정 보 보 호 학 회 지
제 31 권 제6호, 2021. 12

확장된 가상현실인 메타버스에서의 보안 위협 분석

정 수 용*, 서 창 호**, 조 진 만***, 진 승 헌***, 김 수 형****

요 약

사용자들의 간접 경험 및 다양한 커뮤니티 생성을 위해 사용되었던 기존의 2차원 온라인 세상은 시각적 표현 및 사람의 특징을 반영하는 것에 한계점이 뚜렷하다. 따라서, 보다 현실과 유사한 환경을 구축하기 위해 많은 연구가 수행되었으며 특히, 사람의 행동 및 상태 등을 수집하고 활용할 수 있는 기술이 발전하였다. 그 결과 현실과 유사한 3차원 세계인 메타버스가 새롭게 주목받고 있다. 메타버스는 새로운 신분인 아바타로 사용자들의 높은 자유도를 보장하며 현실 세계와 유사한 활동과 함께 현실에서 경험할 수 없는 서비스를 제공하고 있다. 이러한 메타버스의 발전을 위한 연구가 활발히 수행되고 있지만, 메타버스에서 발생할 수 있는 보안 위협에 관한 연구는 상대적으로 부족하다. 현재, 3차원 세계 구축을 위해 기존보다 많은 종류의 데이터 수집으로 새로운 보안 이슈가 꾸준히 발생하고 있으며, AR, VR 등의 다양한 디바이스 활용과 사용자들의 자유도 보장에 따른 보안 위협이 존재한다. 이에, 본 논문에서는 메타버스에서 발생할 수 있는 보안 위협에 대해 분석하고, 이전의 다양한 연구들을 정리하여 새로운 관점에서 보안 위협을 분류한다. 그리고 해당 위협의 대응방안과 함께 앞으로의 연구 방향을 제시한다.

Ⅰ. 서 론

코로나 19 팬데믹으로 인하여 지난 2년 동안 세계 사회는 언택트 시대로 빠르게 변화하였다. 다시 말해, 일과 생활 모두 사람과 사람이 만나지 않는 환경에서 이루어지고 있으며, 더 나아가 온라인 사이버 공간에서 다양한 생활과 업무를 진행하는 온택트 시대로 변화하고 있다[1]. 이러한 흐름에 발맞춰 사이버 공간에서의 다양한 활동 및 경험을 제공할 수 있는 기술이 발전하고 있다. 그 과정에서, 다양한 시각적 표현과 활동을 제공하기 어려운 2차원 사이버 공간의 한계점을 주목하였으며, 이를 극복하기 위해 3차원 공간에 대한 연구를 더욱 활발히 진행하였다[2-6]. 그 결과, 기존 2차원 세계에서의 서비스와 3차원 세계에서의 서비스를 모두 포함하는 메타버스에 대한 관심이 증가하였다.

가상, 초월을 의미하는 메타(meta)와 세계, 우주를 의미하는 유니버스(universe)의 합성어인 메타버스(Metaverse)는 1992년 처음 언급되었다[7]. 당시에는 시각적, 청각적 출력 장치를 이용한 가상세계로 규정되었으며, 현재는 바라보는 시각에 따라 다양한 정의를 내리고 있지만 2차원 및 3차원을 포함한 현실과 유사한 가상세계라고 정리할 수 있다. 이러한 메타버스는 사회적, 경제적 활동이 모두 가능하며 온라인 게임 및 소셜 네트워크 서비스부터 AR, VR 등의 3차원 가상 공간에서 다양한 활동을 지원하는 서비스까지 포함하고 있다. 이러한 메타버스는 사용자들을 대신할 수 있는 아바타 시스템을 통해 높은 자유도를 보장하는 특징이 있다.

현실과 유사한 활동 및 경험을 제공하기 위해 메타버스는 많은 이들이 함께 공존할 수 있는 새로운 가상 공간을 생성하거나 현실의 상태 및 움직임을 가상세계에 반영하기 위한 다양한 연구들이 진행되고 있다. 특히, 현실과 동일한 환경을 구축하여 다양한 실험을 수행하고 현실에서 경험할 수 없는 새로운 활동이 가능한 서비스를 제공하기 위한 기술 연구가 수행되고 있다. 이처럼 메타버스의 순기능을 확장하기 위한 연구들

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00321, 5G 서비스 환경에서 프라이버시가 보장되는 자기통제형 분산 디지털 신원 관리 및 보안 기술 개발)
* 공주대학교 융합과학과 (대학원생, jsy8630@smail.kongju.ac.kr)
** 공주대학교 융합과학과 (교수, chseo@kongju.ac.kr)
*** 한국전자통신연구원 (책임연구원, zmzo@etri.re.kr, jinsh@etri.re.kr)
**** 한국전자통신연구원 (책임연구원/기술총괄, lifewsky@etri.re.kr)

이 많이 수행되고 있으며, 이와 관련된 국내 연구도 지속해서 수행되고 있다. 하지만, 메타버스에서 발생할 수 있는 보안 위협에 관한 국내 연구는 상대적으로 부족하다.

메타버스는 현실과 유사한 환경을 구축하기 위해 다양한 생체데이터를 활용하며, 다양한 입·출력 장치를 활용한다. 이처럼 양질의 서비스 제공을 위해 사용되는 것들이 새로운 보안 취약점으로 활용될 수 있다. 또한, 높은 자유도를 보장하여 다양한 경험을 제공하지만 반대로 개개인의 자유도가 높아짐에 따라 서로 프라이버시 침해를 포함한 보안 이슈들이 발생하고 있다[8,9]. 이에, 본 논문에서는 메타버스에서 발생할 수 있는 보안 위협을 크게 3가지로 분류한다. 메타버스만의 새로운 기준을 세우고, 각각의 분류에 대한 타당성과 함께 실제 발생한 보안 이슈 및 예상되는 공격 시나리오를 서술한다. 또한, 이러한 위협에 대응하는 기술들을 정리하고, 현재의 메타버스 보안 상황과 앞으로의 연구 방향을 제시한다.

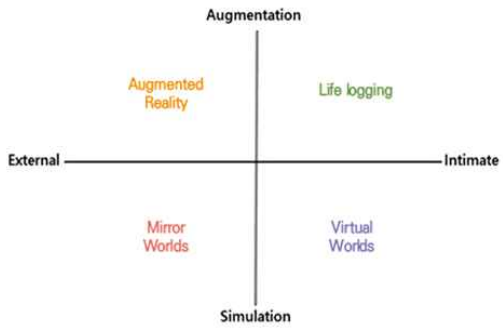
본 논문의 2장에서는 메타버스의 배경과 정의를 서술하고, 대표적인 메타버스 서비스를 몇 가지 제시한다. 3장에서는 메타버스의 보안을 3가지로 분류한 기준, 보안 위협 및 관련 연구와 향후 연구 방향을 제시한다. 그리고 4장에서 결론을 짓는다.

Ⅱ. 메타버스

이번 장에서는 본 연구의 배경인 메타버스를 구체적으로 설명하기 위해 메타버스의 정의와 대표적인 메타버스 서비스를 제시한다. 또한, 국내·외 정책 동향을 통해 메타버스의 현재와 미래를 살펴본다.

2.1. 메타버스의 정의

메타버스는 1992년 닐 스티븐슨(Neal Stephenson)의 소설 ‘스노우 크래쉬(Snow Crash)’[7]에서 가장 처음 등장한 개념으로 ‘가상, 초월’을 의미하는 ‘메타(meta)’와 ‘세계, 우주’를 의미하는 ‘유니버스(universe)’의 합성어이다. 따라서 가상세계, 가상 우주로 해석할 수 있으며, 처음 등장한 소설 속에서는 고글과 이어폰 등의 시청각 출력 장치를 통해 접근하는 가상세계로 묘사하고 있다. 이를 기반으로 메타버스에 대한 다양한 정의를 내리고 있지만, 2차원 및 3차원을 포함하는 현실과 가장 유사한 가상세계라고 정리할 수 있다. 2007년 미국의 기술 연구 단체 ASF(Acceleration Studies Foundation)는 ‘메타버스 로드맵[10]’을 발표하면서 그림 1과 같이 메타버스의 4가지 요소를 언급하였다.



〔그림 1〕 ASF의 메타버스 4대 요소〔10〕

- 증강현실(Augmented Reality)
- 일상기록(LifeLogging)
- 거울세계(Mirror Worlds)
- 가상세계(Virtual Worlds)

첫 번째로, 증강현실은 현실 공간에 2차원 또는 3차원으로 가상의 물체를 겹쳐서 표현하는 환경을 의미한다. 두 번째로, 일상기록은 사람 및 사물에 대한 일상적인 경험 및 정보를 저장하고 묘사하는 기술로, 다양한 SNS 서비스와 함께 스마트 워치와 같이 신체 정보 및 활동 정보를 공유하는 운동 커뮤니티 등을 포함하고 있다. 다음으로 거울 세계는 현실 세계를 최대한 유사하게 표현하되 정보 측면으로 확장된 가상세계를 의미하며, 거울 세계를 통해 현실 세계에 대한 정보를 얻을 수 있다. 마지막으로 가상세계는 현실과 유사하거나 완전히 다른 새로운 세계를 디지털 데이터로 구축한 것으로 사용자들은 아바타라는 새로운 신분으로 현실 세계와 유사한 경제적, 사회적 활동을 보장받는다. 컴퓨터 그래픽환경에서 구현되는 3차원 커뮤니티를 총칭하는 개념으로, 일반적인 온라인 게임을 포함하는 개념이다.

위의 4가지 요소를 통해, 메타버스는 이전에 사용되었던 다양한 온라인 게임 및 SNS 등을 기반으로 VR, AR 등의 새로운 서비스까지 포함하는 것을 알 수 있다.

2.2. 메타버스 서비스

이번 절에서는 위에서 언급한 메타버스의 4요소에 대해 명확하게 살펴보기 위해 각 요소에 해당하는 대표적인 서비스를 제시한다.

2.2.1. 증강현실 : 포켓몬고(PokemonGo)

2016년 미국 나이언틱(Niantic, Inc)에 의해 개발된 포켓몬고는 4대 요소 중 증강현실(Augmented reality, AR)의 대표 사례이다. 스마트폰의 카메라를 통해 현실 세계를 보여주는 화면 속에서 3D로 구현된 포켓몬 캐릭터를 잡거나 교환하는 방식의 게임이다. 2020년 11월 기준 누적 매출액 약 42억 달러로 많은 관심을 받고 있다.

2.2.2. 일상기록 : 페이스북(Facebook)

현재는 메타 플랫폼(Meta Platforms, Inc.)으로 변경된 페이스북(Facebook, Inc)에서 2004년 개발한 서비스로 일상기록의 대표 사례이다. 회사의 명칭을 바꾼 만큼, 기존의 소셜 미디어에서 메타버스로 발전하고 있으며, 추후 VR(Virtual reality)을 포함하는 서비스로의 확장이 예상한다.

2.2.3. 거울세계 : 구글어스(Google Earth)

2005년 구글에서 제공하는 서비스로 전 세계에 대한 다양한 지역 정보를 제공한다. 위성 이미지로 시작된 서비스는 건물 사진과 주변 환경을 확인할 수 있는 스트리트 뷰(Street view)를 제공하고 있으며, 3D 보기 및 VR 서비스까지 제공하고 있다. 거울 세계의 대표적인 예시로 현재도 많은 사용자를 보유하고 있으며, 국내에서는 제한적인 사용만 가능하다.

2.2.4. 가상세계 : 로블록스(Roblox)

2006년 처음 출시한 로블록스는 온라인 게임 플랫폼으로 사용자들이 직접 게임을 설계하고 개발하며, 개발된 게임을 공유하여 함께 즐길 수 있는 서비스이다. 사용자의 50% 이상이 13세 미만으로 확인되며, 실제 미국 초등학생의 3분의 2가 로블록스 사용자라고 한다. 가상세계에 해당하는 서비스로 아바타를 통해 사용자들에게 높은 자유도와 함께 가상화폐를 사용한 경제 활동을 보장한다.

2.3. 국내·외 정책 동향

메타버스의 4요소 중 일상기록, 거울 세계 그리고 가상세계는 이미 기존의 온라인 세상에서 제공되었기 때문에 증강현실이 메타버스에서 중요한 요소로 작용한다고 판단된다. 이는 메타버스 관련 시장 규모에서도 확인할 수 있다. 시장조사업체 스트래티지 애널리틱스(SA)는 2025년 전 세계 메타버스 시장 규모를 약 2800억 달러에 이를 것으로 예측하며, 스태티스타는 2024년 전 세계 메타버스 시장 규모를 약 2969억 달러로 예측한다[11]. 동시에, 내셔널 데이터 코퍼레이션(International Data Corporation, IDC)은 2024년의 XR 시장 규모를 약 1368억 달러로 예상하며, 메타버스 시장 규모의 약 40% 이상을 차지하는 것으로 확인할 수 있다[12]. 다시 말해, 증강현실의 핵심 기술인 XR(VR과 AR을 포함)은 이미 메타버스에서 많은 비중을 차지하고 있으며, 증강현실을 제외한 다른 3요소에도 큰 영향을 주고 있음을 알 수 있다.

이러한 메타버스의 핵심 기술 중 하나인 XR에 대해 국내·외에서는 다양한 정책을 펼치고 있다[13-17].

먼저, 미국은 일찍부터 XR 기술 관련 연구를 진행했으며, 국토안보부는 응급상황에 대한 대응 훈련인 가상훈련플랫폼 EDGE(Enhanced Dynamic Geo-Social Environment)를 사용하고 있다. 또한, '국가교육기술계획 2017(The National Education Technology Plan 2017)'에 해당 기술 활용 방안을 포함하고 있고, 다양한 군사 훈련에 XR을 활용하고 있다[14]. 다시 말해, 미국은 이미 서비스 측면에서의 메타버스가 아닌, 국가 전반적인 분야에서 메타버스를 구축하고 있음을 알 수 있다.

다음으로 유럽에서는 EU 차원의 XR 기술개발을 진행하고 있으며, 특히 영국은 4대 디지털 핵심 기술로 XR을 선정하였다. 현재는 게임 및 미디어 산업뿐만 아니라 전시, 공연 산업부터 미디어, 패션 디자인 등의 분야까지 넓게 확장하고 있다[15].

중국과 일본도 XR 기술개발에 집중하고 있다[16,17]. 중국은 2018년 기준으로 동부지역에 15개의 XR 산업단지를 조성하고 있으며, 교육 혁신 및 경제

발전과 함께 빅데이터 관련 기술발전 전략에 XR 내용을 반영하고 있다. 일본은 초스마트 사회 구축을 위한 'Society 5.0' 전략에서 AI, IoT 등과 함께 XR을 핵심 기술로 포함하고 있으며, 다양한 부처에서 해당 기술의 중요성을 강조하고 있다. 또한, 2020년 4월에는 일본 국토의 디지털 트윈(Digital Twin)을 목표로 하는 '국토 교통 데이터 플랫폼 1.0'을 공개하면서 거울 세계 구축을 위한 개발을 진행하고 있다.

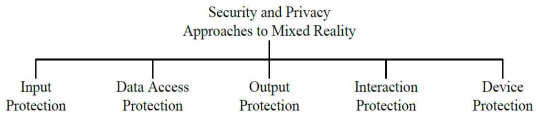
국내에서는 2016년에 발표한 '9대 국가전략'에서 VR 기술 관련 정책지원을 본격화하였으며, 2020년 7월에 발표한 '디지털 뉴딜(Digital New Deal)' 정책에서도 XR 활용 관련 계획을 포함하였다. 그리고 2020년 12월에 XR 기반 '가상융합경제 발전 전략'을 발표하며 국내 기술개발의 현주소를 파악하고 미래의 연구 방향을 제시하였다. 이에 따르면, 국내의 XR 활용은 아직 초기 단계며 문화체험에 집중하고 있는 한계점이 존재한다. 또한, XR 관련 디바이스의 확산과 함께 제도의 정비가 필요하며 국외와 비교할 경우 아직은 경쟁력이 미흡하다[15].

Ⅲ. 메타버스의 보안 위협

현재 메타버스에 대한 연구는 세계적으로 활발히 진행되고 있음을 확인할 수 있다. 이와 함께, 국내에서 다양한 메타버스 관련 연구가 수행되고 있으며 최근 다양한 연구결과들이 발표되고 있다[18-21]. 하지만, 국내의 연구는 2장에서 언급한 것처럼 문화체험에 집중되고 있으며, 플랫폼 및 관련 기술에 관한 연구가 주를 이루고 있다. 이에 본 장에서는 메타버스 관련 보안 위협을 새롭게 정리한다. 먼저, 3.1절에서는 메타버스 관련 기존 연구결과를 소개하며, 3.2절에서 새로운 기준과 함께 관련 보안 위협을 서술하고, 3.3절에서 관련 연구 정리 및 향후 연구 방향을 제시한다.

3.1. 기존 연구 결과

최근 Usenix에서 개최한 SOUPS(The Seventeenth Symposium on Usable Privacy and Security) 2021에서는 'VR4Sec: Security for XR and XR for Security' 워크숍이 열리면서 XR 관련 보안 연구들이 다수 발표되었다[22-25]. 특히, [25]은 해당 워크숍에서 지난 10년간 발표되었던 AR 보안 관련 연구결과들을 정리하였다. 해당 학회에서는 발생할 수 있는 입력값에 대한 프라이버시 이슈와 출력값의 보안, 그리고 다중 사용자와 다중 애플리케이션에서 발생할 수 있는 위협들에 관한 연구가 수행되었다. 또한, 법률 및 정책 관련 연구들을 포함하여 다방면에서의 연구가 수행되었다.



〔그림 2〕 MR 보안의 5가지 분류〔28〕

그리고 [26]에서는 아바타의 사용으로 인하여 발생할 수 있는 메타버스 보안 이슈들을 정리하였으며, 이에 대한 대응방안을 서술하였다. 특히, 아바타를 통해 발생할 수 있는 사용자의 프라이버시 침해에 대한 가능성을 주목하였으며, 다중 사용자로 인해 멈추지 않고 지속적으로 진행되는 메타버스의 특성에 집중하였다. 이에, 해당 문서에서는 사용자의 행동 패턴을 파악하여 유사한 행동을 수행할 수 있는 복제 아바타와 물리적으로 보이지 않은 아바타, 순간이동이 가능한 아바타 등의 해결 방안을 제시하면서 사용자의 프라이버시 보호에 대한 중요성을 한 번 더 강조하였다.

마지막으로, [27]에서는 기존의 MR 보안 관련 연구들을 정리하였다. 해당 논문에서는 MR에서의 다양한 보안 위협을 데이터의 흐름에 따라 그림 2와 같이 총 5가지로 분류하였으며, 관련 위협의 대응방안 연구와 함께 아직 해결되지 않은 문제에 대하여 정리하였다. 하지만 해당 논문에서 제시한 5가지 분류는 데이터의 흐름을 기준으로 정리하였기 때문에, 기존에 존재하는 데이터 보안 이슈를 많이 포함하고 있으며 과도하게 세분되어 있다.

3.2. 메타버스의 3가지 보안 위협

2장에서 언급한 바와 같이, 메타버스에 XR 기술은 핵심 기술로 적용되고 있다. 이에, 본 논문에서는 이전의 XR 관련 다양한 연구들을 기반으로 실제 발생하거나 발생 가능성이 높은 위협을 기준으로 메타버스 관련 보안 위협을 3가지로 새롭게 분류한다. 데이터 측면에서도 확인할 수 있는 입력값 및 출력값 보안과 다중 사용자 및 다중 애플리케이션의 활용으로 발생할 수 있는 상호 작용 보안, 그리고 물리적인 사용자의 행동 및 환경을 파악하는 디바이스 보안이 있다. 3가지 보안

에 대해 각 절에서 실제 발생한 침해 사례 및 관련 연구들을 서술한다. 그리고 관련 연구들의 정리와 함께 향후 연구 방향을 제시한다.

3.2.1. 입력값 및 출력값 보안(Input&Output Protection)

높은 자유도가 다양한 경험 제공이 중요한 메타버스에서는 PC뿐만 아니라 Xbox, Nintendo 등과 같은 콘솔(Console)과 함께 스마트폰에서도 동일한 서비스를 제공하고 있다. 또한, 이전의 키보드 및 마우스와 같은 1차원적인 입력장치만 사용하지 않고, 헤드 마운티드 디스플레이(Head-mounted display, HMD), 카메라 등의 다양한 입·출력 장치를 지원한다.

이러한 다양한 디바이스 중에서 가장 대중적으로 사용되는 카메라를 통해 사용자들이 원하지 않는 많은 정보가 유출된다. 대표적인 예로, 세계적으로 많이 사용되는 Zoom은 사용자들의 배경을 통해 많은 정보가 유출되고 있으며, 이를 방지하기 위해 다양한 수단을 적용하였다. 또한, 2장에서 언급한 포켓몬고는 전 세계적으로 많은 사용자를 보유하고 있으며, 각각의 사용자들은 증강현실을 즐기기 위해 무분별하게 카메라를 사용하고 있다. 사용자들은 실외에서도 스마트폰만 있으면 자유롭게 증강현실을 즐길 수 있지만, 사용자를 제외한 행인 및 주변 사람들은 동의 없이 카메라를 통해 데이터로써 수집되고 있다[9].

또한, 이전에 언급한 사진 및 동영상은 사람이 직접 식별 가능하므로 프라이버시 침해 사례를 쉽게 확인할 수 있다. 하지만 메타버스는 HMD와 스마트 디바이스를 통해 사용자들이 식별하기 어려운 눈동자의 움직임, 맥박, 뇌파 등을 데이터를 수집하여 활용하고 있다. 이처럼 메타버스의 사용자와 그 주변 사람들은 인지하지 못하는 상황에서 많은 프라이버시 침해가 발생하고 있다[28].

다시 말해, 메타버스 서비스를 위해 입력되는 다양한 데이터와 새로운 입력값으로 사용될 수 있는 출력되는 데이터에 대한 보안은 사용자들이 인식하지 못하는 경우가 많아 쉽게 지나칠 수 있다. 따라서, 입력값 및 출력값에 대한 보안은 매우 중요하다.

이러한 입·출력값 데이터 보호를 위해 다양한 기술들이 제안되었다. 먼저, DARKLY 시스템[29]은 입력되는 데이터에 대해 다양한 특징점에 대한 가공처리를 제공한다. 예를 들어, 사용자의 얼굴이 카메라로 인식된다면 해당 얼굴의 각 부분에 대해 사용자가 원하는 만큼 데이터를 숨길 수 있다. 유사하게 [30]은 그림이 아닌 문자로 나타날 수 있는 데이터에 대한 보안에 집중하였다. 민감한 정보가 포함된 글씨 및 그림 등에 대한 가공처리를 가능하게 하며, 이를 통해 의도하지 않은 정보가 노출되는 것을 방지한다. 그리고 [31]는 이미지 데이터에 대해 민감 여부를 판단하여 개인정보 침해를 막는다. 최근에는, 2차원 데이터가 아닌 3차원 데이터에 관한 기술들도 제안되고 있다. 먼저, [32]에서는 스마트폰 카메라로 수집되는 데이터에 대해 중간 계층을 추가함으로써 입력데이터를 보호하는 기술을 제안하였으며, [33]에서는 Microsoft Hololens를 통해 3차원 데이터가 입력될 때 발생할 수 있는 개인정보 침해를 막기 위해 새로운 인식 방법을 제시하여 노출되는 데이터를 감소시켰다. 또한, [34]에서는 3차원 데이터를 새롭게 재구성하여 전달함으로써 개인 프라이버시를 보호하고 있다.

3.2.2. 상호 작용 보안(Interaction Protection)

메타버스에서 단일 사용자를 위한 환경을 구축하는 것이 아닌 다중 사용자가 동일한 공간을 공유하여 다양한 경험을 제공하는 것은 주요 목적 중 하나이다. 또한, 다양한 애플리케이션과 서비스를 연동하여 하나의 세계로 통합하는 장점이 있으며, 관련 기술개발이 진행되고 있다. 이전의 온라인 세상에서도 다양한 사용자 및 애플리케이션의 연동은 존재했지만, 메타버스에서는 다양한 디바이스 및 플랫폼의 활용과 함께 3차원 세계의 구현으로 인하여 새로운 데이터를 다루고 있기 때문에 이에 알맞은 기술개발이 필요하다. 동시에, 이전과 다른 새로운 프라이버시 침해 및 보안 이슈가 발생할 수 있다.

실제로 2017년에 미국의 메신저 서비스인 스냅챗(Snapchat)은 아티스트와 협업하여 증강현실에 예술작품을 전시하였다. 메타버스의 특성 중 하나인 높은 자유로도 인하여 해당 작품은 스냅챗 애플리케이션을 사용하면 누구나 확인할 수 있지만, 반대로 작품을 훼손하는 것도 가능했다. 해당 작품이 전시되는 위치 데이터를 사용하여 악의적인 사용자들은 낙서를 통해 작품을 훼손하였다. 이때, 해킹이 발생한 것이 아닌 동일한 위치 정보에 다른 데이터를 입힌 것으로 밝혀졌다[8]. 다시 말하면, 다중 사용자들에게 허용되는 공유공

간에서의 보안 위협이 발생한 것이다.

메타버스 사용자들의 상호작용은 일반적으로 공유된 공간에서 발생한다. 따라서 해당 공유공간의 설계 방법과 이때 필요한 프로토콜이 매우 중요하다. 또한, 스냅챗의 사례로 알 수 있듯이 높은 자유도로 인한 무분별한 접근은 분명 문제가 될 수 있으며, 적절한 접근 통제가 필요하다. 이러한 문제 해결을 위한 다양한 연구들이 수행되고 있다.

먼저, [35]에서는 공동 MR 환경에서 발생할 수 있는 개인정보 유출을 방지하기 위해 개인정보 관리 및 다른 사용자의 접근통제를 수행하는 메커니즘을 새롭게 제안하였으며, [36]에서는 사용되는 다양한 장치간의 데이터 공유를 위한 인증 프로토콜을 제안하였다. 해당 프로토콜은 거리 정보 및 얼굴 인증정보를 조합하여 사용자들을 교차인증 하는 방식으로 사용자들이 AR HMD를 사용하여 서로 바라보면 인증이 수행되고 데이터 공유가 진행된다. 또한, [37]에서는 다양한 HMD 중 Microsoft Hololens를 사용하여 이전 연구와 유사하게 물리적으로 동일한 공간에서의 사용자 간 페어링을 위한 공유공간을 설계하는 방법을 제안하였으며, 관련 보안 요구사항에 관해 연구를 수행하였다. 그리고 [38]에서는 AR 장치 간 페어링, 즉 다중 사용자를 수용할 수 있는 환경 구축 기술을 제안하였으며 공격 시나리오에 대하여 안전한 상호작용이 가능함을 보였다. 이전의 연구들은 사용자들 간의 연동을 위한 연구를 수행했지만, [39]에서는 사용자들과 로봇과의 협업을 고려하여 발생할 수 있는 보안 위협 및 문제점에 대해 분석하였다.

3.2.3. 디바이스 보안(Device Protection)

메타버스는 사용자들이 아바타를 활용하여 진행하기 때문에 아바타의 접근 여부를 판단하는 사용자 인증이 매우 중요하다. 현재 암호는 가장 대중적인 인증 수단으로 사용되고 있지만, 보다 보안을 강화하기 위하여 두 개 이상의 독립적인 방법을 사용하는 다중요소 인증(Multi-factor authentication)이 사용되고 있다 [40]. 다양한 디바이스를 활용하는 메타버스는 서비스에 접근하는 인증 수단에 디바이스를 포함하는 기술개발이 필요하다. 또한, 디바이스를 기반으로 서비스에 접근하기 때문에 디바이스의 접근 통제를 위한 인증 기술도 함께 개발되어야 한다. 스마트폰의 예시를 살펴보면, 현재 우리는 비밀번호, 생체 정보 등을 통해 스마트폰(디바이스)의 잠금을 해제하고 내부의 애플리케이션에 접근하기 위해 새로운 인증을 진행하고 있다.

스마트폰의 생체 정보 및 비밀번호와 유사하게 가상환경에서 수행할 수 있는 기기접근 통제 및 서비스 접근 인증 기술에 관한 연구들이 수행되고 있으며, 특히 [41]에서는 이러한 인증 기술에 대한 활용 가능성에 관해 연구하였다. 기존의 PC 환경 및 온라인 시스템에서 수행되었던 다양한 인증 기술과 함께 가상 인터페이스에서 수행되는 핀(PIN) 및 패턴 인식 인증 방법을 비교하고 분석하였으며, 실행 시간 측면에서는 유사한 결과를 보였다. 다시 말해, 시선 추적(Eye tracking) 및 동작(Gesture) 등을 활용한 가상 인터페이스 환경의 인증 방법으로 기존의 인증 방법을 대체할 수 있다.

먼저, 동작 인식 방법을 활용한 기술들이 제안되었다. 기존의 마우스와 유사하게 손가락 움직임을 통해 인증을 진행하는 기술[42]이 개발되었으며, 기기를 통해 머리의 움직임을 함께 사용하는 기술이 제안되었다 [43]. 또한, 음악과 같은 소리를 통해 머리의 움직임을 발생시켜 인증을 진행하고[44], 호흡 등과 같은 신체적 움직임을 활용하여 인증이 가능하다[45]. 이와 다르게, 기존의 지문 및 얼굴 인식과 유사하게 생체 정보를 활용하여 인증이 가능하다. [46]은 광전용적맥파 측정기(Photoplethysmography, PPG)를 활용하여 사용자의 맥파형을 수집 및 활용하는 생체 정보 기반 키 교환(Physiological-signal-based key agreement, PSKA) 기술을 개발하였으며, 이는 기존에 혈관 측정이 불가능한 기기에 해당 디바이스를 함께 연동하여 사용할 수 있다. 또한, Google glass를 활용하는 SkullConduct[47]는 골전도 기능을 활용하여 사용자의 인증을 수행한다. 마지막으로, 다중요소 인증에 관한 연구들도 진행되었다. [48]은 사용자의 얼굴 정보(특히, 눈과 홍채 정보)를 통합적으로 활용하는 인증 기술을 제안하였으며, [49]에서는 사용자의 시선 추적과 함께 터치 키를 동시에 활용하는 기술을 개발하였다.

3.3 향후 연구 방향

메타버스 환경에서의 다양한 보안 위협에 관한 연구들은 지속적으로 수행되고 있으며, 본 논문에서 제안한 3가지 분류를 통해 표 1과 같이 각각의 연구를 정리할 수 있다. 비록 다양한 연구가 수행되고 있지만, 다양한

〔표 1〕 관련 연구 정리

분류	관련 연구	연구 내용
입력값 및 출력값 보안	Suman 2013〔29〕	입력되는 그림 데이터에 대한 가공처리
	Eisa 2016〔30〕	문자 데이터에 대한 프라이버시 보호 기술
	Robert 2014〔31〕	이미지 데이터에서의 민감 여부 판단 및 처리
	Guzman 2019〔32〕	스마트폰 카메라의 3차원 데이터 수집에 대한 데이터 보호
	Guzman 2020〔33〕	Microsoft Hololens를 활용한 새로운 인식 기술
	Arpit 2021〔34〕	수집된 3차원 데이터의 재구성으로 프라이버시 보호
상호 작용 보안	Derek 2014〔35〕	공동 MR 환경에서의 개인정보 관리 및 접근통제 메커니즘
	Ethan 2016〔36〕	MR 디바이스간 데이터 공유를 위한 인증 프로토콜
	Kiron 2018〔37〕	Microsoft Hololens를 활용한 사용자 간 페어링 및 공유공간 설계
	Sluganovic 2020〔38〕	다중 사용자 간 공유공간 설계 및 공격 시나리오 대응
	Vasylevska 2021〔39〕	로봇과의 페어링에서 발생 가능한 보안 위협 및 문제점 분석
디바이스 보안	Aslan 2014〔42〕	손가락 동작 인식을 통한 인증 기술
	Cynthia 2015〔43〕	HMD를 활용한 머리 움직임 인식을 통한 인증 기술
	Li 2016〔44〕	소리를 발생시켜 반응하는 머리의 움직임 인식을 통한 인증 기술
	Chauhan 2017〔45〕	호흡 등과 같은 신체적 움직임 인식을 통한 인증 기술
	Krsihna 2009〔46〕	맥박 파형을 통한 키 교환 기술
	Schneegass 2016〔47〕	Google Glass를 활용한 골전도 인식을 통한 인증 기술
	Kiran2015 〔48〕	다중요소 인증을 위해 얼굴 정보를 활용하는 기술
	Khamis 2016〔49〕	다중요소 인증을 위해 시선 추적 및 터치 키를 함께 사용하는 기술

서비스와 함께 다양한 디바이스의 개발로 인하여 앞으로도 많은 연구가 필요하다.

특히, 입력값 및 출력값 보안의 측면에서는 제안된 기술 대부분이 데이터의 접근 및 관리를 위해 새로운 중간 계층을 도입하여 프라이버시 보호를 수행하고 있다. 또한, 프라이버시 보호 강도에 관한 기준점이 모호하여 해당 강도를 사용자가 조절하도록 설계된 것이 많다. 따라서, 추가적인 계층을 추가하지 않으면서 사용자들의 편리성을 위해 자동화된 기술개발이 필요하며, 이러한 프라이버시 보호에 대한 개별적인 표준 확립이 필요하다. 상호작용 보안의 측면에서는 다양한 환경 구축과 함께 프로토콜에 관한 연구들이 수행되고 있지만, 다중 사용자의 공유공간 활용이나 다중 디바이스 연동은 제한적이며 다양한 서비스 및 디바이스가 개발되고 있으므로 이에 발맞춰 관련 환경 구축 및 프로토콜 개발이 지속해서 수행되어야 한다. 그리고 디바이스 보안의 측면에서는 기존의 인증 기술을 뛰어넘는 새로운 방식을 개발하고 있지만, 입력값 및 출력값 보안과 함께 고려하지 않을 수 없다. 인증을 위한 데이터도 결국 디바이스를 통해 수집 및 활용되기 때문에 단순 인증 기술에만 집중하는 것이 아니라, 데이터 보안을 함께 적용하여 활용 가능한 기술개발이 필요하다.

마지막으로, 본 논문에서는 별도로 다루지 않았지만 온·오프라인이 융합된 경제환경에서 발생 가능한 보안 이슈에 관한 연구가 필요하다. 2장에서 언급한 로블록스와 같이 다양한 메타버스는 가상화폐를 통해 현실과 유사한 경제활동을 지원하고 있다. 이러한 가상 화폐는 현실 화폐에 상응하는 가치를 갖고 있으며, 일반적으로 분산된 환경에서 개인의 전자지갑을 통해 관리되고 있다[50]. 따라서, 관련 보안 기술은 핵심 기술로서 중요 연구 방향 중 하나이다. 특히, 현실 화폐의 가상화가 이루어지고 있으므로 다방면으로 보안 기술개발이 필요하다.

Ⅳ. 결 론

메타버스는 기존의 온라인 세상을 포함하는 새로운 세상으로, 우리의 일상생활뿐만 아니라 다양한 군사적,

상업적 등의 분야에서 활용되고 있다. 이러한 메타버스가 핵심 기술로 대두됨에 따라 다양한 방향으로의 연구가 지속해서 수행되고 있다. 국내에서도 관련 연구들을 수행하고 있지만, 현재의 추세와 서비스 측면에서의 연구가 주를 이루고 있으며 보안 관련 연구는 아직 미흡하다. 이에 본 논문에서는 보안 기술 연구의 기반이 될 수 있도록, 실제 발생하거나 발생 가능성이 큰 이슈를 기반으로 보안 위협을 3가지로 분류하였다. 또한, 관련 연구들을 분류하여 현재 연구 진행 상황을 확인하였으며, 앞으로 수행되어야 할 연구 방향을 제시하였다. 메타버스의 관련 기술 및 기기의 개발이 활발히 진행되고 있으며, 이에 발맞춰 보안 기술에 관한 연구도 더욱 활발히 진행되어야 한다.

참 고 문 헌

[1] 민경식, 장한나, “언택트에서 온택트 시대로, 인터넷 이용자 행태 변화 분석”, KISA, 2021

[2] Billinghurst, Mark, and Hirokazu Kato. "Collaborative mixed reality." Proceedings of the First International Symposium on Mixed Reality. 1999.

[3] Grasset, Raphael, and Jean-Dominique Gascuel. "Mare: Multiuser augmented reality environment on table setup." ACM SIGGRAPH 2002 conference abstracts and applications. 2002.

[4] Hua, Hong, Leonard D. Brown, and Chunyu Gao. "SCAPE: supporting stereoscopic collaboration in augmented and projective environments." IEEE Computer Graphics and Applications 24.1 (2004): 66-75.

[5] Regenbrecht, Holger T., Michael Wagner, and Gregory Baratoff. "Magicmeeting: A collaborative tangible augmented reality system." Virtual Reality 6.3 (2002): 151-166.

[6] Schmalstieg, Dieter, and Gerd Hesina. "Distributed applications for collaborative augmented reality." Proceedings IEEE Virtual Reality 2002. IEEE, 2002.

[7] 닐 스티븐슨, 김장환 역, 『스노우 크래쉬』, 새와물고기, 1996,

[8] Lucas Matney, “Jeff Koons’ augmented reality Snapchat artwork gets ‘vandalized’”, Join TechCrunch+, 2017

[9] Joseph Jerome, and Jeremy Greenberg, “Augmented Reality+Virtual Reality, Privacy& Autonomy Considerations in Emerging, Immersive Digital Worlds”, Future of privacy forum, 2021.

[10] John S., Jamais C., Jerry P., Corey B., Jochen H., James H., and Randal M. (2007) "Metaverse Roadmap", ASF

[11] 이건한, “AI보다 유망하다고? 300조원 시장 전망 근거는”, https://www.bloter.net/newsView/blt202108250010, Bloter, 2021

[12] 박정은, “글로벌 XR 시장, 연평균 76.9% 성장... 2024년 159조원 규모”, https://m.etnews.com/20210908000097, 전자신문, 2021

[13] 한상열, 방문영, '글로벌 XR 정책 동향 및 시사점', 2021, 소프트웨어정책연구소

[14] U.S. Army(2019.10.8.), “Army testing synthetic training environment platforms”

[15] 가상융합경제 발전 전략, 2020

[16] Chinabaogao, 2020年全國及各省市虛擬現實 行業相關政策梳理, 2020.8.21.

[17] 국토교통성, 國土交通データプラットフォーム（仮称）整備計畫, 2020.4.

[18] 진승현. "메타버스를 이용한 현황분석과 사례를 통한 예술교육 개발 연구." 예술교육연구 19.3 (2021): 21-40.

[19] 윤경로. "메타버스 표준화 동향." 한국통신학회지(정보와통신) 38.9 (2021): 32-38.

[20] Kim, Sang-Gyun. "메타버스 미디어 플랫폼과 관련 표준화 동향." Broadcasting and Media Magazine 26.3 (2021): 41-49.

[21] 김진. "메타버스를 활용한 조선 해양 분야 정보보호 교육 콘텐츠 개발 방안." 정보보호학회논문지 31.5 (2021): 1011-1020.

[22] Delcombel, Nicolas, et al. "CyberCopter: a 3D helical visualisation for periodic signals of cyber attacks." VR4Sec 2021 (Security for XR and XR for Security). 2021.

[23] Rajaram, Shwetha, Franziska Roesner, and Michael Nebeling. "Designing Privacy-Informed

Sharing Techniques for Multi-User AR Experiences."

[24] Odeleye, Blessing, et al. "Detecting framerate-oriented cyber attacks on user experience in virtual reality." 2021.

[25] Roesner, Franziska, and Tadayoshi Kohno. "Security and Privacy for Augmented Reality: Our 10-Year Retrospective."

[26] Falchuk Ben, Shoshana Loeb, and Ralph Neff. "The Social Metaverse: Battle for Privacy." IEEE Technology and Society Magazine 37.2 (2018): 52-61.

[27] De Guzman, Jaybie A., Kanchana Thilakarathna, and Aruna Seneviratne. "Security and privacy approaches in mixed reality: A literature survey." ACM Computing Surveys (CSUR) 52.6 (2019): 1-37.

[28] Lebeck, Kiron. Security and Privacy for Emerging Augmented Reality Technologies. Diss. 2019.

[29] Jana, Suman, Arvind Narayanan, and Vitaly Shmatikov. "A scanner darkly: Protecting user privacy from perceptual applications." 2013 IEEE symposium on security and privacy. IEEE, 2013.

[30] Zarepour, Eisa, et al. "A context-based privacy preserving framework for wearable visual lifeloggers." 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). IEEE, 2016.

[31] Templeman, Robert, et al. "PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces." NDSS. 2014.

[32] de Guzman, Jaybie Agullo, Kanchana Thilakarathna, and Aruna Seneviratne. "SafeMR: Privacy-aware Visual Information Protection for Mobile Mixed Reality." 2019 IEEE 44th Conference on Local Computer Networks (LCN). IEEE, 2019.

[33] de Guzman, Jaybie A., Kanchana Thilakarathna, and Aruna Seneviratne. "Conservative Plane Releasing for Spatial Privacy Protection in Mixed Reality." arXiv preprint arXiv:2004.08029 2020.

[34] Nama, Arpit, et al. "User configurable 3D object regeneration for spatial privacy." arXiv preprint arXiv:2108.08273 2021.

[35] Reilly, Derek, et al. "SecSpace: prototyping usable privacy and security for mixed reality collaborative environments." Proceedings of the 2014 ACM SIGCHI symposium on Engineering interactive computing systems. 2014.

[36] Gaebel, Ethan, et al. "Looks good to me: Authentication for augmented reality." Proceedings of the 6th International Workshop on Trustworthy Embedded Devices. 2016.

[37] Lebeck, Kiron, et al. "Towards security and privacy for multi-user augmented reality: Foundations with end users." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[38] Sluganovic, Ivo, et al. "Tap-Pair: Using Spatial Secrets for Single-Tap Device Pairing of Augmented Reality Headsets." Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy. 2020.

[39] Mortezapoor, Soroosh, and Khrystyna Vasylevska. "Safety and Security Challenges for Collaborative Robotics in VR.", 2021

[40] Ben Dickinson. “5 authentication methods putting passwords to shame.” https://thenextweb.com/news/5-technologies-will-flip-world-authentication-head, 2016

[41] George, Ceenu, et al. "Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality." NDSS, 2017.

[42] Aslan, Ilhan, et al. "Mid-air authentication gestures: An exploration of authentication based on palm and finger motions." Proceedings of the 16th International Conference on Multimodal Interaction. 2014.

[43] Rogers, Cynthia E., et al. "An approach for user identification for head-mounted displays." Proceedings of the 2015 ACM International Symposium on Wearable Computers. 2015.

[44] Li, Sugang, et al. "Whose move is it anyway? Authenticating smart wearable devices using

unique head movement patterns." 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE, 2016.

[45] Chauhan, Jagmohan, et al. "BreathPrint: Breathing acoustics-based user authentication." Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services. 2017.

[46] Venkatasubramanian, Krishna K., Ayan Banerjee, and Sandeep Kumar S. Gupta. "PSKA: Usable and secure key agreement scheme for body area networks." IEEE Transactions on Information Technology in Biomedicine 14.1 (2009): 60-68.

[47] Schneegass, Stefan, Youssef Oualil, and Andreas Bulling. "SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull." Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. 2016.

[48] Raja, Kiran B., et al. "Multi-modal authentication system for smartphones using face, iris and periocular." 2015 International Conference on Biometrics (ICB). IEEE, 2015.

[49] Khamis, Mohamed, et al. "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices." Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. 2016.

[50] 진승헌, 조진만, 조상래, 조영섭, 김수형.. 경계없는 세상과 사용자 인증기술 동향. [ETRI] 전자통신동향분석, 36(4). 2021

〈저자소개〉

정 수 용 (Jeong Soo Yong)

정회원

2018년 2월 : 공주대학교 응용수학과 학사

2020년 2월 : 공주대학교 융합과학과 석사

2020년 3월~현재 : 공주대학교 융합과학과 박사과정

<관심분야> 데이터 보안, 인공지능, 신경망 암호 기술

서 창 호 (Seo Chang Ho)

정회원

1990년 : 고려대학교 수학과 학사

1992년 : 고려대학교 수학과 이학석사

1996년 : 고려대학교 수학과 이학박사

1996년~1996년 : 국방과학연구소 선임연구원

1996년～2000년 : 한국전자통신연구원 선임연구원, 팀장

2000년～현재 : 공주대학교 응용수학과 교수

<관심분야> 암호알고리즘, PKI, 무선인터넷 보안 등

조 진 만 (CHO, Jin-Man)

정회원

1989년 2월 : 충남대학교 계산통계학과 학사

1991년 2월 : 충남대학교 전산학과 이학석사

1991년 2월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원

<관심분야> 개인정보보호, 스마트카드, 사용자 인증

진 승 헌 (Seung-Hun Jin)

정회원

1993년 2월 : 숭실대학교 전자계산학과 졸업 (학사)

1995년 2월 : 숭실대학교 전자계산학과 졸업 (석사)

2004년 2월 : 충남대학교 컴퓨터과학과 졸업 (박사)

1999년~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원

<관심분야> PKI, 인증/인가, ID관리, 개인정보보호, 핀테크 보안

김 수 형 (Kim Soo Hyung)

정회원

1996년 2월 : 연세대학교 컴퓨터과학과 학사

1998년 8월 : 연세대학교 컴퓨터과학과 석사

2016년 2월 : 한국과학기술원 전산학부 박사

1998년 9월~2000년 12월 : 한국정보통신 연구원

2000년 12월~현재 : 한국전자통신연구원 책임연구원

<관심분야> ID관리, 바이오인증, 핀테크보안 등