요소들에 대한 대책을 충분히 마련하여 사용자들에게 안전하고 견고한 플랫폼을 제공하는 것이며, 사용자들이 메타버스 내에서 서비스 및 컨텐츠를 활용할 때 개인 정보 보호 및 위협 요소들에 대한 대응을 하는 방법을 제시하는 것이다.

참 고 문 헌

[1] Mystakidis S., “Metaverse,” Encyclopedi -a 2.1, pp. 486-497, Feb., 2022.

[2] John S., Jamais C., Jerry P., Corey B., Jochen H., James H., Randal M., “Metaverse Roadmap,” ASF, 2007.

[3] Chi H., Fu C., Zeng Q., Du X., “Delay Wreaks Havoc on Your Smart Home: Delay-based Automation Interference Attacks,” IEEE Symposium on Security and Privacy, pp. 1575-1575, 2022.

[4] 정수용, 서창호, 조진만, 진승헌, 김수형, “확장된 가상현실인 메타버스에서의 보안 위협 분석,” 정보보호학회지, 31(6), pp. 47-57, Dec., 2021.

[5] “2020 Augmented and Virtual Reality Survey Report:: Industry Insights Into the Future Of Immersive Technology,” Perkins Coie LLP, Mar., 2020.

[6] “디지털 뉴딜 2.0 초연결 신산업 육성 – 메타버스 신산업 선도전략,” 과학기술정보통신부, 2022.

[7] IEEE 2888 standards. Accessed: July. 27, 2022. [Online]. Available: https://sagroups.ieee.org/2888/

[8] “디지털 뉴딜 성공의 초석 – 가상융합경제 발전 전략,” 과학기술정보통신부, 2020.

[9] “실감콘텐츠 보안모델 – PART Ⅱ: 메타버스, 디지털 트윈,” 한국인터넷진흥원, 2021.

[10] “금융 메타버스(Metaverse), 사이버위협 동향과 대응방안 – 국내외 금융사 메타버스 사업현황, 사이버위협 분석, 대응방안,” 법무법인(유) 나우, 2022.

[11] 박효주, “유통업계, 메타버스 주도권 잡아라,” https://www.etnews.com/20220315000075, 전자신문,

2022.

[12] Kalamkar S., Biener V., Nouri N., Ofek E., Pahud M., Dudley J. J., Hu J., Kristensson P. O., Weerasinghe M., Copic P. K., Kljun M., Streuber S., Grubert J., “Quantifying the Effects of Working in VR for One Week,” arXiv preprint arXiv:2206.03189, 2022.

[13] Wang Y., Su Z., Zhang N., Liu D., Xing R., Luan T. H., Shen X., “A Survey on Metaverse: Fundamentals, Security, and Privacy,” arXiv preprint arXiv:2203.02662, 2022.

[14] Zhang Y., Egelman S., Cranor L., Hong J., “Phinding Phish: Evaluating Anti-Phishing Tools,” 2007.

[15] 김익수, 최종명, “피싱과 파밍 공격에 대응ㅎ하기 위한 인증 프로토콜 설계,” 디지털산업정보학회 논문지, 5(1), pp. 63-70, 2009.

[16] Damien B., “Identity 3.0? How to guard privacy in the metaverse,” cybernews, 2022.

[17] “Identity Theft vs Impersonation: How are they two different?” EUbusiness, 2021.

[18] Ometov A., Bezzateev S., Makitalo N., Andreev S., Mikkonen T., Koucheryavy Y., “Multi-Factor Authentication: A Survey,” Cryptography, 2(1), Jan., 2018.

[19] Jensen J., Jaatun M. G., “Federated Identity Management-We Built It; Why Won’t They Come?” IEEE Security & Privacy, 11(2), pp. 34-41, Oct., 2012.

[20] Samir E., Wu H., Azab M., Xin C., Zhang Q., “DT-SSIM: A Decentralized Trustworthy Self-Sovereign Identity Management Framework,” IEEE Internet of Things Journal, 9(11), pp. 7972-7988, Sep., 2021.

[21] Vossaert J., Lapon J., De Decker B., Naessens V., “User-Centric Identity Management using Trusted Modules,” Mathematical and Computer Modelling, 57(7-8), pp. 1592-1605, Apr., 2013.

[22] Odeleye B., Loukas G., Heartfield R., Spyridonis F., “Detecting Framerate-Oriented Cyber Attacks on User Experience in Virtual Reality,” VR4Sec, pp. 1-5, Aug., 2021.

[23] 김민상, “러시아 남성 VR 게임 플레이 중 넘어지면서 과다 출혈로 사망,” 중앙일보, 2017.

[24] Wei J., Li J., Lin Y., Zhang J., “LDP-based Social Content Protection for Trending Topic Recommendation,” IEEE Internet of Things Journal, 8(6), pp. 4353-4372, Sep., 2020.

[25] “개인정보 비식별 조치 가이드라인 - 비식별 조치 기준 및 지원·관리체계 안내,” 행정안전부, 2016.

[26] 홍윤기, 윤지원, “생체정보 다분할 분산저장 기법을 통한 보안성 향상의 생체인증 시스템 설계,” 융합보안논문지, 16(7), pp. 31-39, 2016.

[27] Liu H., Yao X., Yang T., Ning H., “Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-based Smart Health,” IEEE Internet of Things Journal, 6(2), pp. 1352-1362, June, 2018.

[28] Gupta S., Arora G., “Use of Homomorphic Encryption with GPS in Location Privacty,” 2019 4th International Conference on Information Systems and Computer Networks, pp. 42-45, March, 2019.

[29] Ometov A., Bezzateev S. V., Kannisto J., Harju J., Andreev S., Koucheryavy Y., “Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things,” IEEE Internet of Things Journal, 4(4), pp. 843-854, July, 2016.

[30] 김형욱, “사물인터넷 환경에서 이기종 기기간 상호 인증 프로토콜 설계,” 숭실대학교 박사 학위 논문, 2017.

[31] Pinto S., Gomes T., Pereira J., Cabral J., Tavares A., “IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices,” IEEE Internet Computing, 21(1), pp. 40-47, Feb., 2017.

[32] 한슬기, 김명주, “사물인터넷 기기 보안평가를 위한 기술요소 기반의 모델 설계 및 체크리스트 적용,” 융합보안논문지, 18(2), pp. 49-58, 2018.

[33] Fan Z., Yu H., “Arbitration of Digital Fingerprint-based Digital Resource Copyright,” Procedia Computer Science, 188, pp. 78-85, July, 2021.

[34] Chen J., Wang J., Peng T., Sun Y., Cheng P., Ji S., Ma X., Li B., Song D., “Copy, Right? A Testing Framework for Copyright Protection of Deep Learning Models,” arXiv preprint arXiv:2112.05588, 2021.

[35] Matta A., Sucharitha G., Greeshmanjali B., Kumar M. P., Kumar M. N. S., “Honeypot: A Trap for Attackers,” The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, pp. 91-101, Mar., 2022.

[36] Wu L., Morstatter F., Carley K. M., Liu H., “Misinformation in Social Media: Definition, Manipulation, and Detection,” ACM SIGKDD Explorations Newsletter, 21(2), pp. 80-90, Dec., 2019.

[37] Guo B., Ding Y., Yao L., Liang Y., Yu Z., “The Future of Misinformation Detection: New Perspectives and Trends,” arXiv preprint arXiv:1909.03654, 2019.

[38] Ma C., Yan Z., Chen C. W., “Scalable Access Control for Privacy-Aware Media Sharing,” IEEE Transactions on Multimedia, 21(1), pp. 173-183, June, 2018.

[39] Fung C., Yoon C. J., Beschastnikh I., “Mitigating Sybils in Federated Learning Poisoning,” arXiv preprint arXiv:1808.04866, 2018.

〈저자소개〉

나 현 식 (Hyunsik Na)

정회원

2021년 2월 : 공주대학교 응용수학과 학사

2021년 2월~현재 : 숭실대학교 소프트웨어학과 석박사통합과정

<관심분야> 인공지능 보안, 엣지 컴퓨팅, 메타버스 보안, 인증

최 대 선 (Daeseon Choi)

종신회원

1995년 2월 : 동국대학교 컴퓨터공학과 학사

1997년 2월 : 포항공과대학교 컴퓨터공학과 석사

2009년 1월 : 한국과학기술원 전산학과 박사

1997년 1월~1999년 6월 : 현대정보기술 선임

1999년 7월~2015년 8월 : 한국전자통신연구원 인증기술연구실 실장/책임연구원

2015년 9월~2020년 8월 : 공주대학교 의료정보학과 부교수

2020년 9월~현재 : 숭실대학교 소프트웨어학부 교수

2016년~현재 : 정보보호학회 이사

<관심분야> 인증, 개인정보보호, 이상거래탐지, 의료정보보안, 머신러닝