Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.725

안전한 다자간 연산을 활용한 메타버스 환경에서의 프라이버시 보존 방안 연구*

장 지 운,[1†] 조 관 태,[2] 조 상 래,[2] 김 수 형[2‡]
[1]과학기술연합대학원대학교 (대학원생), [2]한국전자통신연구원 (책임연구원)

A Study on Privacy Preserving Methods in the Metaverse Environment Using Secure Multi-Party Computation*

Jiun Jang,[1†] Kwantae Cho,[2] Sangrae Cho,[2] Soo Hyung Kim[2‡]
[1]University of Science and Technology (Graduate student),
[2]Electronics and Telecommunocations Research Institute (Principal Researcher)

요 약

최근 급격하게 성장한 메타버스 환경은 건강과 의료, 문화와 게임, 정치 등 다양한 분야에서 각광받고 있다. 하지만 메타버스 환경에서 사용하는 다양한 센서와 기기들의 과도한 개인정보 데이터 수집으로 인해 사용자의 프라이버시가 크게 위협받고 있다. 본 논문에서는 메타버스 환경에서의 사용자 프라이버시 위협을 해결하기 위해 안전한 다자간 연산 응용 연구 사례를 조사하고, 메타버스 환경의 확장에 필요할 것으로 예상되는 서비스를 분석하였다. 또한, 메타버스 환경에 존재하는 프라이버시 이슈와 현실 세계 서비스의 한계점을 정리하였다. 이를 바탕으로 메타버스 환경에서 안전한 다자간 연산을 활용하여 사용자의 프라이버시를 보존하는 응용 연구 시나리오를 제안하였다. 제안한 다자간 연산 응용 연구 시나리오는 메타버스 보안 연구에 새로운 관점을 제시하며, 향후 안전한 메타버스 서비스 구축에 활용할 수 있을 것으로 기대된다.

ABSTRACT

The rapidly growing metaverse environment has received widespread attention across various fields such as health and medicine, culture and gaming, as well as politics. However, the excessive collection of personal data by the diverse sensors and devices used in the metaverse environment poses a substantial threat to user privacy. In this paper, we investigate existing cases of secure Multi-Party Computation(MPC) applications, examine the services anticipated to be necessary for the expansion of the metaverse environment, and analyze the privacy issues present in the metaverse environment as well as the limitations of current real-world services. Based on these findings, we propose application scenarios that utilize MPC to preserve user privacy in the metaverse environment. These proposed MPC application scenarios present a new perspective in metaverse security research. In the future, they are expected to be utilized in the development of secure metaverse services.

Keywords: Metaverse, Multi-Party Computation, Privacy

Received(03. 19. 2024), Modified(06. 07. 2024), Accepted(06. 14. 2024)

* 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (RS-2023-00229400, 안전한 메타버스 환경을 위한 사용자 인증 및 프라이버시 보호 기술 개발)

* 본 논문은 2023년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임.

† 주저자, jiun@etri.re.kr

‡ 교신저자, lifewsky@etri.re.kr(Corresponding author)

I. 서 론

최근 '메타 퀘스트3'나 '애플 비전 프로'와 같은 차세대 XR 기기들의 등장으로 메타버스 환경의 확장과 발전이 기대되고 있다. 메타버스는 가상, 초월을 뜻하는 메타(meta)와 세계, 우주를 뜻하는 유니버스(universe)의 합성어로 1992년 닐 스티븐슨의 소설 '스노 크래시'에서 처음 소개되었다. 가상 세계와 현실 세계의 융합을 의미하는 메타버스 환경에서 사용자는 자신의 분신인 아바타를 통해 사회·경제·문화 활동을 수행하고 가치를 창출할 수 있다.

미국 미래가속화연구재단(acceleration studies foundation)은 '메타버스 로드맵'에서 메타버스는 가상 세계(virtual world), 거울 세계(mirror world), 증강현실(augmented reality), 일상 기록(lifelogging)이라는 4개의 핵심 요소를 제공한다고 발표했다[1]. 해당 발표에 따라 메타버스는 VR·AR뿐만 아니라 사회 관계망 서비스부터 온라인 게임까지 모두를 아우르는 포괄적인 개념임을 알 수 있다.

'게더타운'에 개원된 한림대학교의료원의 '메타버스 어린이 화상병원', '포트나이트'에서 진행된 방탄소년단의 신곡 안무 공개, '제페토'를 활용한 블랙핑크의 가상 사인회 및 뮤직비디오 제작, '모여봐요 동물의 숲' 속 개설된 조 바이든의 선거 캠프, '마인크래프트'에서 진행된 어린이날 '청와대 랜선 특별초청' 행사, '점프 VR'에서 개최된 2021년 순천향대학교 입학식 등 메타버스는 다양한 분야에서 다수의 사용자가 상호작용할 수 있는 환경을 목표로 실현되고 있다.

그러나 시선과 머리의 움직임을 추적하는 HMD(Head Mounted Display), 몸짓을 추적하는 트래커와 컨트롤러, 목소리를 입력받는 마이크 등 다양한 센싱 기기들로부터 수집되는 방대한 양의 사용자 데이터로 인해 메타버스 서비스를 이용하는 사용자의 프라이버시는 심각한 위협을 받고 있다.

본 논문에서는 메타버스 환경에서 사용자의 프라이버시를 보존하기 위해 안전한 다자간 연산(MPC, Multi-Party Computation)을 활용한 응용 연구 시나리오를 제시한다. 2절에서는 MPC를 설명하고, 응용 연구 사례를 조사한다. 3절에서는 확장되고 있는 메타버스 세계에 필요한 서비스를 확인하고, 현실 세계에서의 구현방식을 분석한다. 이어서, 메타버스 환경의 프라이버시 이슈를 살펴보고 분석한 서비스가 프라이버시 보존 관점에서 메타버스 환경에 적절하지 않은 이유를 정리한다. 4절에서는 2절과 3절의 내용을 바탕으로, 메타버스 환경에서의 사용자 프라이버시 보존을 위한 응용 연구 시나리오를 제안한다. 5절에서는 본 논문의 결론과 향후 연구 방향에 대해 기술한다.

II. MPC 소개 및 응용 연구 사례

2.1 MPC 소개

MPC는 다수의 연산 참여자들이 각자 입력값의 기밀성을 유지한 채 공동으로 연산을 수행하고, 결과를 공유하는 보안 기술이다. 연산 참여자의 어떤 정보도 노출하지 않으면서, 모든 참여자가 정직하게 연산을 수행하도록 강제하는 특성이 있다. 1982년, 두 백만장자가 각자의 재산을 공개하지 않고 더 부유한 사람을 알아내는 방법을 다룬 Yao[2]의 백만장자 문제(millionaires' problem)를 시작으로, 불확정 전송(oblivious transfer) 기반의 GMW[3], 비밀 공유(secret sharing)[4] 기반의 BGW[5], 변조된 회로(garbled circuit) 기반의 BMR[6]과 같이 다양한 암호학적 도구를 활용한 프로토콜 연구가 진행되었다. MPC 연구는 효율성 문제로 인해 주로 이론적인 영역에 한정되었지만, 프로토콜의 최적화와 하드웨어 성능의 발전으로, 현실 세계의 보안 문제 해결에 적용되는 사례가 증가하고 있다.

2.2 MPC 응용 연구 사례

2.2.1 광고 효과 분석

안전한 교집합 연산(PSI, Private Set Intersection)은 둘 이상의 참여자가 각자의 데이터 집합을 서로에게 공개하지 않고, 교집합에 해당하는 요소를 파악할 수 있는 프로토콜로, MPC를 통해 구현 가능하다.

전자 상거래에서 광고 대행사와 상품 판매업체는 광고 효과를 확인하기 위해 PSI 프로토콜을 사용할 수 있다. 광고 대행사는 제품 광고를 시청한 사람의 목록을 프로토콜에 입력하고, 판매업체는 제품을 구매한 사람의 목록을 프로토콜에 입력한다. 이를 통해 양측은 광고를 보고 제품을 구매한 사람의 수를 확인할 수 있다.

개인의 광고 시청 내역이나 물건 구매 내역은 선

호, 관심사, 소비 습관 등을 반영하는 개인정보이며, PSI 프로토콜을 위해 이러한 개인정보를 입력 및 처리하는 과정에서 노출이 발생할 위험이 존재한다. MPC를 활용하여 PSI 프로토콜을 구현하면, 개인정보를 보호하며 두 목록 간의 공통 요소를 안전하게 획득할 수 있다[7].

2.2.2 의료 센서 클라우드 데이터 분석

무선 센서 네트워크를 기반으로, 환자 모니터링과 환자 데이터 분석 등의 의료 및 보건 서비스가 발전했다. 서버에서 저장 및 처리되는 정보는 환자의 개인정보 및 의료 정보로, 이를 분석하기 위해서는 민감정보를 노출하지 않고 안전하게 연산을 수행할 방법이 필요하다.

연구나 치료에 필요한 의료통계정보를 안전하게 수집하기 위해 의료 센서 클라우드 시스템은 MPC를 활용할 수 있다. 의료 센서는 암호화된 환자의 데이터를 병원 내 데이터 저장 서버의 수만큼 분할하여 저장하고, 환자 데이터 저장 서버는 각각 MPC 프로토콜의 참여자가 되어 분할 저장된 암호화 데이터를 입력값으로 제공한다. 해당 프로토콜을 통해 의사 또는 의료 전문가는 환자명, 센서 기기의 종류, 환자의 병력과 같은 개인의 민감한 의료 데이터를 알지 못한 채로 의료 데이터 통계 분석 서비스를 활용할 수 있다[8].

2.2.3 항공사 간 탄소배출권 경매

유럽연합 배출권 거래제도에 따라 유럽 경제 지역 내의 항공사들은 매년 항공편에 사용할 수 있는 일정량의 거래 가능한 이산화탄소 배출권을 받는다. 이산화탄소 배출량은 연료 소비량 및 비행기 이륙 중량에 비례하기 때문에 항공사들은 탄소배출권 시장 참여로 인해 기업 기밀 정보인 항공교통관리 정보를 공개하게 된다.

MPC를 활용하여 안전한 탄소배출권 경매 서비스를 구축하면, 항공사는 기밀 정보의 노출 없이 거래에 참여할 수 있다. 이는 항공사별 입찰 내역이 다른 항공사에게 공개되지 않음과 동시에 입찰에 참여한 항공사를 추적할 수 없음을 의미한다[9].

III. 메타버스 환경에서 적용 가능한 서비스 및 관련 프라이버시 이슈

3.1 메타버스 환경의 확장을 위한 서비스

다양한 목적에 따라 확장되는 메타버스 환경은 사용자에게 충분한 경험을 제공하기 위해 발전 중이다. 현실 세계와의 융합을 목표로 하는 메타버스 환경은 현실에서 사용 중인 서비스를 구현할 필요가 있다. 특히, 생체인증과 전자투표 서비스는 메타버스 환경을 더욱 유용하고 편리하게 만들어 줄 것으로 기대된다.

3.1.1 사용자 생체인증

메타버스 환경은 현실 세계를 초월한 상호작용과 경험을 제공한다. 사용자는 아바타를 통해 행사나 회의에 참석할 수 있고, 교육을 듣거나 공연을 개최 또는 관람할 수 있다. 또한 콘텐츠와 시장을 창출하여 아바타의 아이템은 물론 월드나 맵과 같은 3D 가상 공간을 제작 및 거래할 수 있다. 사용자가 경험할 수 있는 다양한 활동들은 메타버스 환경에서 보안성 높은 사용자 인증의 필요성을 강조한다.

기존 웹 환경에서 주요 인증 수단으로 사용된 비밀번호는 지식기반 인증 방식으로, 사용자에게 친숙하고 구현 및 유지 관리 비용이 저렴하여 널리 사용되었다. 하지만, 중앙 집중식 인증 시스템의 한계로, 공격과 유출에 취약하다는 단점을 가지고 있다. 특히, 다양한 센싱 기기들을 활용하여 사용자의 데이터를 수집하는 메타버스 환경에서는 시선이나 손짓, 목소리 등을 통한 비밀번호 유출 위험이 추가로 발생한다.

메타버스 가상환경에 접속하기 위해 사용자는 HMD나 컨트롤러 등의 부수적인 센싱 기기를 사용한다. 비밀번호를 암기하거나 별도의 인증키를 소지하지 않아도 되며, 인증 절차가 간편한 생체기반 인증 방식은 가상환경 부수기기들의 발전과 함께 메타버스 환경의 주요 인증 방식이 될 것으로 전망된다. 메타버스 환경에서의 생체인증은 HMD를 통한 홍채인식, 컨트롤러를 통한 지문인식, 마이크를 통한 음성인식 등이 예상된다. 그러나 바이오정보는 변경이 불가능한 정보로, 유출 시 사용자에게 심각한 피해를 초래한다. 따라서 생체인증을 활용하기 위해서는 보안에 더욱 유의해야 한다.

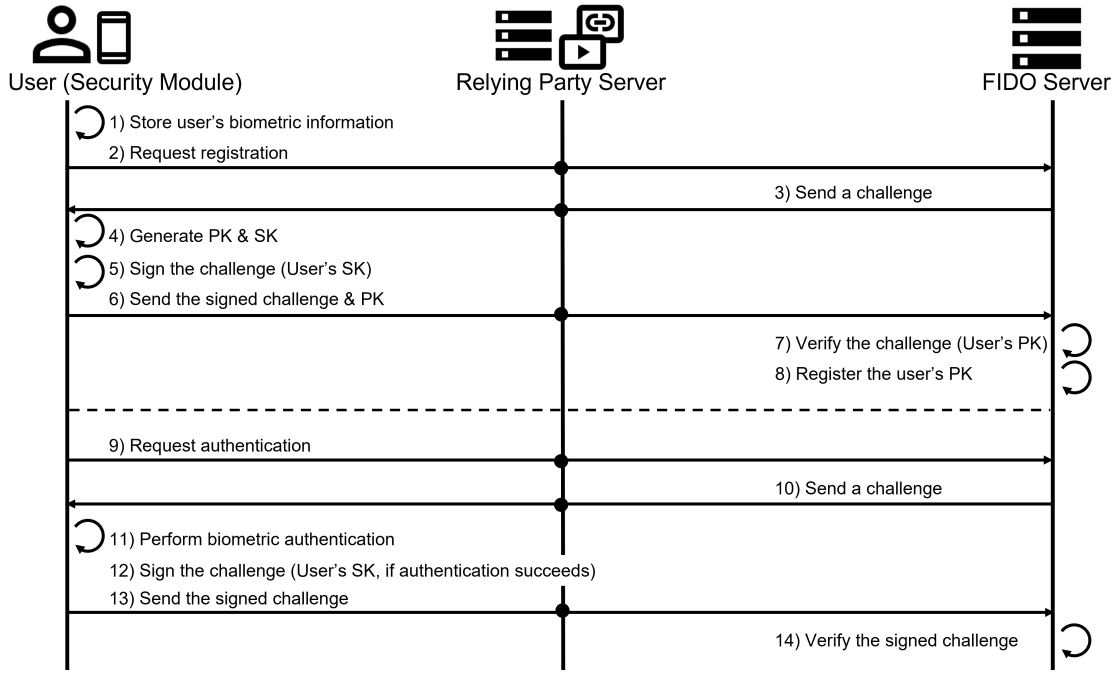

Fig. 1. FIDO2 user registration and authentication service process.

FIDO2(Fast IDentity Online2) 기술은 스마트폰의 보급에 힘입어 디지털 시대의 주요 인증 방식으로 자리 잡은 공개키 기반의 생체인증 기술로, Fig. 1.과 같이 진행된다. 서비스 제공자의 서버에는 사용자의 공개키를 등록하고, TPM(Trusted Platform Module), SE(Secure Element), TrustZone 또는 TEE(Trusted Execution Environment)와 같은 사용자 기기의 보안 모듈에는 사용자의 개인키와 바이오정보 템플릿을 저장한다. 서비스 제공자가 사용자에게 인증 요청 시, 사용자는 보안 모듈에 저장된 자신의 바이오정보 템플릿을 통해 기기 내부에서 생체인증을 진행한다. 생체인증의 결과에 따라 서비스 제공자가 보낸 요청은 사용자의 개인키로 서명되어 서비스 제공자에게 전송된다. 서비스 제공자는 서버에 저장된 사용자의 공개키를 사용하여 서명을 검증하고 사용자를 인증할 수 있다. FIDO2는 바이오정보를 사용자 기기 내의 보안 모듈에서만 저장 및 사용하므로, 유출의 위험 없이 안전하게 생체인증을 진행할 수 있다. 또한, 소유 기반 인증도 함께 제공함으로써 보안성을 더욱 강화할 수 있다[10-12].

3.1.2 온라인 전자투표

인터넷 시대 이후, 온라인 전자투표에 대한 수요는 점차 증가해왔다. 사용자가 직접 토론과 유세를 할 수 있는 메타버스 환경은 유권자에게 투표의 필요성을 알리고 참여를 독려하는 데 효과적이다. 이러한 예로, 2022년 9월 14일, '싸이월드'의 메타버스 토론장 '싸이아고라'에서 진행된 '방탄소년단 병역특례 찬반 토론·투표', 2023년 8월, 서울시에서 진행된 '서울시 2023 제 1대 청소년시의원 메타버스 투표'와 같이 메타버스 환경에서 투표를 실시한 사례가 존재한다.

편리성과 접근성, 그리고 저렴한 사회적 비용 등의 장점을 가진 온라인 전자투표는 유권자의 참여를 유도할 수 있는 효과가 기대되지만, 보안 취약성과 복잡성, 투명성 부족 등의 문제로 인해 널리 활용되지 못하고 있다. 중앙 신뢰 기관(trusted third party)의 신뢰성 부족은 유권자들에게 비밀선거 원칙의 위배에 대한 우려를 유발하는 것은 물론, 해킹이나 결과 조작에 관한 염려로 인해 투표 결과에 대한 불신을 초래한다.

에스토니아는 2005년 지방선거와 2007년 총선을 시작으로, 지속해서 전자투표를 실시하고 있는 국가

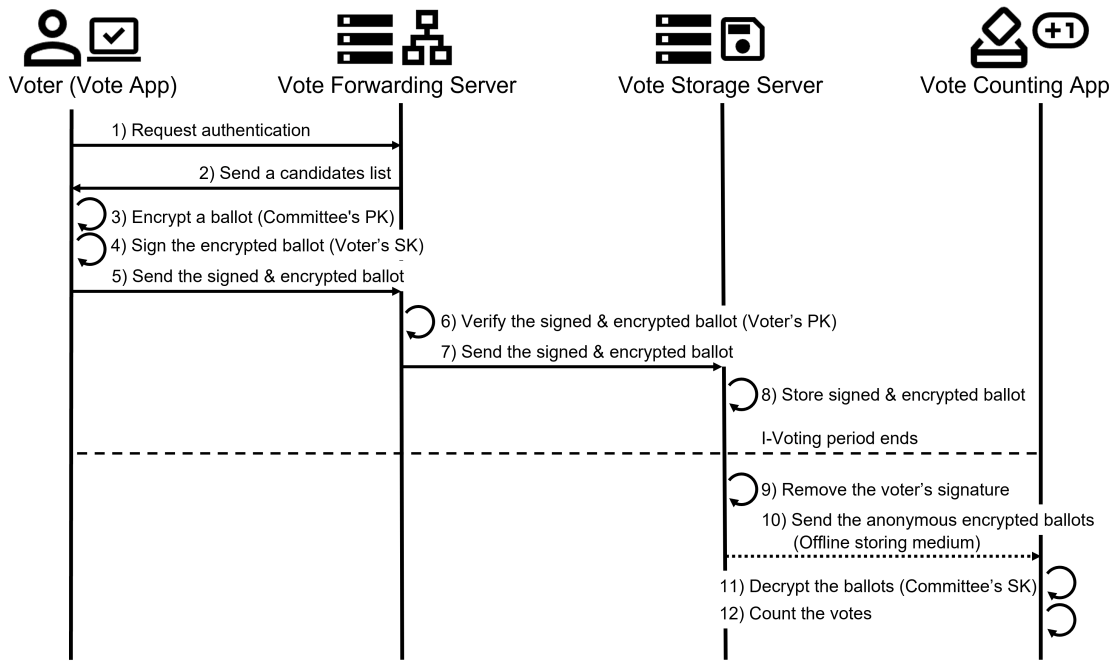

Fig. 2. Estonian I-voting service process.

이다. 에스토니아 국민은 인증과 전자서명을 위해, 공개키 기반의 두 가지 디지털 인증서가 포함된 eID 카드를 신분증으로 소유한다. 에스토니아는 eID 카드를 활용한 본인인증과 안전성을 확보한 시스템을 통해, 전자투표로 국가 단위의 공직 선거를 실시한 세계 최초의 나라가 되었다[13].

에스토니아의 전자투표 시스템은 이중봉투 시스템(double-envelope scheme)을 기반으로 한다. Fig. 2.와 같이 유권자들은 개인 컴퓨터에서 독립형 애플리케이션인 투표 애플리케이션을 사용하여 투표를 진행한다. 유권자는 eID 카드를 통해 본인을 인증하고, 후보자 목록을 받은 후, 기표한다. 기표 된 투표용지는 내부 봉투(encrypted ballot)에 담겨 에스토니아 선거관리위원회의 공개키로 암호화되고, 내부 봉투는 유권자가 전자서명한 외부 봉투(signed & encrypted ballot)에 담겨 투표 전송 서버(vote forwarding server)로 전송된다. 투표 전송 서버는 네트워크에 연결된 유일한 서버로서, 유권자 인증, 선거권 확인, 후보자 목록 전송, 서명 및 암호화된 투표용지 수신 등의 작업을 수행한다. 수신된 외부 봉투는 서명 확인 후 투표 저장 서버(vote storage server)로 전송되며, 투표 전송 서버는 투표 저장 서버로부터 수신한 확인 메시지를 유권자에게 전달한다. 전자투표 기간이 끝나면 투표 전송 서버는 작업을 종료한다. 투표 저장 서버는 투표 기간 동안 서명된 투표용지를 저장하고, 관리를 책임진다. 투표 기간 종료 후, 유권자가 전자서명한 외부 봉투는 제거되고, 암호화된 내부 봉투는 오프라인 저장매체를 통해 투표 집계 애플리케이션(vote counting application)으로 전송된다. 투표 집계 애플리케이션은 모든 암호화된 투표용지를 집계하여 투표 결과를 확인하는 오프라인 애플리케이션으로, 에스토니아 선거관리위원회의 개인키로 내부 봉투를 복호화하여 투표를 집계한다. 추가로, 전자투표 시스템은 독립적인 로그 파일을 제공하여 투표 과정의 투명성을 보장하고, 분쟁 발생 시 이를 해결하는 데 활용한다[14,15].

3.2 메타버스 환경의 프라이버시 이슈

메타버스는 사용자가 자신의 분신인 아바타를 통해 다양한 활동에 참여하며 새로운 가치를 생산할 수 있는 획기적인 기술이지만, 그만큼 보안 측면에서 주의해야 할 사항들이 존재한다. '제페토'의 실제 얼굴 사진을 기반으로 생성되는 아바타로 인한 사용자 얼굴 이미지 노출 가능성 및 설문조사를 통한 개인정보

유출, '나이키 런 클럽'과 '포켓몬 고'의 GPS를 통한 생활 반경 및 일상 노출, '모여봐요 동물의 숲'의 계정 정보 유출, '로블록스'의 관리자 계정 해킹 사례와 같이 메타버스 환경에서의 프라이버시 위협은 지속적으로 발생하고 있다[16]. 이외에도 환자의 의료 정보, 생체인증에 필요한 바이오정보, 경매 입찰자의 입찰 정보, 투표 참여자의 정치 성향 등 다양한 행위를 통해 노출될 수 있는 개인정보를 안전하게 처리할 필요가 있다

한국인터넷진흥원은 생체정보, 몸짓, 시선과 같은 기존과 다른 정보의 수집 및 활용, 개인정보 공유 및 활용 등 과도한 개인정보 데이터 수집이 사용자의 프라이버시 보존에 위협을 끼칠 수 있다고 발표했다[17]. 이러한 위협을 고려할 때, 메타버스 환경의 확장을 위한 현실 세계 서비스 도입 시, 유의할 사항들이 존재한다.

생체인증을 위한 FIDO2 기술의 경우, FIDO2 프로토콜을 실행하기 위한 운영체제와 안전한 인증정보 보관을 위한 보안 모듈이 생체인증 장비에 탑재되어야 한다. 가상환경 센싱 기기들은 연산 능력에 한계가 존재하고, 사용자별로 다양한 기기들을 조합하여 사용할 수 있기 때문에 메타버스 환경에서 FIDO2 기술을 범용적으로 적용하는 것은 현실적으로 어렵다. 또한, 인증 장비가 자신이 소유한 기기로 한정되므로 기기나 장소와 같은 환경에 구애받지 않고 접속이 가능한 메타버스의 특성에 부합하지 않는다.

에스토니아의 전자투표 시스템은 중앙집중된 신뢰 기관에 과도하게 의존한다. 이는 중앙 서버의 무결성 유지와 선거 관리자의 정직성 확보가 필수적이라는 것을 의미하며, 이로 인해 다양한 운영 및 보안 취약점이 발생할 수 있는 구조적 한계를 가지고 있다. 에스토니아 전자투표 시스템에 대한 보안 분석 연구에 따르면, 이러한 취약점으로 인해 정직하지 않은 내부자나 국가 지원 공격(state-sponsored attacks)이 선거 서버나 유권자의 클라이언트를 악용하여 선거 결과를 조작할 가능성이 존재한다[18].

IV. 메타버스 환경에서의 프라이버시 보존을 위한 MPC 응용 시나리오

본 절에서는 메타버스 환경의 기능을 확대하고 사용자의 프라이버시를 보존하기 위해 기존 현실 세계 서비스의 한계점을 극복한 MPC 응용 연구 시나리오를 제안한다. 사용자 기기의 외부에서도 바이오정보를 안전하게 보호하는 생체인증 서비스와 신뢰 기관으로부터 비밀성과 무결성을 보장하는 전자투표 서비스가 이에 해당한다.

4.1 바이오정보 노출을 최소화하는 사용자 생체인증

접속 환경에 종속되지 않고 사용자의 바이오정보를 안전하게 처리할 수 있는 생체인증 시나리오로 Fig. 3.와 같은 사용자 바이오정보 저장 및 인증 서비스를 제안한다. 안전한 사용자 바이오정보 저장 및 인증을 위하여, 메타버스 서비스 제공자는 다수의 독립된 바이오정보 인증 서버와 사용자 바이오정보 등록 및 생체인증을 위한 MPC 프로그램이 필요하다.

바이오정보 등록 시, 사용자는 자신의 바이오정보를 암호화한 후 바이오정보 등록을 위한 MPC 프로그램의 입력값으로 활용한다. MPC 프로그램 내부에서 사용자의 바이오정보는 비밀 공유 방식으로 안전하게 분할되고, 분할된 비밀 조각들은 각 바이오정보 인증 서버에 분산 저장된다.

사용자 인증 시, 사용자는 자신의 암호화된 바이오정보를 생체인증을 위한 MPC 프로그램의 입력값으로 제공하고, 서비스 제공자의 바이오정보 인증 서버들은 각기 분산 저장된 사용자의 바이오정보 비밀 조각들을 생체인증 MPC 프로그램의 입력값으로 사용한다. 프로그램 내부에서는 MPC 연산을 통해 분산 저장된 바이오정보를 복원하고 사용자가 인증에 제공한 바이오정보와 비교한다. MPC 연산 중 생성된 값은 외부에 노출되지 않으므로, 사용자는 바이오정보가 유출될 염려 없이 안전하게 생체인증을 진행할 수 있다.

본 논문에서 제시된 방법을 활용하면, 사용자는 기기에 종속되지 않고 장소의 제약 없이 생체인증을 통해 자신을 인증할 수 있다. 메타버스 센싱 기기 제조사의 경우 바이오정보 인식 센서를 통해 생체인증 작업을 지원할 수 있다.

4.2 무결성과 프라이버시 보호를 강화한 전자투표

전자투표 서비스의 신뢰 기관은 투표 과정의 보안성과 공정성을 보장하고, 시스템을 감독하여 투표 결과의 신뢰성을 확보한다. 하지만, 신뢰 기관은 전체 투표 시스템의 취약점으로 작용할 수 있다. 특히, 불특정 다수가 참여하는 메타버스 환경에서는 투표 관리 기관의 신뢰성을 보장하기 어렵다. 메타버스 환경

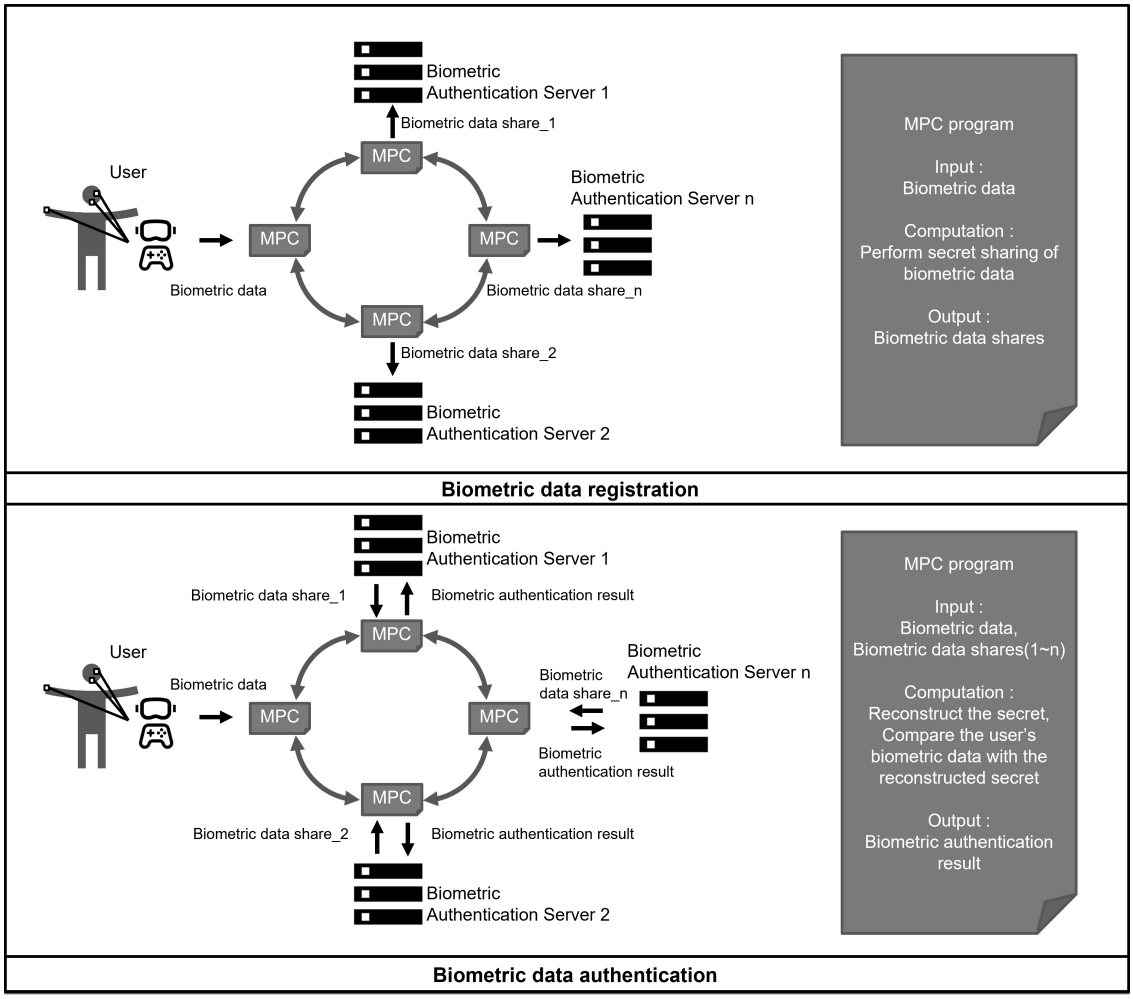

Fig. 3. Biometric data registration and authentication service.

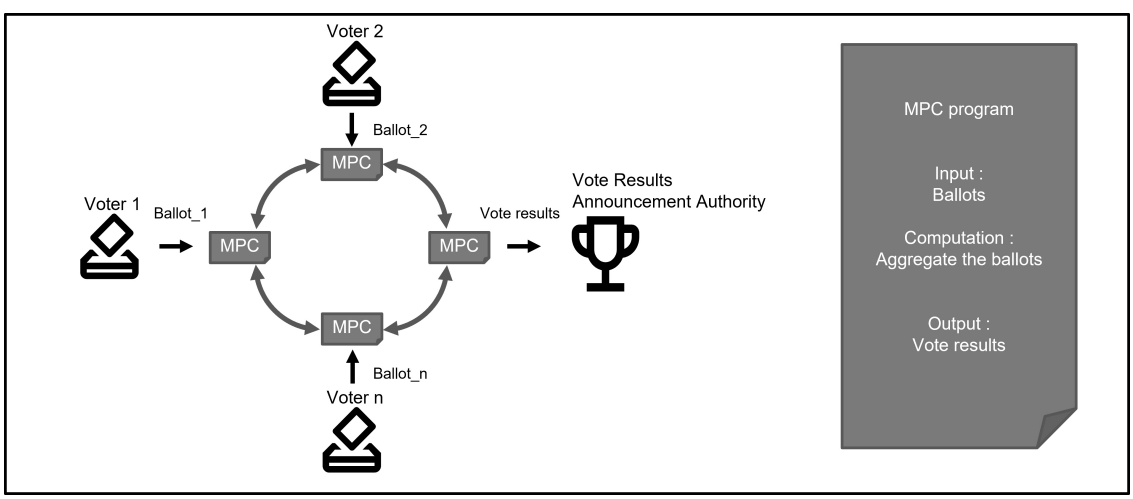

Fig. 4. Confidentiality and integrity assured electronic voting service.

의 투표 관리 기관으로부터 사용자의 프라이버시를 보존하고 투표 결과를 신뢰하기 위해 Fig. 4.와 같은 MPC 기반의 투표 서비스 시나리오를 제안한다.

유권자는 Fig. 3.와 같이 메타버스 환경에 적합한 생체인증을 통해 자신의 신원을 인증하고 투표를 위한 MPC 프로그램에 접속할 수 있다. 정당한 투표권을 가진 유권자는 후보자 목록을 확인하고 기표를 진행한다. 투표용지 작성을 마친 유권자는 다른 유권자들과 투표 결과 집계를 위한 MPC 연산을 실행한다. MPC 연산에 참여한 각 유권자는 자신의 투표용지를 연산의 입력값으로 사용하고, 공동 연산을 통한 집계 결과를 투표 결과 발표 기관과 공유한다.

MPC는 진행 중인 연산을 통해 입력값을 포함한 참여자의 어떤 정보도 노출하지 않으므로, 유권자와 투표 내용을 분리하기 위한 복잡한 연산이 불필요하다. 또한, 유권자의 투표용지에 대한 투표 관리 기관의 접근을 차단하여 투표 내용을 확인하거나 수정 및 삭제하는 행위를 방지한다. 이를 통해 투표 관리 기관에 대한 신뢰가 충분하지 않은 메타버스 환경에서 투표자의 프라이버시를 보존하며 투표 결과의 신뢰성을 보장할 수 있다.

V. 결 론

본 논문에서는 메타버스와 MPC를 소개하고, 개인정보 노출을 최소화한 광고 효과 분석, 의료 센서 클라우드 기반의 안전한 의료 데이터 통계 분석, 기업 기밀 정보를 보존하는 탄소배출권 경매와 같은 MPC 응용 사례를 조사하였다. 또한, 메타버스 세계의 발전에 필요한 생체인증 서비스와 전자투표 서비스에 해당하는 FIDO2 기술과 에스토니아의 온라인 전자투표를 분석하고, 메타버스 환경에 존재하는 프라이버시 이슈와 현실 세계 서비스의 한계점을 정리하였다. 이러한 연구를 바탕으로, 사용자의 바이오정보 노출을 최소화하는 생체인증 서비스, 비밀성과 무결성이 보장되는 전자투표 서비스와 같이 메타버스 환경에서 사용자의 프라이버시를 보존하기 위해 MPC를 활용한 응용 서비스 시나리오를 제안하였다.

제안한 시나리오들은 사용된 MPC 프로토콜의 구성 방식에 따라 성능에 유의미한 차이가 발생할 수 있다. 향후 연구에서는 최적화된 연산을 위한 MPC 프로토콜을 설계하고, 제시한 시나리오를 실제로 구현하여 효율성과 보안 취약성을 분석할 것이다. 이를 통해 다양한 메타버스 환경에서 사용자의 프라이버시를 보존하기 위한 체계화된 방법을 연구하고자 한다.

References

[1] J. Smart, J. Cascio, J. Paffendorf, C. Bridges, J. Hummel, J. Hursthouse, and R. Moss, "A cross-industry public foresight project," Metaverse Roadmap Pathways 3D Web, Acceleration Studies Foundation, Apr. 2007.

[2] A.C. Yao, "Protocols for secure computations," Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, pp. 160-164, Nov. 1982.

[3] O. Goldreich, S. Micali and A. Wigderson, "How to play any mental game, or a completeness theorem for protocols with honest majority," Proceedings of the 19th Annual ACM Symposium on Theory of Computing, pp. 218-229, May. 1987.

[4] A. Shamir, "How to share a secret," Communication of the ACM, vol. 22, no. 11, pp. 612 - 613, Nov. 1979.

[5] M. Ben-Or, S. Goldwasser and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," Proceedings of the 20th Annual ACM Symposium on Theory of Computing, pp. 1-10, May. 1988.

[6] D. Beaver, S. Micali and P. Rogaway, "The round complexity of secure protocols," Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, pp. 503-513, May. 1990.

[7] M.S. Riazi, M. Javaheripi, S.U. Hussain, and F. Koushanfar, "MPCircuits: optimized circuit generation for secure multi-party computation," Proceedings of the 2019 IEEE International Symposium on

Hardware Oriented Security and Trust, pp. 198-207, May. 2019.
[8] R. Tso, A. Alelaiwi, S.M. Mizanur Rahman, M.E. Wu, and M.S. Hossain, "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud," Journal of Signal Processing Systems, vol. 89, no. 1, pp. 51-59, Oct. 2017.
[9] M. Zanin, T.T. Delibasi, J.C. Triana, V. Mirchandani, E. Álvarez Pereira, A. Enrich, D. Perez, C. Paşaoğlu, M. Fidanoglu, E. Koyuncu, G. Guner, I. Ozkol, and G. Inalhan, "Towards a secure trading of aviation CO2 allowance," Journal of Air Transport Management, vol. 56, no. Part A, pp. 3-11, Sep. 2016.
[10] R. Lindemann, D. Baghdasaryan, B. Hill, J.E. Hill and D. Biggs, "FIDO security reference," fido-security-ref-v2.1-ps-20220523, May. 2022.
[11] J. Bradley, J. Hodges, M.B. Jones, A. Kumar, R. Lindemann, C. Armstrong, K. Georgantas, F. Kaczmarczyck, N. Satragno and N. Sung, "Client to authenticator protocol (CTAP)," fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621, Jun. 2022.
[12] J. Hodges, J.C. Jones, M.B. Jones, A. Kumar, E. Lundberg, J. Bradley, C. Brand, A. Langley, G. Mandyam, N. Satragno, N. Steele, J. Tan, S. Weeden, M. West and J. Yasskin, "Web authentication: an API for accessing public key credentials level 2 - W3C recommendation," REC-webauthn-2-20210408, Apr. 2021.
[13] H.J. Cho, "E-democracy and internet voting: a case study of the Estonia," Journal of Korean Association of Party Studies, 7(2), pp. 159-187, Aug. 2008.
[14] Estonian National Electoral Committee, "E-voting system: General overview," Estonian National Electoral Committee, 2010.
[15] P. Vinke, "Internet voting in estonia," Proceedings of the 16th Nordic Conference on Secure IT Systems, LNCS 7161, pp. 4-12, 2012.
[16] A.Y. Kim, "Private data ecosystem in metaverse platforms," 2021 KISA Report 6(8), Korean Internet & Security Agency, Jul. 2021.
[17] K.S. Min, G.Y. Kim, J.S. Park, J.H. Baek, H. Kwon, and J.D. Jang, "Metaverse and NFT, cybersecurity threat outlook and analysis," KISA Insight 2022 Vol.04, Korean Internet & Security Agency, Jun. 2022.
[18] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J. A. Halderman, "Security analysis of the Estonian internet voting system," Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 703-715, Nov. 2011.

〈저 자 소 개〉

장 지 운 (Jiun Jang) 학생회원
2021년 2월: 고려대학교 컴퓨터융합소프트웨어학과 학사
2021년 3월~현재: 과학기술연합대학원대학교 정보통신공학 석·박사통합과정
〈관심분야〉 개인정보보호, 바이오인증, 다자간 연산

조 관 태 (Kwantae Cho) 정회원
2005년 2월: 고려대학교 컴퓨터학과 학사
2008년 2월: 고려대학교 정보보호대학원 석사
2013년 2월: 고려대학교 정보보호대학원 박사
2013년 3월~현재: 한국전자통신연구원 사이버보안연구본부 책임연구원
〈관심분야〉 개인정보보호, 바이오인증, 다자간 연산

조 상 래 (Sangrae Cho) 정회원
1996년: Imperial College London, Computing 학사
1997년: Royal Holloway, University of London, Information Security 석사
1997년~1999년: LG 종합기술원 연구원
1999년~현재: 한국전자통신연구원 사이버보안연구본부 책임연구원
〈관심분야〉 인증, ID 관리, 바이오인증

김 수 형 (Soo Hyung Kim) 정회원
1996년 2월: 연세대학교 컴퓨터과학과 졸업
1998년 8월: 연세대학교 컴퓨터과학과 석사
2016년 2월: KAIST 전산학 박사
2000년 11월: 한국정보통신연구원
2000년 12월~현재: 한국전자통신연구원 사이버보안연구본부 책임연구원
〈관심분야〉 ID 관리, 바이오인증, 핀테크 보안, 모바일 보안, 개인정보보호