Journal of KIIT. Vol. 20, No. 9, pp. 1-11, Sep. 30, 2022. pISSN 1598-8619, eISSN 2093-7571 1
http://dx.doi.org/10.14801/jkiit.2022.20.9.1

안전한 메타버스 환경을 위한 속성레벨 프라이버시 보호 메커니즘

이 동 혁*

Attribute-level Privacy Protection Mechanism for a Secure Metaverse Environment

Donghyeok Lee*

요 약

최근 메타버스 기술은 진화를 거듭하여 크게 발전하고 있으며 향후 디지털 대전환을 위한 중요한 기술로서 자리잡게 될 것이다. 그러나 메타버스 서비스 제공 과정에서는 다양한 개인정보 노출이 발생할 수 있다. 특히 현실연계형 메타버스 서비스를 이용하는 과정에서 사용자의 생체 민감정보, 라이프로그, 위치정보 등 다양한 데이터가 외부에 노출될 수 있다. 메타버스 서비스 제공 관점에서는 사용자의 생체신호 등 민감정보를 적극적으로 수집하는 것이 유용하지만 개인정보보호 관점에서는 최대한 적게 공개하는 것이 바람직하다. 본 논문에서는 메타버스 환경에서 취급되는 개인정보를 안전하게 보호하기 위한 속성레벨 프라이버시 보호 메커니즘을 제안한다. 제안한 방식은 서비스 제공에 반드시 필요한 데이터만 선별적으로 제공하며, 사용자의 명시적 승인을 득한 개인정보만 공개하여 불필요한 정보 노출을 원천적으로 차단하여 악의적인 데이터 유출을 방지한다.

Abstract

Recently, metaverse technology has been greatly developed through evolution and will be established as an important technology for a great digital transformation in the future. In particular, in the process of using the reality-connected metaverse service, various data such as the user's bio-sensitive information, life log, and location information may be exposed to the outside. From the viewpoint of providing metaverse services, it is useful to actively collect sensitive information such as users' biosignals, but from the viewpoint of protecting personal information, it is desirable to disclose as little as possible. In this paper, I propose an attribute-level privacy protection mechanism to safely protect personal information handled in the metaverse environment. The proposed method prevents malicious data leakage by selectively providing only the data necessary for service provision.

Keywords
metaverse security, privacy protection, metaverse privacy, VR/AR

* 청주대학교 교양학부/소프트웨어융합학부 조교수
- ORCID: https://orcid.org/0000-0001-7516-469X

· Received: Jul. 29, 2022, Revised: Sep. 07, 2022, Accepted: Sep. 10, 2022
· Corresponding Author: Donghyeok Lee
Faculty of Liberal Arts, Cheongju University, Korea
Tel.: +82-43-229-7829, Email: dhlee@cju.ac.kr

Ⅰ. 서 론

최근 메타버스 환경의 중요성이 부각되고 있다. 과거에는 메타버스를 단순 가상현실이나 게임공간 정도로 생각하는 경향이 있었으나, 최근 메타버스 기술이 발달되면서 현실과 이어지는 또 하나의 세계로 받아들여지고 있다. 메타버스 플랫폼은 다양한 컨텐츠 감상, 온라인 거래, 가상 원격근무, 사이버 교육 등 여러 분야에서 적극적으로 활용될 수 있으며, 향후 주요한 기술로 각광받는 추세이다[1][2].

메타버스 환경의 진화에 따라 현실연계형 메타버스 서비스도 등장하게 될 것이다. 사용자의 신체적 특징 및 생체 신호를 실시간으로 수집하여 사이버 상의 아바타와 연계하거나, 사용자의 현재 상태를 분석한 다양한 형태의 서비스 제공이 가능하게 될 것이다[3][4]. 이러한 현실연계형 메타버스 환경에서는 다양한 형태의 개인정보가 이용될 수 있다. 사용자의 시선 추적 정보, 근육 활동 정보 뿐만 아니라 뇌파 신호와 같은 민감도가 높은 개인정보까지 활용될 수 있으며, 이러한 생체 신호의 제공은 높은 수준의 현실연계로 이어질 수 있지만 보안적 측면에서의 우려가 있는 것이 현실이다. 따라서 메타버스 환경을 안전하게 활용하려면 반드시 메타버스 서비스는 프라이버시 보호를 고려하여 설계/제작될 필요가 있다[5][6].

과거에는 시스템에 사전 설정된 접근 정책에 의한 정적인 접근제어 기술에 의하여 보안 대책을 구성하는 경우가 일반적이었다. 그러나 현실연계 메타버스 환경에서는 정적인 개인정보 뿐만 아니라 사용자의 생체 신호 등 동적인 개인정보가 적극적으로 활용될 것이며, 이러한 동적인 개인정보에 대하여 실시간으로 데이터 접근 여부를 결정해 주는 구조가 필요하다.

메타버스 서비스 제공자 측면에서 원활하고 실감 있는 메타버스 서비스를 제공하려면 개인의 생체정보 등 동적 개인정보를 적극적으로 수집하여야 한다. 그러나 이 경우 데이터 수집은 반드시 필요한 정보에 국한하여야 하며, 또한 서비스 제공에 반드시 필요한 데이터라 할지라도 개인의 동의 없이는 수집할 수 없어야 한다. 그러나 실시간 생체정보와 같은 동적인 개인정보에 대해 실시간으로 개인이 동의 여부를 확인하고 결정하는 것은 효율적이지 않으며, 사용자는 메타버스 서비스를 원활히 이용할 수 없게 될 것이다. 따라서 본 논문에서는 안전한 메타버스 환경을 제공할 수 있는 속성레벨 프라이버시 보호 기법을 제안한다. 제안한 기법은 메타정보 서비스 제공 과정에서 명시적 승인을 득한 개인정보에 한하여 실시간으로 속성별 등급을 결정할 수 있으며, 불필요한 정보 노출을 차단하여 개인정보를 안전하게 관리할 수 있다.

Ⅱ. 관련 연구

2.1 메타버스 주요 요소와 프라이버시

2.1.1 메타버스의 주요 요소

메타버스는 크게 4가지 영역으로 구분할 수 있다. 비영리 단체인 ASF(Acceleration Studies Foundation)에서는 메타버스 로드맵을 발표한 바 있으며, 그림 1과 같이 메타버스의 요소를 4가지 관점에서 정의하였다[7]. 해당 보고서에 따르면, 메타버스의 요소는 각각 증강현실(Augmented reality), 거울세계(Mirror worlds), 라이프로그(Lifelogging), 가상세계(Virtual worlds)로 나눌 수 있다[8].

증강현실이란 현실의 정보를 기반으로 한 추가적인 가상의 정보를 제공하는 것을 의미하며, GPS를 활용한 위치인식 시스템 및 지리적 정보, 다양한 인터페이스를 이용하여 사용자가 속한 물리적인 세계를 더욱 확장시킬 수 있는 환경을 의미한다.

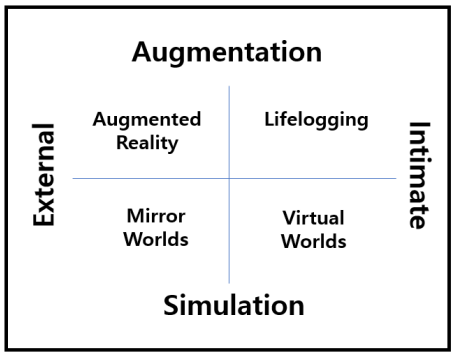

그림 1. 메타버스의 4대 요소[7]
Fig. 1. 4 Elements of the metaverse[7]

거울세계는 현실세계를 최대한 유사하게 표현하는 것으로, 공간적으로 참조되는 데이터 및 관련 특성을 캡쳐, 저장, 분석, 및 관리하여 사용자 주변의 세계를 모델링하는 것이다. 따라서 거울세계를 활용하면 현실세계에 대한 정보 습득이 가능할 수 있다.

라이프로그의 경우, 사용자의 현재 상태 혹은 일상적인 경험과 정보가 디지털 공간에 저장되는 것을 의미한다. 예를 들어 나이키와 애플의 결합을 통하여 GPS를 기반으로 사용자의 이동정보가 관리되는 서비스가 대표적인 라이프로그 서비스에 속한다.

가상세계의 경우 현실과 완전히 구분되는 별도의 디지털상의 세계를 의미하며, 사용자는 아바타를 이용하여 마치 현실세계와 같이 사회적, 경제적 활동을 할 수 있는 가상의 세계이다. 가상세계의 영역에는 일반적인 온라인 게임까지도 포함된다고 볼 수 있다.

2.1.2 메타버스와 데이터 프라이버시

개인정보는 특정한 개인에 관한 정보를 의미한다. 개인정보는 다양한 속성으로 구분할 수 있다. 여기에는 이름, 주소, 연락처와 같은 정적인 개인정보가 있으며, 뇌파, 맥박, 아이트래킹, 위치정보 등과 같은 동적인 개인정보 또한 존재할 수 있다.

메타버스 환경에서는 정적 개인정보 뿐만 아니라 동적 개인정보를 적극적으로 활용하게 된다. 예컨대 손가락 동작 인식, 맥박 파형, 호흡, 머리 움직임 등의 제스쳐, 안면인식에 따른 표정 등 실시간으로 수집될 수 있는 다양한 정보를 활용하여 실제 메타버스 아바타에 해당 정보를 실시간으로 반영함으로서 사용자는 더욱 실감나는 메타정보 서비스를 제공받을 수 있을 것이다.

지금까지 메타버스에 대한 개인정보보호 문제제기는 있어 왔으나, 충분히 연구되지 않은 측면이 있다. 예를 들어, 메타버스 환경에서 사용자가 가상환경에 얼마나 자주 접속하는지, 그리고 얼마나 메타버스 서비스를 오랫동안 사용하는지 여부 뿐만 아니라 신체 운동, 제스쳐, 아이트래킹(시선 추적) 정보, 뇌파 신호, 경험에 대한 생리적인 반응 등이 취급될 수 있다. 이러한 정보는 사용자에게 충분히 인지되지 않은 채 메타버스 서버에서 임의로 수집될 수 있으며, 향후 기술의 발전에 따른 다양한 센서를 탑재한 AI 지원 장치, AR 안경, VR 헤드셋 등이 메타버스에 활용될 것이다. 이 기기들에서 발생되는 다양한 생체정보 및 민감정보 등의 데이터가 메타버스 서버에서 관리된다면 이는 심각한 사용자 프라이버시 문제로 이어질 수 있을 것이다. 이러한 프라이버시 침해 문제를 방지하기 위해 개인정보를 안전하게 관리할 수 있는 보안 구조 확립이 시급한 상황이다.

이러한 문제를 해결하려면 기존의 일괄적인 데이터 접근제어 방식으로는 해결되지 않는다. 개인이 민감하게 느끼는 속성정보라 할지라도 개인 연락처와 같은 적절한 수준의 보안이 필요한 정보가 있는 반면 매우 높은 수준의 관리를 필요로 하는 속성정보(예:주민등록번호, 뇌파, 위치정보 등)는 중요도를 달리하여 취급하여야 하며, 특히 생체정보와 같은 동적 속성정보는 서비스 제공에 반드시 필요한 범주를 고려하여 실시간으로 데이터 공개 여부가 결정되어야 한다.

본 논문에서는 이러한 메타버스 환경에서의 개인정보 노출에 따른 프라이버시 침해 문제를 해결하고자 속성레벨 데이터 보안 메커니즘을 제안한다. 제안하는 메커니즘은 각각의 데이터 속성별로 세밀한 등급 부여가 가능하며, 필요시 하위등급을 별도로 추가하여 확장이 가능하다는 장점이 있다. 따라서 메타버스 환경에서 취급되는 다양한 생체 신호 등의 민감정보에 대하여 적극적인 보안 대책을 마련할 수 있다.

2.2 기존의 메타버스 연구

2.2.1 Mortezapoor의 연구

미래의 VR 환경은 단순히 사용자에 국한되지 않고 로봇과 상호작용하는 방식을 통해 다양한 서비스 제공이 가능할 것이다. Mortezapoor 등은 VR 환경에서 로봇이 활용될 경우 데이터 보안 측면에서 발생하는 보안 위협에 대하여 지적한 바 있다[9]. 특히, VR 환경에서 안전하게 로봇을 사용하기 위한 데이터 취급 과정에서의 최소화 및 중복 데이터 수집을 언급하였다.

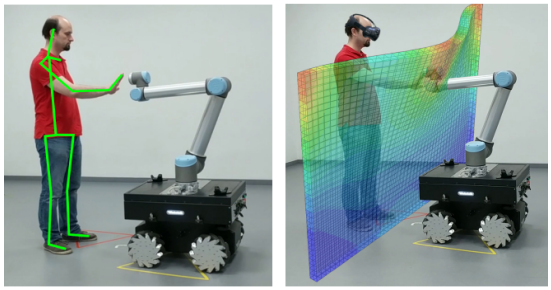

그림 2. VR 공간에서의 상호작용 표현[9]
Fig. 2. Interactive representation in VR space[9]

해당 논문에서는 악의적인 공격자에 의해 VR 환경에 대한 보안 문제가 발생할 수 있음을 지적하고 있으나, 이를 해결하기 위한 구체적인 기술적 메커니즘에 대해서는 별도로 제공하고 있지 않다. 메타버스의 주요 영역인 VR 환경에서는 다양한 개인정보 노출이 발생할 수 있다. 특히, 사용자의 뇌파 인식 신호와 같은 다양한 민감 생체정보가 인터넷상으로 전송될 것이며, 서비스 제공에서 반드시 필요할 경우 특정 시간, 구간별로 최소한의 필요한 정보를 동적으로 결정하고 전송되어야 한다. 기존의 데이터 보안 및 접근제어 정책으로는 이러한 문제를 해결할 수 없으며, 이를 해결하기 위한 안전한 대책이 확보될 필요가 있다.

2.2.2 Scargill의 연구

Scargill 등은 진화된 AR 환경 제공을 위해 AR 어플리케이션과 사용자의 주변 환경에 따른 상황인식 기술을 제공할 수 있는 SLAM 알고리즘을 제안하였다[10]. 해당 방식은 AR 장치와 IoT 장치의 데이터 스트림에 대한 조합을 통해 사용자 주변 환경과 사회적인 영역을 고려한 개선된 상황인식 기술을 제공하고, 이를 기반으로 향상된 AR 서비스를 제공하는 방법을 제안하고 있다. 그림 3은 Scargill 등이 제안한 AR 서비스를 위한 상황인식 기술을 나타내고 있다.

그러나 해당 연구에서는 복합적인 상황인식을 바탕으로 하는 향상된 AR 서비스 제공이 가능하지만 해당 상황인식 정보를 어떻게 보호할 것인지에 대해서는 언급하지 않고 있다. 실질적으로 사용자 주변의 IoT, 웨어러블, AR 장치 등에서 수집되는 정보가 인터넷을 통하여 전달될 경우 불법적인 수집에 따라 의도치 않는 데이터가 분석될 수 있다.

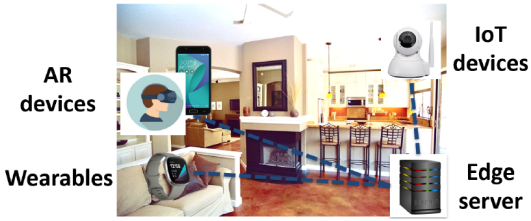

그림 3. AR 서비스를 위한 상황인식 기술[10]
Fig. 3. Context-aware technology for AR services[10]

그리고 경우에 따라 악의적인 공격자에 의해 개인 민감정보가 노출될 수 있어 프라이버시를 보호하는 방안을 반드시 고려할 필요가 있다.

2.2.3 Chong의 연구

최근 대학 등에서도 메타버스 가상교육이 점차 확대되는 추세에 있다[11]. Chong 등은 메타버스 상에서의 원활한 가상교육 환경을 위하여 가상서비스 제공자의 비용 최소화를 위한 확률적 자원 할당 방식(SORAS)를 제안하였다[12]. 해당 방식을 통해 할당 리소스 초과를 방지함으로써 메타버스 서비스 제공자의 비용을 최적화하여 사용자 수요에 따른 자원 할당 문제를 해결할 수 있다는 장점이 있다. 그림 4는 Chong 등이 제안한 메타버스 환경에서의 가상교육 환경을 나타내고 있다.

그러나 효과적인 메타버스 자원 할당 관리를 위해 자체 시스템이 아닌 외부 클라우드 서비스 등에 자원을 위탁하는 과정이 필요할 것이며, 이 과정에서 사용자의 데이터 보안 침해가 발생할 수 있다. 특히 메타버스 서비스 제공 과정에서 발생되는 생체정보와 같은 민감정보를 특별한 조치없이 일괄적으로 외부 위탁 관리를 수행한다면 사용자 프라이버시상 큰 문제가 발생할 수 있다. 본 논문에서 제안하는 방법은 데이터를 외부에 위탁하는 과정에서 별도의 등급을 생성하고 관리할 수 있게 하여 데이터 위탁시의 위험을 크게 줄일 수 있다.

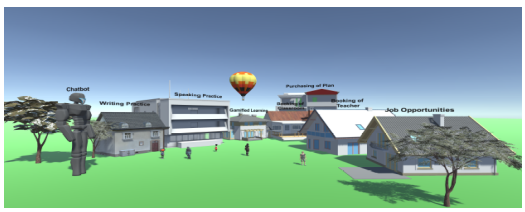

그림 4. 메타버스 환경에서의 가상교육 환경[12]
Fig. 4. Virtual education environment in metaverse environment[12]

III. 제안 방식

본 장에서는 메타버스 환경에서의 개인정보 취급 시 고려사항을 먼저 살펴보고, 이를 해결하기 위해 제안하는 데이터 보호 방식에 대해 설명한다.

3.1 메타버스의 개인정보 취급시 고려사항

3.1.1 증강현실에서의 위치노출 문제

증강현실 서비스 과정에서 사용자의 주변 위치가 파악될 수 있으며 이는 결국 사용자 위치정보에 대한 노출로 이어질 수 있다. 사용자 주변 환경에 대한 영상정보가 서버로 전송되며, 악의적인 해커가 이를 습득할 경우, 사용자가 어디에 있고 무엇을 하고 있다는 것이 파악되어 프라이버시 침해 소지가 있게 된다. 위치정보는 GPS 뿐만 아니라 영상 내부의 표지판, 지형 등 다양한 경로를 통하여 추정될 수 있을 것이다.

3.1.2 라이프로그 노출 문제

실질적으로 프라이버시 침해 위협이 가장 높은 부분이 바로 라이프로그 영역이다. 라이프로그 서비스에서 수집된 데이터에는 민감 데이터가 포함될 수 있다. (예: 생체 신호 정보 등) 기본적으로 라이프로그 데이터는 매우 높은 수준으로 관리되어야 하며, 정적인 개인정보에 대한 취급 동의 후 정보 수집을 하게 되는 것이 일반적이지만, 동적으로 변하는 위치정보나 생체 신호에 대해서는 실시간으로 정보 수집 여부가 달라져야 하므로 적시적으로 동의를 구하는 것이 쉽지 않다. 따라서 동적인 개인정보에 대해 정보 공개 여부가 자동으로 결정되는 구조가 필요하다.

3.1.3 안전한 보안 통신 제공

메타버스 장치와 서버간의 안전한 통신을 위해 안전한 암호화 메커니즘이 필요하다. 정상적인 사용자가 아닌 악의를 가진 자가 해킹 등에 의해 불법적인 경로로 접근하여 데이터에 대한 위/변조를 수행할 경우 사이버 공간에서의 가상인격(사이버 정체성) 훼손, 불법적인 결제 등 메타버스 생태계에 다양한 악영향을 끼칠 수 있다. 제안하는 메커니즘은 별도의 키 관리 서버를 거치지 않는 클라이언트/서버 자체적으로 수행 가능한 암호키 생성 절차를 제공하여 인가되지 않은 자의 데이터 접근을 차단할 수 있다.

3.1.4 정보의 중요도에 따른 접근제어

개인정보의 종류는 다양하며, 메타버스 서비스 제공 과정에서는 정적 개인정보 뿐 아니라 생체 신호 등 동적 개인정보가 적극적으로 전달될 것이다. 이러한 개인정보 중 각 사용자가 개별적으로 민감하게 생각하는 정보는 각각 상이할 수 있을 것이다. 따라서 서비스 제공 과정에서 취급되는 개인정보는 등급을 구분하여 보다 세밀하게 취급하여야 한다. 예컨대 생체정보를 민감정보라고 가정한다고 하더라도, 생체정보에 속하는 모든 데이터를 동일한 정책으로 취급되는 것은 바람직하지 않다. 예를 들어 시선 추적 정보와 뇌파 측정 데이터는 생체 신호라는 동일한 카테고리에 속하지만 중요도는 완전히 다르게 되므로 속성별로 세부적인 등급을 구분하여 취급할 필요가 있다.

3.2 제안 방식 개요

3.2.1 메타버스 속성레벨 프라이버시 보호 모델

본 논문에서 제안하는 메타버스 속성레벨 개인정보보호 모델은 그림 5와 같다. 현실세계와 메타버스 간 데이터의 안전한 전송을 위하여 제안하는 속성레벨 프라이버시 보호 기술을 적용하여 데이터를 안전하게 보호한다. 여기에서 메타버스상에서 제공되는 VR, AR, XR 서비스 제공에 반드시 필요한 정보를 선별하는 과정이 포함되며, 서비스 제공에 필요한 정보이더라도 사용자가 공개를 원하지 않는 정보는 전달되지 않는다. 또한 선별된 개인정보는 세부 등급을 구분하여 차등화된 관리가 가능하므로 메타버스 환경에서 VR, XR, AR 서비스 제공 시 안전하게 개인정보를 취급 및 관리할 수 있다.

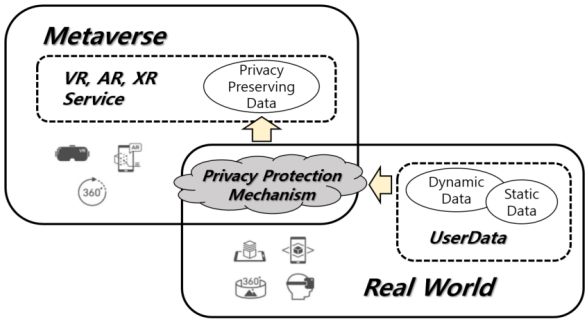

그림 5. 메타버스 속성레벨 프라이버시 보호 모델
Fig. 5. Attribute-level privacy protection model

3.2.2 데이터 속성레벨 등급 분류

메타버스 환경에서는 데이터의 속성이 등급별로 분류될 필요가 있다. 표 1은 메타버스 환경에서 전달될 수 있는 속성단위의 데이터 등급 분류 예를 나타내고 있다. 이러한 등급 분류는 정적으로 정해져 있는 것이 아니라, 본 논문에서 제안한 메커니즘에 의해 사용자가 서비스 이용시 클라이언트와 서버의 상호작용을 통해 실시간으로 등급을 확립하고 결정하게 된다.

표 1. 메타버스 제공 데이터 등급 분류의 예
Table 1. Examples of data classification

Grade	Category	Contents
1	dynamic data	- brain-wave(EEG) - location information
	static data	- fingerprint information - resident registration number - credit card information
2	dynamic data	- pulse & heart rate - facial recognition data
	static data	- physical condition - body measurement data
3	dynamic data	- electromyogram(EMG) - motion capture
	static data	- date of birth - cell phone number
4	dynamic data	- eye tracking information - head gesture recognition
	static data	- religion - job / affiliation
5	dynamic data	- finger motion tracking - touch, pressure
	static data	- certificate, license - favorite sport
Public	static / dynamic data	- Data accessible to anyone

안전한 프라이버시 보호를 위해 정보공개 등급은 실시간으로 결정될 수 있어야 하며, 데이터의 전송은 서비스 제공시간에 한정하여야 한다. 또한, 수집하는 데이터는 해당 메타버스 서비스 제공에 꼭 필요한 영역에 대한 수집만 이루어져야 한다. 본 논문에서는 사용자 프라이버시를 충분히 고려하여 데이터의 민감도를 반영한 등급을 서버-클라이언트 상호간 동적으로 확립할 수 있는 구조를 제안하고 있다.

3.3 세부사항

3.3.1 데이터 속성 등급부여 및 확립

1) 데이터 속성단위 등급 부여

데이터 속성에 따른 등급을 정할 경우, 일반적으로 시스템 정책에 의한 정적 등급을 부여하게 된다. 그러나 이러한 정적 등급 부여 대책은 실시간으로 변하는 메타버스 서비스 환경에는 맞지 않는다. 예를 들어, 특정 서비스를 제공하는 데 있어 필수적인 정보(예: 아이트래킹 정보 등의 생체정보)는 해당 서비스의 제공 시점 이외에는 필요하지 않은 정보이다. 따라서 데이터 속성의 등급은 등급표에 의해 일률적으로 적용될 것이 아니라, 각각의 세부 서비스 제공 시점에 따라 적절한 값으로 적용될 필요가 있다.

본 논문에서 제안하는 방법은 데이터 속성의 등급을 사용자 preference, 그리고 서비스 제공에 꼭 필요한 데이터 범위, 마지막으로 시스템에 사전 정의된 데이터 보안정책의 3가지 기준을 복합적으로 고려하여 실시간으로 결정할 수 있다. 따라서 서비스에 반드시 필요하되 사용자에게 동의를 구한 데이터만 전송이 가능하며, 데이터 전송 시 등급별 차등화된 키로 암호화하므로 안전하게 개인정보를 전송 및 관리할 수 있다.

2) 데이터 속성 확립

데이터 속성 확립 절차는 민감정보에 대한 적절한 접근제어를 위해 클라이언트와 메타버스 서버간 통신 과정에서 서비스 제공을 위해 수집해야 할 정보를 사전 확립하는 절차이다.

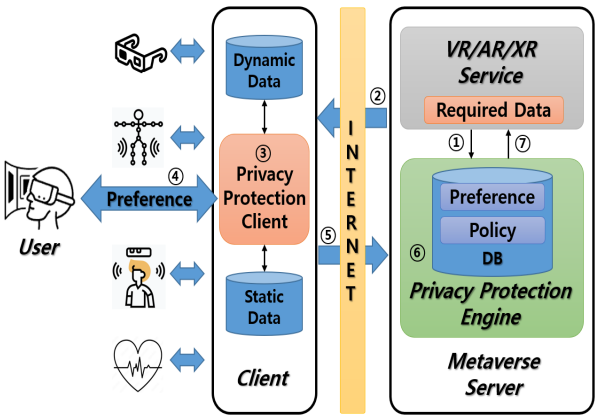

그림 6. 데이터 속성 확립 절차
Fig. 6. Data attribute establishment procedure

서버에서 필요로 하는 정보이더라도 사용자가 허가하지 않은 경우는 서버로 전송되지 않으며, 인가된 정보에 대해서만 서버 전송이 가능하다. 그림 6은 데이터 속성 확립 절차에 대하여 나타내고 있다.

그림 6에 나타난 데이터 속성 확립 절차에 대해 설명하면 다음과 같다.

① VR/AR/XR 서비스는 해당 서비스 제공에 필요한 개인정보 목록을 결정하고 프라이버시 보호 엔진에 요청한다.

② 메타버스 서버는 서비스에 필요한 데이터 목록을 클라이언트에 전달한다.

③ 프라이버시 보호 클라이언트는 서비스 목록 가운데 동적 데이터, 정적 데이터 유무를 확인한다.

④ 클라이언트는 사용자로부터 해당 데이터 목록을 사용자에게 전달하고 공개여부 승인을 받는다.

⑤ 데이터 목록은 민감도에 따라 각 속성레벨로 차등화를 두어 암호화하고 인터넷으로 전달한다.

⑥ 프라이버시 보호 엔진은 차등 암호 데이터에 대한 복호화 권한을 확인하며, 서버 보안 정책을 확인하여 정보 공개 여부를 최종 결정한다.

⑦ 프라이버시 보호 엔진은 최종 공개로 결정된 데이터에 한하여 VR/AR/XR 서비스에 전달한다.

이러한 절차를 통하여 서비스에 필요한 데이터 속성 중 사용자가 명시적으로 승인한 정보만 전송할 수 있어 동적인 프라이버시 보호가 가능하다.

3.3.2 등급별 암호키 생성 메커니즘

1) 약어 설명

본 절에서의 등급별 암호키 생성 메커니즘에 대한 설명을 위한 약어는 표 2에 나타나 있다.

먼저, 1등급 속성의 데이터에 접근하려면 데이터 속성 아이디 DAID와 최상위 비밀키인 K_T를 알아야 정상적으로 데이터에 접근할 수 있다. 데이터 고유 아이디인 DAID는 특정 데이터 속성이 가지고 있는 고유한 아이디이다. 데이터 속성 아이디는 중복 없이 유일해야 하며, 하나의 DAID는 반드시 한 종류의 데이터 속성과 매핑되어야 한다. 아울러 DAID는 특별히 비밀스럽게 취급하지 않아도 되는 공개 가능한 정보이다. 즉, 데이터 속성 아이디는 기밀성을 유지하여 취급하지 않아도 되며, 일종의 속성 구분을 위한 식별자로서의 역할을 수행한다.

최상위 비밀 키인 K_T는 인가된 1등급 구성원 끼리만 공유하고 있는 키이다. K_T는 반드시 기밀성을 유지하여 공유되어야 한다. 즉, K_T는 최상위 암호키의 역할을 하므로 반드시 K_T가 노출되어서는 안된다. 1등급 구성원 이외의 멤버는 K_T를 알아서는 안되며, 알 필요 또한 없다. K_T를 인지하지 못하여도 하위등급에서는 자신이 속한 등급에 대한 보안 해제에 아무런 문제가 없게 된다.

표 2. 약어
Table 2. Abbreviation

Abbreviation	Explanation
KG	Grade key of group G
KGn	Grade key of n-th group
KT	Top secret key
KP	Pre-shared key
DAID	Data Attribute Identifier
HMAC(x)K	Result of HMAC operation with key K for value x
H(x)	Result of hash operation on value x
⊕	XOR(exclusive OR)
s	Static information disclosure rate predefined by system policy
r	Dynamic information disclosure rate required to provide metaverse services
u	Information disclosure rate set by users
g(d)	The determined security level of data attribute d

또한, 사전 공유된 키인 K_P는 모든 등급간 전체 구성원끼리 공유하는 키이다. 전체 등급이 공유하되, 외부로 노출되지 않게 주의할 필요가 있다.

K_G^n은 n번째 등급 암호키를 의미한다. 만약 3등급의 암호키라면 K_G^3으로 표현한다. 본 논문에서 제안하는 암호키 생성 알고리즘을 이용하면 상위의 등급을 가진 정보 접근자는 하위 n번째 등급에 해당하는 암호키를 특별한 추가 정보 없이 바로 연산할 수 있는 장점이 있다. 그러나 하위의 등급을 가진 정보 접근자는 상위의 등급 키를 연산하는 것은 계산적으로 매우 어렵다. 이는 해시함수의 역함수를 찾는 어려움과 동일한 수준의 어려움을 가지게 되므로 개인정보에 대해 안전하게 기밀성을 유지할 수 있어 등급별 키 보안 관리에 매우 적합하다.

2) 1등급 키 생성 절차

1등급 속성의 등급키는 아래의 식 (1)을 통하여 계산할 수 있다.

$$K_G^1 = HMAC(H(DAID) \oplus H(K_T))^{K_T} \quad (1)$$

1등급 속성 등급키를 계산한 이후에는 n등급 속성의 등급 키를 아래의 식 (2)로 계산할 수 있다.

$$K_G^n = HMAC(H(DAID) \oplus H(K_G^{n-1}))^{K_P} \quad (2)$$

키 생성 과정을 예를 들어 설명하면 다음과 같다. 1등급이 접근 가능한 데이터 속성인 '뇌파 측정' 데이터 DAID가 'DA123'라고 가정하며, 최상위 비밀키 K_T가 'sec'이라고 가정해 보자. 여기에서 K_T는 1등급에게만 공유되어 있다. 나머지 멤버는 K_T에 대한 정보를 알 수 없다. 따라서 1등급에 속하는 접근자는 다음의 식 (3)과 같이 1등급 암호키를 계산할 수 있다. 만약, 1등급에 속하지 않은 자가 1등급 데이터에 접근하려고 해도 최상위 비밀키 K_T인 'sec'를 알 수 없으므로 1등급 암호키를 생성할 수 없다. 먼저, 데이터 속성 아이디 'DEV_12345'를 입력값으로 해쉬연산 결과를 생성한다.

$$K_G^1 = HMAC(H(DA123) \oplus H(\mathrm{sec}))^{\mathrm{sec}} \quad (3)$$

그리고, K_T인 'sec'에 대한 해쉬연산을 수행하고, 두 값의 결과에 대한 XOR 연산을 수행한다. 해당 결과값에 대하여 최종적으로 K_T인 'sec'을 키로 하는 HMAC 연산을 수행하여 1등급의 비밀키를 생성할 수 있게 된다.

3) 하위 등급의 키 생성 절차

1등급은 최상위 등급이므로 모든 등급에 대한 키를 생성할 수 있다. 여기에서, 전체 구성원간 사전 공유된 키인 K_P는 'psk'라고 가정한다. 만약, 1등급 구성원이 2등급의 키를 알고자 한다면 아래와 같은 식 (4)를 통하여 연산할 수 있다.

$$K_G^2 = HMAC(H(DA123) \oplus H(K_G^1))^{psk} \quad (4)$$

마찬가지로 3등급의 키는 식 (5)와 같이 연산할 수 있다. 이러한 절차를 반복하면 이론적으로 등급 개수의 제한 없이(예를 들어 100등급, 1000등급 등) 신규 키 생성이 가능하며, 상위 등급의 접근 권한을 가지고 있는 자는 하위 등급의 키를 생성하는데 별도의 새로운 추가 정보가 필요하지 않게 되므로 쉽게 연산이 가능하다.

$$K_G^3 = HMAC(H(DA123) \oplus H(K_G^2))^{psk} \quad (5)$$

제안하는 방식은 등급 개수에 대한 제한이 별도로 존재하지 않는다는 특징을 갖는다. 서비스 제공 과정에서 필요한 만큼 동적으로 등급을 생성하고, 해당 등급에 따른 암호키를 제한 없이 생성할 수 있다는 장점이 있다. 메타버스 환경에서 취급해야 할 데이터는 지속적으로 증가할 것이며, 이에 대응할 수 있는 등급 키 또한 제한없이 생성할 수 있다.

3.3.3 데이터 속성의 동적 등급 결정

특정 데이터 속성 d에 대하여 아래의 식 (6)을 이용하여 최종적으로 등급을 결정할 수 있다. 이 식의 입력값인 s, r, u는 1부터 100사이의 실수이며 사전에 결정되어 있어야 한다. 만약, 식의 결과에서 0등급이 발생할 경우는 프라이버시 침해가 없는 정보를 의미하며 모든 구성원이 데이터 속성에 접근할 수 있다.

$$g(d) = \begin{cases} t(s,r) & \text{if } \frac{s+r}{2} \le u \\ 0 & otherwise \end{cases} \quad (6)$$

표 3. 등급 판별 테이블
Table 3. Grading table

Grade	s value	condition	r value
1	s ≥ 80	OR	r ≥ 80
2	s ≥ 60	OR	r ≥ 60
3	s ≥ 40	OR	r ≥ 40
4	s ≥ 20	OR	r ≥ 20
5	s ≥ 0	AND	r ≥ 0
Public	s = 0	AND	r = 0

s, r 값을 기준으로 결정되는 t(s,r)은 표 3에서 나타난 등급 판별 테이블을 기준으로 결정된 최종 등급 결과를 의미한다. 아래의 등급 판별 테이블은 하나의 예시로서, 서비스 제공자에 따라 세부적인 등급 판별 테이블을 구성할 수 있으며 이를 통해 최종적으로 데이터 속성에 대한 등급을 결정할 수 있다. 만약 '공개' 등급으로 결정된 경우에는 자유롭게 공유 가능한 데이터 속성이며, 사용자의 프라이버시를 침해하지 않는 민감도가 극히 낮은 데이터로 간주하게 되며 자유로운 데이터 활용이 가능하다.

그림 7은 등급에 따른 정보공개의 변화를 나타내는 구현화면이다. 등급 판별 테이블에 따라 등급이 결정되면, 등급별로 차등화된 정보 노출을 수행할 수 있다. 그림은 등급의 변화에 따라 정보공개율이 변화하는 예시화면이며, 시스템 정책에 따라 다양한 방식으로 개인정보의 노출 정도를 정할 수 있다.

Ⅳ. 제안 방식 분석

4.1 안전성 측면

4.1.1 스니핑 공격 방지

개인정보의 데이터 통신 과정에서 모든 데이터는 암호화되어 전송된다. 특히, 제안하는 방식에 의한 차등 데이터 암호화 메커니즘에 의하여 암호화된 보안 터널이 형성되므로 악의를 가진 공격자가 스니핑 공격을 수행하더라도 등급 암호화키를 알 수 없으므로 복호화가 불가능하다. 따라서 스니핑 공격을 수행하더라도 암호화된 데이터로부터 어떠한 원본 개인정보도 복원하거나 추정할 수 없다.

4.1.2 내부자 공격 방지

메타정보 서버 관리자 혹은 VR/AR/XR 서비스 관리자가 사용자의 정보에 대한 해독을 시도할 수 있다. 그러나 복호화 권한이 있는 그룹은 특정 보안 등급을 획득한 그룹에 한하며, 만약 서버 관리자라 할지라도 해당 보안 등급 키를 알지 못하면 암호화된 데이터를 복호화할 수 없다. 즉, 단순 서버 관리자나 제3의 위탁 관리자는 개인정보를 열람할 수 없으며, 특정 등급의 키를 생성 가능한 권한이 있는 내부자에 의해서만 열람될 수 있으므로 개인정보를 안전하게 관리할 수 있다.

4.1.3 악의적 해킹 및 외부 노출 방지

서버가 해킹되어 데이터베이스상의 값이 노출된 경우를 생각해 볼 수 있다. 이 경우 서버의 데이터베이스에는 등급별 암호화 메커니즘에 의해 암호화된 데이터만 저장되어 있으며, 만약 데이터베이스 접근권한이 노출되었거나 데이터 자체가 노출되더라도 적절한 보안등급 열람 권한을 획득하지 못하면 데이터를 복원할 수 없다.

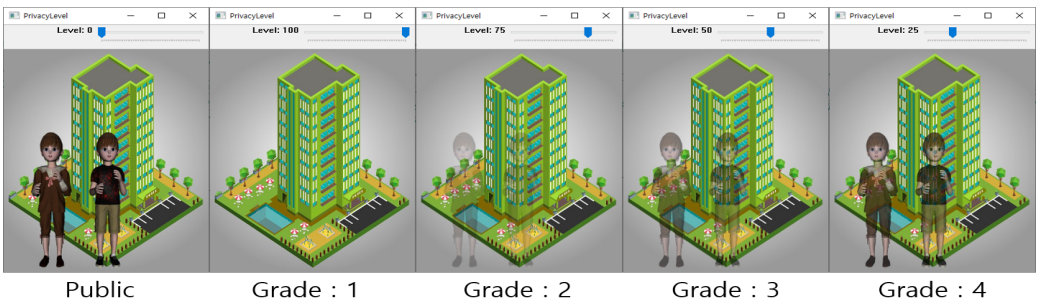

그림 7. 등급에 따른 정보공개의 변화
Fig. 7. Changes in information disclosure

모든 데이터 속성은 등급별로 암호화되어 있어 만약 하위등급의 키를 인지하고 있더라도 이보다 상위등급의 키는 생성할 수 없으며, 접근 권한을 벗어나는 등급의 정보는 열람이 불가능하다.

4.2 효율성 측면

본 절에서는 제안한 암호화 메커니즘 방식에 대한 성능을 측정하였다. 본 절에서 측정한 성능은 데이터 사이즈 단위로 연산에 소요되는 경과시간(Elapsed time)을 의미하며, 제안한 암호화 메커니즘 방식이 처리되는 데 필요한 경과시간을 각각의 데이터 사이즈 단위로 측정하여 그림으로 나타내었다. 실험에 사용된 각각의 데이터 사이즈는 1K부터 512K 사이즈 구간에 대하여 밀리세컨드(ms)단위로 제안한 암호화 메커니즘의 성능을 측정하였다. 성능 측정을 위하여 Intel i5-10400 CPU와 16G 사이즈의 RAM 환경의 하드웨어가 사용되었다. 그림 8은 제안한 방식의 성능 측정 결과를 나타낸다.

제안한 방식은 보안 등급 설정 및 암복호화에 필요한 별도의 외부 서버 통신과 키 관리 서버를 필요로 하지 않는다. 또한 등급별 키 생성 메커니즘에 의하여 권한이 있는 자는 별도의 통신 없이 바로 키 생성이 가능하다는 장점이 있다. 따라서 제안한 방식을 통하여 메타버스 환경에서의 효율적인 프라이버시 보호를 실현할 수 있다.

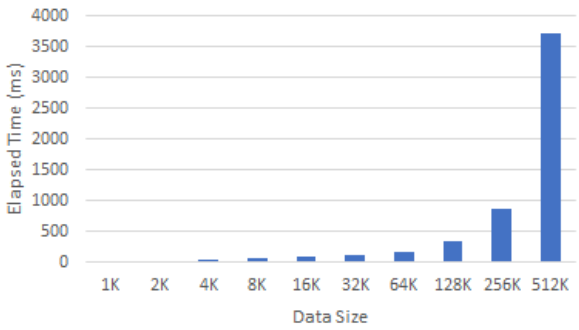

그림 8. 제안방식 성능 측정 결과
Fig. 8. Performance measurement results

V. 결 론

메타버스는 다양한 산업 분야에 응용이 가능하여 최근 들어 큰 관심을 모으고 있으며, 향후 미래사회에서는 메타버스가 주요한 플랫폼으로 자리잡게 될 것이다. 특히 현실세계와 밀접한 실감기술 기반의 메타버스 환경이 성공적으로 자리잡기 위해서는 메타버스 환경의 프라이버시 보호 대책이 필히 고려되어야 한다. 현실세계와 밀접한 디지털 세계로 사용자가 인지하지 못하는 사이 개인정보가 송출될 수 있으며, 이 과정에서 노출된 개인정보는 상업적인 목적이나 악의적인 목적으로 활용될 수 있다.

따라서 본 논문에서는 안전한 메타버스 환경을 위한 속성레벨 프라이버시 보호 메커니즘을 제안하였다. 제안한 방식은 개인정보의 속성 단위로 자동화된 등급분류 방식에 따라 동적인 등급을 부여할 수 있으며, 각 등급별 암호화 키를 별도의 키 관리 서버 없이 생성할 수 있다. 또한 각각의 등급별 암호화 키는 제안한 메커니즘에 의해 적절한 권한을 가진 자에 의해서만 생성될 수 있다. 또한 외부 위탁시에 별도의 등급과 그에 따른 키를 추가적으로 생성할 수 있어 취급 및 관리에 유용하며, 스니핑 공격, 내부자 공격, 외부 데이터 노출로부터 안전을 보장할 수 있다.

향후 다양한 센싱기술, 실감기술 등의 메타버스를 위한 기반기술이 발전함에 따라 메타버스의 품질은 크게 향상될 것이며, 현실세계와 더욱 밀접한 메타버스 서비스도 제공될 것이다. 그러나 메타버스 환경에 대한 보안 연구는 아직 많이 진행되지 않은 편이다. 진화하는 메타버스의 역기능 방지를 위한 선제적인 보안기술 연구 또한 시급히 진행되어야 할 것이다.

References

[1] J. Y. Chun, H. M. Lee, S. J. Noh, and Eung-Hyuk Lee, "The Static Analysis of Visual Scanning using HDM-VR Driving Simulator", The Journal of Korean Institute of Information Technology, Vol. 19, No. 9, pp. 133-140, Sep. 2021. https://doi.org/10.14801/jkiit.2021.19.9.133.

[2] J. Dionisio, W. Burns III, and R. Gilbert, "3D Virtual worlds and the metaverse: Current status and future possibilities", ACM Computing Surveys,

Vol. 45, No. 3, pp. 1-38, Jun. 2013. https://doi.org/10.1145/2480741.2480751.

[3] M. Choi and J. Y. Kim, "A Study of Converging Technologies towards the Development of AR/VR-based u-Healthcare Systems", Journal of KIIT, Vol. 19, No. 7, pp. 113-122, Jul. 2021. https://doi.org/10.14801/jkiit.2021.19.7.113.

[4] E. Ha, K. Choi, and S. Y, "VR Remote Education System using Real-Time Motion Capture", Journal of KIIT, Vol. 20, No. 1, pp. 171-180, Jan. 2022. https://doi.org/10.14801/jkiit.2022.20.1.171.

[5] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy", IEEE Technology and Society Magazine, Vol. 37, No. 2, pp. 52-61, Jun. 2018. https://doi.org/10.1109/MTS.2018.2826060.

[6] S. Y. Jeong, C. H. Seo, J. M. Cho, S. H. Jin, and S. H. Kim, "Security threat analysis in Metaverse, an extended virtual reality", Review of KIISC, Vol. 31, No. 6, pp. 47-57, Dec. 2021.

[7] J. Smart, J. Cascio, and J. Paffendorf, "Metaverse roadmap: pathways to the 3D web", A cross-industry public foresight project, 2007.

[8] J. E. Jeon, "The Effects of User Experience-Based Design Innovativeness on User-Metaverse Platform Channel Relationships in South Korea", Journal of Distribution Science, Vol. 19, No. 11, pp. 81-90, Nov. 2021. https://doi.org/10.15722/jds.19.11.202111.81.

[9] S. Mortezapoor and K. Vasylevska, "Safety and Security Challenges for Collaborative Robotics in VR", Proc. of the 1st International Workshop on Security for XR and XR for Security, 2021.

[10] T. Scargill, Y. Chen, S. Eom, J. Dunn, and M. Gorlatova, "Environmental, User, and Social Context-Aware Augmented Reality for Supporting Personal Development and Change", 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, Christchurch, New Zealand, Mar. 2022. https://doi.org/10.1109/VRW55335.2022.00042.

[11] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and Wei Cai, "Metaverse for Social Good: A University Campus Prototype", Proc. of the 29th ACM International Conference on Multimedia, pp. 153-161, Oct. 2021. https://doi.org/10.1145/3474085.3479238.

[12] W. C. Ng, W. Y. B. Lim, J. S. Ng, Z. Xiong, D. Niyato, and C. Miao, "Unified Resource Allocation Framework for The Edge Intelligence-Enabled Metaverse", In ICC 2022-IEEE International Conference on Communications, pp. 5214-5219, May. 2022. http://dx.doi.org/10.1109/ICC45855.2022.9838492.

저자소개

이 동 혁 (Donghyeok Lee)

2007년 2월 : 동국대학교 전자상거래기술전공(공학석사)
2018년 2월 : 제주대학교 컴퓨터교육전공(공학박사)
2007년 6월 ~ 2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월 ~ 2015년 6월 : KT 플랫폼개발단 과장
2018년 3월 ~ 2021년 2월 : 제주대학교 과학기술사회연구센터 학술연구교수
2021년 3월 ~ 현재 : 청주대학교 교양학부/소프트웨어융합학부 조교수
관심분야 : 메타버스 보안, 지능형 영상보안, 5G 보안, IoT 보안, 프라이버시 보호, 컴퓨터교육