논문 2023-4-13 http://dx.doi.org/10.29056/jsav.2023.12.13

디지털휴먼 구성요소의 SW 패키지 관리를 위한 분산신원증명 기반 아바타 명세서 검증 기법

최창준*, 김현수*, 박경엽*, 노창현*, 신동명*†

A DID-based Avatar Bill of Materials Verification Method for SW Package Management of Digital Human Components

Chang-Jun Choi*, Hyun-Soo Kim*, Kyung-Yeob Park*, ChangHyun Roh*, Dong-Myung Shin*†

요 약

메타버스 환경에서 활용되는 3D 아바타는 가상공간 내에서 사용자의 개성을 표현하는 주요 매개체로 활용된다. 이러한 아바타는 단순한 외모 데이터가 아니라 다양한 구성요소로 이루어져 있어 사칭 및 도용과 같은 사이버범죄에 활용되지 않도록 체계적인 관리가 필요하다. 하지만, 중앙 집중식으로 사용자 개인정보 및 아바타 관련 정보를 관리하는 메타버스 환경에서 사이버범죄 사례가 증가하면서 보안 문제가 대두되고 있다. 이에 따라, 본 논문에서는 분산신원증명 기술을 활용하여 아바타 소유자가 개인정보와 아바타 정보를 안전하게 관리하고, 이를 메타버스 환경에서 신뢰할 수 있는 방법으로 검증할 수 있는 방안을 제안하고자 한다. 제안된 기법에서 활용되는 아바타 명세서는 3D 아바타 파일 정보를 BoM(Bill of Materials) 형태로 제공하여 아바타의 상업적 이용과 무단 재배포·수정 가능 여부를 검증할 수 있도록 하며, 서비스 제공자인 메타버스 플랫폼에서는 이를 통해 아바타 소유자의 신원 일치성을 검증할 수 있다.

Abstract

The 3D avatar used in the metaverse environment is used as a main medium for expressing the user's personality within the virtual space. These avatars are not just appearance data, but are composed of various components, so systematic management is needed to prevent them from being used for cybercrime such as impersonation and theft. However, security issues are emerging as cybercrime cases increase in a metaverse environment that centrally manages user personal information and avatar-related information. Accordingly, this paper proposes a way for avatar owners to safely manage personal information and avatar information using distributed identity verification technology and verify it in a reliable way in a metaverse environment. The avatar specification used in the proposed technique provides 3D avatar file information in the form of a bill of materials (BoM) to verify the commercial use of avatars and whether they can be redistributed or modified without permission, and the service provider, the metaverse platform, can verify the identity consistency of the avatar owner.

한글키워드 : 디지털휴먼, 분산신원증명, 소프트웨어 자재명세서, 메타버스, 오픈소스 3D 아바타 파일 포맷

keywords : Digital Human, DID(Decentralized Identity), SBoM(Software Bill of Materials), Metaverse, Open-source 3D Avatar File Format

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부
† 교신저자: 신동명(email: roland@lsware.com)

접수일자: 2023.11.30. 심사완료: 2023.12.09.
게재확정: 2023.12.20.

1. 서 론

메타버스(Metaverse)는 가상현실(VR, Virtual Reality)과 증강현실(AR, Augmented Reality) 기술 등을 결합한 가상공간으로, 사용자들이 가상공간 내에서 상호작용할 수 있도록 비교육, 엔터테인먼트, 소셜 네트워킹 등과 같은 다양한 서비스를 제공해주는 플랫폼이다. 현실 세계를 모방하는 메타버스 플랫폼에서는 사용자의 외모 및 스타일 등이 반영된 3D 아바타를 통해 몰입형 현실감을 제공한다. 아바타는 가상공간에서 사용자의 개성을 자유롭게 표현할 수 있게 해주는 주요 매개체 역할을 하며, 서비스를 이용하는 플랫폼 사용자 간 상호작용을 촉진시키기 위해 다양한 분야에서 활용되고 있다[1].

이러한 3D 아바타는 사용자의 외모나 스타일을 반영하는 단순한 데이터가 아닌 다양한 구성요소(e.g., 상의, 하의, 악세서리 등)들로 이루어져 있다. 메타버스 환경에서는 복합적인 요소로 이루어진 아바타 정보를 효율적으로 관리하고, 이에 따른 아바타 사용자의 신원과 아바타 구성요소 정보를 안전하게 보호하는 것이 중요한 보안 과제로 대두되고 있다. 하지만 메타버스 내에서의 사용자 개인정보 및 아바타 정보가 중앙 집중식으로 관리되면서 사용자의 개인정보 통제 권한 제한과 서로 다른 플랫폼 간 아바타 정보 호환성 문제가 발생하고 있다. 특히, 실사 데이터를 활용한 아바타 생성으로 인해 사칭, 도용 등과 같은 사이버범죄 위협이 증가하고 있다.

아바타 사용자의 개인정보 보호와 아바타의 일관성 유지를 위해서는 아바타 관련 데이터를 신뢰성있게 검증하고, 서로 다른 메타버스 플랫폼에서 아바타 소유자 신원 검증이 필수적으로 고려되어야 한다. 또한, 여러 메타버스 플랫폼에서 아바타를 통해 사용자의 신원을 증명함과 동시에 아바타 정보를 개인이 제어하기 위해서는 아바타 소유자가 자신의 아바타 구성요소에 대한 속성 정보를 관리할 수 있어야 한다.

이에 따라, 본 논문에서는 3D 모델링에 사용된 아바타 구성요소의 소프트웨어 패키지 정보를 명세서 형태로 생성하고, 더 나아가 분산신원증명(DID, Decentralized Identify) 기술을 활용하여 탈중앙화된 네트워크 환경에서 개인정보에 대한 자기 결정권을 보장하여 이종 메타버스 환경에서 아바타 소유자의 신원을 신뢰성있게 검증하는 방법을 제안하고자 한다.

2. 기술적 배경

2.1 오픈소스 3D 아바타 파일 포맷

메타버스에서는 사용자를 대변하는 3D 아바타를 통해 플랫폼 사용자 간 실시간 상호작용을 가능하게 하며, 사용자의 개성을 표현하는 외모, 동작, 의상 등을 현실적으로 반영하기 위해 다양한 3D 아바타 파일 포맷들을 지원하고 있다. 그러나, 3D 파일 포맷은 일반적으로 특정 3D 모델링 소프트웨어 및 응용 프로그램에 종속되어 있으므로 서로 다른 소프트웨어와의 상호호환성 문제가 발생하며, 이러한 문제를 방지하기 위해 최근 gITF 2.0 표준을 준수하는 오픈소스 3D 파일 포맷들이 다양하게 표준화 및 개발되고 있다.

대표적인 포맷인 VRM(Virtual Reality Model)은 플랫폼 비의존적인 오픈소스 3D 아바타 범용 파일 포맷으로, Unity 등과 같은 게임 엔진을 통해 다양한 플랫폼 환경에 적용된다[2]. 이는 3D 캐릭터를 모델링하기 위해 3D 콘텐츠의 기하학적 정보, 텍스처, 애니메이션 및 관련 제작 정보 등을 제공하며, 3D 콘텐츠의 폭력적 및 성적 표현, 인격 허락 범위 및 상용 이용허락 관련 정보들을 참조할 수 있도록 라이선스 조건 정보를 URL 형태로 명시하고 있다[3]. VRM 파일 포맷에서의 제작 및 라이선스 정보는 표 1과 같다.

표 1. VRM 파일에서의 제작 및 라이선스 정보[4]
Table 1. Product & License Information in VRM File

구 분	항 목	설 명
제작 정보	파일 제목	- 모델링된 3D 콘텐츠의 이름
	파일 버전	- 모델링된 3D 콘텐츠의 버전
	제작자 정보	- 3D 콘텐츠를 제작한 개인, 그룹 또는 조직 정보
	연락처 정보	- 3D 콘텐츠 제작자의 이메일 주소 및 웹사이트의 URL 등
	참조 정보	- 모델링된 3D 콘텐츠의 출처 등을 제공하는 URL 링크
라이선스 정보	의인화/특성화 관련 허가사항	- 모델링된 3D 콘텐츠의 적용 범위 및 다른 캐릭터로 의인화/변형 가능 여부를 규정 **[세부 항목]** - 인격 부여 가능 유형 - 상업적 이용 가능 여부 - 콘텐츠의 폭력적/성적 표현 (행위) 허용 여부
	재배포/수정 관련 라이선스	- 모델링된 3D 콘텐츠의 재배포 및 수정 유형을 규정 **[세부 항목]** - 재배포/수정 관련 유형(CCL) - 재배포/수정 관련 기타 라이선스 URL 링크

VRM 파일에는 3D 아바타의 Materials 정보를 JSON 포맷으로 표현하며, 제작 및 라이선스 정보를 포함하고 있다. 제작 정보에는 VRM 제작자를 식별할 수 있는 정보가 포함되며, 라이선스 정보에는 아바타의 인격 허락 범위, 3D 파일의 재배포/수정 허용 범위와 관련된 CCL(Creative Commons License) 유형 등이 포함된다.

2.2 SBoM 개념 및 구성요소

SBoM(Software Bill of Materials)은 소프트웨어 제품의 오픈소스 패키지 및 라이브러리 정보 등이 포함된 문서로, 소프트웨어 컴포넌트의 버전, 라이선스 정보, 의존성, 출처 등과 같은 정보를 제공한다. 최근 솔라윈즈 해킹, Log4j 취약점 등과 같은 소프트웨어 공급망 공격 사례가 급증하면서 소프트웨어의 구성요소를 구조화하여 추적할 수 있는 SBoM의 중요성이 대두되고 있다.

SBoM은 일반적으로 SPDX(Software Package Data eXchange)와 같은 개방형 표준 포맷으로 작성되며, 이를 통해 오픈소스 패키지 및 라이브러리 정보 간 종속성 관계를 체계적으로 기록 및 추적할 수 있어, N차적으로 업데이트되거나 재사용되는 오픈소스 패키지 간 의존성 및 취약점 등을 신속하게 식별할 수 있다[5]. 미국 국가통신정보청(NTIA, National Telecommunications and Information Administration)에서는 소프트웨어 공급망 환경에서의 보안 강화, 소프트웨어 구성요소의 취약점 관리, 라이선스 준수 등을 위해 표 2와 같이 SBoM의 최소 구성요소를 정의하여 공급망 보안 및 관리에 필요한 정보를 효율적으로 기록하고 활용할 수 있도록 지원하고 있다.

표 2. SBoM의 최소 구성요소[6]
Table 2. Minimum Required Elements of SBoM

데이터 필드	설 명
공급자 이름	- 컴포넌트를 생성 및 정의한 주체의 이름
컴포넌트 이름	- 최초 공급자에 의해 정의된 SW 이름
컴포넌트 버전	- 이전에 식별된 버전에서 SW의 변경사항을 명시하기 위해 사용하는 식별자
기타 고유 식별자	- 컴포넌트를 식별하는 데 사용되거나, 관련 DB의 조회 키 역할을 하는 식별자
종속성 관계	- 업스트림 컴포넌트 *X*가 SW *Y*에 포함된다는 관계를 명시한 정보
SBoM 작성자	- 컴포넌트의 SBoM을 생성한 주체의 이름
SBoM 생성 일자	- SBoM이 생성된 날짜 및 시간 기록

NTIA에서는 SBoM 최소 구성요소 외에도 공급망 보안 강화를 위해 구성요소의 해시, 라이프사이클 정보, 라이선스 정보 등과 같은 데이터 필드를 권장하고 있다[7]. 이를 통해 소프트웨어에서의 잠재적인 위험 요소를 파악하고 사전 위험분석을 수행할 수 있으며, 구성요소의 아웃소싱 정보 등을 확인 및 검증하여 소프트웨어 구성요소의 보안성과 안정성을 확보할 수 있다.

2.3 분산신원증명 생태계 구조

분산신원증명(DID) 기술은 기존 사용자 인증 과정에서 개인정보를 제3의 신뢰 기관이 통제하는 방식에서 벗어나, 본인이 관리하는 자기주권 신원증명(SSI, Self-Sovereign Identity) 모델을 통해 정보 노출 없이 신원인증에 필요한 개인정보를 본인이 선택적으로 제공할 수 있도록 하는 디지털 신원증명 기술이다[8]. W3C(World Wide Web Consortium)에서 제시한 SSI 모델 기반 분산신원증명의 기술 흐름도는 그림 1과 같다.

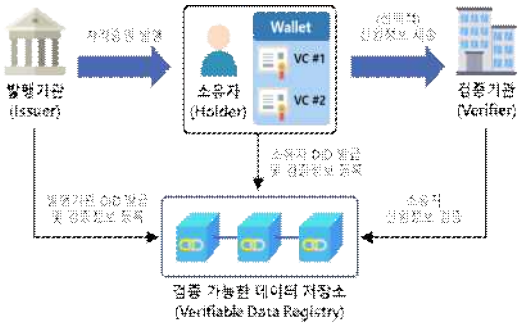

그림 1. SSI 모델 기반 분산신원증명 기술 흐름도
Fig 1. SSI model-based DID Flowchart

발행기관은 소유자가 제공한 Claim 정보를 기반으로 검증 가능한 자격증명(VC, Verifiable Credential)을 발행한다. VC에는 식별 대상의 신원정보가 기록되어 있으며, 발행된 VC는 소유자의 단말기 지갑에 저장된다. 추후 소유자가 특정 서비스를 이용하고자 할 때, 자신이 보유한 VC 중 인증에 필요한 정보만을 선택하여 검증 가능한 프레젠테이션(VP, Verifiable Presentation)으로 생성 후 검증기관(서비스 제공자)에게 제출한다. VP를 수신한 검증기관은 검증 가능한 데이터 저장소에서 소유자/발행기관의 DID 및 공개키를 조회하여 소유자 신원정보의 진위여부 및 VC 위변조 여부를 검증하고, 검증 성공 시 소유자가 요구하는 서비스를 제공한다[9].

3. 검증 가능한 아바타 명세서

최근 메타버스 내에서의 사칭, 도용 등을 통한 사이버범죄 사례가 증가하면서 사용자 개인정보 및 아바타 관련 정보의 보안이 중요해지고 있다. 메타버스의 특성상, 가상공간 내에서 사용자 간 미디어 거래 등과 같은 서비스들이 활발하게 이루어지기 때문에 다양한 유형의 사용자 개인정보들이 수집되고 있다. 이러한 사용자 개인정보들은 서비스 개선을 위해 데이터 레이크와 같은 중앙 집중식 레포지토리에서 저장 및 관리되는데, 이로 인해 사용자의 개인정보 통제 권한이 제한될 뿐만 아니라 서로 다른 메타버스 플랫폼 간에 아바타 정보가 연동되지 않아 아바타 소유자의 신원정보에 대한 호환성 문제가 발생하고 있다.

특히, 이 과정에서 사용자의 실사 데이터(e.g., 얼굴 도형, 신체 정보 등)를 적용하여 아바타를 생성할 경우, 사칭·도용 등과 같은 사이버범죄가 발생[10]할 수 있으므로 서로 다른 메타버스 플랫폼에서 아바타에 대한 소유자 신원 검증을 필수적으로 수행할 수 있어야 한다.

또한, 메타버스와 같은 디지털 환경에서는 콘텐츠 불법 복제 및 무단 상업 이용 등을 방지하기 위해 콘텐츠의 저작권, 상업적 이용, 재배포, 수정, 라이선스 수익화, 유지 관리 등을 명확하게 정의하는 것이 중요하다. 특히, 사용자 아바타와 관련된 정보, 아바타 구성요소의 라이선스 및 권한을 명시하여 아바타 정보의 정확성과 신뢰성을 보장할 수 있어야 하며, 이를 통해 아바타 구성요소의 불법 사용을 방지할 수 있어야 한다.

이에 따라, 본 장에서는 VRM 파일 포맷의 소프트웨어 패키지 정보를 관리하기 위해 아바타 명세서를 검증 가능한 형태로 생성하고, 이를 통해 서로 다른 플랫폼에서 아바타 소유자의 신원을 보장할 수 있는 방안을 기술하고자 한다.

3.1 아바타 명세서(ABoM) 생성

오픈소스 3D 파일 포맷인 VRM은 일반적으로 GitHub와 같은 웹 기반 호스팅 서비스에서 공유되거나, VroidHub와 같은 3D 모델 공유 플랫폼에서 배포된다. 본 논문에서는 웹 상에서 공유되고 있는 기존 VRM 파일의 제작·라이선스 정보 및 3D 모델링에 사용된 소프트웨어 패키지 정보 등을 문서 형태로 관리하기 위해 아바타 명세서(ABoM, Avatar Bill of Materials)를 제공한다.

아바타 명세서는 VRM 파일의 오픈소스 소프트웨어 패키지와 관련된 메타데이터를 표준 데이터 교환 포맷으로 제공하기 위해 SPDX 표준을 기반으로 생성되며, SBoM의 최소 구성요소와 NTIA의 권장 데이터 필드인 소프트웨어 패키지(구성요소) 해시값, VRM 파일의 제작·라이선스 정보를 확인할 수 있는 레퍼런스 URL이 포함된다. SPDX 포맷으로 생성된 원본 아바타 명세서는 3D 아바타 제작자의 GitHub 레포지토리에서 업데이트 및 관리되며, 블록체인 원장에 기록되어 VRM 파일에 사용된 오픈소스 소프트웨어 구성 정보에 대한 신뢰성 및 투명성을 제공한다.

3.2 아바타 구성요소 VC 발행

본 논문에서는 구성요소의 SW 패키지 정보 및 VRM 제작·라이선스 정보를 검증 가능한 형태로 제공하기 위해 아바타 구성요소의 VC 데이터 구조를 그림 2와 같이 정의하였다. 아바타 구성요소 VC에는 VRM 파일에 사용된 소프트웨어의 구성 정보를 식별 및 파악하기 위해 아바타 명세서의 URL이 포함되며, 아바타 소유자 DID로 소유자 신원을 식별한다. 또한, 구성요소의 대표 이미지를 IPFS(Inter Planetary File System)와 같은 P2P 분산 파일 시스템에 저장하여 원본 이미지의 무결성을 확보하고, 해당 이미지의 레퍼런스 해시 값을 자격증명 형태로 제공한다.

아바타 명세서에 기록되어 있는 VRM 제작·라이선스 정보의 레퍼런스 URL의 경우, 외부 레포지토리 혹은 웹 상의 특정 위치를 가리키는 단순 참조 정보이기 때문에 데이터의 무결성 및 가용성을 보장할 수 없다. 본 제안 방식에서는 이를 방지하기 위해 VRM 3D 파일 포맷의 원본 메타데이터를 아바타 구성요소 VC에 포함시켜 VRM 제작·라이선스 정보의 신뢰성을 보장한다.

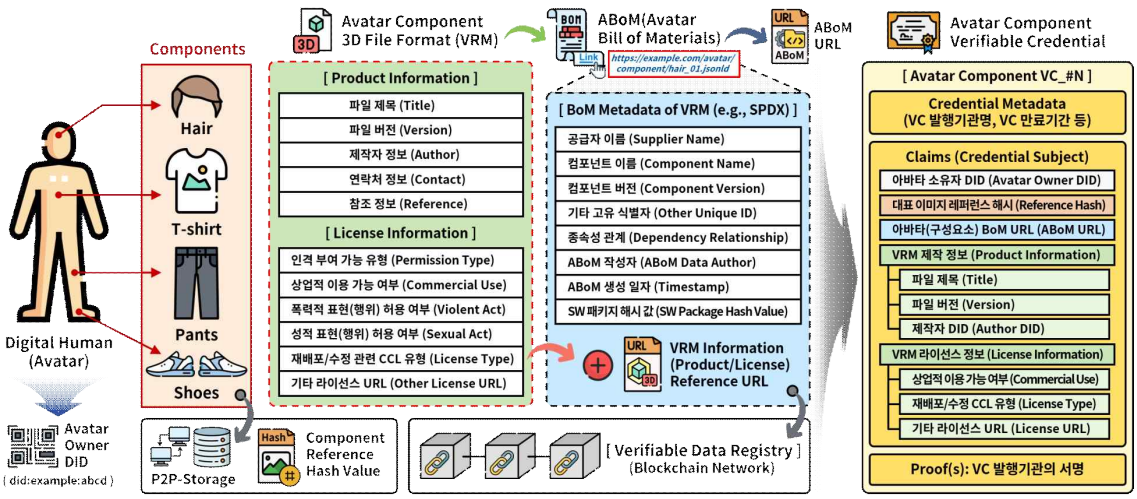

그림 2. 아바타 구성요소의 검증 가능한 자격증명(VC) 데이터 구조
Fig 2. Verifiable Credential Data Structure of Avatar Components

아바타 구성요소 VC는 그림 3과 같이 Linked Data 형식인 JSON-LD 포맷으로 구성되기 때문에 객체 내에 속성 정보뿐만 아니라 속성 정보의 URL을 함께 제공하여 서로 다른 서비스 및 시스템 간에 데이터 연계를 용이하게 한다. 해당 데이터 구조에서의 VC 발행기관은 VRM 컨소시엄 등이 될 수 있으며, Claim(e.g., 아바타 구성요소) 정보의 유효성을 보증하기 위해 VC 관련 ID 및 Schema 발급내역은 블록체인 원장에 기록된다.

그림 3. 아바타 구성요소 VC 예시
Fig. 3. Example of Avatar Component VC

@context는 VC 데이터 형식을 정의한 파일의 URL 정보를 나타내는 배열 형태의 속성으로, 여러 시스템에서 VC를 서로 교환할 때 호환성을 유지하기 위한 중요한 정보이다. id는 VC를 식별하는 URI 형태의 정보이며, 필수적인 요소는 아니지만 객체를 명확하게 참조하기 위해 사용된다. type은 해당 데이터가 어떤 유형인지 정의하며, VC는 “VerifiableCredential”과 같이 기록된다. issuer는 발행기관의 정보를 나타내는 URI 또는 DID 정보 등을 포함한다. issuanceDate와 expirationDate는 VC의 발행시간 및 만료 기간을 의미하며, credentialSubject에는 해당 VC가 명시하고 있는 식별 대상(아바타 소유자)의 신원정보(아바타 구성요소)들이 기록되어 있다. proof에는 VC가 위조되지 않고, 유효한 VC인지 판별하기 위해 발행기관의 서명 값 등이 포함된다[11].

VC 발행기관이 발행한 아바타 구성요소 VC는 아바타 소유자 디바이스와 연동된 지갑에 저장된다. 아바타 소유자의 디바이스에서 애플리케이션 형태로 설치되어 있는 지갑의 경우, 사용자 신원정보 유출 및 위변조를 방지하기 위해 신뢰 실행환경(TEE, Trusted Execution Environment) 혹은 디바이스의 물리적인 환경에서 하드웨어 보안모듈(HSM, Hardware Security Module)을 이용하여 사용자 개인키 및 신원정보를 안전하게 관리할 수 있다. 아바타 소유자의 지갑에 저장된 각 아바타 구성요소 VC들은 메타버스 플랫폼에서의 아바타 착장 정보를 나타내며, 아바타의 신원을 인증하기 위한 자격증명 정보로 활용된다.

3.3 아바타 VP 생성 및 검증

아바타 소유자는 자신이 보유한 아바타 구성요소 VC 중 검증에 필요한 정보 혹은 아바타 소유권을 증명하기 위한 VC를 적절히 선택하여 아바타 VP를 생성한다. 아바타 VP는 그림 4와 같이 아바타 소유자의 DID 식별자, 구성요소 대표 이미지의 레퍼런스 해시 값, 아바타 명세서 URL 링크, VRM 제작·라이선스 정보로 구성될 수 있다. 아바타 VP를 수신한 메타버스 플랫폼에서는 아바타 소유자 및 VC 발행기관의 DID를 통해 블록체인 원장에서 DID Document를 조회하여 아바타 소유자와 VC 발행기관의 공개키를 추출한다. 이후 다음과 같이 VP 검증을 수행한다.

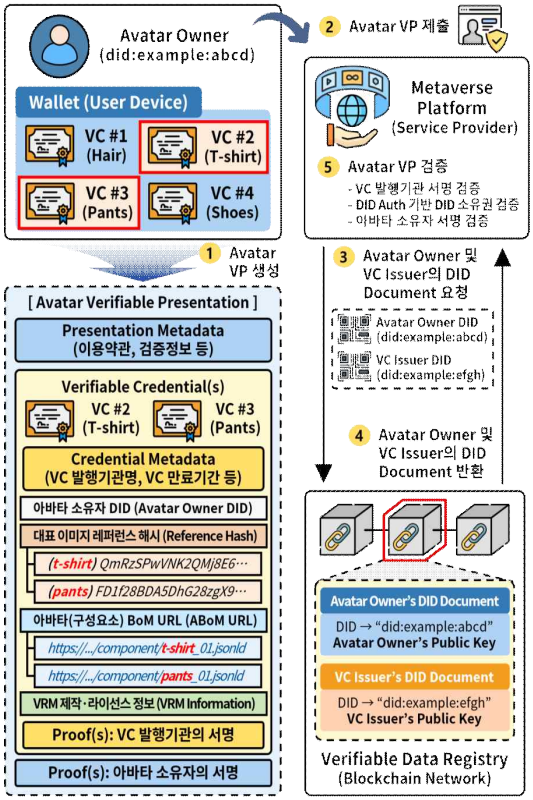

그림 4. 아바타 VP 생성 및 검증 프로세스
Fig. 4. Avatar VP Creation and Validation Process

3.3.1 VC 발행기관 서명 검증

아바타 구성요소 VC의 Proof 필드는 VC가 위변조되지 않았고, 유효한 VC인지 판별하기 위해 사용되며, 내부적으로 VC 발행기관의 서명 값과 서명에 사용된 암호 알고리즘, 서명 생성시간 등이 포함되어 있다. 해당 필드는 규격이 정해져 있지 않아 인증 수단으로 사용되는 암호 알고리즘들이 다양하게 정의될 수 있다. 메타버스 플랫폼은 블록체인 원장에서 아바타 구성요소 VC ID와 Schema 발급내역을 확인한 후, 아바타 구성요소 VC 발행기관의 공개키로 VC 서명 값을 검증한다. 이를 통해 아바타 구성요소 VC가 올바르게 발행되었고, 구성요소 정보가 위변조되지 않았다는 것을 확인한다.

3.3.2 DID Auth 기반 DID 소유권 검증

메타버스 플랫폼은 일회성 인증을 위한 임의의 Challenge 값을 생성하여 아바타 소유자의 공개키로 암호화한 후, 아바타 소유자에게 전송한다. 아바타 소유자는 암호화된 Challenge 값을 DID Document의 공개키와 쌍을 이루는 개인키로 복호화하여 Response 값을 생성하고, 이를 메타버스 플랫폼에 전송한다. 메타버스 플랫폼은 원본 Challenge 값과 아바타 소유자가 전달한 Response 값의 동일 여부를 비교 검증하여 아바타 소유자의 DID 식별자가 VC에서 명시한 올바른 식별 대상(Credential Subject)인지 확인한다.

3.3.3 아바타 소유자 서명 검증

메타버스 플랫폼에서는 아바타 VP를 제출한 사용자가 실제 아바타 소유자인지 확인하고, 제출된 아바타 VP가 위변조되지 않았는지를 검증하기 위해 아바타 소유자의 DID Document에서 추출한 공개키를 활용한다. 아바타 VP의 Proof 필드에는 아바타 소유자가 생성한 서명 값과 함께, VP의 유출을 방지하고 재사용을 방지하기 위한 추가적인 속성 정보도 포함한다. 이러한 속성 중에는 재전송 공격(Replay Attack)을 방지하기 위한 Challenge 값과 허가되지 않은 도메인에서의 아바타 VP가 재사용되는 것을 방지하기 위한 Domain 값이 존재하며, 이를 통해 사용된 아바타 VP가 다른 플랫폼에서 부적절하게 재사용되지 않도록 보호한다[12]. 아바타 소유자의 서명 값은 아바타 소유자의 공개키를 통해 검증할 수 있으며, 서명 검증 성공 시 메타버스 플랫폼에서는 아바타 VP가 실제 아바타 소유자에 의해 생성되었고, 아바타 정보가 위변조되지 않았음을 확인할 수 있다. 아바타 소유자의 신원 검증이 성공적으로 완료된 이후 메타버스 플랫폼에서는 아바타 소유자가 요구하는 서비스를 제공한다.

3.4 아바타 명세서 검증 시스템 구현방안

아바타 명세서를 이용하여 아바타 소유자의 신원을 검증하기 위해서는 SSI 모델 기반 DID 기술을 실현할 수 있는 탈중앙화된 신원인증 시스템이 필요하다. 본 논문에서 제안한 아바타 명세서 검증 기법의 경우, 독립적인 신원인증 체계를 지원하는 하이퍼레저 인디(Hyperleder Indy)와 같은 오픈소스 블록체인 프레임워크를 활용할 수 있다. 하이퍼레저 인디는 사용자의 디지털 신원을 관리하기 위해 인증 관련 툴킷과 라이브러리를 지원하여 신뢰할 수 있는 신원 검증을 제공할 뿐만 아니라, 신원 관리 표준 준수를 통해 서로 다른 플랫폼 간의 호환성을 보장한다. 구체적으로, 시스템 관리자는 indy-node를 기반으로 분산 네트워크 환경에서 SSI 데이터에 특화된 노드를 설정하여 합의에 필요한 네트워크 Pool을 생성하고, indy-sdk에서 지원하는 RESTful API를 통해 디지털 신원을 생성, 저장, 검증함으로써 사용자의 신원을 효과적으로 관리할 수 있다.

또한, 프라이빗 블록체인 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)을 통해 아바타 명세서에 대한 버전 추적 및 변동 이력 관리 등을 수행할 수 있다. 하이퍼레저 패브릭에서는 월드 스테이트(World State)라는 데이터베이스를 통해 블록체인 원장 데이터의 현재 상태를 기록 및 조회하며, 이를 통해 아바타 명세서의 최신 버전과 상태 정보를 유연하게 관리한다. 원장에 기록된 아바타 명세서들은 허가된 참여 노드만이 접근할 수 있는 채널 내에서 관리되며, 체인코드(i.e., 스마트 컨트랙트)를 통해 적절한 권한이 있는 사용자만이 업데이트를 수행할 수 있도록 한다. 블록체인 네트워크에 참여한 각 피어 노드들은 아바타 명세서의 변경 내역에 대한 트랜잭션 실행 결과를 상호 검증하여 해당 결과를 원장에 기록함으로써 데이터의 무결성을 제공한다.

4. 제안 기술 평가 및 분석

4.1 아바타 무단 상업 이용 방지

메타버스 플랫폼에서는 일반적으로 창작물의 라이선스 정보와 관련된 이용약관이 명시되어 있다. 그러나 N차 창작자가 원본 창작물의 라이선스 정보를 의도적으로 생략하는 경우, 원본 창작물을 무단으로 이용하는 문제가 발생할 수 있다. 플랫폼에서 명시하는 이용약관만으로는 창작물에 대한 저작권 이슈를 완전히 해결하기 어려울 뿐만 아니라, 개별 플랫폼의 자체 규정에 의존하는 메타버스의 특성상 N차 창작물에 대한 저작권 법 준수 여부를 확인하기 어렵다[13].

본 논문에서 제안한 “아바타 명세서(ABoM) 생성” 단계에서는 아바타 구성요소의 SW 패키지 정보 및 VRM 파일의 제작·라이선스 정보 URL을 통해 3D 아바타의 사용 권한 조건 및 파일 제작자 정보를 제공한다. 아바타 명세서를 통해 아바타 구성요소의 SW 패키지 정보를 BoM 형태로 제공함으로써, 서로 다른 메타버스 플랫폼 간에 별도의 VRM 파일 변환과정 없이도 아바타에 대한 소프트웨어 패키지 정보를 확인할 수 있도록 한다. 이를 통해 메타버스 플랫폼에서 VRM 파일의 상업적 이용 및 재배포/수정 가능 여부 등을 검증할 수 있도록 하며, N차(N≥2) 창작물이 발생할 경우, N차 창작물의 기반이 된 N-1차 창작물의 라이선스 정보와 소프트웨어 구성요소의 추적을 용이하게 한다. 이는 아바타의 변천 과정을 추적하고, 다양한 버전의 아바타들 간의 관계를 명확히 함으로써 아바타의 근원을 추적하는 데에 중요한 역할을 한다.

4.2 아바타 정보의 호환성 및 신뢰성 강화

JSON-LD 형식으로 구성된 아바타 구성요소 VC는 Linked Data 형식으로 다양한 시스템 간 데이터 연계를 용이하게 한다. 이는 서로 다른

메타버스 플랫폼이나 서비스 간에 데이터를 교환하고 활용하는 데 있어서 호환성과 유연성을 제공하는 중요한 역할을 한다. 본 논문의 “아바타 구성요소 VC 발행” 단계에서는 아바타 명세서에 포함된 VRM 파일의 소프트웨어 패키지 정보 및 제작·라이선스 정보를 검증 가능한 형태로 발행받아 해당 아바타의 3D 모델링 파일에 대한 메타데이터를 메타버스 플랫폼에서 검증할 수 있도록 한다. 아바타 구성요소 VC와 관련된 ID 및 Schema 발급내역은 블록체인 원장에 기록되어 아바타 구성요소 VC 데이터의 유효성을 보장하고, 신뢰할 수 있는 아바타 구성 정보를 서비스 제공자에게 제공한다. 이를 통해 메타버스 플랫폼에서 아바타 구성요소 VC가 아바타 소유자의 신원을 확인하는 자격증명 정보로 활용됨으로써 아바타 정보의 신뢰성을 제고할 수 있다.

4.3 아바타 소유자 신원 검증

기존의 메타버스 서비스 구조는 사용자 계정에 해당하는 아바타를 메타버스 플랫폼에 저장하여 활용하는 구조로 각 플랫폼 간 연동, 인증 기능이 대부분 제공되지 않기 때문에 사용자가 개인정보에 대한 자기결정권을 가지고 데이터 제공 여부를 관리할 수 있는 방안이 필요하다. 메타버스 환경에서 아바타 소유자의 신원을 확인하기 위해, 본 논문의 제안 방식인 “아바타 VP 생성 및 검증” 단계에서는 아바타를 식별할 수 있는 구성요소에 대한 단일 속성을 선택하여 VP에 표현하고, 해당 구성요소의 소유자 DID 식별자를 포함시켜 제공한다. 이 과정에서 생성된 아바타 VP는 서비스 제공자에게 전달되며, 수신자는 아바타 소유자의 DID Document에서 추출한 공개키로 VP를 검증함으로써 소유자의 신원을 확인한다. 이를 통해 서로 다른 3D 파일 포맷을 사용하는 복수의 메타버스 플랫폼 간 아바타 소유자에 대한 신원 일치성을 보장할 수 있다.

5. 결 론

메타버스를 형성하는 기술의 발전과 함께 사용자의 개인정보 및 아바타 정보 보안에 대한 필요성이 강조되고 있으며, 이러한 정보의 안전한 관리와 신뢰성있는 검증 절차가 중요하게 인식되고 있다. 본 논문에서는 분산신원증명 기술을 활용하여 아바타 소유자가 자신의 개인정보 및 아바타 정보를 안전하게 관리하고, 다양한 메타버스 플랫폼 환경에서 일관된 신원정보를 유지할 수 있도록 하는 아바타 명세서 검증 기법을 제안하였다. 이를 통해 아바타 소유자는 자신의 개인정보 및 아바타 관련 정보를 소유하고 통제할 수 있으며, 메타버스 플랫폼에서는 신뢰할 수 있는 방법으로 아바타 소유자에 대한 신원 일치성을 검증할 수 있다. 또한, 3D VRM 파일에 대한 사용 권한 조건, 제작 및 라이선스 정보를 BoM 형태로 제공함으로써 아바타의 상업적 이용과 무단 재배포·수정 가능 여부를 검증할 수 있도록 한다.

이러한 검증 가능한 아바타 명세서는 메타버스 사용자 개인정보와 아바타 관련 정보의 관리 측면에서 신뢰성을 제공할 뿐만 아니라, 아바타 구성요소의 불법 복제 및 무단 상업 이용을 방지하는 데 중요한 역할을 할 것으로 기대한다. 다만, 본 논문의 제안 기법을 실제 메타버스 환경에 적용할 때에는 보안적인 측면과 법적인 쟁점 등을 고려하여 신원 검증에 관한 보다 구체적이고 심층적인 연구가 요구된다.

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2023-00229451, 이종 플랫폼간 상호호환이 가능한 디지털휴먼(아바타) 연동 기술 개발)

참 고 문 헌

[1] A. Nagendran, S. Compton, W. C. Follette, A. Golenchenko, A. Compton, and J. Grizou, “Avatar led interventions in the Metaverse reveal that interpersonal effectiveness can be measured, predicted, and improved”, Scientific Reports, vol. 12, no. 1. Springer Science and Business Media LLC, 19-Dec-2022. DOI: 10.1038/s41598-022-26326-4

[2] S. Woksepp and T. Olofsson, “Credibility and applicability of virtual reality models in design and construction”, Advanced Engineering Informatics, vol. 22, no. 4. Elsevier BV, pp. 520 - 528, Oct-2008. DOI: 10.1016/j.aei.2008.06.007

[3] P.-H. Cheng, L.-W. Chen, and C.-H. Lin, “A Customizable No-Code Realistic Motion Editor for VRM-Based Avatars”, Sustainability, vol. 15, no. 2. MDPI AG, pp. 1182, 08-Jan-2023. DOI: 10.3390/su15021182

[4] VRM consortium, Inc. VRM: 3D Avatar File Format for VR. [Online]. Available: https://vrm.dev/en/ (accessed on 1 November 2023).

[5] K. Stewart, P. Odence, and E. Rockett, “Software Package Data Exchange (SPDX) Specification”, International Free and Open Source Software Law Review, vol. 2, no. 2. International Free and Open Source Software Law Review, pp. 191-196, 31-Dec-2010. DOI: 10.5033/ifosslr.v4i1.45

[6] H.-H. Son, D.-H. Kim, and S.-J. Kim, “A Study on the Software Supply Chain Security Policy for the Strengthening of Cybersecurity: Based on SBOM Policy Cases”, Journal of Digital Convergence, vol. 20, no. 2, pp. 9-20, 28-Feb-2022. DOI: 10.14400/JDC.2022.20.2.009

[7] NTIA, “Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)”, [Online]. Available: https://ntia.gov/files/ntia/publications/framingsbom_20191112.pdf (accessed on 7 November 2023)

[8] O. Dib and K. Toumi, “Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions”, Annals of Emerging Technologies in Computing, vol. 4, no. 5. International Association for Educators and Researchers (IAER), pp. 19-40, 20-Dec-2020. DOI: 10.33166/aetic.2020.05.002

[9] B. Alangot et al., “Decentralized Identity Authentication with Auditability and Privacy”, Algorithms, vol. 16, no. 1. MDPI AG, p. 4, 21-Dec-2022. DOI: 10.3390/a16010004

[10] Y.-W. Chow, W. Susilo, Y. Li, N. Li, and C. Nguyen, “Visualization and Cybersecurity in the Metaverse: A Survey”, Journal of Imaging, vol. 9, no. 1. MDPI AG, p. 11, 31-Dec-2022. DOI: 10.3390/jimaging9010011

[11] World Wide Web Consortium (W3C), Verifable Credentials Data Model 1.1, [Online]. Available: https://www.w3.org/TR/vc-data-model/ (accessed on 1 November 2023)

[12] R. Soltani, U. T. Nguyen, and A. An, “A Survey of Self-Sovereign Identity Ecosystem”, Security and Communication Networks, vol. 2021. Hindawi Limited, pp. 1 - 26, 17-Jul-2021, DOI: 10.1155/2021/8873429

[13] R. García, A. Cediel, M. Teixidó, and R. Gil, “Semantics and Non-Fungible Tokens for Copyright Management on the Metaverse and Beyond”, ACM Transactions on Multimedia Computing, Communications, and Applications. Association for Computing Machinery (ACM), 24-Feb-2023. DOI: 10.1145/3585387

저 자 소 개

최창준(Chang-Jun Choi)

2019.02 : 상명대학교 컴퓨터공학과 졸업
2021.08 : 세종대학교 정보보호학과 석사
2021.09-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 주임연구원
<주관심분야> 정보보호, 블록체인, 네트워크 보안, 분산신원증명, 저작권 기술

김현수(Hyun-Soo Kim)

2019.02 : 단국대학교 소프트웨어학과 졸업
2023.08 : 숭실대학교 AI·SW융합학과 석사
2019.01-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 선임연구원
<주관심분야> 인공지능, 머신러닝, 컴퓨터 비전, 분산신원증명, 빅데이터

박경엽(Kyung-Yeob Park)

2019.02 : 서울과학기술대학교 컴퓨터공학과 석사
2019.01-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 선임연구원
<주관심분야> 정보보호, IoT 보안, 블록체인, 빅데이터, 분산신원증명, 저작권 기술

노창현(ChangHyun Roh)

2017.08 : 순천향대학교 소프트웨어공학과 졸업
2020.02 : 순천향대학교 컴퓨터학과 석사
2020.05-2022.02 : 에스지에이퓨쳐스㈜ 컨설팅팀 사원
2022.02-현재 : 가천대학교 정보보호학과 박사과정
2022.12-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 수석연구원
<주관심분야> 정보보호, CPS 보안, 블록체인, DID, NFT, 저작권 기술, 메타버스, 디지털 휴먼

신동명(Dong-Myung Shin)

2003.02 : 대전대학교 컴퓨터공학과 박사
2001-2006 : 한국정보보호진흥원 응용기술팀 선임연구원
2006-2014 : 한국저작권위원회 저작권기술팀 팀장
2014-2016 : 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/네트워크 보안, SW 취약점 분석·감정, 블록체인 기술