정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

메타버스의 진화에 따른 ID 관리 기술 현황

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

요 약

메타버스는 가상, 초월을 의미하는 ‘메타(meta)’와 세계, 우주를 의미하는 ‘유니버스(universe)’의 합성어로 현실 세계를 초월한 디지털 세계라고 정의할 수 있다. 이러한 메타버스는 현실 세계와 평행한 디지털 세계의 구축을 시작으로 블록체인(Blockchain), 인공지능(AI) 등의 기술과 고성능 웨어러블 디바이스(Wearable Device) 기반의 높은 몰입감을 제공하여 현실과 상호 작용하는 디지털 세계로 진화하고 있다. 이에 따라, 현재의 메타버스는 기존의 디지털 세계를 구축하고 활용하는 다양한 서비스가 포함된 개념으로 확장되고 있으며, 최종적으로는 현실과 디지털 세계의 경계가 없는 초현실적인 세계로 발전할 것이다. 이러한 메타버스 발전의 뒤에는 많은 보안 기술들이 필요하며, 실제 개인의 프라이버시 문제 및 보안 위협에 대한 우려가 증가하고 있다. 특히, 높은 몰입감을 제공하기 위해 이전보다 더욱 다양한 생체정보를 포함한 개인정보가 사용될 것이며, 이러한 데이터는 개인을 특정하는 ID(Identity)로 활용될 수 있다. 이에, 개인정보에 대한 보안 위협은 더욱 다양해질 것이고, 동시에 안전한 개인정보 활용이 가능한 ID 관리 기술개발의 필요성도 높아질 것이다. 따라서, 본 논문에서는 메타버스의 개념과 함께 진화 과정을 제시하고, 메타버스의 진화에 따라 다양해지는 ID 관련 보안 위협 및 대응 기술을 분석을 통해 ID 관리 기술의 현황을 정리한다.

Ⅰ. 서 론

현실에서의 활동을 디지털 세계에서 동일하게 수행하기 위해 메타버스는 현실 세계와 평행한 가상세계의 구축을 시작으로 발전되고 있으며, 이에 메타버스는 현실 세계를 초월한 새로운 가상세계를 의미하는 단어로 정의되었다[1]. 이를 기반으로, 현실에서 수행될 수 있는 다양한 인간관계 및 신체 활동을 보장할 수 있는 즉, 현실과 상호작용이 가능한 디지털 세계로 진화하고 있다. 동시에, 메타버스의 개념도 단순한 가상세계를 의미하는 것이 아닌 기존의 디지털 세계를 구축하는 모든 서비스를 포함하는 개념으로 확장되고 있다.

메타버스의 다양한 특성은 이러한 발전 방향의 근거를 제시하고 있다. 2007년 ASF(Acceleration Studies Foundation)에서 처음 발표된 메타버스의 로드맵[2]은 메타버스의 4대 요소로 증강현실(Augmented Reality, AR), 라이프 로깅(Life logging), 거울세계(Mirror World) 그리고 가상세계(Virtual World)를 제시하였다. 이를 기반으로, 메타버스의 특성에 대한 다양한 분석들이 수행되고 있으며, 몰입감(Immersiveness), 상호운용성(Interoperability), 확장성(Scalability), 경제활동(Economic activity) 등이 중요한 특징으로 분류되고 있다[3-7]. 특히, 몰입감은 현실에서와 유사한 체험을 제공하고 신체 활동능력을 보장하기 위한 메타버스의 중요한 특징 중 하나이며, 다양한 웨어러블 디바이스를 활용하여 높은 몰입감을 제공하기 위한 연구들이 수행되고 있다[8-10]. 또한, 다수의 사용자를 수용하고 현실과 유사한 품질의 서비스를 제공하는 확장성과 다양한 메타버스간의 상호작용이 가능한 상호운용성은 메타버스의 발전 방향을 나타내는 특징이다. 즉, 이러한 메타버스의 특징들을 통해 미래의 메타버스는 현실과 유사한 환경에서 동일한 신체적, 경제적 활동이 가능하고 현실과 상호작용이 가능한 디지털 세계로 발전하고 있음을 확인할 수 있다.

이 논문은 2022년도 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, 책임연구원, jinsh@etri.re.kr)
**** 한국전자통신연구원 (책임연구원/기술총괄, lifewsky@etri.re.kr)

현실과 유사한 환경에서의 신체 활동을 보장하여 높은 몰입감을 제공하는 미래의 메타버스에서 생체정보 활용을 위해 다양한 웨어러블 디바이스의 사용이 필수적이다. 이때, 사용자들의 생체정보는 자연스럽게 수집되고 활용될 것이며, 이는 현재와는 다른 보안 문제를 발생시킨다. 과거의 ID는 사용자들이 직접 제출한 이름, 성별 등의 정보를 기반으로 수행되었다. 하지만, 다수의 웨어러블 디바이스에 수집되는 생체정보는 간접적으로 수집되기 때문에 해당 데이터에 대한 수집 및 관리 문제가 발생한다. 또한, 현재의 지문, 홍채 등의 생체정보에 기반한 신원인증 기술과 뇌파 및 혈류 등의 다양한 생체정보를 활용한 신원인증이 가능해질 것이며, 동시에 관련 보안 이슈가 발생할 수 있다. 이에, 메타버스에 발생 가능한 보안 위협에 대한 연구가 수행되었다[6,7,11-13].

우리가 현재 경험하고 있는 메타버스와 이상적으로 생각하는 메타버스의 간극이 존재하며, 이로 인한 관점의 차이가 발생할 수 있다. 예를 들어, 현재는 제페토, 로블록스 등과 같은 온라인 게임의 메타버스를 이용하고 있지만, 이상적인 메타버스로 웨어러블 장비를 통해 폭넓은 생체정보의 활용이 가능한 '레디 플레이어 원', '아바타' 등을 가정하고 있다. 이에, 본 논문에서는 모두가 동일한 관점에서 메타버스의 보안을 분석할 수 있도록 메타버스의 진화 과정을 기준으로 제시한다. 총 3단계로 분류된 진화 과정은 가상세계와 현실 세계 간의 영향력에 따라 분류하였으며, 이를 통해 메타버스의 진화 단계를 확인할 수 있다. 이러한 진화 과정을 기반으로, 생체정보를 포함한 개인정보를 다루는 ID 관리 기술에서 발생 가능한 보안 위협을 단계별로 분석하고, 해당 위협에 대한 대응 기술을 정리한다.

본 논문의 2장에서는 메타버스의 정의, 특징 및 진화 과정을 서술하고, 메타버스에서의 보안 관련 연구를 분석한다. 3장에서는 메타버스의 진화 과정에 따라 변화되는 ID 및 보안 위협을 분류하고, 이에 상응하는 대응 기술을 분석한다. 그리고 4장에서 결론을 짓는다.

Ⅱ. 메타버스 보안

이번 장에서는 본 연구의 배경이 되는 메타버스의 정의 및 특징들을 분석하고, 메타버스의 분류 기준이 되는 메타버스의 진화 단계를 제시한다. 또한, 메타버스 관련 보안 연구들을 분석하여, 메타버스 보안의 현주소를 살펴본다.

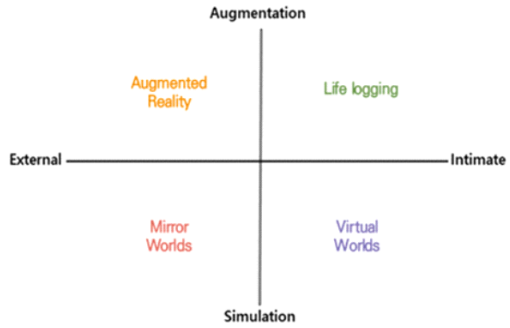
2.1. 메타버스의 정의

소설 '스노우 크래쉬(Snow Crash)'[14]에서 가장 처음 등장한 메타버스는 '가상, 초월'을 의미하는 메타(meta)와 '세계, 우주'를 의미하는 '유니버스(universe)'의 합성어이다. 메타버스는 가상세계, 가상 우주로 해석할 수 있으며, 소설 속에서는 다양한 시청각 출력 장치를 활용하여 접근하는 가상세계로 묘사되고 있다. 이러한 메타버스에 대해 다양한 정의를 내리고 있지만[1], 이제는 현실 세계를 초월한 디지털 세계라고 정의할 수 있다.

이러한 메타버스의 4대 요소는 2007년 ASF(Acceleration Studies Foundation)에서 발표한 로드맵[2]에서 그림 1과 같이 언급되었다. 4대 요소인 증강현실, 일상기록, 거울 세계, 가상세계는 메타버스가 다양한 온라인 서비스를 포함하고 있음을 의미한다. 이러한 4가지 요소에 기반하여 메타버스의 특징에 대한 분석들이 수행되었으며, 공통적으로 아래와 같은 4가지 특징이 제시되었다[3-7,11].

- 몰입감(Immersiveness)
- 경제활동(Economic activity)
- 확장성(Scalability)
- 상호운용성(Interoperability)

첫 번째, 몰입감은 디지털 환경에서 만들어진 가상의 세계가 얼마나 현실감이 있는지를 판단할 수 있는 특징이다. 이는, 사용자가 가상세계와 신체적 활동 및 감각(시각, 청각, 촉각 등)을 공유함을 의미하며, 높은 몰입



〔그림 1〕 메타버스의 4대 요소〔2〕

감을 보장하는 메타버스는 현실에서의 행동과 감각이 가상세계에서 동일하게 반영되며, 반대로 가상세계에서의 감각이 현실로 피드백되는 것을 의미한다.

두 번째로, 각각의 메타버스는 독자적인 경제활동을 보장한다는 것이다. 메타버스에서는 다양한 생산 활동이 가능해지며 이에 따라 생산된 물건에 대한 가치가 측정되고 거래가 진행된다. 이때, 메타버스에서의 화폐가 현실 화폐와의 거래가 가능해짐에 따라 가상 물건의 가치가 높아지고, 현실에서와 유사한 독자적인 경제활동이 가상세계에서도 이루어진다.

세 번째로, 확장성은 메타버스의 능력을 판단할 수 있는 특성이다. 메타버스의 수용 가능한 사용자 수와 아바타 수, 구현된 가상세계의 품질 등을 포함하며, 높은 확장성은 메타버스의 사용자들에게 가장 매력적인 특징이라고 할 수 있다.

마지막으로, 상호운용성은 현실세계와 메타버스의 관계가 아닌 메타버스간의 호환성을 의미한다. 사용자가 가상세계를 이동하면서 어려움과 끊김이 없을 때 높은 상호운용성을 갖는다고 할 수 있다. 메타버스 중 하나인 '포트나이트'를 통해 상호운용성을 확인할 수 있다. 포트나이트는 총 3가지의 게임 모드가 존재하며, 각각의 모드를 포트나이트라는 메타버스에 종속된 소규모 메타버스로 생각할 수 있다. 이때, 3가지 모드간의 이동이 어렵고 많은 시간이 발생한다면, 낮은 상호운용성을 갖는다고 말할 수 있다. 향후에는 대규모 메타버스 간의 상호연동을 지원하기 위한 개방형 메타버스 구축에 대한 고려가 늘어날 것으로 보인다.

2.2. 메타버스의 진화 단계

메타버스의 4대 요소를 통해 메타버스는 우리가 사용하였던 온라인 서비스를 포함하고 있다고 판단할 수 있다. 또한, 각각의 특징들을 통해 경제적, 물리적으로 현실 세계와 경계가 없는 가상세계 즉, 현실을 초월한 디지털 세계로 발전하고 있음을 확인할 수 있다.

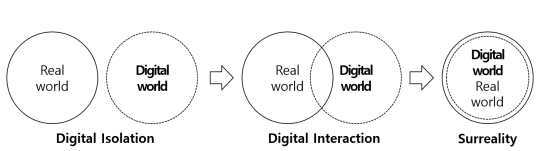
이에, [7]에서는 현실 세계(Real World)와 가상세계(Virtual world)의 콘텐츠를 기준으로 메타버스의 발전을 구분하였다. 각각의 단계를 현실과 대칭되는 콘텐츠만 존재하는 디지털 트윈(Digital Twin), 가상세계만의 독자적인 콘텐츠가 존재하는 디지털 네이티브(Digital Native), 그리고 이러한 경계가 없는 초현실(Surreality)로 정의하였다. 그러나, 콘텐츠 기준의 분류 방법으로는 메타버스에 대한 다양한 관점의 간극을 좁히는 것이 어렵다.

이에, 본 논문에서는 동일한 관점에서 메타버스의 보안 문제를 다룰 수 있도록, 메타버스의 진화 과정을 현실과 디지털 세계의 상호 영향력을 기준으로 그림 2와 같이 3단계로 분류하였다.

각각의 단계는 디지털 분리(Digital Isolation), 디지털 상호작용(Digital Interaction), 초현실(Surreality)로 정의될 수 있다.

디지털 분리 단계는 현실과 디지털 세계의 독립적인 관계로 이루어진 상태로 현실 세계에서 디지털 세계로 영향력을 끼칠 수 있지만, 디지털 세계에서 현실 세계로의 영향력은 존재하지 않는다. 다시 말해, 사용자들이 디지털 세계의 아바타를 조종하여 게임을 하거나 사람들과의 커뮤니케이션을 진행한다. PC 환경에서의 온라인 게임이 이러한 디지털 분리 단계에 해당한다. 해당 단계에서는 입출력 장치로 PC의 모니터와 키보드 및 마우스만을 주로 사용하기 때문에 높은 몰입감을 제공하는 것은 어려우며, 경제활동 측면에서 현실과 가상에서의 화폐 거래가 가능할 수 있지만, 이는 매우 제한적이다. 또한, 다른 메타버스와의 연동성은 크게 고려되지 않은 상황이기 때문에 상호운용성을 확인하는 것은 어렵다.

다음으로 디지털 상호작용 단계는 현실 세계와 디지털 세계의 상호 영향력을 끼치는 단계를 의미한다. 영화 '레디 플레이어 원'에 나오는 가상현실 '오아시스'가 상호작용 단계에 해당하는 메타버스의 대표적인 예시로 사용될 수 있다. 높은 몰입감을 제공할 수 있는 상호작용 단계에서는 영화의 예시에서 확인할 수 있듯이, 다양한 웨어러블 디바이스를 활용하여 현실에서의 움직임을 디지털 세계에서의 아바타로 반영할 수 있다. 또한, 반대로 디지털 세계에서의 아바타가 느끼는 다양한 감각(시각, 청각, 촉각 등)을 현실의 사용자에게 피드백(feedback)할 수 있다. 또한, 독립적인 경제활동과 함께 현실 세계와 디지털 세계의 화폐 거래가 가능하며, 높은



〔그림 2〕 메타버스 진화 3단계[7]

확장성과 함께 다양한 메타버스간의 상호운용성도 높아진다고 할 수 있다.

현재의 메타버스는 디지털 분리 단계에서 상호작용 단계로 발전하는 단계로 판단된다. 상호작용 단계의 확장성 및 경제활동을 보장하기 위해 블록체인, 인공지능 등의 기술을 적용하는 방안에 대한 연구가 수행되고 있다[15,16]. 또한, 높은 몰입감을 위해 웨어러블 디바이스의 고도화에 대한 연구가 수행되고 있으며, 다양한 기업에서는 활용 가능한 웨어러블 디바이스 및 관련 서비스를 제공하고 있다[17,18].

최종적으로 메타버스는 현실과 가상의 경계가 없는 초현실을 이룰 것이다. 아직 디지털 상호작용 단계로 발전하고 있는 현재의 단계에서 최종 단계로 생각되는 초현실 단계를 예측하는 것은 한계가 있을 수 있으나, 공상 과학 영화를 통해 우리는 상상해 볼 수 있다. 먼저, 영화 “써로게이트‘에서의 사람들은 디지털 세계의 아바타를 사용하는 것이 아닌, 현실 세계에서 로봇을 아바타로 사용하여 본인과 다른 외모와 성별을 갖는 사람으로 살아간다. 누군가에게는 현실 세계이지만 누군가에게는 로봇을 통해 경험하는 디지털 세계가 될 수 있는 세계를 표현한 영화로, 초현실의 한 가지 가능성으로 바라볼 수 있다. 또한, 영화 ’아바타‘에서는 인간이 ’링크룸‘이라는 장비를 통해 ’판도라 행성‘의 ’나비족‘으로 활동하는 내용을 다룬다. 이때, 판도라 행성이 메타버스의 디지털 세계로 생각한다면 나비족은 아바타로 대응되며, 이를 통해 초현실 단계의 메타버스를 생각해 볼 수 있다. 현실 세계의 자원 문제를 해결하기 위해 디지털 세계 자원을 활용하는 것이 초현실 단계에서의 메타버스가 될 수 있다.

이처럼 메타버스는 과거의 온라인 게임과 같은 디지털 분리 단계와 현재 메타버스 발전 방향인 디지털 상호작용 단계, 그리고 가상과 현실의 경계가 없는 초현실 단계로 분류할 수 있다.

2.3. 메타버스 보안 관련 연구

메타버스는 다음 단계로의 진화를 위해 다양한 기술의 적용과 새로운 웨어러블 디바이스를 활용하는 방향으로 발전하고 있다[15-18]. 동시에, 새롭게 발생 가능한 보안 이슈에 집중하고 있으며, 실제로 이러한 보안 관련 연구들이 꾸준히 수행되고 있다[6,7,12,19,20].

먼저, [19]에서는 메타버스를 아래와 같은 5가지 관점으로 분석한 후에 3가지 특징인 다중기술(multi-technology), 사회성(sociality), 초시공간성(hyper spatiotemporality)을 소개하고, 관련된 다양한 기술들을 정리한다.

- network infrastructure
- management technology
- basic common technology
- virtual reality object connection
- virtual reality convergence

그리고 메타버스에서의 보안 관련 문제를 프라이버시, 윤리적 문제들을 포함하여 상호작용 및 표준화 등의 6가지 문제로 정리하였다. 또한, [20]에서는 메타버스 관련 기술을 HW, SW, 컨텐츠(Contents) 요소 및 3가지 접근법을 기준으로 정리하였으며, 영화, 게임, 학습 분야에서의 메타버스 예시를 통해 관련 기술을 분석하였다. 그리고 각각의 분야에서 해결해야 할 보안 문제를 함께 제시하였다. 위의 연구들과 유사하게 [6]에서도 기본적인 메타버스의 개념 및 특성을 정리하고 개인의 프라이버시 관련 문제와 기술적 및 사회적으로 발생 가능한 보안 문제를 제시하였다. 하지만, 위의 연구결과는 보안 이슈에 대한 대응방안을 구체적으로 제시하지 않았으며, [7]에서는 이전의 다양한 조사논문을 분석하고 정리하여 보안 문제를 ID, 데이터, 프라이버시, 네트워크, 경제, 경영 그리고 물리적/사회적 영향, 총 7가지로 분류하고 관련 대응 기술을 함께 정리하였다.

현실 세계의 사물에 대응되는 디지털 세계의 디지털 트윈(Digital Twin)은 메타버스의 중요한 컨텐츠 중 하나이며, [12]에서는 이에 대한 연구를 수행하였다. 먼저, 디지털 트윈과 관련된 블록체인, NFT(non-fungible token) 등의 기술에 대해 정리하고 구체적인 디지털 트윈의 구조를 제시한 후에 관련된 보안 이슈들을 분석하였다.

또한, 높은 몰입감을 제공하기 위해 사용되는 웨어러블 디바이스는 메타버스의 핵심 기술 중 하나이며, 관련된 보안 위협 사례가 증가함에 따라 관련 기술 연구들이 수행되고 있다[13,21-23]. 이는 가상현실(Virtual Reality, VR), 증강현실(Augmented Reality, AR) 그리고 혼합현실(Mixed Reality, MR)로 분류할 수 있으며,

[13]에서는 VR 관련 최신 기술을 정리하고 DoS(Denial of Service)와 같은 기존의 공격 기법에 대한 안전성 및 VR에 대한 새로운 공격 기법을 분석하였다. 또한, [21]에서는 VR 및 AR에 대한 기존의 다양한 취약점 분석 연구를 정리하고 다양한 공격들을 분류한 후, VR/AR 인터페이스 취약점 분석 모델을 새롭게 설계하였다. MR에 대하여 [22]에서는 기존의 공격 기법들을 정리하고 MR 상에서 안전한 데이터 활용이 가능한 모델을 새롭게 제안하였다. 특히, 기계학습(Machine Learning, ML)을 활용하여 공격 탐지 기술인 MR-forensics을 새롭게 제안하였다. 또한, [23]에서는 협업이 가능한 MR(Collaborative Mixed Reality, CMR)에 대한 다양한 보안 위협을 정리하고 이에 대한 대응 기술들을 분석하였다.

메타버스 보안 관련 연구들은 다방면으로 수행되었지만, 현재 제공되는 메타버스 세상이 아닌 우리가 예상하는 디지털 상호작용 단계에서의 메타버스를 가정하고 다양한 보안 위협을 분석하고 있다. 이러한 메타버스 발전 단계의 차이로 인해, 보안 이슈를 바라보는 시점에 따라 괴리감이 발생할 수 있다. 따라서, 본 논문에서는 2.2에서 정의한 메타버스의 진화 단계를 기준으로 관련 보안 이슈를 정리한다.

Ⅲ. 메타버스에서의 ID 관리 기술 현황

2장에서 언급한 바와 같이 메타버스는 총 3단계로 구분할 수 있다. 단계별 메타버스는 4가지 특징에 대해 제공되는 정도가 다르며, 이에 활용되는 기술 및 데이터도 다르다. 특히, 사용자를 특정할 수 있는 ID의 구체적인 사항은 메타버스의 진화에 따라 변화하고 있으며, 이에 따라 ID 관리 기술도 변화해야 한다. 이번 장에서는 이러한 메타버스의 진화에 따라 ID로 활용될 수 있는 생체정보를 포함한 개인정보에 대해 정리하고, 이러한 ID 관련 보안 위협을 정리한다. 그리고 해당 위협에 대한 대응 기술 분석을 통해 ID 관리 기술 현황을 정리한다.

3.1. 메타버스의 ID

2.2에서 정의한 메타버스의 진화 단계 중, 첫 번째 디지털 분리 단계의 메타버스를 생각한다면, 기존의 SNS 서비스 및 온라인 게임이 이에 해당한다. 이때, 사용자들은 해당 서비스 이용을 위해 개인정보(이름, 주민등록번호, 성별 등)만을 제공하며, 이러한 정보가 ID로 활용될 수 있다.

디지털 분리와 디지털 상호작용 단계 사이에 존재하는 현재의 메타버스를 살펴보면, 높은 몰입감을 제공하기 위해 AR/VR/MR 등의 다양한 가상현실을 생성할 수 있는 기술이 적용되고 있으며, 이는 디지털 분리 단계의 메타버스보다 확장된 다양한 개인정보를 다루게 된다. 사용자의 다양한 행동을 반영하고 감각을 피드백하기 위해 사용되는 웨어러블 디바이스는 사용자의 다양한 생체정보를 활용한다. 예를 들어, 일반적인 VR 서비스는 헤드 마운티드 디스플레이(Head Mounted Display, HMD)를 통해 이루어지며, 이때 사용자의 머리 움직임 및 눈동자의 움직임 등을 수집할 수 있다. 이러한 생체정보는 기존의 id/pw와 같이 개인을 인증할 수 있는 수단이 될 수 있다. 또한, 기존의 PC 환경을 포함한, 스마트폰 등의 다양한 장치에서 메타버스의 접근이 가능하므로, 각 장치에서 사용되는 인증 수단인 지문, 홍채, 안면 등의 생체정보가 수집되고 활용될 수 있다.

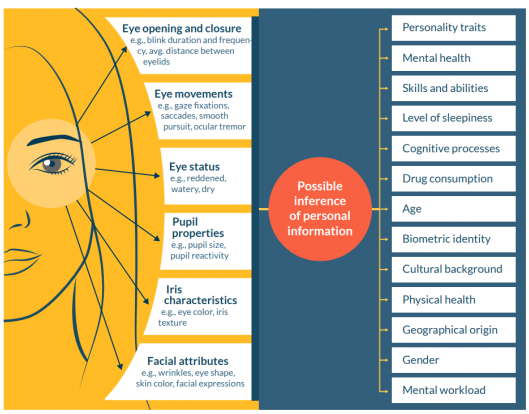
〔표 1〕 메타버스 보안 관련 연구 정리

관련 연구	연구 내용
Ning 2021 [19]	메타버스를 5가지 관점, 3가지 특성, 6가지의 보안 문제 정리
Park 2022 [20]	영화, 게임, 학습 항목에 대한 예시 및 보안 이슈 정리
Pietro 2021 [6]	메타버스에서의 개인 프라이버시 관련 문제 및 사회적, 기술적 보안 문제 정리
Wang 2022 [7]	메타버스에서의 보안 문제를 7가지로 분류하고 대응 기술 분석
Far 2022 [12]	Digital Twin관련 기술 정리 및 보안 문제 제시
Giaretta 2022 [13]	VR 최신 기술 정리 및 DoS 등의 기존 공격에 대한 취약점 분석
Zhernova 2021 [21]	VR/AR 관련 취약점 분석 및 공격 기법 정리, 취약점 분석 모델 설계
Kilger 2021 [22]	MR상에서 안전한 데이터 관리 모델 제시 및 ML 기반 공격 탐지 기술 설계
Happa 2019 [23]	CMR에 대한 보안 위협 정리 및 대응 기술 분석

다양한 기술의 발전으로 영화 '레디 플레이어 원'과 같은 디지털 상호작용 단계에 도달한다면, 사용자의 자유로운 행동이 디지털 세계에 반영되기 위해 고도화된 웨어러블 디바이스를 활용하여 사용자의 세부적인 움직임을 수집하여 활용할 것이다. 또한, 다양한 감각을 디지털 세계에 반영하고 현실 세계로 피드백하기 위해 심박 수, 뇌파 등의 생체정보가 활용될 것이다. 이처럼 메타버스 이용에 지금보다 다양한 생체정보가 필요할 것이며, 이는 현재 사용되고 있는 지문과 유사하게 개인을 인증하는 정보로 활용될 수 있다. 이와 관련하여, 몰입형 환경에서의 개인정보보호 등을 세우는 비영리조직 XRSI(XR Safety Initiative)에서는 앞으로 사용될 생체 데이터를 다음과 같이 정리하였다[24].

- 얼굴 인식(Facial recognition)
- 지문 인식(Dactyloscopic data)
- 홍채 스캐닝(Iris scanning)
- 망막 분석(Retinal analysis)
- 음성 인식(Voice recognition)
- 귀 모양 인식(Ear shape recognition)
- 자판 타이핑 인식(Keystroke analysis)
- 손 글씨 인식(Handwritten signature analysis)
- 걸음걸이 분석(Gait analysis)
- 시선 추적(Gaze analysis)

또한, 시선 추적장치 및 센서(Eye trackers and sensors)를 통해 수집된 데이터와 이를 통해 추론 가능한 사용자의 개인정보를 그림 3과 같이 정리하였다. 눈과 관련된 정보만으로 사용자의 나이, 성별뿐만 아니라 다양한 생체 상태 정보 및 정신적 상태까지 알 수 있다.



〔그림 3〕 시선 추적장치 및 센서(Eye trackers and sensors)로 수집 가능한 정보 및 추론 가능한 개인정보〔24〕

이처럼, 디지털 상호작용 단계에서는 다양한 생체정보를 포함하는 개인정보가 ID로 활용될 것으로 예상하며, 더 나아가 초현실 단계에서는 이러한 생체정보를 포함하는 새로운 개인정보가 활용되고 개인의 ID로 활용될 것이다. 다양한 ID의 사용은 새로운 보안 취약점으로 활용될 것이며, 현실 세계와 디지털 세계가 상호작용함에 따라 이전의 보안 위협들이 확장되어 새로운 침해 사례가 발생할 것이다. 이에, 메타버스의 발전에 따라 발생할 수 있는 ID 관련 보안 이슈를 새롭게 정리한다.

3.2. ID 관련 보안 이슈

메타버스에서의 ID는 진화에 따라 다양해지고 있으며, ID 관리의 중요도가 높아지고 있다. 특히, 기존의 개인정보에 대한 유출 문제를 시작으로 사회적 연결 공격, 디지털 세계를 통한 현실 세계에서의 물리적 공격 등이 가능하다. 이러한 보안 위협에 대한 다양한 가능성 및 관련 피해 사례를 정리한다.

3.2.1. 디지털 분리 단계에서의 ID 관련 보안 이슈

메타버스의 초기 단계인 디지털 분리에서는 다양한 ID 유출 이슈가 발생하였다. 2006년에는 세컨드라이프(SecondLife)에서 ID를 저장하는 데이터베이스 보안 문제가 발생하였다. 해당 데이터베이스는 '제로-데이 공격(Zero-Day Attack)'으로 인하여 사용자가 해당 서비스에 제공한 이름, 주소 및 신용카드 정보 등이 유출된 사고가 발생하였다[25]. 또한, 다수의 사용자가 이용하는 메타버스 중 하나인 소셜 네트워크 서비스(Social Network Service, SNS)에서도 사용자의 정보가 유출될 수 있다. SNS에서의 피싱 공격으로 인하여 사용자의 개인정보가 유출될 수 있으며, 타인을 사칭하는 위장 공격(Impersonation Attack)을 통해 부분적으로 공개된 정보의 탈취가 가능하다[26]. 이러한 피싱 공격은 온라인 게임의 계정 탈취를 목적으로도 진행되었으며, 이는 유료결제를 통해 이용할 수 있는 서비스에서 공격자가 피해자의 계정을 탈취하여 무료로 이용하고 피해자는 해당 계정을 사용할 수 없는 사례가 발생하였다[27].

이처럼 디지털 분리 단계에서는 ID 저장 데이터베이스에 대한 공격을 통해 개인정보를 탈취하거나, 위장 공격을 통해 피해자로 둔갑하여 다른 사용자들의 정보를 수집, 또는 피해자의 서비스를 대신 이용하는 등의 다양한 보안 이슈가 발생하였다.

3.2.2. 디지털 상호작용 단계에서의 ID 관련 보안 이슈

메타버스의 발전으로 인해 높은 몰입감을 제공하고 현실 세계와 디지털 세계의 상호작용이 가능한 상호작용 단계의 보안 이슈는 현재의 메타버스를 통해 유추할 수 있다. 현재의 메타버스는 디지털 분리에서 상호작용으로 발전하는 시기로, 디지털 분리 단계에서의 보안 위협과 함께 새로운 보안 위협이 증가하고 있다.

디지털 상호작용 단계의 메타버스에서는 디지털 세계에서의 화폐가 현실에서의 화폐와 동등한 가치를 가질 것이며, 이는 현재의 다양한 가상화폐 및 NFT를 기반으로 이루어질 것이다. 따라서, 계정 탈취는 다양한 금전적 피해를 발생시킬 것이며, 실제로 지난 2월 NFT 마켓인 Opensea에서는 17명의 사용자 계정 탈취로 인해 약 170만 달러의 피해가 발생하였다[7].

또한, 디지털 상호작용 단계에서의 위장 공격은 기존 분리 단계에서와는 다르게 다양한 웨어러블 디바이스를 활용하여 가능하다. [28]에서는 악의적인 장비를 사용하여 Bluetooth에 접근한 후, 피해자의 메타버스 서비스에 접근 가능함을 증명하였다.

한편, 웨어러블 디바이스를 통해 현실 세계의 사용자에 대한 직접적인 공격이 가능하며, [29]에서는 VR 헤드셋이나 안경을 통해 현실 세계에서의 사용자 위치 추적이 가능함을 증명하였으며, [30]에서는 웨어러블 디바이스인 HTC Vive 및 Oculus Rift를 사용하여 현실 사용자에게 물리적 악영향을 줄 수 있는 Human Joystick Attack을 제안하였다.

높은 몰입감을 제공하기 위해 더욱 다양한 웨어러블 디바이스가 사용될 것으로 예측되는 디지털 상호작용 단계에서는 디바이스에 대한 보안이 매우 중요하다. 특히, 현재 사용되고 있는 지문, 홍채, 얼굴 등의 생체정보는 기존의 id/pw와 같이 자유로운 갱신이 어려우므로 지속적인 악용이 가능하다. 실제 2015년 미국에서는 지문정보 약 560만 건이 유출되는 사건이 발생하였으며, 이는 미국 역사상 파급력이 큰 유출 사건 중 하나로 기록되었다[31]. 이처럼 생체정보는 중요한 개인정보로 판단되고 있으며, 디지털 세계에서 현실 세계로의 감각 피드백이 가능한 메타버스에서는 심박 수, 뇌파 등이 신체 상태 정보의 중요성이 더욱 높아질 것이다. 따라서, 신체의 움직임과 신체 상태 정보를 포함하는 개인정보에 대한 안전한 관리 기술이 필요하다.

그리고, 메타버스의 높은 상호운용성을 위해 아바타를 활용한 사용자의 인증 및 다중 메타버스간의 상호인증은 매우 중요한 기술이며, 이는 메타버스의 경제활동을 보장하기 위해서도 중요하다. 이를 위하여, 현재 블록체인 기반의 메타버스에서는 다중 기관 및 연합에서 ID를 관리하고 인증하는 연합 ID 관리(Federated ID Management)를 적용하기 위해 노력하고 있다. 또한, 경제활동 특성을 위해 블록체인 기반의 메타버스(Decentraland, Cryptovoxels, etc)가 주목받고 있으며, 일부의 메타버스(로블록스, 포트나이트 등)에서는 디지털 세계에서의 화폐를 위해 블록체인 기술을 적용하고 있다. 하지만, 이러한 블록체인 기반의 게임은 보안 위협이 존재하며, 실제로 지난 3월 블록체인 게임 '액시 인피티니'는 약 6억 2천만 달러의 피해가 발생하였다[32].

디지털 상호작용 단계의 메타버스로 발전하기 위해서는 현재 메타버스의 보안 침해 사례를 기반으로 전자지갑 등의 안전한 ID 관리 및 경제활동을 보장할 수 있는 기술개발이 선행되어야 한다.

3.2.3. 초현실 단계에서의 ID 관련 보안 이슈

초현실 단계의 메타버스는 현실과 가상의 경계가 없는 세계가 될 것으로 예상할 수 있다. 2.2에서 정의한 것처럼, 영화 '써로게이트' 및 '아바타'가 초현실 단계의 메타버스와 가장 유사할 것이다. 현재의 메타버스 단계에서는 초현실 단계에서의 메타버스를 구체적으로 설계할 수 없다. 그러나, '아바타'의 '링크룸'과 같이 사람의 생각만으로 기계 및 디지털 세계의 아바타를 조종할 수 있는 고도화된 웨어러블 디바이스의 사용을 예상할 수 있으며, 이때 디지털 세계에서의 ID는 현실 세계에서의 ID와 동일한 가치를 가질 것이다. 따라서, 현재 단계에서 예측하기 어려운 다양한 ID 관련 위협들이 발생할 것이며, 이에 대한 대응 기술 연구가 지속되어야 한다.

〔표 2〕 현재 메타버스의 ID 관리 기술 현황

분류	관련 자료			
보안 위협	신원 유출 [7]	위장 공격 [28-30]	생체정보 관리 [31]	상호 인증 [32]
대응 기술	생체기반 인증 [34]	웨어러블 디바이스 인증 [33,35]	데이터 프라이버시 보호 기술 [35,40]	새로운 PKI [41,42]

3.3. 대응 기술

3.2에서는 메타버스의 진화 단계에 따라 발생한 보안 이슈 및 발생 가능한 보안 위협에 대해 정리하였다. 이에, 이번 장에서는 현재의 메타버스 및 향후 상호작용 단계의 메타버스에서 발생 가능한 보안 위협에 대한 대응 기술을 분석한다.

먼저, 높은 몰입감을 제공하기 위하여 메타버스에서는 다양한 웨어러블 디바이스의 사용이 필수적이다. 이러한 웨어러블 디바이스는 사용자의 생체정보를 포함한 개인정보를 수집하여 디지털 세계로 반영하고, 디지털 세계에서의 감각을 현실 세계로 피드백하는 다리 역할을 한다. 또한, 웨어러블 디바이스는 사용자의 인증 수단으로 사용될 수 있다. 따라서, 이러한 인증 기술은 계정 탈취 위협으로부터 안전한 메타버스 활용을 가능하게 한다. [33]에서는 클라우드 기반의 웨어러블 디바이스의 인증 기법을 제안하였다. 디바이스 간의 인증을 통해 세션 키를 생성하여 지속적인 사용이 가능하지만, 사용자의 몰입감을 고려하지 않은 문제점이 존재한다. 또한, [34]에서는 사용자의 광혈류측정(Photoplethysmogram, PPG) 센서를 사용하여 인증하는 기술을 제안하였다. 이는 심장 박동에 따라 변화하는 혈류를 생체정보로 활용하는 인증 기술로, 사용자의 움직임으로 인해 발생할 수 있는 혈류측정의 오류를 최소화하였다.

이러한 웨어러블 디바이스의 사용 중, 사용자의 중요한 생체정보 및 위치 정보를 포함한 개인정보가 유출될 가능성이 높다. 이러한 개인정보는 위장 공격으로 인한 피해가 발생할 수 있으며, 더 나아가 사용자에게 물리적인 공격을 가능하게 한다. [35]에서는 이러한 데이터 프라이버시 문제를 해결함과 동시에 웨어러블 디바이스에 대한 인증을 수행하는 기술을 새롭게 제안하였다. 해당 논문에서는 두 가지 환경을 고려하였으며, 첫 번째 공간 기반의 엣지 컴퓨팅 모드에서는 Secret Sharing(SS)과 MinHash 기반의 인증 기술을 사용하여 개인의 민감한 정보가 공개되지 않은 상태에서 디바이스를 통한 인증을 수행하였다. 그리고 시간 인식 클라우드 컴퓨팅 모드에서는 암호문의 속성 기반 암호화(Ciphertext-policy attributed-based encryption, CP-ABE)[36]과 블룸필터(Bloomfilter)를 사용하여 개인정보가 노출되지 않는 효율적인 데이터 구조를 구성하여 개인의 인증을 수행하였다. [37]에서는 데이터 프라이버시를 보존하면서 데이터의 효율적인 활용이 가능한 차분 프라이버시(Differential Privacy, DP)[38] 중 하나인 로컬 차분 프라이버시(Local DP)[39]를 사용하였다. 특히, 그래프 기반의 로컬 차분 프라이버시(Graph-based LDP)를 사용하여 개인의 정보는 숨기고 고품질의 서비스를 이용할 수 있는 시스템을 설계하였다. 또한, [40]에서는 가장 기본적으로 사용되는 얼굴 정보에 대한 안전한 데이터 공유 기술을 제안하였다. 현재도 사용되고 있는 카메라를 활용한 다양한 메타버스 서비스에서 사용자의 얼굴은 중요한 정보이며, 동시에 사용자가 아닌 제 3자의 얼굴 공유는 프라이버시 침해이다. 이에, 사용자와 비사용자에 대한 개인화된 얼굴인식 기술을 제안하였으며, 해당 기술은 분산 합의 방법을 사용하여 안전한 데이터 공유를 가능하게 한다.

3.2에서 언급한 바와 같이, 현실과 가상의 경계가 점점 사라짐에 따라 현실에서의 신분증과 유사한 디지털 세계에서의 전자지갑에 대한 중요성은 계속 높아질 것이다. 또한, 메타버스에서의 전자지갑은 메타버스의 특성(상호운용성, 경제활동, 확장성)을 만족하기 위해 중앙화된 PKI(Public Key Infrastructure)가 아닌 탈중앙화된 형태로 이루어질 가능성이 크다. 이에, [41,42]에서는 이러한 메타버스 간의 상호인증이 가능한 인증서를 제안하였다. 먼저, [41]에서는 메타버스의 상호운용성을 높이기 위해 다양한 도메인에서의 상호인증이 가능한 XAuth를 제안하였다. 기존의 PKI는 다양한 도메인 상에서의 활용이 제한적이며, 블록체인의 분산 합의(Distributed Consensus)가 이러한 문제를 해결할 수 있는 방안으로 제시되었다. 하지만, 기존의 블록체인 방식은 해결 불가능한 문제가 존재하며, 해당 논문에서는 PKI의 저장소와 제어 계층을 분리하여 기존의 PKI 및 CT(Certificate Transparency) 시스템과 호환이 가능한 기술을 제안하였다. 이는 영지식 증명(Zero-Knowledge

Proof, ZKP)를 사용하여 프라이버시 보호가 가능하다. 또한, 기존의 PKI가 제공하였던 2가지 특성인 ID의 정확한 등록(Accurate registration)과 신원유지(Identity Retention)를 달성하기 위해 [42]에서는 탈중앙화된 PKI를 새롭게 제안하였다. 해당 기술은 다양한 탈중앙화된 모델이 만족하기 어려운 신원유지 제공하기 위해 Certcoin을 제시하였으며, 기존의 PKI와 유사한 구조를 갖는 특징이 있다. 하지만, XAuth 및 Certcoin 모두 큰 규모의 현실 서비스에서 적용하는 것은 여전히 한계가 존재한다.

Ⅳ. 결 론

현재의 메타버스는 기존의 다양한 온라인 서비스를 포함하는 현실 세계를 초월한 디지털 세계로 정의할 수 있다. 이러한 메타버스는 현실과 가상의 경계가 없어지는 형태로 발전하고 있으며, 동시에 보안 침해에 대한 우려가 증가하고 있다. 이러한 메타버스에서의 보안 문제는 다양한 주제로 분석되고 있지만, 현재의 메타버스가 아닌 앞으로 다가올 메타버스를 고려하고 있다. 이처럼 메타버스를 바라보는 시점의 차이로 인하여 괴리감이 발생할 수 있으며, 이를 보완하기 위해 본 논문에서는 메타버스의 진화 과정에 따른 ID 관리 기술에 대한 현황을 정리하였다. 먼저, 메타버스의 현주소와 미래를 확인하기 위해 현실과 디지털 세계의 영향력을 기준으로 메타버스의 진화를 3단계로 구분하였다. 또한, 각각의 단계에서 발생하였거나, 발생할 수 있는 ID 관련 위협을 정리하고, 이에 대한 대응 기술을 분석하였다.

메타버스의 ID 관리 기술은 메타버스의 발전에 따라, 핵심이 되는 웨어러블 디바이스, 블록체인 등의 기술 개발과 함께 ID 관리 기술에 관한 활발한 연구가 필요하다.

참 고 문 헌

[1] Jeong, Soo Yong, et al. “확장된 가상현실인 메타버스에서의 보안 위협 분석.” Review of KIISC 31.6 (2021): 47-57.

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

[3] Han, Jinsoo, et al. “User-friendly home automation based on 3D virtual world.” IEEE Transactions on consumer electronics 56.3 (2010): 1843-1847.

[4] Dionisio, John David N., William G. Burns III, and Richard Gilbert. “3D virtual worlds and the metaverse: Current status and future possibilities.” ACM Computing Surveys (CSUR) 45.3 (2013): 1-38.

[5] Lee, Lik-Hang, et al. “All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda.” arXiv preprint arXiv:2110.05352 (2021).

[6] Di Pietro, Roberto, and Stefano Cresci. “Metaverse: Security and Privacy Issues.” 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2021.

[7] Wang, Yuntao, et al. “A survey on metaverse: Fundamentals, security, and privacy.” arXiv preprint arXiv:2203.02662 (2022).

[8] Meier, Manuel, et al. “TapID: Rapid touch interaction in virtual reality using wearable sensing.” 2021 IEEE Virtual Reality and 3D User Interfaces (VR). IEEE, 2021.

[9] Lee, Lik Hang, et al. “Hibey: Hide the keyboard in augmented reality.” 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom. IEEE, 2019.

[10] Hartmann, Jeremy, Yen-Ting Yeh, and Daniel Vogel. “AAR: Augmenting a wearable augmented reality display with an actuated head-mounted projector.” Proceedings of the 33rd Annual ACM Symposium on User Interface Software and Technology. 2020.

[11] Zhao, Ruoyu, et al. “Metaverse: Security and Privacy Concerns.” arXiv preprint arXiv: 2203.03854 (2022).

[12] Far, Saeed Banaeian, and Azadeh Imani Rad. “Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges.” Journal of Metaverse 2.1 (2022): 8-16.

[13] Giaretta, Alberto. “Security and Privacy in Virtual

Reality－A Literature Survey.” arXiv preprint arXiv:2205.00208 (2022).

[14] 닐 스티븐슨, 김장환 역, 『스노우 크래쉬』, 새와 물고기, 1996

[15] Yang, Qinglin, et al. “Fusing blockchain and AI with metaverse: A survey.” IEEE Open Journal of the Computer Society (2022).

[16] Huynh-The, Thien, et al. “Artificial Intelligence for the Metaverse: A Survey.” arXiv preprint arXiv:2202.10336 (2022).

[17] Park, Sebeom, Shokhrukh Bokijonov, and Yosoon Choi. “Review of microsoft hololens applications over the past five years.” Applied Sciences 11.16 (2021): 7259.

[18] Zuckerberg, Mark, and Gayle King. “Facebook launches” Horizon Workrooms. “Here's how it works.” (2021).

[19] Ning, Huansheng, et al. “A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges.” arXiv preprint arXiv:2111.09673 (2021).

[20] Park, Sang-Min, and Young-Gab Kim. “A Metaverse: Taxonomy, components, applications, and open challenges.” Ieee Access 10 (2022): 4209-4251.

[21] Zhernova, Ksenia, and Andrey Chechulin. “Overview of vulnerabilities of decision support interfaces based on virtual and augmented reality technologies.” International Conference on Intelligent Information Technologies for Industry. Springer, Cham, 2021.

[22] Kilger, Fabian, et al. “Detecting and Preventing Faked Mixed Reality.” 2021 IEEE 4th International Conference on Multimedia Information Processing and Retrieval (MIPR). IEEE, 2021.

[23] Happa, Jassim, Mashhuda Glencross, and Anthony Steed. “Cyber security threats and challenges in collaborative mixed-reality.” Frontiers in ICT 6 (2019): 5.

[24] XR Safety Initiative. “The XRSI Privacy Framework version 1.0.” 0) (2020).

[25] 데이터넷관리자, “개인정보 유출 위해 데스크톱 노린 공격 심화”, IT정보마당 데이터넷, 2006.11.24.

[26] 고준영, and 이근호. “M2M 환경에서의 SNS 개인정보 유출 위협 및 대응방안.” 한국융합학회논문지 5.1 (2014): 29-34.

[27] “악성코드는 ‘디아블로3’를 타고?..게임계정 탈취 급증”, 아주경제, 2012.07.15.

[28] Antonioli, Daniele, Nils Ole Tippenhauer, and Kasper Rasmussen. “BIAS: bluetooth impersonation attacks.” 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020.

[29] Shang, Jiacheng, et al. “ARSpy: Breaking location-based multi-player augmented reality application for user location tracking.” IEEE Transactions on Mobile Computing (2020).

[30] Casey, Peter, Ibrahim Baggili, and Ananya Yarramreddy. “Immersive virtual reality attacks and the human joystick.” IEEE Transactions on Dependable and Secure Computing 18.2 (2019): 550-562.

[31] 금융보안원 보안연구부 보안기술팀, “바이오정보 사고사례 및 대응방안 조사”, 금융보안원, 2016.03.04.

[32] 정성호, “인기 블록체인 게임서 대규모 해킹...7천500억원 상당 탈취”, 연합뉴스, 2022.03.30.

[33] Srinivas, Jangirala, et al. “Cloud centric authentication for wearable healthcare monitoring system.” IEEE Transactions on Dependable and Secure Computing 17.5 (2018): 942-956.

[34] Zhao, Tianming, et al. “Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics.” IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020.

[35] Liu, Hong, et al. “Cooperative privacy preservation for wearable devices in hybrid computing-based smart health.” IEEE Internet of Things Journal 6.2 (2018): 1352-1362.

[36] Bethencourt, John, Amit Sahai, and Brent Waters. “Ciphertext-policy attribute-based encryption.” 2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007.

[37] Wei, Jianhao, et al. “LDP-based social content protection for trending topic recommendation.” IEEE Internet of Things Journal 8.6 (2020): 4353-4372.

[38] Dwork, Cynthia, et al. “Calibrating noise to sensitivity in private data analysis.” Theory of cryptography conference. Springer, Berlin, Heidelberg, 2006.

[39] Erlingsson, Úlfar, Vasyl Pihur, and Aleksandra Korolova. “Rappor: Randomized aggregatable privacy-preserving ordinal response.” Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. 2014.

[40] Xu, Kaihe, et al. “My privacy my decision: Control of photo sharing on online social networks.” IEEE Transactions on Dependable and Secure Computing 14.2 (2015): 199-210.

[41] Chen, Jing, et al. “XAuth: Efficient privacy-preserving cross-domain authentication.” IEEE Transactions on Dependable and Secure Computing (2021).

[42] Fromknecht, Conner, Dragos Velicanu, and Sophia Yakoubov. “A decentralized public key infrastructure with identity retention.” Cryptology ePrint Archive (2014).

〈저 자 소 개〉

정 수 용 (Soo Yong Jeong)

학생회원

2018년 2월 : 공주대학교 응용수학과 학사

2020년 2월 : 공주대학교 융합과학과 석사

2020년 3월~현재 : 공주대학교 융합과학과 박사과정

<관심분야> 데이터 보안, 인공지능, 신경망 암호 기술, 메타버스 보안

서 창 호 (Chang Ho Seo)

종신회원

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, 메타버스 보안 등

조 진 만 (in-Man CHO)

종신회원

1989년 2월 : 충남대학교 계산통계학과 학사

1991년 2월 : 충남대학교 전산학과 이학석사

1991년 2월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원

<관심분야> 개인정보보호, 스마트카드, 사용자 인증, 메타버스 보안

진 승 헌 (Seung-Hun Jin)

종신회원

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, 핀테크보안, 메타버스 보안

김 수 형 (Soo Hyung Kim)

종신회원

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, 메타버스 보안 등