메타버스 환경에서 금융서비스 보안 위협 연구

유수경[1]*, 서영재[2], 곽병일(지도교수)[3]
한림대학교 소프트웨어학부

Financial Service Security Threats in the Metaverse Environments

Soo Kyung Yoo[1]*, Yeong Jae Seo[2], Byung Il Kwak[3]

요약 : 코로나19로 인하여 사회는 언택트 시대로 빠르게 변화하였다. 이에 따라 메타버스 기술은 차세대 디지털금융 채널로 발전할 것이라는 가능성을 보고 있지만, 동시에 보안 위협에 노출되어있다. 메타버스 보안에 관한 연구는 아직 부족한 상태이다. 본 논문은 메타버스 환경에서 금융서비스 사업 현황을 살펴보고, 금융과 접목한 메타버스의 보안 위협과 대응 방안을 4가지 공격 대상으로 분류하여 제시한다.

Key Words : Metaverse, NFT, Security Threats, Financial Service, BlockChain

1. 서 론

코로나19 팬데믹의 영향으로 세계 사회는 언택트 시대로 빠르게 변화하였다. 최근 AR·VR 기기와 플랫폼 소프트웨어 등 메타버스와 관련된 기술이 급격히 발전했다[1]. 불필요한 접촉을 피하는 비대면 소비가 활성화되면서 모바일 디바이스를 이용한 간편 결제 시장이 빠르게 확산하고 있다. 정보 전달력과 고객 편리성을 제공하는 메타버스의 특징을 이용한 금융권 메타버스 시장이 확대되고 있다[2].

본 논문은 최근 메타버스의 보안 취약점 사례를 살펴보면서, 메타버스 사용 확산에 따른 보안 동향과 메타버스 내에서 발생할 수 있는 보안 취약점 및 해결 방안을 제시한다. 또한, 메타버스와 금융이 접목한, 즉 NFT(Non-Fungible Token) 사용 변화를 조사한다.

2. 배경지식

2.1 메타버스 정의

메타버스(metaverse)는 초월을 뜻하는 'Meta'와 세계를 의미하는 '-verse'를 합성한 용어이다[3]. 가상과 현실의 상호작용을 통해 그 속에서 금융, 교육, 의료 게임 등 다양한 활동들을 하며 가치를 창출하는 세계이다. 메타버스는 시·공간 제약 없이 소통 가능하며, 현실에서 불가능했던 경험과 즐거움을 느낄 수 있다.

2.2 메타버스 환경에서의 금융서비스 활용

최근 메타버스 플랫폼과 콘텐츠를 제공하는 주요 기업의 성장세가 이어지고 있으며, 투자 및 기술 개발이 늘어나고 금융상품이 출시되는 등 관련 시장이 확대되고 있다. 국내외 금융회사는 메타버스 관련 펀드, ETF, ETN 등 다양한 금융상품을 출시하는 등 투자에 대한 관심도가 상승하였다. 메타버스를 통해 정보의 전달력 및 고객의 편리성을 높일 수 있을 것이라는 특징으로 금융업과 메타버스가 연계된 서비스를 제공하는 금융사가 증가하고 있다[1].

표 1. 국내 주요 금융사 메타버스 사업 현황

구분	사업
J.P. Morgan	자체적인 블록체인 플랫폼 오닉스(Onyx) 구축
신한은행	메타버스 플랫폼 '제페토'의 MOU를 통한 메타버스 특화 카드 출시
하나은행	메타버스 플랫폼 '제페토'에 하나카드 월드 구축
KB국민은행	메타버스 플랫폼 'KB 금융타운' 구축 및 모바일 지점의 연동 등의 서비스 구현
NH농협은행	메타버스 플랫폼 '독도 버스' 구축

해당 논문에서는 다섯 가지의 금융사를 기준으로 표 1과 같이 메타버스 환경에서의 금융서비스 사업에 대하여 정리하였다.

미국 투자은행 J.P. Morgan은 메타버스를 금융서비스와 연계하는 시도로써 블록체인 플랫폼 오닉스(Onyx)를 구축하며 정보 이전, 결제처리, 가상자산 교환 등의 기술을 확보하였다. 또한, J.P. Morgan은 해당 플랫폼을 통해 직원 교육, 외부 홍보 등 소통 수단으로 활용 외에 지급 결제(디지털 지갑), 대출 등의 금융서비스를 제공하는 공간으로 활용할 계획이다[2].

신한은행과 하나은행은 메타버스 플랫폼인 제페토와의 협력을 통해 아바타를 카드 디자인에 반영하고, 현금 캐시 카드와 혜택을 연계하여 메타버스 마케팅 상품을 추진하였다. 이러한 전략으로 메타버스 행동 및 소비 패턴 등의 데이터를 수집할 수 있을 것으로 기대된다. 또한, 전용 결제 플랫폼이 구축되어 메타버스와 현실의 소비를 연동이 가능해진다. 그 외에 KB국민은행과 NH농협은행은 자체 메타버스 플랫폼을 구축하여 금융서비스를 제공하고 있다. 두 은행은 해당 플랫폼에 암호화폐 수탁, 디지털 자산 투자 서비스 등을 추가하는 방안을 고려하고 있다[4].

그림 1. 메타버스 내 금융서비스 프로세스

메타버스에서의 금융서비스는 그림 1과 같은 과정으로 이루어진다. 가상세계에 설치된 지점을 방문하여 금융 서비스(카드 신청, 대출, 예금 가입 등)를 받는다. 은행은 NFT를 발행하고, 회원들은 이를 거래하는 과정을 반복하며 하나의 시장을 형성한다.

3. 본론

3.1. 금융권 메타버스 환경 보안 위협 요소 분석

메타버스와 블록체인 기반 가상자산 업계는 영역을

구축해 나가고 있지만, 이와 관련된 기술은 그 속도를 따라가지 못하여 '관리 공백'의 발생이 우려된다. 메타버스에서는 많은 양의 개인정보가 실시간으로 자동 수집되고 처리돼 이전과는 비교할 수 없는 수준의 개인정보가 노출돼있다는 문제가 있다.

메타버스 시대에서의 계정 해킹은 개인정보부터 민감정보까지 다양한 유형의 데이터가 위·변조될 수 있다. 아직 개념만이 거론되고 구체화한 서비스 고도화가 이뤄지지 않은 상황에서 메타버스 속의 개인정보가 어떤 방식으로 어떤 대상에게 어떤 범위로 공유되는지는 불명확하다[2].

본 논문에서는 표 2과 같이 4가지 관점의 공격 대상을 기준으로 보안 위협을 정리하였다. 특히 공격 대상이 데이터인 경우, 가상자산에 대한 탈취 및 불법 복제의 보안 위협이 있다. NFT 거래 시장의 성장으로 대규모 자금을 노리는 해킹과 거래 사기 등의 보안 위협이 증가하는 추세이다. 따라서, 메타버스와 융합된 가상경제에도 위협이 될 것으로 전망된다[5]. NFT는 토큰을 통해 소유자나 거래 이력을 안전하게 보관할

표 2. 메타버스 보안 위협 이슈 종류 및 내용 [5]

공격 대상	내용
인프라 및 시스템	① 가상환경 플랫폼 및 시스템(AR, VR SW, 플랫폼, 데이터 관리 시스템 등)에 대한 보안 위협 ② 메타버스 서비스 구축, 관리, 서버 등 인프라에 대한 물리적 및 SW 보안 취약점에 따른 위협 ③ 메타버스 플랫폼 및 서비스 이용을 위한 WEB, 어플리케이션 등 취약점으로 인한 보안 위협
네트워크	① 정보 송수신 네트워크 취약점을 이용한 정보 탈취 및 시스템 해킹, 서비스 공격
데이터	① 서비스 시스템에 저장된 개인정보, 콘텐츠 데이터 위변조 및 유출, 개인정보 암호화 및 가명 처리 미흡 ② 아바타, 게임머니, 포인트, NFT 등 가상자산에 대한 탈취 및 불법 복제 등 보안 위협
서비스	① 사용 단말기, 디바이스 펌웨어 취약점, 보안패치 미적용 및 패치 파일 자체 취약점에 따른 보안 위협 ② 실시간으로 수집되는 위치정보, 민감정보 및 개인정보 유출에 따른 사생활 침해, 데이터 변조 위협

표 3. 메타버스 보안 위협 대응 방안 [5]

구분	방안 예시
인프라 및 시스템	① 사용 단말기의 사용자별 인증 및 수집 데이터 암호화 등의 보안 기능 구현 ② 사용 단말기의 펌웨어, OS 등에 대한 취약점 상시 모니터링 및 업데이트 제공 ③ 사용 단말기의 보안 위협 완화를 위한 통신 데이터 암호화 등 보안 기능 구현 ④ 사용 단말기의 이상 행위 감지(모니터링)
네트워크	① 사용 단말기 및 메타버스 플랫폼의 통신 간 데이터 암호화 및 안전성이 검증된 통신 프로토콜 구현 ② 서비스 플랫폼 제공자의 계정관리, 접근통제 등의 보안 정책 수립 및 운영 ③ DDoS, 스푸핑 방지를 위한 보안 장비 구축 및 실시간 모니터링
데이터	① 서비스 플랫폼 개발 및 운영 간 개인정보보호 수집, 관리 정책 수립 ② 서비스 플랫폼 데이터 암호화 및 개인정보 비식별화 ③ 사용자 보호를 위해 사용자 계정의 이상 행위 탐지 및 통보 시스템 구현 ④ 사용자 보호를 위한 신원인증 체계 강화 구현 (2단계 인증, 생체인증, OTP 등)
서비스	① SW 개발 보안 원칙을 준수하여 개발하고, 소스코드와 디지털 자산에 대한 취약점 점검 ② 서비스 플랫폼 개발을 위한 오픈소스 관리, 취약점(제로데이 등) 모니터링 및 신속한 보안패치 적용 ③ 서비스 플랫폼 관리자 접근제어와 같은 내부 보안 정책 수립 및 정기적인 보안감사

수 있지만, 개인 소유인 디지털 파일은 사용자의 실수로 원본 파일을 삭제하거나 해킹을 통해 원본이 위·변조될 수 있다. 더욱 현실적인 메타버스 환경을 구현하기 위해서는 사용자들을 대상으로 더 많은 개인정보를 수집해야 한다. 이에 발견될 수 있는 각종 보안 취약점으로 해커들의 공격 통로가 다양해질 수 있다[6].

3.2. 대응 방안

이러한 취약점 및 위협에 대응 가능한 다양한 방법들이 있다. 이에 표3에 나타낸 것과 같이 위협 대응 방안을 4가지 관점으로 분류했다.

현재 메타버스 내 금융서비스 사용 시 신원을 증명하는 보안 및 인증 절차 등이 미흡한 상태이며, 이에 따라 금융결제원에서 언급한 바와 같이 지급 결제 수단 개발, 즉, 메타버스 내에서의 결제 수단에 따른 보안성을 강화하는 연구가 필요한 실정이다. 또한, 현재까지 메타버스 내에서의 결제 수단 방법 및 기술을 개발 중이기 때문에 메타버스 내 금융서비스 이용 시 필요한 결제 수단에 따른 보안 기술 내재화, 보안 인증 절차에 관한 기술 개발, 사용자의 행위 분석을 통한 사용자 신원인증 체계 수립, 보안 사고 발생 관련 대응 방안 및 사후 처리 등의 개발이 필요하다.

4. 결론

코로나19로 인해 메타버스와 관련된 기술이 급격히 발전함에 따라 메타버스의 활용도가 급증하였다. 금융업에서는 메타버스 플랫폼을 통해 정보의 전달력과 고객의 편리성을 높일 수 있을 것으로 기대하며 메타버스와 연계된 금융서비스를 제공하고 있다. 그러나 이러한 메타버스 금융 거래 서비스를 제공하는 금융회사가 늘어남에 따라 보안에 대한 염려가 커지고 있다. 이에 따라 본 논문에서는 인프라 및 시스템, 네트워크, 데이터, 서비스의 4가지 공격 대상에 따른 보안 위협을 조사하고 이에 대한 대응 방안을 제시하였다. 현재 보안 전문가들은 제로데이(zero-day)공격에 대한 우려를 표하고 있는데, 메타버스의 취약점에 대한 꾸준한 논의와 연구를 통해 안정적인 보안 체계를 구축해야 한다. 향후 연구에서는 메타버스 내에서의 금융서비스 관련 도메인 외에 일반적인 메타버스 도메인에서의 보안성 검토 및 위협에 따른 대응 방안과 사후 처리 방법 등을 다룰 예정이다.

참고문헌

[1] 윤정현, 김가은, "메타버스 가상세계 생태계의 진화 전망과 혁신전략", 과학기술정책연구원, 2021

[2] 이광욱, 이주용, 이근우, 최용호, 주민석, 백재환, "금융 메타버스, 사이버 위협 동향과 대응방안", 법무법인(유) 화우, 2022.

[3] 정지수, "메타버스 관련 국내외 금융업의 현황과 이슈", 자본시장연구원(KCMI), 2021

[4] 정명섭, "메타버스는 JP모건처럼... "교육,홍보,금융서비스까지 한 번에", 아주경제, 2022

[5] 박진상, "메타버스와 NFT, 사이버보안 위협 전망 및 분석", KISA, 2022

[6] 이상우, "디지털 파일에 희소성을 더하다, 대체 불가능 토큰(NFT)", 보안뉴스, 2021