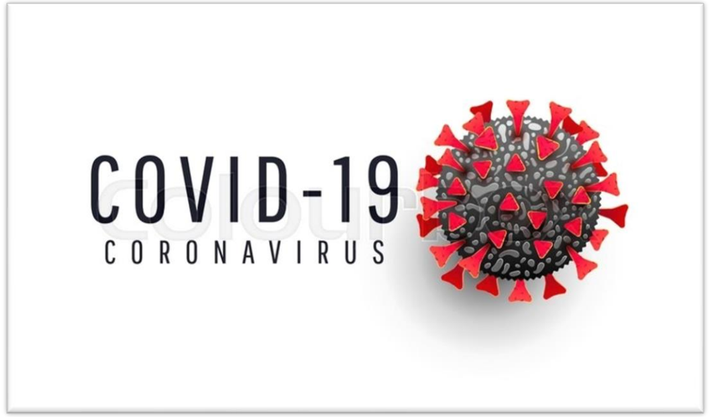
메타버스 동향과 보안 이슈

METAVERSE TRENDS AND SECURITY ISSUES

IT 정보공학과 최홍석| seok9246@gmail.com| +82 010 2421 9246

메타버스 연구 및 목적

01



메타버스 연구 및 목적

01

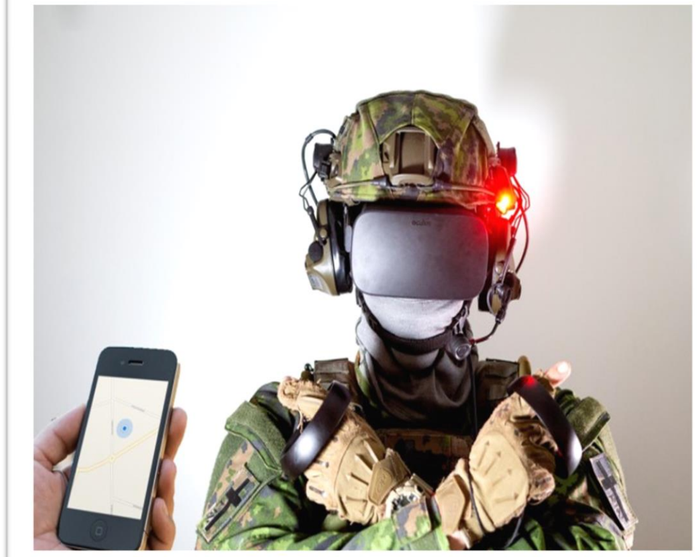
META(가상, 초월)

+

UNIVERSE(세계, 우주)

메타버스 연구 및 목적

01



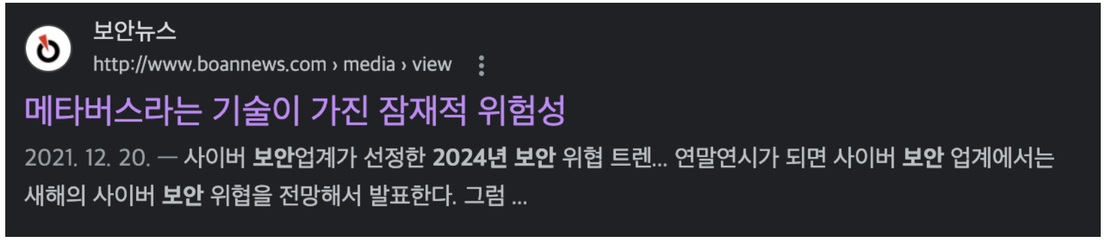
메타버스 연구 및 목적

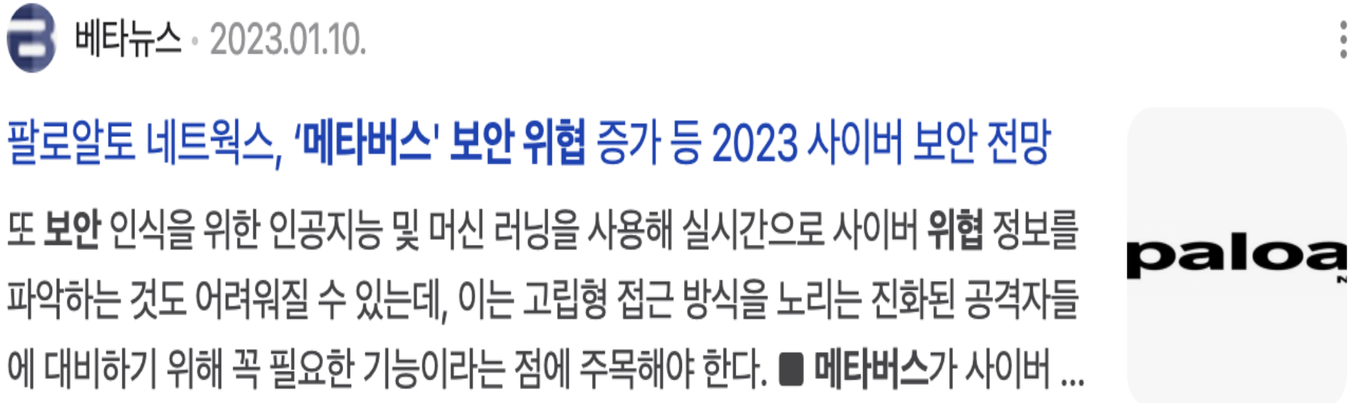
01

Metaverse

“메타버스”… 보안 이슈

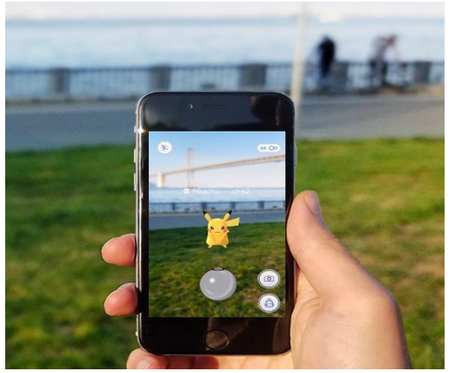
플랫폼에 접속 위한 VR/AR 기기, 모바일, PC 등 보안 취약 사이버
메타버스 아키텍처 기반의 보안 위협 예상
가상세계와 현실세계에서 "위협의 동기화” 예방 위한 법·제도적 필



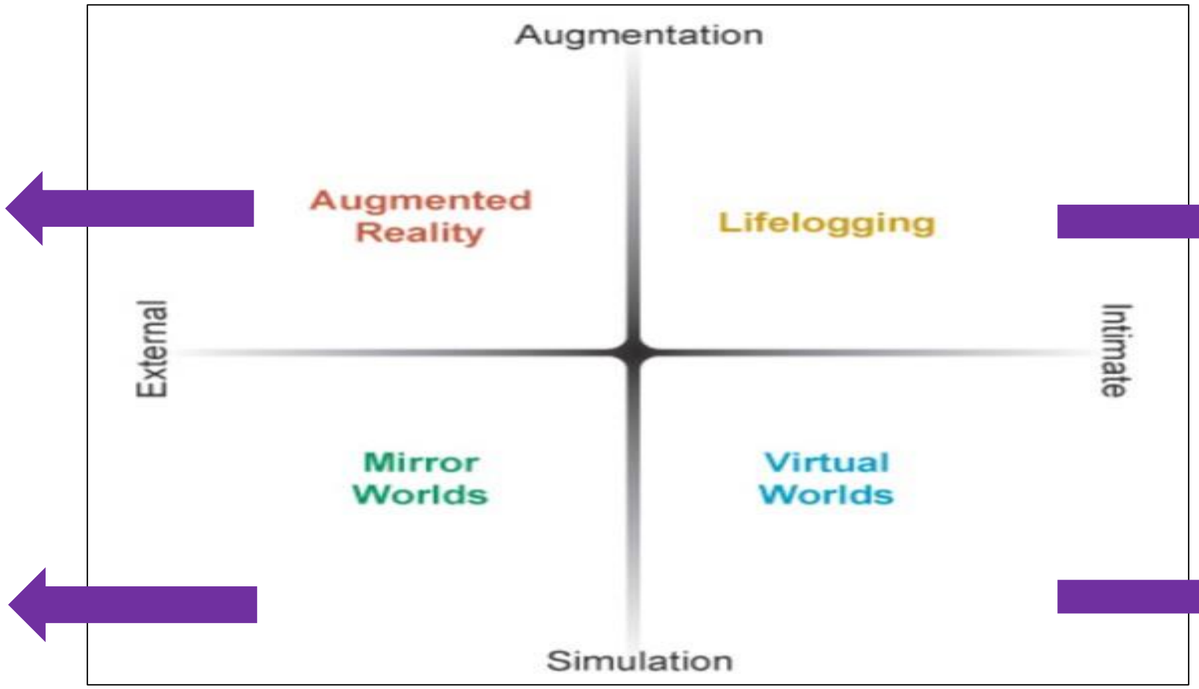


메타버스 정의

02

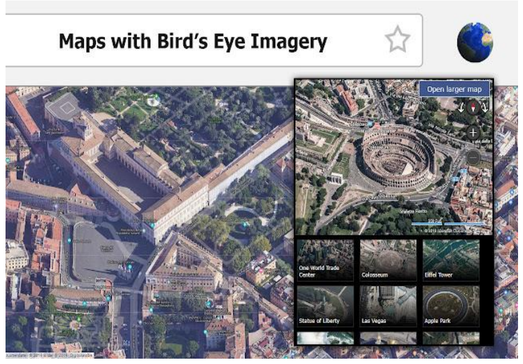


[그림] AR 기술을 활용한 PockemonGO 어플



[그림] 미국 미래가속화연구재단(Acceleration Studies Foundation)
에서 정의한 메타버스의 네 가지 요소

[그림] 라이프로깅 기술을 활용한 Apple Watch



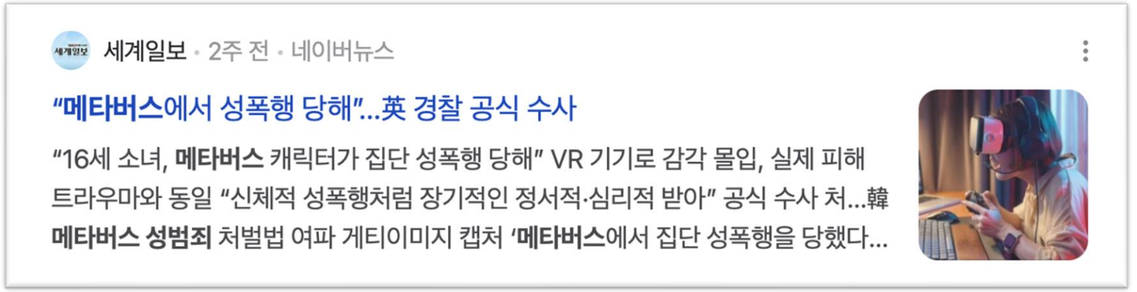
[그림] 미러월드 기술을 활용한 Google Earth 3d map

[그림] VR 기술을 활용한 3D 아바타 서비스

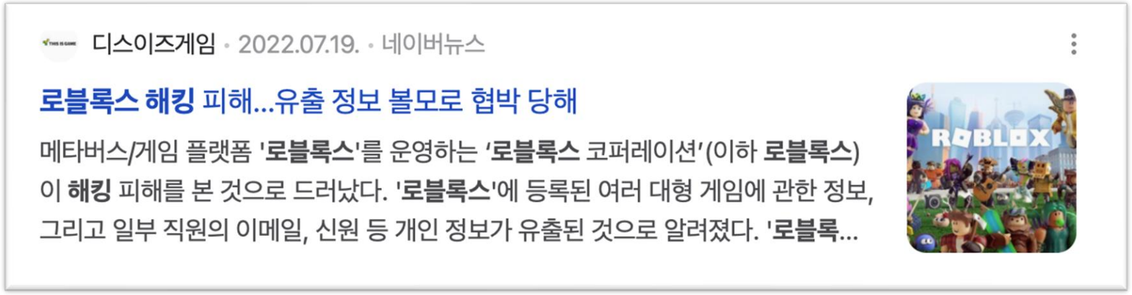
메타버스 정의

02

2021년 익명의 미술가 뱅크시의 작품을 사칭한 가짜 NFT 거래



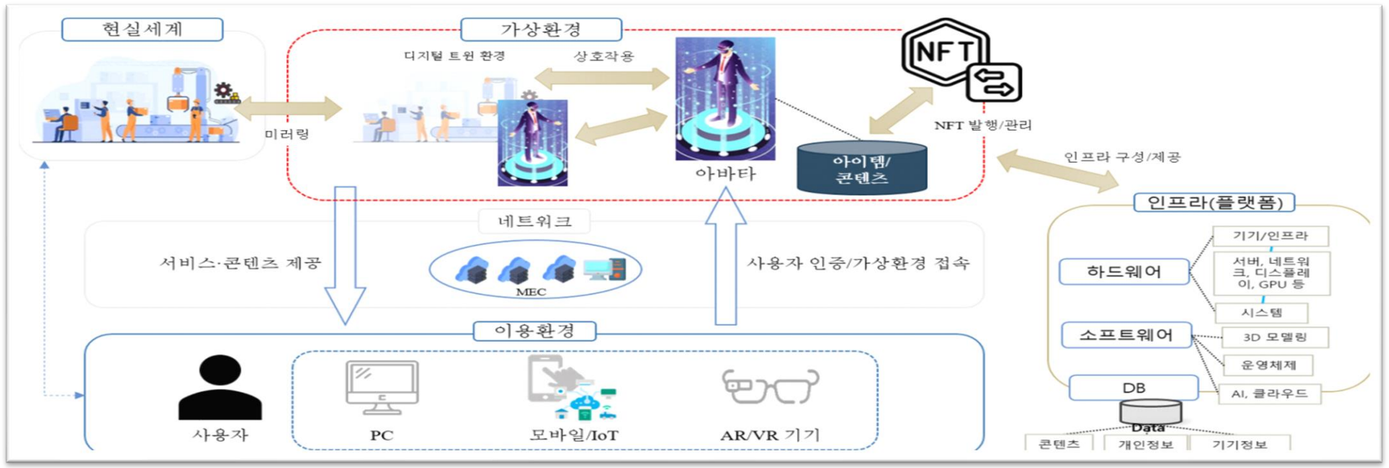
아동 청소년을 대상으로 한 스토킹 및 성폭행 사건



메타버스 게임 '로블록스' 해킹 피해

메타버스의 이용환경과 가상환경

03



[그림] 메타버스 아키텍처

구분	구성요소	역할 / 핵심 요소
현실 / 가상 환경	디지털 트윈 (디지털 가상 사물을 만들어냄)	- 현실 세계를 가상 공간에 동일하게 표현 위한 모델링 / 분석 - 센서, 액추에이터, 디지털 스레드, 3D 모델링
	NFT	- 가상환경 내 디지털 자산의 고유한 가치와 소유권을 기록 - ERC(이더리움), 블록체인
기반 환경 제공	MEC	- 데이터가 수집되는 현장에서 바로 데이터를 처리하고 연산
	인프라(플랫폼)	- 가상 환경 구성을 위한 인프라 구성/제공 - HCI 기반 하드웨어, GPU, 인공지능, 클라우드

메타버스 이용 환경의 보안위협 및 대응방안

04

구분	보안 위협	대응 방안
사용자 이용환경 측면	메타버스 사용자 신원정보 탈취를 통해 범죄 악용	- 안티 피싱, 안티 파밍 - P2P 기반 직접 인증
	인증 도용 후 메타버스 내 사용자 사칭을 통해 범죄 악용	- 생체 정보기반 FIDO 적용
	사용자의 감각 왜곡 및 위험 행동 유발	- 컨텐츠 및 기기 변조 방지 적용 - 악의적 컨텐츠 필터링 제도 수립
	공포 / 충격 컨텐츠 등 유해한 컨텐츠 표시로 사용자에 피해	- 유해 컨텐츠 탐지 / 필터링 AI 적용
디바이스 이용환경 측면	사용자 생체 정보 유출 및 악용	- 생체 정보 암호화 및 비식별화 - 생체 정보 저장 안전성 확보
	사용자 프로파일링 기반 신원 정보 및 주변 환경 정보 유출	- 엣지 컴퓨팅 구조 적용 - 사용자 로컬기기 신원 인증
	메타버스 기기 정보 및 전송 데이터 탈취 공격	- 기기 간 상호 인증 제도 도입 - 민감정보는 로컬 기기 내 처리
	메타버스 기기 DoS 공격 및 인증 공격	- 주기적 기기 패치, 인증 절차 적용 - 행위 기반 인증 기술 개발

메타버스 가상 환경의 보안위협 및 대응방안

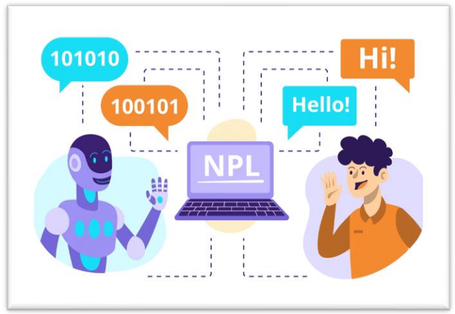
04

구분	보안 위협	대응방안
아바타 관련 위협 측면	가상 환경 내 아바타 이동 경로 추적, 스토킹 행위	- 아바타 클론, 아바타 위장/투명화(사용자 프라이버시 강화) - 아바타 간 거리두기, 개인공간 제공
	ID 추적 및 다른 메타버스 서비스 연결 공격	- 플랫폼 별 다른 아바타 생성
	아바타 도용 및 복제를 통한 인증 도용 공격	- 아바타 워터마킹 - 아바타 소유권 인증 기능 제공
데이터 및 컨텐츠 관련 위협 측면	디지털 컨텐츠 소유권 탈취, 저작권 침해	- 디지털 워터마킹, 고유 링크 지문 - 유사도 인증 등 증명 수단 제공
	허위 컨텐츠로 인한 부정적인 정보 전달	- 허위 컨텐츠 통제 수단 마련
상호 작용 측면	사용자 상호 작용 무단 도청 및 유출	- 공간 기밀성, 무결성, 가용성 보장 - 가상 보안 회의 및 일부 모자이크
	다수 거짓 아바타 생성 통한 시빌 공격	- 캡챠(CAPTCHA), 연합학습 탐지
	불법 프로그램, 계정 도용 등 어뷰징	- 메타버스 포렌식, 법적 제도 수립
디지털 트윈 환경 측면	테러 훈련, 기계 고장 유도 시뮬레이션 등 가상 환경 악용	- 사용자 행동 모니터링 / 프로파일링 - 가상환경 비인가 사용자 접근 통제
	의도적으로 잘못된 결과를 유도하여 현실에서 수행 시 사고 유도	- 메타버스 내 서비스 무결성 보장 - 메타버스 서비스 상호 인증

향후 연구 방향

05

메타버스 상에서의 데이터 분석 및 유해 콘텐츠 차단 시스템



- 데이터 분석과 모니터링
- 자연어 처리(NLP) 기술
- 이미지 및 비디오 분석
- 사용자 행동 패턴 분석
- 분산형 시스템 및 블록체인 활용

결론

06

References

07

1. Lee, J. Y., “A study on metaverse hype for sustainable growth”, International journal of advanced smart convergence, 10(3), pp. 72-80, 2021.

2. 정수용(공주대학교 융합과학과), 서창호(공주대학교 융합과학과), “확장된 가상현실인 메타버스에서의 보안 위협 분석” pp. 47– 57, 2021

3. 김현경(육군사관학교), “메타버스에서의 보안 취약점 분석 연구, pp 1454 – 1455, 2021

4. “완전한 메타버스 생태계 구현을 위한 메타버스 보안 모델” , pp 5 – 8, 2022

5. 나현식, 최대선, “메타버스 보안 위협 요소 및 대응 방안 검토”, pp 1– 2, 2022

요약

08

이번에 메타버스 동향과 보안 이슈에 대한 주제를 가지고 와봤습니다. 먼저 메타버스에 대해 알아보겠습니다. 메타버스는 가상을 의미하는 메타와 공간을 의미하는 유니버스의 합성어로 헤드 마운티드 디스플레이 같은 디바이스를 통해 자신의 분신인 아바타에 접속하여 현실과 유사한 경험을 제공하는 가상환경입니다. 이를 통해 사회적, 문화적 및 경제적 활동 등이 가능한 3차원 가상세계로 정의할 수 있습니다.
메타버스는 다양한 분야에서 활용됨에 따라 많은 사용자들이 메타버스 플랫폼에 가입해서 서비스를 이용하고 있으며, 사용자의 몰입감 향상을 위해 다양한 연구를 진행하고 있는 반면에, 아직까지 메타버스에서 발생할 수 있는 위협요소와 대책에 대한 연구는 상대적으로 부족하다는 것을 알게 되었습니다. 그래서 저는 보안 위협에 대응할 수 있는 관련 기술과 연구에 대해 조사하면서 앞으로 진행할 연구 방향에 대해 제시해보려고 합니다.
다음은 미국의 비영리연구단체인 ASF에서 메타버스를 구성하는 주요기술로 크게 4가지로 분류했습니다.
우선, 증강현실은 현실 공간에 가상 오브젝트를 배치하고 그것과 상호작용할 수 있게 하는 환경을 뜻합니다. 증강현실의 대표적인 예시로 스마트폰의 카메라를 통해 포켓몬 캐릭터가 현실 세계에 나타나서 해당 캐릭터를 잡는 포켓몬 고가 있습니다.
라이프 로깅은 사물과 사람에 대한 일상적인 경험과 정보를 서버에 저장하여 타인과 공유하는 환경을 의미합니다. 예시로 Nike Plus나 웨어러블이 있습니다.
미러 월드는 실제 세계를 가능한 한 사실적으로 반영하여 구축한 가상의 디지털 환경입니다. 예시로 Google earth 3dmap이 있습니다.
가상세계는 현실과 유사하거나 완전히 다른 대안적 세계를 디지털 데이터로 구축한 환경입니다. 예시로 제페토가 있습니다.
현재 서비스 되고 있는 메타버스 플랫폼들은 이미 몇 차례 보안의 취약점에 노출되어 서비스 업체나 소비자들이 피해를 입게 된 사건들이 있었으며, 주로 공격자들의 해킹이나, 시스템 변형, 사기 등에 의해 위험에 노출되어 있습니다. (사례설명) 이러한 문제를 방지하기 위해 서비스 제공자는 이에 대한 대책을 마련할 필요합니다.
다음은 메타버스의 아키텍처를 설명하는 그림과 구성요소와 역할을 간단하게 나타낸 표입니다. 이를 통해 메타버스 서비스는 기존 it 서비스와는 달리 빅데이터,인공지능, 블록체인 등 최신 기술이 결합되어 복합적인 형태를 보이므로 메타버스 이용환경과 가상 환경의 다양한 보안위협에 대한 대응방안 수립이 필요합니다.
메타버스 이용환경의 보안위협과 대응방안을 나타낸 표입니다.
p2p 기반 직접인증이 도움되는 이유가 p2p 기반 시스템에서는 데이터 전송과 저장을 안전하게 보호하기 위해 암호화 기술과 블록체인과 같은 분산원장 기술이 활용되기때문에 데이터의 무결성과 안전성을 강화시킬 수있습니다.
Fido는 생체정보기반 FIDO는 생체 인식 기술을 활용하여 지문, 홍채, 얼굴 인식 등의 생체 정보를 사용자 인증에 활용합니다. 이는 생체 정보를 복제하기 어렵게 만들어 높은 보안성을 제공합니다.
이 중에서 저는 사용자 이용환경 측면에서 ai기술을 활용한 솔루션인 유해컨텐츠 탐지로 연구방향을 제시해보려고 합니다.
다음은 메타버스 가상 환경의 보안위협 및 대응방안입니다. 이에 대한 설명은 다음 표와 같습니다. 이 중에서 대응방안으로 소개되는 디지털 워터마킹은 복제 방지 저작권 보호 기술로 이미지 같은 데이터를 공간적 측면으로 분석하여 삽입 정보를 공간 산에 흩어 놓거나, 이미지를 주파수 영역으로 변환시키는 방법이있습니다.
다음은 그 전에 연구방향으로 제시했던 유해콘텐츠 차단 시스템입니다. 유해이미지를 판별하는 알고리즘과 자연어처리, 블록체인 기술, AI를 활용한 연구를 토대로 메타버스에서 사용자와 플랫폼 서버 간 안전한 통신을 보장될 것으로 기대됩니다.

THANK YOU!