메타버스: 보안 및 개인 정보 보호 문제

Ruoyu Zhao, Yushu Zhang, Youwen Zhu, Rushi Lan 및 Zhongyun Hua

추상적인—현실과 흡사한 3차원 가상 세계인 메타버스(metaverse)는 1990년대에 등장한 이래 늘 상상의 연속이었다. 최근에는 다양한 기술의 지속적인 출현과 발전으로 메타버스를 실현할 수 있어 다시 주목받고 있다. 차별을 줄이고, 개인차를 없애고, 사교하는 등 인간 사회에 많은 이익을 가져다줄 수 있다. 그러나 모든 것이 보안 및 개인 정보 보호 문제가 있으며 이는 메타버스도 예외가 아닙니다. 이 글에서는 먼저 메타버스의 개념을 분석하고 다른 VR 기술에 비해 초가상현실(Super Virtual Reality, VR) 생태계임을 제안한다. 그런 다음 사용자 정보, 커뮤니케이션, 시나리오, 상품, 그리고 즉시 잠재적인 솔루션이 그에 따라 제시됩니다. 한편, 우리는 철학적 관점에서 보안 및 개인 정보 보호 문제를 포괄적으로 해결하기 위해 새로운 버킷 효과를 활용할 필요성을 제안하며, 이는 메타버스 커뮤니티에 약간의 진전을 가져오기를 바랍니다.

나. 나서론

WAN 앨리스는 수천 마일 떨어진 곳에 사는 친구들과 몰입형 상호작용을 하고 있습니까? 밥은 순식간에 영화관에서 쇼핑 센터로 원활하게 이동할 수 있을까요? 다리에 장애가 있는 피터가 정상인처럼 서고 달릴 수 있을까요? 전 세계의 많은 사람들이 매일 이와 유사한 질문을 할 수 있습니다.

최근 유행하는 용어인 메타버스(metaverse)는 이러한 질문을 쉽게 해결할 수 있을지도 모릅니다. 사실 이것은 신생아가 아니라 palingenesis입니다. 메타버스(metaverse)라는 용어는*눈 충돌* 1992년 [1], "메타"와 "절"이라는 두 단어의 조합이었습니다. 전자는 현실 너머, 즉 가상 환경을 의미합니다. 후자는 우주를 의미하는데, 이는 사람들이 현실처럼 살기 위해 이 환경에 몰입할 수 있음을 의미합니다. 이 용어가 등장한 이후 그 정의는 라이프로깅, 미래 소셜 네트워크, 차세대 인터넷, 가상 세계 등 매우 다양해[2], 미스터리의 층을 형성합니다. 그러나 전반적으로 현실 세계에 거주하는 사용자들은 그림 1과 같은 3차원 가상 세계에 몰입하기 위해 접속 단말을 통해 메타버스에 있는 자신의 아바타를 연결하고 조작한다는 데 동의한다.

간단히 말해서, 사용자의 지시를 포함한 다양한 정보는 단말기를 전송하기 위해 센서에 의해 수집됩니다. 터미널

R. Zhao, Y. Zhang 및 Y. Zhu는 중국 Nanjing 211106, Nanjing University of Aeronautics and Astronautics, 컴퓨터 과학 및 기술 대학에 있습니다(이메일: zhaoruoyu@nuaa.edu.cn ; yushu@nuaa. edu.cn ; zhuyw@nuaa.edu.cn).

R. Lan은 Guilin 541004, China(이메일: rslan2016@163.com)에 있는 Guilin University of Electronic Technology의 Guangxi Key Laboratory of Image and Graphic Intelligent Processing에 있습니다.

Z. Hua는 Institute of Technology(Shenzhen), Shenzhen 518055, 하브 China(e-mail: hongyun@hit.edu.cn)에 있는 컴퓨터 과학 및 기술 학교에 사무실이 있습니다.

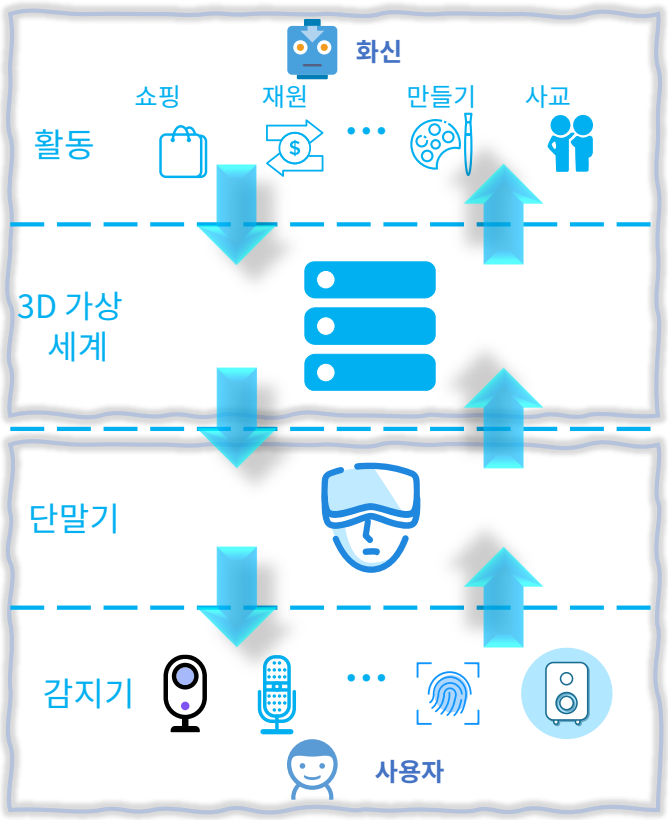

그림 1. 메타버스의 기본 인프라.

센서에서 정보를 합성한 다음 인터넷을 통해 서버로 전송하여 메타버스에서 해당 아바타를 제어합니다. 서버는 많은 사용자의 정보를 종합적으로 처리하고 3D 가상 세계에 반영합니다. 사용자가 보낸 각각의 법적 아바타 활동이 실행됩니다. 반대로, 아바타가 활동을 실행할 때 메타버스의 상태는 서버에 피드백됩니다. 예를 들어 아바타가 예술 작품을 만든 경우 콘텐츠와 같은 정보를 서버에 알려야 합니다. 서버는 모든 사용자 단말기에 방송되는 해당 3D 가상 시나리오를 기록하고 생성합니다. 터미널은 서버 정보를 수신한 후 메타버스의 실시간 시나리오를 사용자에게 표시하고 추가로 센서에 자세한 지침을 보냅니다. 각 센서는 지시에 따라 해당 신호를 보내 사용자를 몰입시킵니다. 예를 들어 메타버스에서 해당 아바타가 다른 사람과 악수할 때 손의 센서가 적절하게 반응하면 사용자에게 더 현실적입니다.

메타버스는 현실 세계의 사람들에게 많은 이점을 가져다 줄 수 있습니다. 이 글의 서두에서 언급한 문제들은 가상의 특성으로 인해 메타버스에서 잘 해결될 수 있다. 한편, 현실에서의 차별의 오랜 문제는 완화될 수 있다.

예를 들어, 신체 장애가 있는 사람들은 의식이 있는 한 메타버스에서 일반 사람들처럼 움직일 수 있습니다. 노인과 젊은이 사이에 체력의 차이가 없습니다. 성별은 더 이상 타고난 것이 아닙니다. 외모는 마음대로 바꿀 수 있습니다. 그리고 피부색과 인종은 더 이상 다른 사람들에게 알려질 필요가 없습니다.

한편, 메타버스는 명백한 가치에도 불구하고 새롭고 심각한 보안 및 개인 정보 보호 문제에 직면해 있습니다. 첫째, 아바타는 온라인 게임과 같은 다른 가상 세계보다 사용자와 밀접한 관계가 있기 때문에 단말을 통한 현실 세계의 더 중요하고 민감한 정보는 악의적인 타인에 의해 도용될 수 있다. 둘째, 아바타는 다른 아바타 및 비플레이어 캐릭터와 많은 상호작용을 하며, 모두 다른 사람이 이해할 수 있는 것은 아닙니다. 셋째, 우주에는 메타버스를 제외하고는 물론이고 문화의 차이로 인해 일부 사람들이 부적절하다고 느끼는 시나리오가 필연적으로 있을 것이고, 괴롭힘과 같은 악의적인 아바타 행동은 말할 것도 없다. 넷째, 메타버스에서의 소유권, 불법복제, 상품거래 역시 골칫거리다. 메타버스의 보안과 사생활 보호 문제를 해결하는 가장 간단한 방법은 사용자의 진입을 금지하는 것이지만[3], 이 가장 조잡한 방법은 아기를 목욕물과 함께 던지는 이점을 완전히 포기합니다. 이 기사에서는 메타버스 자체의 잠재적인 보안 및 개인 정보 보호 문제에 초점을 맞춘 다음 이익을 완전히 손상시키지 않는 대안 솔루션을 제안합니다. 이 글의 요점은 다음과 같이 요약할 수 있다. 우리는 메타버스 자체의 잠재적인 보안 및 개인 정보 보호 문제에 초점을 맞춘 다음 이익을 완전히 손상시키지 않는 대안 솔루션을 제안합니다. 이 글의 요점은 다음과 같이 요약할 수 있다. 우리는 메타버스 자체의 잠재적인 보안 및 개인 정보 보호 문제에 초점을 맞춘 다음 이익을 완전히 손상시키지 않는 대안 솔루션을 제안합니다. 이 글의 요점은 다음과 같이 요약할 수 있다.

- 메타버스의 개념을 분석하여 다른 VR 기술에 비해 슈퍼 3D 가상현실(VR) 생태계를 제안합니다.
- 메타버스에서 보안 및 개인 정보 보호 문제의 심각한 문제를 지적하고 요약합니다.
- 메타버스에서 이러한 보안 및 개인 정보 보호 문제에 대한 몇 가지 잠재적인 솔루션이 이에 따라 제안됩니다.
- 새로운 버킷 효과는 메타버스에서 보안 및 개인 정보 보호 문제를 포괄적으로 처리하는 방법에 대해 철학적으로 생각하기 위해 적용됩니다.

II . 영형개요중에타버스

직관적으로 메타버스와 VR, 증강현실(AR), 혼합현실(MR)의 경계가 모호해 보인다. 사실 메타버스는 슈퍼가상현실로 고도로 요약될 수 있다.*생태계*VR, AR, MR, 인공 지능, 머신 러닝, 컴퓨터 비전, 음성 인식, 블록체인, 사물 인터넷과 같이 그림 2와 같은 학제간 기술로 구성된 인터넷을 기반으로 합니다. 이에 반해 VR/AR/MR은 일종의 가상화, 디지털화 기술일 뿐이며 메타버스의 중요한 구성요소임에도 불구하고 포괄적인 생태계, 규칙, 인터넷을 필요로 하지 않는다.

"생태계"라는 용어는 메타버스의 구성 요소가 서로 상호 작용하고 제한하며 상대적으로 안정적인 동적 평형 상태에 있으며 지속적이고
통합 가상 세계. 그동안 수많은 사용자들이
퍼에생태계의 기초. 사용자가 없는 경우 가능
y라엘 부르기보다는 3D 가상 비전 시스템으로 레이블을 지정해야 합니다.

그림 2. 메타버스의 주요 기술 구성에 대한 그림입니다.

아무리 완벽해도 "시". 온갖 상품이 다 모여 있지만 대금을 지불하는 고객이 없는 곳처럼 쇼핑몰이라기 보다는 창고라고 할 수 밖에 없습니다. 실제로 사용자는 메타버스의 발전을 자극하기 위해 수요를 생성하고, 이는 다시 사용자를 유치하여 긍정적인 생태계를 만듭니다. 즉, 사용자가 없는 메타버스는 실패할 수밖에 없으며, 이는 아마도 소수의 메타버스 플랫폼만 결국 번성하고 나머지는 죽을 것이라는 의미이기도 합니다. 이러한 추세는 현재 인터넷 플랫폼에서 이미 분명합니다. 예를 들어, 사람들은 다른 대안이 있음에도 불구하고 사진을 공유하기 위해 Instagram을 선택하고 짧은 비디오를 위해 Tiktok을 선택하는 것을 선호합니다.

이 개념이 수년 동안 제시되어 최근에 메타버스가 palingenesis가 될 수 있는 두 가지 주요 이유가 있습니다. 첫째, COVID-19 전염병은 사람들이 가상 디지털 세계에 익숙해지도록 훈련시켰고, 소셜화를 어느 정도 오프라인에서 온라인으로 전환하도록 촉진했습니다[4]. 둘째, 최근 그림 2와 같이 위의 관련 기술의 빅뱅과 같은 비약적인 발전으로 메타버스를 기술적으로 구축할 수 있게 되었다.

III. 에스에큐리티와피리바시씨ONCERN

어떤 것의 개발에는 필연적으로 메타버스를 제외하고 보안 및 개인 정보 보호 문제가 수반됩니다. 구체적으로 이러한 우려는 네 가지 범주로 나눌 수 있습니다.

- 사용자 정보: 다중 센서 융합은 그림 1과 같이 메타버스의 특징 중 하나로 수집해야 할 사용자 정보가 많다. 사용자가 메타버스에 빠져들게 하는 경험을 개선하는 데 도움이 되기 때문에 센서가 필요하다는 데는 의심의 여지가 없습니다. 반면에 많은 사용자가 문제를 인지하지 못하거나 인식하지 못할 수도 있지만[3], 센서에 의해 수집된 일부 사용자 정보(예: 생리적, 신체적, 생체 인식 및 사회적 관련),

너무 개인적인 것입니다. 유출될 경우 사용자의 보안과 사생활을 크게 위협할 수 있다[5]. 따라서 사용자 정보를 보호하는 것이 중요합니다.

- 커뮤니케이션: 메타버스의 특징 중 하나는 높은 상호작용성과 사회성이므로 필연적으로 많은 커뮤니케이션이 발생합니다. 메타버스에서의 공유, 협력, 상호 신뢰와 이해 증진 등의 많은 활동은 의사 소통의 도움 없이는 하기 어렵습니다. 위에 언급된 사용자 정보가 포함되어 있지 않을 수도 있지만 대부분의 사용자는 커뮤니케이션 콘텐츠가 매우 사적이며 민감하기 때문에 커뮤니케이션을 하지 않는 사람에게 말하기를 꺼립니다. 따라서 의사소통을 보호하는 것이 중요하며, 법적인 의사소통자가 할 수 있는 동안 비통신자가 의사소통의 내용을 이해하고 복구할 수 없도록 해야 합니다.

- 시나리오: 메타버스는 초현실적 우주이기 때문에 실제 영역과 동일한 보안 및 개인 정보 보호 문제에 직면하는 것을 생각할 수 있습니다. 고려해야 할 두 가지 주요 측면이 있습니다. 시나리오 자체와 시나리오의 아바타입니다. 전자의 경우 메타버스 플랫폼에 수많은 사용자가 클러스터되어 있기 때문에 (사실 선택할 수 있는 대체 플랫폼이 많지 않음) 문화, 종교 등에 대한 이해가 달라질 수 밖에 없습니다. 따라서 시나리오는 모든 사람의 바람을 충족시키지 못하고 일부 아바타에게 오해를 불러 일으 킵니다. 후자의 경우 사용자의 유입은 필연적으로 일부 악의적이고 부도덕한 사용자를 도입하여 메타버스에서 다른 아바타를 모욕하거나 추적하거나 심지어 성희롱할 수 있으며 이러한 활동은 온라인 게임에 나타납니다[6].

- 상품: metaserve는 상상력, 높은 창의성, 높은 자유도 및 높은 개인화의 특성을 가지고 있습니다. 따라서 아바타는 캐릭터 모델링, 외모, 의상, 건물, 예술품 등 개인의 희망에 따라 모든 종류의 굿즈를 만들 수 있습니다. 이러한 재화는 창작자에 의해 적용되거나 판매될 수 있습니다. 즉, 노력을 통해 생성되거나 금전적 비용으로 생성됩니다(물론 친구가 무료로 제공할 수도 있음). 이는 정신적 및 재정적 가치를 모두 포함함을 의미합니다. 아바타는 가치가 불법적으로 손상되는 것을 원하지 않습니다. 예를 들어 아바타는 자신을 위해 맞춤 드레스를 만들고 다른 사람에게 보여주고 싶지 않을 수 있습니다. 한편, 상품 거래도 악의적인 사용자에 의해 피해를 입을 수 있으며 아바타도 거래에 대한 권리를 익명화할 것을 요구합니다. 따라서,

IV. 유SER나정보

사용자 정보는 현대 사회에서 보안 및 개인 정보 보호와 관련하여 항상 매우 중요하고 민감한 관심사였습니다. 메타버스에서 더 자세한 사용자 정보는 사회 네트워크 등 이전 플랫폼보다 수집됩니다
몰입의 특성, 가상과 현실의 구별 불가능, 다중 센서 때문이다. 이것은 만든다
나쁜 정보에 더 관심이 있는 법적 제3자는

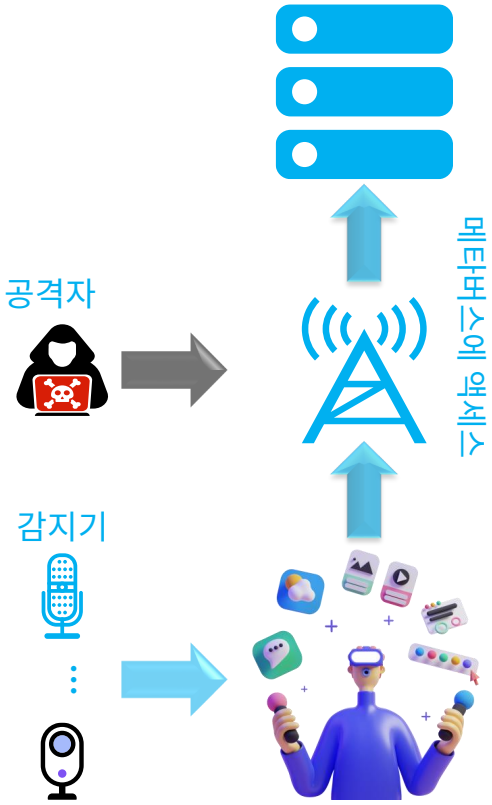

그림 3. 공격자에 의해 공격받는 메타버스의 그림.

한편, 정보가 단말기에서 외부로 전송되는 한 더 이상 사용자의 실제 물리적 통제 하에 있지 않으므로 단말기를 떠난 후 정보가 위험에 처하게 됨을 의미하며, 즉, 단말에서 사용자 정보 보호가 이루어져야 합니다.

모든 사람이 다른 문화적 습관과 수용을 가지고 있기 때문에 모든 사람이 개인 정보 보호에 대한 다양한 견해를 가지고 있다는 점은 주목할 가치가 있습니다. 또한 어떠한 솔루션도 대가를 치르지 않고는 모든 정보를 보호할 수 없습니다. 따라서 솔루션은 사용자가 달성하고자 하는 목표를 위한 표적 보호여야 하며, 그 누구도 직접 사용을 포기하는 것 외에는 모든 위험을 완벽하게 막을 수는 없습니다. 다음으로 메타버스에서 사용자 정보를 보호하기 위한 몇 가지 솔루션에 대해 설명합니다.

센서가 획득한 심박 정보와 같은 정확한 단일 신호 정보에 대해서는 신호를 차폐하고 전송을 금지하는 것만으로 보호할 수 있습니다. 반면 메타버스에서 주류를 이루고 있는 영상, 영상 등의 영상 멀티미디어는 민감한 정보를 많이 담고 있으며, 심박수[7], 건강, 사회적 지위 등 훨씬 정확한 정보를 추출할 수도 있다. . 영상 멀티미디어는 메타버스의 적용과 떼려야 뗄 수 없는 관계이기 때문에 단순히 차폐될 수는 없다. 따라서 일반화, 화이트리스트, 블랙리스트의 세 가지로 분류할 수 있는 구체적인 치료와 보호가 필요합니다.

*일반화된 보호*이는 사용자가 개인 정보 문제가 있을 수 있다고 느끼기 때문에 일부 시각적 콘텐츠를 보호하기를 원한다는 것을 의미합니다. 고려하지 않고 일반적으로 보호된다.

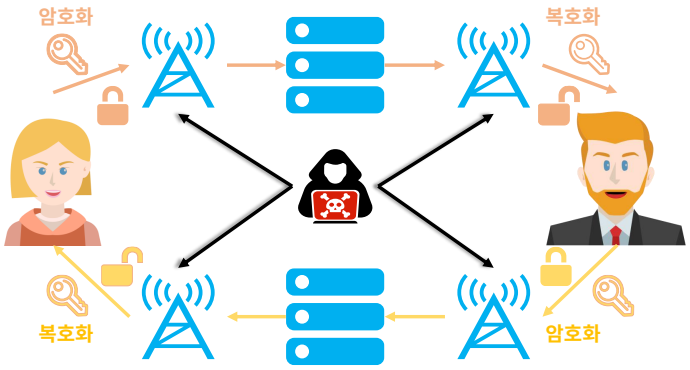

그림 4. 보호되는 통신의 그림.

화이트리스트 및 차단리스트 솔루션에 비해 구체적이고 섬세한 프라이버시를 제공합니다. 멀티미디어 영상 콘텐츠에서는 한 부분만 필요하고 나머지 부분은 중복될 수 있습니다. 예를 들어 사람만 등장하면 되고, 메타버스의 화상회의에서는 너무 많은 정보가 노출될 수 있는 배경이 불필요하다. 이 문제는 매트를 사용하여 해결할 수 있습니다. 즉, 시각적 콘텐츠를 보존 및 폐기해야 하는 콘텐츠로 나누어 그에 따라 처리할 수 있습니다. 실제로 적용되었습니다. 예를 들어 Zoom과 Tencent Conference를 통해 사용자는 1년 전에 가상 배경 옵션을 선택할 수 있었습니다. 유사하게, 얼굴 교환 및 3D 모델 교체와 같은 솔루션은 얼굴이 제기할 수 있는 개인 정보 위험을 고려하여 적용될 수 있습니다.

*화이트리스트 보호*사용자가 선택한 정보(화이트리스트와 유사) 외에 모든 것을 처리하고 보호하는 것을 의미하며, 이는 위와 비교하여 표적화된 보호입니다. 간단한 예를 들자면 메타버스에서 스마일 대회가 조직되고 가장 밝은 미소를 가진 아바타가 게임에서 승리할 수 있습니다. 사용자의 얼굴 콘텐츠는 대회 참가를 위해 필요하지만 사용자는 분석 미소를 위한 얼굴 콘텐츠만 사용할 수 있습니다. 따라서 멀티미디어의 얼굴에는 미소 이외의 정보가 포함되어서는 안됩니다. 이 문제에 대해 우*et al.* 특정 정보의 유용성만 유지하고 다른 정보는 삭제되어 추출할 수 없는 시각적 콘텐츠를 보호하기 위해 머신러닝을 통해 모델을 학습시키는 솔루션을 제안했습니다[8].

*블랙리스트 보호*이는 사용자가 선택하는 것(블랙리스트와 유사)을 제외하고 멀티미디어의 시각적 콘텐츠에 대해 아무 것도 처리되지 않음을 의미합니다. 이러한 종류의 보호는 종종 얼굴을 겨냥하여 우수한 시각적 관찰 가능성과 함께 매우 정확합니다. 이러한 보호를 위해 더 정확한 처리를 위해 얼굴이 종종 특정 벡터로 파괴되고 각 벡터는 신호를 나타냅니다. 이러한 벡터는 일반적으로 ID와 속성의 두 가지 클래스로 구분됩니다. 사용자가 보호하고자 하는 정보와 관련된 일부 벡터는 보호를 위해 처리되고 나머지는 변경되지 않습니다. 그런 다음 이러한 벡터를 통합하고

익명화라는 모델을 생성하여 얼굴을 보호하고
애트리부에 따라 각각 보호
아이덴티티 ity 또는 속성이 처리됩니다.

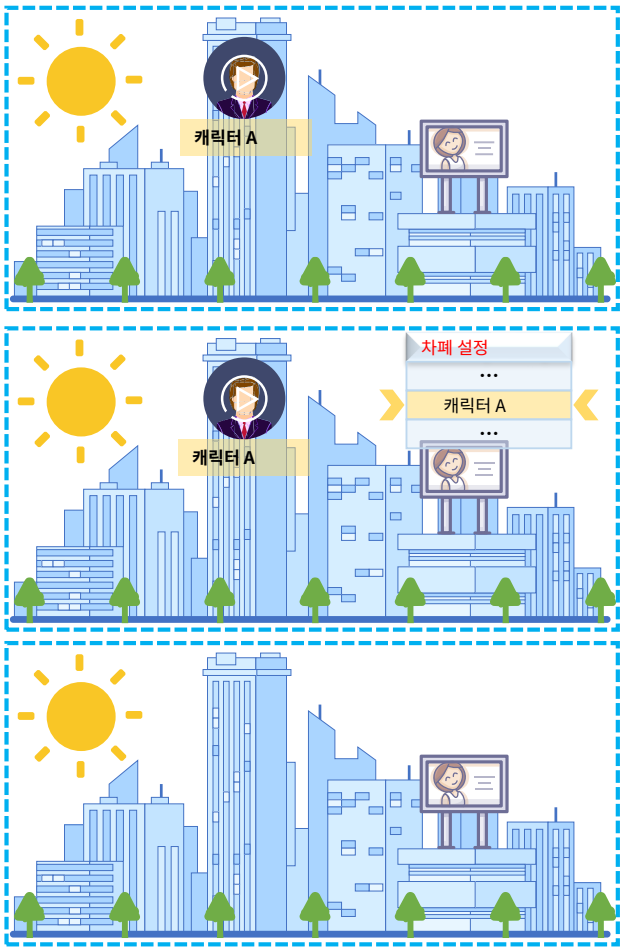

그림 5. 사용자 선택에 따라 차폐된 시나리오의 예.

V.C의사소통

메타버스에서는 인터랙션과 소셜이 필요하기 때문에 커뮤니케이션이 빈번하다. 통신은 표면의 아바타에 의해 수행되지만 실제로는 사용자가 제어합니다. 통신 참여자는 제3자가 알지 못하는 동안 대상 당사자, 즉 정당한 수신자만 통신 내용을 알기를 원합니다. 사용자 정보의 경우와 같이 솔루션에서 콘텐츠를 직접 제거할 수는 없지만 대상 당사자를 위해 복구할 수 있어야 함을 나타냅니다.

이 목표에 대한 강력한 솔루션은 그림 4와 같은 암호화입니다. 즉, 발신자는 키로 암호화한 후 정보를 보내고 합법적인 수신자는 정보를 수신한 후 올바른 키를 사용하여 정보를 해독합니다. 따라서 통신 과정에서 의미 없는 암호문을 전송하게 되며, 암호문을 가로채더라도 올바른 키가 없으면 공격자는 암호문을 해독할 수 없습니다. 그건 그렇고, 키와 암호화 알고리즘은 주로 암호문의 보안, 즉 올바른 키가 없는 공격자가 암호문을 깨뜨리는 것을 방지하는 기능을 담당합니다. 키의 경우 공격자가 과격한 공격을 하지 못하도록 키 공간이 충분히 길어야 하며, 한편 키가 누출되면 통신이 위험하므로 키를 보관해야 합니다.

기밀이며 정기적으로 교체됩니다. 암호화 알고리즘은 공격 가능성을 방지하기 위해 충분한 암호화 테스트와 분석을 거쳐야 하며, 실제 필요에 따라 해당 보안 표준에 맞는 알고리즘을 선택해야 합니다.

영상, 이미지 등 영상 멀티미디어에 대한 일반적인 암호화 기법은 의미 있는 영상 콘텐츠를 불필요한 잡음과 같은 콘텐츠로 변환하는 방식으로 보안과 프라이버시의 요구를 충족시킬 수 있었지만 시각적 관찰 가능성은 고려하지 않고 있다. 사실 이 기능은 커뮤니케이션을 즐기는 데 중요할 수 있습니다. 발신자는 모두 노이즈와 유사하여 브라우징으로 구별할 수 없는 암호화된 이미지를 다수 공유합니다. 즉, 모두 복호화되지 않으면 선택할 수 없으므로 수신자에게 좋지 않은 경험이 될 수 있습니다. 썸네일 보존 암호화는 개인정보 보안과 시각적 관찰 가능성[9] 간의 모순을 완화하기 위해 적용될 수 있습니다. 최종 결과는 모자이크 효과와 유사하며,

VI. 에스세나리오

종교, 정치, 성별, 성소수자 사이에서 발생하는 갈등과 같이 현실 세계에서 다양한 문화와 다양한 사람들의 아이디어로 인해 때때로 갈등이 발생합니다. 이 현상은 거리 부족 및 기타 제한(예: 소셜 네트워크에서의 사이버 괴롭힘 및 온라인 게임의 대규모 폭력)으로 인해 가상 세계에서 훨씬 더 심각합니다. 그러나 현재 네트워크 플랫폼 사용자의 경우 이러한 불쾌한 장소에서 벗어나 비슷한 관심사와 의견을 가진 사람들과 작은 가상 커뮤니티를 형성하여 부정적인 영향을 피할 수 있습니다. 그러나 메타버스는 그 자체가 완전한 우주이기 때문에 이런 방식은 존재하지 않는 것 같고, 소수의 개인이 새로운 출발을 하기는 어렵다. 한편,

사용자 친화적인 메타버스 환경을 위해서는 사용자가 아바타 주변의 일부 시나리오를 방지하도록 설정할 수 있는 설정 창이 제공되어야 합니다. 예를 들어, 건물 밖에서 정치인의 선전 영상이 재생되고 있지만 일부 아바타는 그를 싫어하여 그림 5와 같이 그를 보호하기로 선택합니다. 시나리오가 화면에서 사라지지 않는다는 점은 주목할 가치가 있습니다. 메타버스지만 특정 아바타에 대해서는 볼 수 없으며, 이를 개인화 시나리오 프리젠테이션이라고도 할 수 있다. 유사하게, 다른 아바타의 말과 텍스트의 공격적이고 모욕적인 내용에 대해 차폐를 위한 음성 및 텍스트 감지 모델을 통해 특정 키워드를 설정하여 감지할 수도 있습니다.

반면, 이 솔루션은 아바타의 공격적 및 따돌림 행위를 감지하기 어렵습니다. 첫째, 아바타 행동의 의미는 종종 미묘하며 악의적인지 여부는 실제 상황 및 컨텍스트와 결합되어야 합니다. 둘째, 행동 자체가 매우 다양하고 악의적인 행동은 말이나 행동에 비해 명확한 정의가 없는 경우가 많다.

텍스트. 예를 들어 아바타가 총을 가지고 노는 것이 항상 악의적인 것으로 간주되는 것은 아니지만, 총이 다른 아바타를 향하면 악의적이기 때문에 특정 상황이 보완되지 않는 한 단순히 총을 감지하여 악의가 있는지 여부를 판단하는 것은 불가능합니다. . 연구에 따르면 아바타에 의한 악의적인 괴롭힘 감지는 신체 포즈, 얼굴 감정, 손짓, 사물, 사회적 요소와 같은 여러 요소를 결합하여 만족스러운 결과를 얻을 수 있다고 합니다[10].

괴롭힘 및 스토킹의 경우 이러한 아바타가 우리 자신의 시나리오에서 보호되더라도 우리는 여전히 악성 아바타 시나리오에 존재하고 이러한 종류의 활동을 할 수 있기 때문에 앞의 솔루션은 유용하지 않습니다. 이에 대한 좋은 해결책은 은폐 및 순간이동[3]과 같이 갑자기 사라지고 결과적으로 악의적인 아바타가 대상을 찾지 못하는 것입니다. 또한 사용자는 메타버스에 액세스할 때마다 여러 아바타를 만들고 무작위로 다른 아바타를 선택하여 일부 악의적인 아바타가 시간이 지남에 따라 패턴을 찾는 것을 방지할 수 있습니다.

VII. Goods

이처럼*et al.*지적[2], 창조는 메타버스의 지속 가능한 발전의 중요한 부분입니다. 또한 메타버스의 높은 자유도와 개방된 환경은 개인의 심리적 욕구나 돈에 의한 창조 활동의 출현을 크게 부추기며, 이는 곧 창조에 의해 생산되는 많은 재화들이 나타날 것임을 의미한다. 동기가 무엇이든 물건의 소유자는 다른 사람이 불법적으로 복사하고 남용하는 것을 원하지 않을 것입니다. 이를 바탕으로 이를 보호할 수 있는 방안을 강구할 필요가 있다.

실행 가능한 솔루션은 보이지 않는 워터마킹(invisible watermarking)으로, 상품이 생성되거나 소유권이 이전될 때 상품에 정체성과 관련된 특정 마크를 삽입하는 것을 목표로 하는 기술입니다. 투명화로 인해 메타버스에서 자체 상품의 시각적 효과에 영향을 미치지 않으며 필요할 때 추출하거나 감지할 수 있습니다. 따라서 콘텐츠 보호, 인증 및 변조 방지를 포함한 일부 기능이 구현되어[11], 이는 악의적인 아바타가 상품을 훔치고 불법적으로 복사하는 것을 더욱 억제합니다. 또한 실제 시나리오와 비교하여 워터마킹이 메타버스에 더 적합합니다. 현실 세계에서는 본질적으로 시각적 콘텐츠가 아무리 눈에 띄지 않더라도 수정되어 일부 물리적 특징이 파괴되므로 일부 기술적 수단을 통해 워터마킹의 존재를 불법적으로 감지할 수 있습니다.

블록체인은 탈중앙화, 변조 방지, 익명성 등의 특성을 지닌 소유권, 추적성 및 상품 이전 문제에 대한 탁월한 솔루션입니다[12]. 탈중앙화는 각 아바타가 블록체인 활동에 공정하게 참여할 수 있도록 하여 아바타 스스로 각 재화의 소유권을 등록할 수 있도록 하는 보호의 전제입니다. 변조 방지 기능은 블록체인을 변조하려면 시스템에서 지원하는 컴퓨팅 성능의 51% 이상이 필요하기 때문입니다. 그것

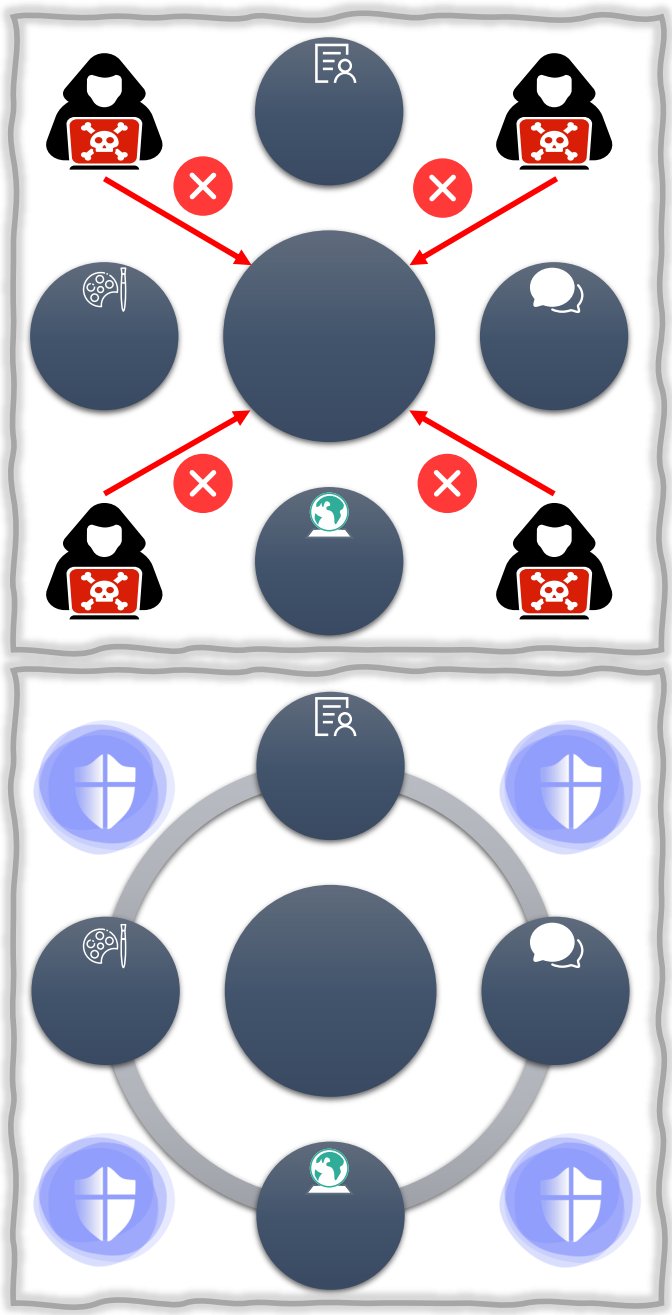

그림 6. 보안 및 개인 정보 보호를 위한 새로운 버킷 효과의 예.

최대의 이점을 얻기 위해 시스템의 안정성을 유지해야 하기 때문에 컴퓨팅 파워가 많은 사람들의 이익이 아닙니다. 따라서 소유권 등록 이후의 실효성에 대해 걱정할 필요가 없습니다. 익명성을 통해 아바타는 등록 후 소유권이 있는 사람을 공개하거나 거래 중 신원이 노출되는 것에 대해 걱정할 필요가 없습니다. 또한 블록체인에는 스마트 계약[13]이라는 효과적인 도구가 있어 양 당사자가 상품 거래를 불이행하는 것을 방지할 수 있습니다. 특히 거래의 양측

사전에 합의에 도달한 후 작성해야 합니다.
ㅏ 서명하는 계약. 일단 약관에 명시된 조건 계약이 충족되면 자동으로 실행되기 시작하며 인간의 의지에 의해 변경되지 않습니다. 따라서 메타버스에서 재화의 소유권 거래를 안전하게 수행할 수 있습니다.

VIII. New비우켓이자형효과

위의 솔루션이 제기된 문제의 각도에 서 있을 때 해당 보안 및 개인 정보 보호 문제를 처리하는 데 보호 효과를 얻을 수 있다는 것은 의심의 여지가 없습니다. 한편, 연구자들은 기존 솔루션의 단점을 인지하고 각 보드를 확대하여 더 많은 물을 담을 수 있는 고전적인 버킷 효과와 같은 더 나은 효과를 얻기 위해 지속적으로 개선하기 위해 노력하는 것이 일반적입니다. 하지만 각 판 사이에 틈이 있어 고정하지 않으면 아무리 물을 담아도 누수가 된다. 마찬가지로 사람들이 한 가지 문제만 따로 연구하고 다른 사람에게 눈을 돌린다면 그에 상응하는 효과를 낼 수 있는 솔루션을 제시할 수 있을지 모르지만 전체 생태계의 보안과 프라이버시를 완화하는 데는 그림과 같이 별로 도움이 되지 않습니다. 도 6의 상부 패널. 예를 들어, 아바타가 마타버스에서 다른 사람과 채팅할 때 예상치 못한 방식으로 일상적인 사소한 것을 공개하고 현실 세계에서 자신의 사용자 정보를 노출할 수 있습니다. 의도적인 아바타가 이를 악용하여 의도적으로 아바타와 통신을 한다면, 이러한 방식으로 사용자 정보를 성공적으로 획득할 수 있다.

따라서 누수, 즉 새로운 버킷 효과를 최소화하기 위해 버킷에 잠금 링을 추가해야 합니다. 마찬가지로 보안 및 개인 정보 보호 문제를 해결하는 방법에 대한 P2P(Peer-to-Peer)가 아닌 종합적인 고려가 필요하며 솔루션 패키지가 제공됩니다. 사용자가 여러 개의 밀접하게 관련된 솔루션을 동시에 선택하고 실행할 수 있도록 해야 합니다. 그러면 그림 6의 하단 패널과 같이 메타버스의 우려를 효과적으로 완화할 수 있습니다. 이 설명은 메타버스의 보안 및 개인 정보를 더 잘 보호하는 데 도움이 될 수 있습니다. 그러나 그것은 또한 연구자들에게 더 큰 도전을 제기하기 때문에 포괄적이고 글로벌한 사고를 바탕으로 체계적이고 일관된 솔루션을 설계해야 합니다.

IX. 씨결론

보안 및 개인 정보 보호 문제는 모든 개발에 불가피하며 해결해야 합니다. 이 글에서는 먼저 메타버스의 개념을 다듬고 사용자 정보, 통신, 시나리오, 상품을 포함하는 메타버스의 보안 및 개인 정보 보호 문제를 분석하고 요약합니다. 그런 다음 우리가 요약한 주요 문제를 반영하여 차폐, 기계 학습, 암호화, 워터마킹, 블록체인 등을 기반으로 해당 잠재적 솔루션을 제안합니다. 이러한 문제를 해결합니다. 마지막으로 철학적 반성을 통해 생태계의 보안 및 개인 정보 보호 문제를 포괄적이고 효과적으로 완화하기 위해 새로운 배럴 효과에서 교훈을 도출한다는 아이디어를 제시합니다.

아르 자형참고문헌

[1] N. 스티븐슨,*눈 충돌: 소설*. 스펙트라, 2003.
[2] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, P. Hui, "메타버스에 대해 알아야 할 모든 것: 기술적 특이점, 가상 생태계 및 연구 의제에 대한 완전한 조사",*arXiv 사전 인쇄 arXiv:2110.05352*, 2021.
[3] B. Falchuk, S. Loeb 및 R. Neff, "사회적 메타버스: 개인 정보를 위한 전투", *IEEE 기술. 사회 잡지.*, 권. 37, 아니. 2, pp. 52–61, 2018.
[4] Z. Chen, H. Cao, Y. Deng, X. Gao, J. Piao, F. Xu, Y. Zhang 및 Y. Li, "가정에서 배우기: 코로나19 팬데믹 기간 동안 중국 대학에서 라이브 스트리밍 기반 원격 교육 경험에 대한 혼합 방법 분석",*회의 흠. 사실. 계산 시스템 절차*, 씨. CHI'21, 2021.

[5] H. Liu, X. Yao, T. Yang 및 H. Ning, "하이브리드 컴퓨팅 기반 스마트 건강에서 웨어러블 장치에 대한 협력 개인 정보 보호",*IEEE 인터넷 사물 J.*, 권. 6, 아니. 2, pp. 1352–1362, 2019.
[6] J. Fox, M. Gilbert 및 WY Tang, "대규모 멀티플레이어 온라인 게임에서의 플레이어 경험: 성능, 동기 부여 및 사회적 상호 작용에 대한 일기 연구",*뉴미디어 Soc.*, 권. 20, 아니. 11, pp. 4056–4073, 2018.

[7] Q. Zhu, M. Chen, C.-W. Wong, M. Wu, "법의학 애플리케이션에서 강력한 주파수 추적을 위한 적응형 다중 추적 조각",*IEEE 트랜스. 정보 포렌식 보안.*, 권. 16, pp. 1174–1189, 2021.
[8] H. Wu, X. Tian, Y. Gong, X. Su, M. Li, F. Xu, "DAPter: 딥 러닝 추론 서비스에서 사용자 데이터 남용 방지", in*절차 월드 와이드 웹 Conf.*, 2021, pp. 1017–1028.
[9] Y. Zhang, R. Zhao, X. Xiao, R. Lan, Z. Liu 및 X. Zhang, "HF-TPE: 고화질 썸네일 보존 암호화," *IEEE 트랜스. 회로 시스템 Video Technol., 보도자료, doi: 10.1109/TCSVT.2021.3070348*, 2021.
[10] N. Vishhwamitra, H. Hu, F. Luo 및 L. Cheng, "실제 이미지에서 사이버 괴롭힘을 이해하고 감지하는 방향으로", in*IEEE 국제 회의 마하. 배우다. 적용*, 2021.
[11] M. Begum과 MS Uddin, “디지털 이미지 워터마킹 기법: 리뷰,” *정보*, 권. 11, 아니. 2, p. 2020년 110월.
[12] H.-N. Dai, Z. Zheng, Y. Zhang, “사물 인터넷을 위한 블록체인: 설문조사”, *IEEE 인터넷 사물 J.*, 권. 6, 아니. 5, pp. 8076–8094, 2019.
[13] 이성, 김명, 이재, R.-H. Hsu, TQS Quek, “블록체인이 데이터 신선도에 적합합니까? 정보화 시대의 시각,*IEEE 네트워크.*, 권. 35, 아니. 2, 96–103페이지, 2021.