https://doi.org/10.33778/kcsa.2023.23.4.003

메타버스 환경에서 Data Preprocessing 기능을 개선한 Trust-based Decentralized User Authentication 시스템 설계 및 개발 연구★

박 수 완*, 이 상 민*, 김 경 진**

요 약

비대면 서비스의 확산과 원격근무 등의 생활이 일상화되면서 메타버스의 이용자가 급증하였으며, 세컨드 라이프를 위한 금융, 부동산 등 자산 실거래로써 사람들의 생활반경이 자연스럽게 확대되고 있다. 하지만 실세계에서와 같이 경제 활동을 자유롭게 하기에는 전혀 다른 쟁점의 보안 이슈들이 발생할 수 있으며, 기존의 사이버 공간과 비교해도 완전히 새로운 유형의 문제들이 발생할 가능성이 크다. 본 논문에서는 이러한 문제를 해결하기 위해 인증 및 프라이버시를 중점으로 방안을 제안한다. 메타버스에서 수집되는 데이터의 특수성에 기반하여 데이터 전처리 기능을 개선하고, W3C의 DID의 표준 방식을 준수하는 가운데 NFT를 활용한 메타버스 내 새로운 인증 서비스를 정의하며, 이에 대한 시스템 설계 및 개발 방안을 제시한다. 제안한 시스템은 하이퍼레저 인디 블록체인을 활용하여 구현하고, 결과를 분석하여 본 연구의 적용 가능성 및 우수성을 검증한다.

Design and Development Study of a Trust-based Decentralized User Authentication System with Enhanced Data Preprocessing Functionality in a Metaverse Environment

Suwan Park*, Sangmin Lee*, Kyoungjin Kim**

ABSTRACT

As remote services and remote work become commonplace, the use of the Metaverse has grown. This allows transactions like real estate and finance in virtual Second Life. However, conducting economic activities in the Metaverse presents unique security challenges compared to the physical world and conventional cyberspace. To address these, the paper proposes solutions centered on authentication and privacy. It suggests improving data preprocessing based on Metaverse data's uniqueness and introduces a new authentication service using NFTs while adhering to W3C's DID framework. The system is implemented using Hyperledger Indy blockchain, and its success is confirmed through implementation analysis.

Key words : Metaverse, DID, Privacy, NFT

접수일(2023년 08월 31일), 게재확정일(2023년 09월 26일)

★ 본 논문은 2023년도 성신여자대학교 학술연구조성비 지원에 의하여 연구되었음.

★ 본 논문은 금융보안원·금융정보보호협의회·금융보안포럼이 주최한 「제6회 금융보안원 논문공모전」에서 우수논문으로 선정된 논문을 수정 보완한 논문임.

* SK쉴더스(공동저자)

* SK쉴더스(공동저자)

** 성신여자대학교/융합보안공학과(교신저자)

1. 서 론

코로나19로 비대면과 온라인 서비스가 빠르게 확산되면서 메타버스(Metaverse)의 이용자가 급증하였으며, 현재까지도 지속적으로 증가하고 있다.[1] 보고서 분석에 따르면, 2021년 말 기준 메타버스 내 가상자산 거래 규모는 약 68조7000억원으로, 향후 2030년에 수수료 수익 규모는 약 8조2500억원에 달할 것으로 전망하고 있다.[2] 즉, 이는 다양한 산업 분야에 영향을 끼치며 메타버스 내 신규 서비스를 개발하고 수익을 창출하기 위한 수단으로써 주목하고 있다.[3,4] 최근 JP모건에서 메타버스 플랫폼으로 개설된 '오닉스(ONYX) 라운지'[5] 역시 전통적인 글로벌 금융회사가 메타버스를 활용하여 사용자에게 혜택 폭을 확장하고 있음을 알 수 있다. 한국 기업에서도 메타버스 플랫폼에서 임원진 미팅[6]이나 가상 캠퍼스[7] 등을 추진하거나, 직접 자체 메타버스 플랫폼[8]을 개발하여 금융, 부동산 등 시스템과 직접 연계 가능할 수 있도록 하고 있다. 이처럼 다양한 산업 분야에서 메타버스로 경쟁력을 갖추며 가상현실 시스템 구축에 속도를 올리고 있다.

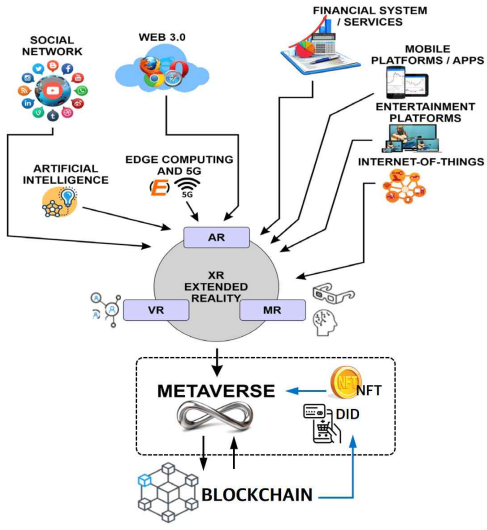
메타버스라는 새로운 형태의 공간에서 서비스의 변화는 필수적으로 뒤따른다. 이러한 패러다임 변화 시기에 가장 우려되는 것이 프라이버시와 보안이다. 메타버스의 주요 기술이라 할 수 있는 가상현실(VR, Virtual Reality)과 증강현실(AR, Augmented Reality)은 HMD(Head Mounted Display)의 사용자 화면에서 중요정보를 캡쳐하거나 주민등록증 및 신용카드 유출 위험성이 있으며 인증, 결제 등을 통한 해킹 가능성이 높다. 특히나 VR의 경우 가상현실 내 아바타를 통해 금융정보나 개인정보 탈취 가능성이 존재하며, 소유자에 대한 프라이버시 권리는 제공하지 않는다.[9] 메타버스가 초연결 플랫폼으로 주목받고 있지만, 이에 대한 보안성 강화 연구가 필요한 실정이다.

아직 메타버스 점포에 대해 신뢰 기반의 정형화된 모델은 없다. 본 논문은 이에 주목하여 Web 3.0 기반으로 W3C의 DID(Decentralized Identity) 표준 방식을 준수하는 메타버스 내 새로운 인증 모델을 정의하고, 사용자 데이터 및 가상자산의 신뢰성을 보장하기 위한 NFT(Non-Fungible Token)를 활용하여 기술적 방안인 TDUA(Trust-based Decentralized User Authentication) 시스템을 제안한다. 메타버스 내 적용할 수 있는 서비스 시나리오를 구성하고, 이를 기반으로 개발 및 성능 평가를 수행함으로써 제안한 모델의 실 활용성을 검증한다. 본 연구를 통해 메타버스 환경에서 안전한 인증 및 프라이버시 보호가 향상된 환경을 제공하고자 한다.

2. 관련 연구

2.1 메타버스 보안을 위한 관련 기술

메타버스는 가상공간에서 서비스 제공받는 것을 넘어 물리적인 현실 세계의 활동을 가상세계로 확장하며, 시공간에 제약을 받지 않고 다양한 산업 분야에서 새로운 창조적 생태계를 선도할 수 있게 되었다. 본 논문에서는 탈중앙화된 온라인 네트워크 구축을 목표로 하는 Web 3.0을 기반으로 DID 인증 기술 및 자산의 안전한 디지털화를 실현할 NFT를 이용하여 메타버스 내 안전한 서비스를 제공한다.[10]



(그림 1) The technology ecosystem enabling the metaverse (출처 : https://www.mdpi.com/2079-9292/12/2/391 그림 수정)

2.1.1 Web 3.0

기존 Web 2.0은 한 플랫폼을 통해 다른 사용자와 콘텐츠 및 데이터를 주고받음으로써, 구글, 아마존과 같은 대기업들은 중앙화 서버에 데이터를 수집하였다. 이러한 환경에서 사용자는 데이터를 직접 저장, 제어 및 관리하기 어려운 구조가 되었고, 웹에 존재하는 모든 데이터는 중앙 플랫폼이 통제하는 이슈가 발생하였다.

Web 3.0은 이러한 인터넷 생태계의 가장 중요한 문제를 극복하기 위해 구상되었다.[11] 사용자가 생성한 데이터, 정보, 콘텐츠 등의 권리를 플랫폼에 맡기지 않고 사용자가 가져오는 것이다. 즉, 정보의 투명성과 함께 웹상에서 발생하는 데이터를 사용자가 소유(own)하고 직접 관리하는 것이다. 그래서 Web 3.0을 기반으로 만들어지는 새로운 프로토콜은 블록체인 기술을 통해 실현할 가능성이 높다.[12] 블록체인은 중앙 집중화를 벗어나 분산된 소규모 단위로 자율적으로 운영되어 자연스레 Web 3.0이 추구하는 탈중앙화 기반 기술의 접근이 가능하다.

현재의 Web 3.0은 가상 자산과 NFT, 메타버스, AI 기반의 초개인화된 인터넷 환경 등 최신 IT 기술들이 결합된 탈중앙형의 새로운 공간웹 생태계를 제시한다. 본 연구에서는 Web 3.0 기반의 최신 기술을 결합하여 탈중앙화를 구현할 수 있는 안전한 메타버스 플랫폼을 제안하고자 한다.

2.1.2 DID(Decentralized Identifier)

DID[13]는 탈중앙화된 디지털 신원증명체계를 의미한다. 중앙 등록 메커니즘 없이 신뢰 분산 프레임워크 하에서 활용되며 정보 주체가 스스로 신원에 대한 증명 관리와 신원정보 제출 범위 및 제출 대상을 통제할 수 있는 기술이다. DID 문서는 개인정보가 포함되어 있지 않고 문서의 위치만을 나타내어 인증만을 위해 활용되며 블록체인과 같은 분산원장에 저장되어 위변조가 불가능하다. 본 연구에서는 W3C에서 공표한 Decentralized Identifiers v1.0을 참조하여 메타버스 내 분산 ID를 이용해 사용자에게 디지털 신원증명 발급 및 서비스 제공을 수행한다.

2.1.3 NFT(Non-Fungible Token)

NFT[14]는 대체 불가능 토큰으로 디지털 콘텐츠에 자체적인 고유값을 부여하고 각각의 토큰은 콘텐츠에 대한 증명서 역할을 한다. 부여된 고유한 값을 통해 사용자의 유일성과 희소성을 나타낼 수 있어 권리 보호 측면에서 콘텐츠 보호 방안으로 활용할 수 있다.

또한, 블록체인에 기록하는 특징을 갖고 있어서 데이터는 해킹을 통한 위변조가 거의 불가능하다. NFT는 대부분의 디지털 객체를 토큰화할 수 있는 이점을 기반으로, 본 논문에서는 메타버스 내 디지털 데이터 및 자산을 NFT로 토큰화하여 활용함으로써 사용자들에게 소유권을 부여할 수 있다. 더불어 메타버스 내에서 또한 특정한 자산을 고유하고 영속적으로 증명하는 도구로 사용되며, 이러한 기술을 활용해 기존의 전자 서명보다 안전한 시스템을 구축하는 것을 목표로 한다.

2.2 선행연구 조사 분석

최근 메타버스 기술이 화두에 오르면서, 다양한 연구가 진행되고 있다. 이러한 최신의 기술 도입 단계에서 더욱 발전하기 위해서는 보안은 필수적으로 충족되어야 하는 요소이다.

R.D. Pietro and S. Cresci[15]와 B. Falchuk 외 2[16]에서는 메타버스 내 발생 가능한 보안 이슈에 대해 논의했다. 물리적 제약이 없는 가상환경에서 동작하는 메타버스의 특성에 따라 플랫폼 내부에서 수집되는 데이터가 다양한 형태로 이동할 수 있고 사용자의 프라이버시 유출로 이어질 수 있음을 언급하고 있다. 정수용 외 4[17]은 헤드마운티드 디스플레이, 카메라 등의 다양한 입·출력 장치 등을 활용하는 메타버스 환경에서 디바이스 관련 인증 수단이 필요함을 주장했다. 디바이스를 활용한 메타버스 서비스는 기존의 웹 서비스들과 달리, 장비에 부착된 마이크, 카메라 등을 통한 도촬 및 도청 가능성과 장비 해킹을 통해 뇌의 자극이나 환각을 주입하는 등 디바이스를 통해 전

달하는 현실성은 사용자의 일상생활 속에 직접적인 영향을 끼친다. 특히 전자 상거래가 가능한 메타버스에서는 가상세계 내 창작물이나 소유물을 이용자 간 거래를 통해 현실 세계에서 금전적 이윤을 실현할 수 있어 이에 따른 개인 금융 자산에 영향이 존재한다. 이는 메타버스 내 금융 플랫폼에서 디바이스 활용 시 다양한 보안 위협의 발생 위험성을 시사한다.

특히 실 금융 거래가 가능한 메타버스 내 금융 서비스 보안 위협을 주제로 논의한 유수경 등[18]의 연구에서는 현재 메타버스 내 금융 서비스 사용 시 신원 증명하는 보안 및 인증 절차 등이 미흡한 상태임을 주장했다. 특히 메타버스 내에서 금융 서비스 이용 시 일어날 수 있는 보안 위협을 최소화하기 위한 디지털 멀티 통합인증과 제로 트러스트 기반으로의 시스템 구축에 대한 필요성을 언급하였다.

그 외에 메타버스 내 보안에 관한 연구로는 보안 위협 대비 이해관계자들 관점에서 대안을 마련한 나현식 외 1[19], 법적 보호방안 관점에서 연구한 이준형 외 1[20], 메타버스 서비스를 위해 보안 모델을 제시한 조도은[21] 연구 등이 있다.

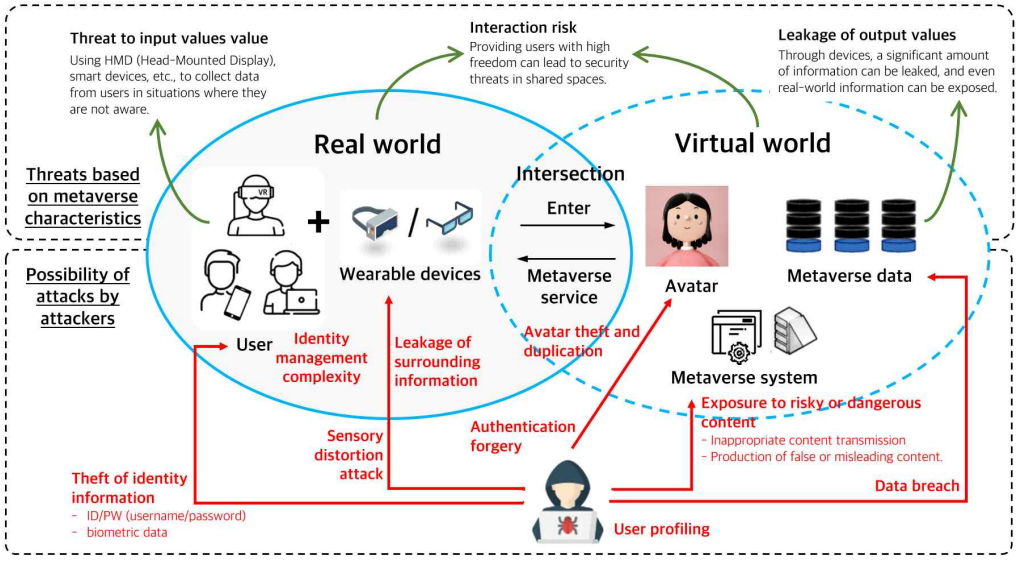
이처럼 선행연구들은 메타버스 기술 적용 시 보안의 필요성을 시사하며 대안을 제시하고 있다. 하지만, 대부분은 메타버스의 포괄적인 보안 이슈로 언급하고 있고 구체적인 보안대책에 관한 실증연구가 미흡한 실정이다. [18] 연구 역시 실제 메타버스 환경에서 금융 서비스를 이용하는데 보안 위협 대비 현실적인 개선안을 제시하는 데 있어 한계가 있다.

이처럼 메타버스에 대한 보안 이슈를 다루는 연구가 늘어나고 있지만, 다수의 선행연구는 메타버스의 제도적인 측면 또는 포괄적인 보안 이슈와 보안성을 강화하는 연구의 필요성만을 언급만을 언급하고 있다. 따라서 민감정보를 이용할 수 있는 메타버스 플랫폼 내에서 현실 세계와 유사한 서비스를 제공할 시 사용자 인증 및 보안성 강화에 대한 실증적 연구가 필요하다. 따라서 본 연구는 메타버스 내 신뢰기반의 인증 서비스를 제공하여 안전한 및 활용 방안에 대해 구체적인 방안을 제시한다는 점에서 기존 연구와 차별성을 가진다.

3. 메타버스 내 안전한 인증 서비스를 위한 보안 요구사항

메타버스 내 가상공간에서 활용되는 의류, 신발 등 상품이 실거래가 되며, 실체가 없는 가상 부동산 또한 분양 거래가 되고 있다. 전통적인 기업들도 메타버스 기술의 적극적인 도입을 추진하며 다양한 서비스들이 초기 단계서부터 진행되고 있다. 이는 메타버스에서도 사회적 및 경제적 활동이 가능해짐을 의미하며 실 기업에서 디지털 투자의 확장뿐만 아니라, 외부에서 또한 새로운 파트너십을 도모할 수 있다. 또한, 기업들은 새롭고 젊은 사용자들의 데이터에 즉각적인 흐름을 확인하고 민감하게 수용하고자 메타버스 기술을 적극 활용하고 있다. 디지털이 주류가 된 현재 이용자들은 메타버스에서 즉각적이고 자신의 상황에 맞는 맞춤형 솔루션을 기대하고 있다.

하지만 메타버스와 같은 새로운 환경의 도입은 새로운 보안 문제와 연결된다. 메타버스는 현실과 유사한 활동과 경험을 제공하기 위해 현실의 상태나 움직임을 가상세계에 반영하기 위해 다양한 형태의 데이터와 입출력 장치들을 활용한 시도가 이루어지고 있다. 그러나 사용자에 의해 입력된 데이터와 새로운 데이터로 활용되는 출력 데이터의 보안은 사용자들이 인지하기 어렵다. 예를 들어, 현실 세계에 있는 기존 금융기관들이 메타버스를 통해 서비스를 제공하고 이를 사용자가 이용하기 위해 금융거래에 대한 증명서들을 각각의 금융회사에서 인증하여 접속한다고 했을 때, 기존의 중앙화된 금융 인프라에서 처리되고 있는 데이터들이 메타버스를 통해 사이버 공격으로 침해 및 사고가 발생한다면 실세계에서의 보안 사고보다 훨씬 피해가 확대되어 발생할 수 있다. 중앙화된 구조에서의 보안 사고는 한 명이 아닌 수많은 이용자의 정보가 유출되기에 대량의 피해가 발생할 수 있으며, 사고가 발생한 금융기관은 이용자의 신뢰를 크게 잃는 문제가 발생한다. 즉, 현실 세계와의 동일한 위협은 이용자로 하여금 메타버스 이용에



(그림 2) Security threats and vulnerabilities that can arise within the metaverse

대한 의구심을 들게 하고 이는 메타버스 기술의 발전을 저해시킨다. 발생 가능한 보안 위험에 대해서는 그림 2에 나타낸다.

그림 2와 같이 다양한 침해 사고의 가장 큰 원인은 미흡한 사용자 인증이 될 수 있다. 인증 서비스는 엄밀하게 누구인지를 알 수 있는 '식별(Identification)'과 본인임을 확인하고 권한을 부여받아 서비스에서 활용하는 '인증(Authentication)'으로 구분된다. 현재 온라인에서는 ID/PW를 이용하는 지식기반 인증, 공동인증을 이용하는 소유기반 인증, 휴대폰 본인확인을 통한 기기 기반 인증 등 다양한 방법을 제공하고 있다. 그중에서도 특히 인증기능이 중요한 금융 분야에서는 PC나 휴대폰이 아닌 안전한 금융결제원의 클라우드에 인증서를 보관해 도용 및 분식의 걱정 없이, 언제나 이용할 수 있는 인증 서비스를 금융회사가 이용자에게 제공하며, 이용자들은 손쉽게 온라인에서 서비스를 받고 있다. 이러한 인증기능을 메타버스에 그대로 적용하기에는 이슈사항이 다양하게 존재한다. 메타버스는 HMD, 스마트 디바이스 등을 통해 사용자의 접속이 이뤄지는데 이러한 인터페이스를 통해 신원정보가 캡처되거나 탈취될 수 있으며, VR 및 AR 기반 제품을 착용한 사용자에게 공격자가 조작으로 현실 환경에서의 사용자에게 위협을 가할 수도 있고, 공격자가 악의적인 컨텐츠를 유포하여 사용자에게 공포나 충격을 느끼게 할 수도 있다. 즉, 몰입형 리얼리즘을 추구하는 메타버스로 인해 이러한 위협 요소가 곧 공격자의 공격 도구가 되며 사용자에게 직접적으로 큰 피해를 줄 수가 있다.

본 연구에서는 메타버스 내에서 신뢰 기반의 인증을 통해 사용자가 안전한 서비스를 이용할 수 있도록 방안을 제시하고자 한다. 필요한 보안 요구사항은 다음과 같다.

- **메타버스 특성상 전 세계적으로 통용될 수 있는 표준 인증 서비스 필요** : 메타버스 서비스를 제공하는 기업마다 여러 개의 아바타를 만들어야 하는 과정을 반복해야 하며, 서비스 접속 때마다 매번 불편한 본인인증 방식을 거쳐야 하는 번거로움이 발생하게 된다. 다양한 메타버스 서비스 및 플랫폼만큼 사용자에게는 불편함을 제공하게 된다.
- **VR, AR 등 기기 접속 및 아바타를 활용한 안전한 인증기술** : 기존의 보안체계와는 달리, 메타버스 서비스 자체가 VR 및 AR 단말기나 새로운 기기장치로 접속해 서비스가 진행되는 것들이 많으므로 입력장치에 해당하

는 안전한 인증기술을 제공해야 한다. 또한, 아바타를 통해 가상공간에서 모든 활동을 진행하는 메타버스 특성상 확실한 사용자 신원 인증이 필요하다.

- **개인 데이터의 소유권 보장을 위한 탈중앙화 인프라** : 메타버스 시스템 구조는 빅데이터와 클라우드 등 융합된 새로운 구조로 메타버스 서비스가 만들어지는 것들이 많기 때문에 기존의 중앙 집중식 인프라 구조가 적합하지 않다. 새로운 구조뿐만 아니라 프라이버시 및 데이터 보안 문제를 해결하기 위해 중앙화를 벗어난 탈중앙화 구조를 적용함으로써 사용자에게 개방형 소유권을 보장하며 보안체계 변화를 요구한다.

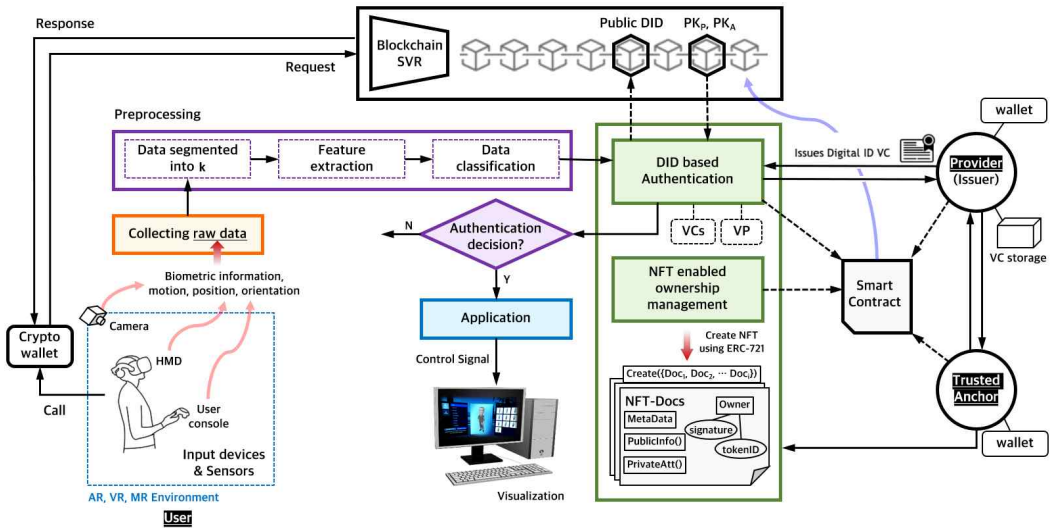
메타버스는 결국 실제 세상과 가상공간을 구분하기 어려운 형태로 변화해 나갈 것이다. 메타버스의 발전을 위해서는 기업 및 정부의 협력을 통해 선제적으로 신뢰 기반의 보안 기술 및 서비스를 개발해 나갈 필요가 있다. 본 연구는 보안 요구사항이 적용된 기법을 제안한다.

4. TDUA(Trust-based Decentralized User Authentication) 시스템

본 연구에서 제안하는 TDUA 시스템은 메타버스 서비스를 이용하기 위해 입력장치 등을 통해 신뢰 기반의 인증을 거쳐 접속할 수 있다. 본 절에서는 전반적인 아키텍처를 기반으로 메타버스 내 Web 3.0을 활용한 인증 서비스가 어떻게 구성되는지를 알아본다. 3개의 참여 주체가 있으며, User(사용자), Provider(메타버스 서비스 제공자), Trusted Anchor(신뢰 기반의 주체)이다.

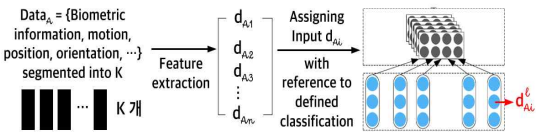
A라는 사용자가 접속하고 있다면 $User_A$라고 정의하며, $User_A$에게 수집되는 데이터들은 텍스트뿐만 아니라 생체정보, 모션, 위치 등 다양하게 수집될 수 있다. 이러한 정보는 $Data_A$라고 정의한다. Crypto wallet은 암호화된 전자지갑으로 메타버스 내 User agent라 할 수 있으며 사용자의 소유이다. $User_A$의 전자지갑으로 $Wallet_{U_A}$라고 한다. $Wallet_{U_A}$에는 사용자의 Secret key인 sk_A가 있으며 Public key PK_A에 의해 만들어진 개인키로 sk_A와 PK_A는 한 쌍으로 이뤄진다. 이는 DID 인증 시 활용된다.

데이터 분할(Data segmented into k)은 수집된 데이터 $Data_A$에 이미지, 위치정보 등 포함되어 있어 데이터를 처리할 수 있게 정보를 분류하여 어떤 정보인지 식별한다. 식별된 데이터는 **데이터 추출(Feature extraction)**에서 분류된 클



(그림 3) The entire diagram of TDUA system

래스에 적합하게 일부를 제거하거나 선택하여 간결해진 유용한 데이터 특징을 추출한다. **데이터 분류(Data classification)**를 통해 수집된 데이터를 정의된 계층적 분류표에 기반하여 개별 레이블을 지정한다. 즉 Preprocessing을 통해 거친 데이터는 아래와 같이 표현할 수 있다.



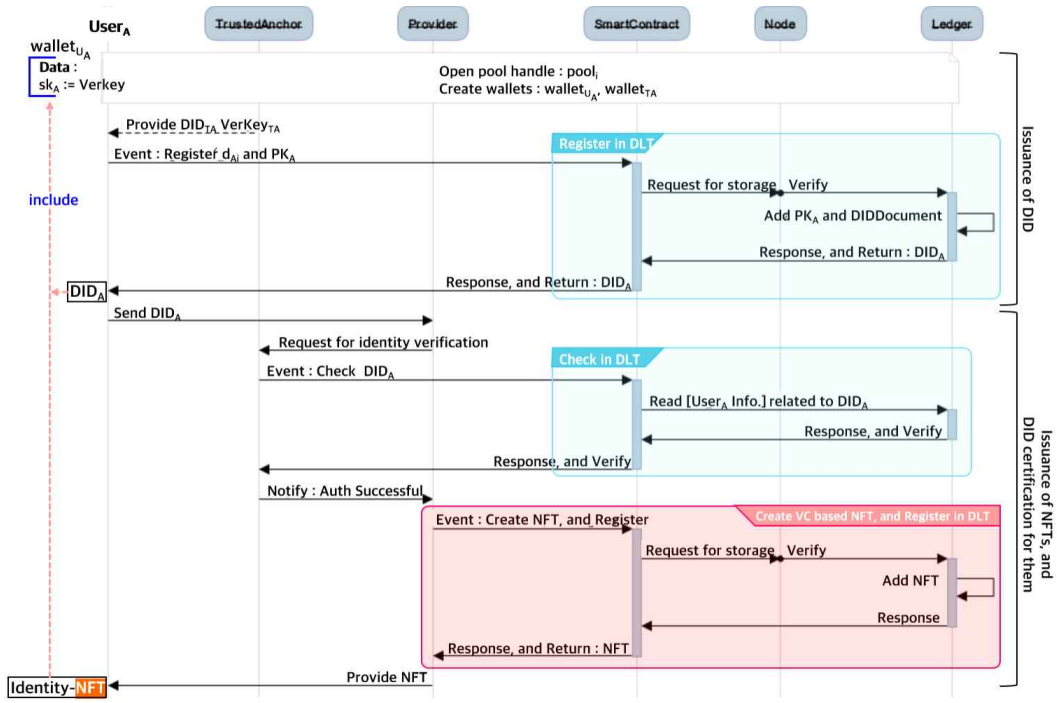
(그림 4) Data preprocessing

메타버스 내 입력장치들을 기반으로 수집한 데이터 d_{Ai}^{l}와 함께 User$_A$의 전자지갑 정보로 인증 과정을 거친다.

4.1 DID 및 NFT 발급

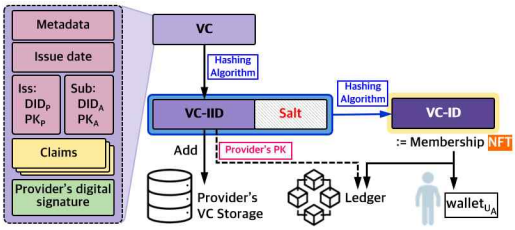
User$_A$는 메타버스 내 Provider의 서비스를 이용하기 위한 VC 발급하기에 앞서 Trusted Anchor를 통해 신원인증을 받고 DID를 발급받아 Wallet$_{U_A}$에 연결한다. DID 내 정의된 VerificationMethod는 DID 소유자 검증을 위한 하나 이상의 공개키 방식을 명시함으로써 sk$_A$는 전자지갑에 보유하고 PK$_A$는 블록체인에 저장하여 안전성을 도모한다. 또한, User$_A$에게 수집한 데이터 d_{Ai}^{l}는 Node들의 검증을 거쳐 DID$_A$ 정보로써 포함되어 텍스트 위주의 정보가 아닌 메타버스의 입력장치를 통해 획득된 정보를 기반으로 DID 인증을 할 수 있게 한다. 발급받은 DID는 해당 메타버스 내에서 현실 세계의 고유식별번호처럼 활용되는 하나의 번호로써, 즉 DID$_A$는 User$_A$의 신원을 증명하는 수단이다.

User$_A$는 메타버스 내 Provider 서비스를 이용하기 위해 회원가입을 진행하고, 가입 결과인 NFT를 발급받아 전자지갑에 보관한다. Provider는 NFT 발급을 위해 Trusted Anchor에게 User$_A$의 DID$_A$를 활용한 검증을 요청한다. User$_A$는 본인의 전자지갑 내 보관된 DID$_A$를 통해 인증을 진행한다. DID$_A$는 DID document의 주소



(그림 5) The issuance process of DID and NFT within the TDUA system

(address)를 가리키고, DID document는 신뢰기관의 DID Storage database와 Ledger에 저장되어 있어, 블록체인에서 관리하는 식별자로 개개인이 자신의 개인정보를 제어할 수 있으며 서명을 통해 자신의 신원을 인증한다. 그리고 Provider는 DID 인증이 완료된 User에게 NFT를 발급한다.



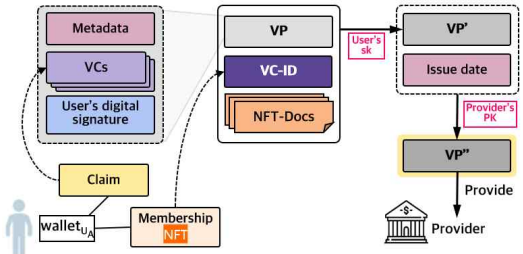
(그림 6) Issuance Method of VC

본 연구에서는 그림과 같이 크레덴셜의 메타데이터(Credential metadata)와 $User_A$가 회원가입 시 입력한 신원정보인 Claim, 데이터를 증명할 수 있는 서명(Digital signature)과 공개키를 포함한 VC(Verifiable Credential) Content로 구성된다. 이를 해싱(hashing)하여 VC-IID를 생성하고 Provider의 VC storage에 저장된다. VC-IID와 함께 Salt를 포함하여 한 번 더 해싱한 결과값을 VC-ID라고 하며, 이는 NFT 형태로 $User_A$에게 발급하여 $Wallet_{U_A}$에 보관되고 {VC-ID, E_{PK_P}[VC-IID]}로 블록체인에 저장된다. 여기서 Salt는 random value로써 Rainbow table 공격 및 Brute-force 공격에 원본이 노출될 확률이 감소된다. 또한, 전체적인 해싱 과정은 악의적인 공격자가 크리덴셜을 탈취했을 때 $User_A$의 정보에 대해 알 수 없게 하고, 해싱의 특성으로 무결성을 보장하여 VC-ID의 변조를 예방한다.

TDUA가 기존의 신원증명 방식과 다른 점은 Provider에 개인정보를 저장해놓는 중앙관리 시스템이 아닌 분산 시스템을 기반으로 User가 Identity를 발급받고 관리한다는 점이다. 그리고 해당 과정에서 본인인증이 필요한 경우 $User_A$는 발급받은 DID_A를 활용하므로 User 입장에서 인증절차가 간소화됨과 동시에 발급받은 NFT로써 블록체인의 특징으로 인한 신뢰성까지 유지할 수 있다.

4.2 인증 과정을 통해 서비스 이용

$User_A$는 메타버스 내 부동산거래, 금융서비스 등 신뢰가 중요한 서비스를 이용하기 위해 현재 오프라인에서 요구하는 것과 유사하게 본인인증 및 각종 증명서와 서류가 필요하다. 본 연구에서는 $User_A$가 메타버스 내 자산 거래를 하는 과정으로 인증 및 검증을 설명한다.



(그림 7) Verification Method of VP

$User_A$는 자산 거래를 위해 필요로 하는 필수 서류를 NFT로 사전 발급받은 후, VC-ID와 사전에 준비된 NFT들로 조합하여 VP(Verifiable Presentation)와 함께 제출한다. 여기서 VP는 크리덴셜로부터 유도 가능한 클레임의 최소 집합체이다. W3C 표준에서는 모든 클레임은 VC에 있으므로 서비스 제공자에게 필요한 정보만 제공하면 되는데 최소한 정보공개를 원칙으로 필요한 정보만을 제공할 수 있도록 VP를 마련하였다. 본 연구에서도 W3C 표준에 의거하여 분산ID 식별자와 메타데이터(Credential metadata), VCs, 데이터를 증명할 수 있는 서명 및 공개키를 포함하는 프레젠테이션을 준수하면서, 서비스의 보안을 위해 확장 필드를 정의하였다. 즉, 추가적으로 $User_A$가 보유한 Identity-NFT 내의 VC-ID를 추출하고, 서비스에서 필수적으로 요구하는 NFT들로 구성되어 있다. VP는 sk_A로 암호화하여 해당 발급날짜와 함께 PK_P로 암호화한 VP"를 생성해 Provider에게 전달한다. 이 과정은 $User_A$가 제출한 VP"를 검증하여 Provider에 가입된 사용자임을 증명한다. 즉, Provider가 VC-ID를 이용해 서비스 이용자로써 유효한지 확인하고, Trusted Anchor에게 $User_A$의 DID_A로 신원검증을 요청함

으로써 강화된 보안 인증체계를 제공한다.

Provider는 DID_A 검증을 통해 VP"를 sk_P로 복호화하여 {VP', Issue date} 데이터를 획득한다. VP'는 $User_A$의 PK_A로 복호화한 후 {VP, VC-ID, NFTs}로 데이터를 획득한다. 여기서 VP 정보를 확인하여 $User_A$의 최소한의 필요정보를 확인한다.

Provider는 획득한 VC-ID로 블록체인에서 확인하여 암호화되어 있는 VC-IID 정보를 획득한다. 이 값이 Provider의 VC Storage에 보유하고 있는 Salt와 해싱하여 결과값이 VC-ID와 일치하는지 검증한다.

이러한 인증 절차를 통해 Provider는 전달받은 VP"로 자신의 sk_P를 이용하여 위변조 여부 및 신원인증을 검증할 수 있으며, $User_A$는 무분별한 개인정보 데이터 사용을 감시하고 신뢰성 있는 거래를 할 수 있다. 또한, User와 관련한 검증을 Trusted Anchor와 Provider, 2번 이상 진행하며 가상 현실인 메타버스에서의 거래이지만 실제 개인의 경제 활동과 연관된 자산 거래인만큼 철저한 인증 과정은 반드시 필요하다.

사용자 검증이 완료되었다면, 실질적인 자산 거래를 위해 Provider는 VP'에서 복호화된 {VP, VC-ID, NFTs}에서 필수 NFT들이 모두 존재하는지 확인하고 각각의 NFT에 기재된 발행일도 확인하여 서비스를 이용할 수 있도록 한다. 이는 자산거래 서비스를 이용할 수 있는 하나의 통합 NFT로 생성하여 $User_A$의 $Wallet_{U_A}$에 보관된다. 이후 자산거래 서비스를 이용할 때 처음과 같은 인증 과정을 거치지 않고 한 번의 접속으로 이용할 수 있으며, 자산거래 서비스와 유사한 업무에 해당하는 것 역시 해당 NFT를 활용하거나 재사용할 수 있도록 하여 증빙을 대체할 수 있다. 이러한 과정은 불필요한 과정의 반복을 줄일 수 있어 효율성이 높고, 발급 시간 또한 단축시킬 수 있다. 간소화된 발급 절차와 안전한 보관으로 $User_A$는 메타버스 내 신뢰성 있는 서비스를 이용할 수 있다.

5. 성능 분석 및 고찰

본 연구에서는 상기 내용을 바탕으로 TDUA 시스템 구현 방법을 살펴보고, 구현한 결과를 분석한다. 기본 인프라는 분산원장 기반의 Hyperledger Indy를 활용하여 탈중앙형 DID 신원 서비스를 구축한다. 여기서 Hyperledger Indy는 신원증명 플랫폼 구조의 블록체인으로써 라이브러리, 도구, 컴포넌트를 제공해준다. 더불어 메타버스 내 이용 환경을 위해 본 연구에서 제안한 Data Preprocessing과 NFT를 구현한다. 리눅스 기반의 블록체인 구동을 위해 Virtual Box와 Docker를 이용하며 구현환경은 다음과 같다.

- □ CPU : Intel core i7-8700 CPU 3.20GHz
- □ OS : Ubuntu 22.10
- □ Memory : 4096 MB
- □ Library : Hyperledger Indy, libsodium, libindy, indy-cli
- □ Number of indy-node : User, TrustedAnchor, Provider, Nodes--consists of didInfo, config, ipport and audit ledger
- □ Smart contract language : Javascript, Java

5.1 메타버스 내 활용 데이터 정의

메타버스 내 현실과 같은 움직임이 가능한 가상현실 서비스를 위해 HMD 등의 입력장치를 이용한다. 사용자의 움직임을 인식하고 메타버스에 전달하기 위한 센서를 물리 객체 센서라고 한다. 즉, 물리 객체 센서는 공간 내 각종 물리 객체의 위치, 속도, 가속도의 정보를 감지하고 이를 메타버스에 전달하는 것으로, 측정 및 수집되는 데이터의 포맷은 ETRI 자료[22]를 참고하였으며, 본 연구에서 재정의하여 다음 표와 같이 설정하였다.

(표 4) Sensor data format for physical objects

Category	Data	Semantics
Credential	PIN	Authentication information(optional)
	pattern or password	Authentication information(optional)
Biometric	fingerprint	User's fingerprint
	voice pattern	User's voice information
	iris	User's iris recognition information

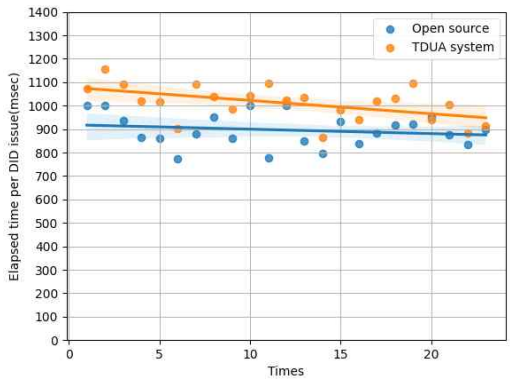
	palm vein	user's hand vein
Position sensor	sensor_id	Unique identifier of the sensor
	msg_time_sec	The unit of time used for calculating rotational acceleration
	pos[3]	Expressing the sensor information acquisition time in seconds using a 32-bit integer.
	quat[4]	The location of the spatial sensor
Speed sensor	sensor_id	The accurate positioning of the spatial sensor (x, y, z, w)
	msg_time_sec	The unit of time used for calculating rotational acceleration
	vel[3]	Unique identifier of the sensor
	vel_quat[4]	Expressing the sensor information acquisition time in seconds using a 32-bit integer.
Acceleration sensor	sensor_id	The speed of the spatial sensor
	msg_time_sec	The unit of time used for calculating rotational acceleration
	acc[3]	The spatial sensor's rotational speed per unit of time(x, y, z, w)
	acc_quat[4]	Unique identifier of the sensor
	acc_quat_dt	Expressing the sensor information acquisition time in seconds using a 32-bit integer.
Activity range sensor	workspace_min[3]	The acceleration of the spatial sensor
	workspace_max[3]	The rotational acceleration of the spatial sensor per unit of time

이를 기반으로 Data Preprocessing을 거친 데이터 d_{Ai}^{l}는 메타버스 내 DID 인증에 활용된다.

5.2 성능 측정 및 분석

본 연구를 구현하여 성능을 측정하고 비교 분석하기 위해 github에서 제공하고 있는 DID가 구현되는 open source[23]를 build 하였으며, 이와 함께 관련 연구인 sDID 논문[24]과 본 연구에서 제안한 TDUA 시스템의 인증 성능을 비교 분석한다. 성능은 초기 DID를 발급하는 시간과 서비스 제공을 위해 VC 발급 및 VP 검증 시간으로 분리하여 측정하였다.

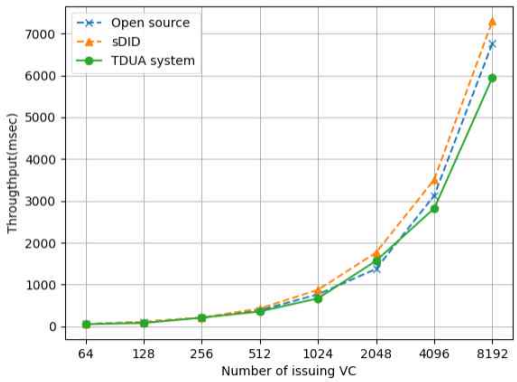
첫 번째 성능 테스트는 사용자가 DID 발급하는 시간을 측정하여 그래프로 표현하는 것으로 약 20회 이상 실시하였다. DID 발급의 경우, open source는 895.91ms, TDUA 시스템은 1010.85ms로써 평균 114.94ms의 차이가 발생하였다. 제안한 TDUA 시스템은 메타버스에서 실거래를 대비하여 보안이 강화된 안전한 인증 서비스를 제공하는 것이 목적으로 수집된 데이터의 Data Preprocessing과 추가적인 자격 증명 발행을 수행하기 때문에 그로 인한 소요시간이 필수적으로 증가하였다.



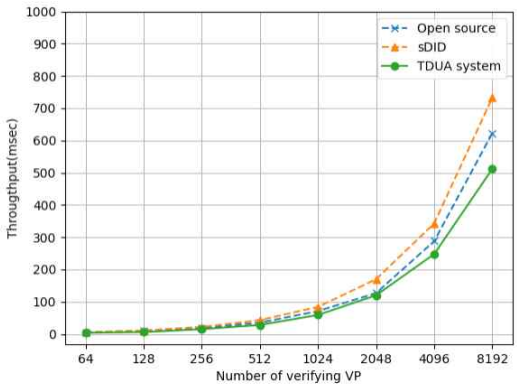
(그림 8) Comparing the time taken to issue DIDs

두 번째 성능 테스트는 Provider가 제공하는 VC 발급과 사용자가 제공하는 VP 관련한 테스트로써, VC 발급 횟수와 VP 검증 횟수를 증가시키고 소요시간을 측정하였다. 이는 open source뿐만 아니라 기존의 sDID 연구와 함께 비교 분석한다. VC 발급은 서비스 속성에 맞춰 발급이 진행되므로 기본적으로 VP 검증보다 더 많은 시간이 소요된다. 측정 결과 VC 발급 1개당 평균시간은 open source는 785.34ms, sDID는 851.36ms이며, 제안한 인증 시스템은 742.31ms로 이를 8,192개 VC 발급하면 6,396ms가 걸린다. VP 검증의 경우, 검증 1번의 평균시간으로 open source는 72.25ms이

며 sDID는 84.97ms, 제안한 인증 시스템은 71.61ms로써 8,192개 VP 검증을 하면 562ms가 걸린다. VC 발급과 VP 검증은 타 연구 대비 근소한 차이로 성능이 우수함을 알 수 있다. 이는 처음 발급에서 이뤄진 추가적인 자격 증명과 해시 알고리즘, NFT를 이용하면서 이후의 계속적으로 발생하는 VC 발급과 VP 검증 횟수가 증가할수록 1개당 소요시간이 감소한 것으로 판단된다.



(그림 9) Increasing the number of VC issuances to measure the duration



(그림 10) Increasing the number of VP verifications to measure the duration

6. 결론

현재 메타버스 내 자산거래 서비스의 보안 인증 절차는 서비스 제공자와 사용자 모두에게 신뢰성의 문제와 함께 비효율적이며, 새로운 공간에서의 자산거래 서비스 확장은 현실 세계와 같은 보안 위협을 고려해야 할 필요성이 존재한다. 또한, 메타버스 환경은 HMD, 스마트 디바이스 등을 통해 사용자의 접속이 이뤄지므로 수집되는 데이터가 기존 사이버 보안 방식과는 다르다. 본 논문에서 제안한 시스템은 Data Preprocessing 기능을 개선하여 수집되는 데이터를 체계적으로 분류하고 이를 인증정보로 활용하여 사용자의 신뢰도를 나타낼 수 있도록 한다. 그리고 신뢰 기반의 자산거래를 위한 인증방식은 1차적인 검증방식으로 DID 기반을 채택함으로써 탈중앙화 인증방식을 기반으로 사용자의 개인정보자기결정권을 보장하며, 2차적인 자격검증은 NFT 기반의 검증을 거쳐 안전한 자산거래 서비스를 메타버스 내에서 제공함으로써 편리성과 무결성 모두 기대한다. 또한, DID를 이용함으로써 자신의 정보 이동 및 활용 여부를 파악할 수 있으며 개인정보자기결정권을 보장함으로써 서비스를 제공하는 기업의 무분별한 데이터 활용 예방을 할 수 있다. 블록체인 기반의 NFT 관리는 안전성과 신뢰성, 무결성을 기반으로 현실 세계에서의 실거래를 메타버스 내에서도 같은 활용을 기대하며 NFT의 활용 및 재사용을 통해 기존의 서류에 대한 복잡성과 에너지 소비를 줄일 수 있어 사용자에게 간편하게 서비스를 제공하고자 한다.

본 논문에서는 메타버스 내 자산거래 서비스 인증 방식과 관련하여 Hyperledger Indy 플랫폼의 라이브러리를 사용하여 구현하여 성능을 측정하였으며, 다른 선행연구들과 비교 분석하였다. 단, 전체적인 프로세스를 제시한 것에 반해 일부분에 대한 검증만을 진행했다는 한계가 존재한다. 따라서 향후 연구로는 본 연구를 확장해 제시 방안의 전체적인 프로세스를 적용하고 검증하는 연구를 진행하려고 한다.

참고문헌

[1] 오정희, "코로나19 이후 주목받는 메타버스, 온라인 버즈량 최근 1년간 10배 이상 증가", Daily Pop, 2022.03.30. https://www.dailypop.kr/news/articleView.html?idxno=58884.

[2] 우리금융경영연구소, "Industry Watch 2021-07

메타버스 가상세계", 2021.

[3] S. Y. Shin, “The Rise of Metabus and Changes in the Financial Industry”, Emerging Tech & Biz Hana, Industry Info vol 2, no 2, 2021.04.

[4] K.W.Lee, J.Y.Lee, K.W.Lee 외 2명, "Trends and Countermeasures of Cyber Threats in Financial Metabus", Law firm (Yoo) Hwawoo, 2022.

[5] 김광우, "JP모건, 메타버스 진출...디센트럴랜드에 '오닉스 라운지' 오픈", tech42, 2022.02.16. https://www.tech42.co.kr/jp모건-메타버스-진출-디센트럴랜드에-오닉스-라운-2/.

[6] 구현주, "농협캐피탈, ;MZ 세대' 직원과 타운홀 미팅", 이뉴스투데이, 2022.10.27. https://www.enewstoday.co.kr/news/articleView.html?idxno=1609956.

[7] 임지윤, "하나은행, 가상공간에 '글로벌 캠퍼스' 오픈", 한국금융. 2021.07.03. https://www.fntimes.com/html/view.php?ud=2021071309164611429249a1ae63_18.

[8] 김영희, "메타버스(Metaverse) 산업 현황 보고서", 저작권 기술 산업 현황 보고서. 2023.07.

[9] 최대선, "메타버스와 보안", 보안뉴스, 2022.04.25. https://www.boannews.com/media/view.asp?idx=106299.

[10] Ankur Gupta,Habib Ullah Khan, Shah Nazir, Muhammad Shafiq and Mohammad Shabaz, "Metaverse Security: Issues, Challenges and a Viable ZTA Model", Electronics 2023, Vol. 12 Issue. 2, 2023.01.12. https://doi.org/10.3390/electronics12020391.

[11] 윤준탁, "인터넷 세상의 새로운 시대 개발? 웹 3.0이 온다!", LG CNS 기술블로그, 2022.01.11.

[12] 임태범, 김동화, 변성우, "메타버스에서의 탈중앙화 자율 조직과 Web 3.0 동향 및 미래 가능성에 대한 고찰", 방송과 미디어-특집: 메타버스 시사점과 응용, Vol.27, No.3, 2022.07.

[13] W3C, Decentralized Identifiers (DIDs) v1.0, 2022.07.19.

[14] 민경식, 김관영, 박진상, “NFT 기술의 이해와 활용, 한계점 분석, 한국인터넷진흥원(KISA), 2020.12.

[15] R.D. Pietro & S. Cresci, "Metaverse:Security and Privacy Issues. The Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS'21)", US EST, 2021.

[16] B. Falchuk , S. Loeb, & R. Neff, "The Social Metaverse:Battle for Privacy", IEEE Technology and Society Magazine, pp.52-61, 2018.

[17] 정수용, 서창호, 조진만, 진승헌, 김수형, "확장된 가상현실인 메타버스에서의 보안 위협 분석", 정보보호학회지, Vol.31, No.6, 2021.12.

[18] S.K.Yoo, Y.J.Seo, B.I.Kwak, "Financial Service Secrity Threats in the Metaverse Environment", Korea Convergence Security Association, pp.79-80, 2022.

[19] 나현식, 최대선, "메타버스 보안 위협 요소 및 대응 방안 검토", 정보보호학회지, Vol.32, No.4, pp.19-32, 2022.08.

[20] 이준형, 민홍기, "메타버스 관련 보안위협에 대한 법적 보호방안 검토", 한국공안행정학회보, Vol.31 No.3, pp.321-344, 2022.

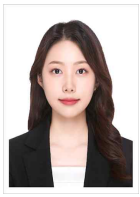
[21] 조도은, "메타버스 서비스를 위한 보안 모델 연구", Journal of Platform Technology, Vol.10, No.4, pp.82-90, 2022.12.

[22] 최정환, "가상현실에서 대공간 인지를 위한 센서 데이터 포맷", TTA저널, Vol.197, 2021.10.

[23] https://github.com/anstnsp/Hyperledger-indy-practice

[24] 김현곤, "프라이버시 보호가 가능한 익명성 기반 차량용 분산ID", The Journal of Korean Institute of Communications and Information Sciences, Vol.47 No.01, pp.151-159, 2022.01.

〔저자소개〕



박 수 완 (Su-wan Park)
2023년 2월 성신여자대학교 학사
2023년 3월 ~ 현재 SK쉴더스 재직

email : swan981104@gmail.com

이 상 민 (Sang-min Lee)
2023년 2월 성신여자대학교 학사
2023년 3월 ~ 현재 SK쉴더스 재직

email : min2min76@gmail.com

김 경 진 (Kyoung-jin Kim)
2007년 2월 성신여자대학교 학사
2009년 2월 성신여자대학교 석사
2013년 2월 성신여자대학교 박사
2016년 2월 고려대학교 무인자율 및 적응형 소프트웨어센터 연구교수
2017년 2월 성균관대학교 스마트핀테크연구센터 박사후과정
2017년 3월 ~ 현재 성신여자대학교 융합보안공학과 조교수

email : kyoungjin@sungshin.ac.kr