Innovating Education: Exploring the Metaverse, Cybersecurity, and Secure AI Platforms

EU-CHECK Workshop

May 13th-14th, 2024

Computer Technology Institute and Press (CTI)

Mitropoleos 26-28,

Athens, Greece

by Vasiliki Liagkou

EU CHECK

The Metaverse: Reimagining the Classroom

Virtual Classrooms

The metaverse enables the creation of virtual classrooms where students can interact, collaborate, and learn in a fully digital environment.

Holographic Instructors

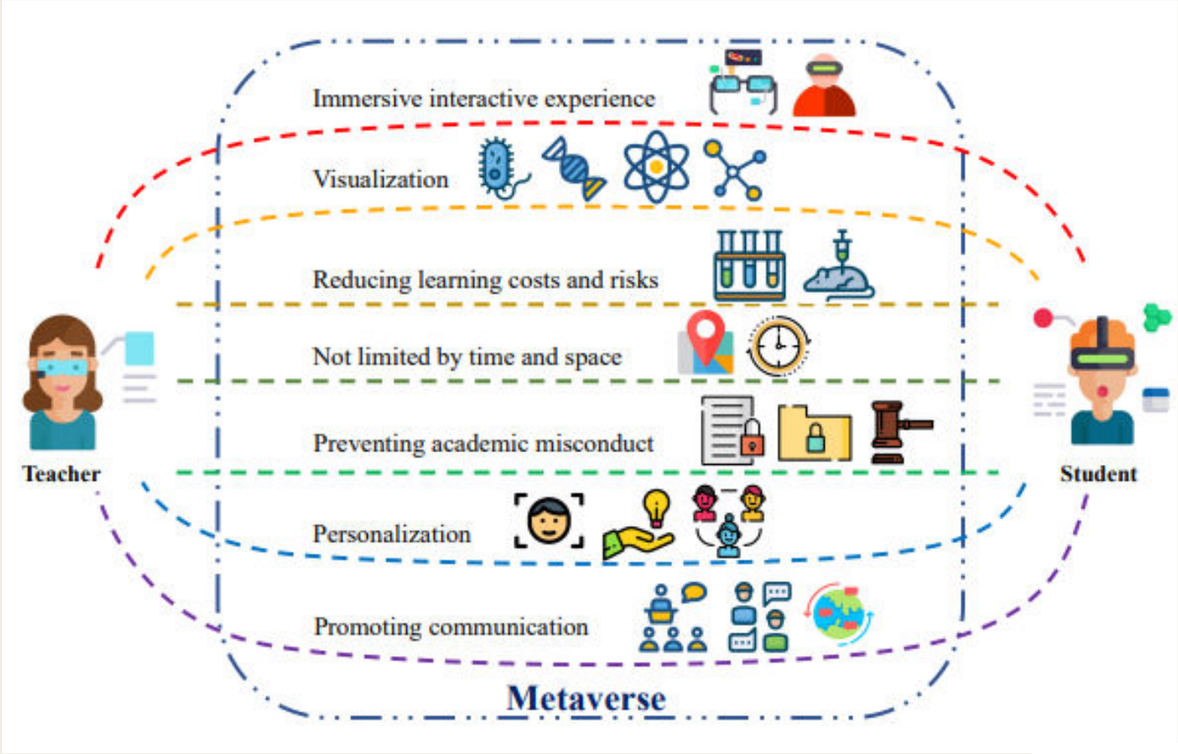
Holographic instructors can bring lessons to life, providing a more engaging and interactive learning experience.

Immersive Field Trips

Students can virtually explore historical sites, scientific laboratories, and other locations, expanding their horizons without leaving the classroom.

Evolution of educational technology

- **From chalkboards to virtual classrooms**
- VR, XR, and AR integration: immersive skills training and enhanced learning experiences
- AI in Education (AIED): personalized learning experience and support



Cybersecurity in Education: Protecting Digital Environments

1 Data Privacy

Safeguarding student and institutional data is crucial in the digital age.

2 Network Security

Ensuring secure network infrastructure to prevent cyber attacks and unauthorized access.

3 Device Management

Implementing robust policies for the use of personal and school-owned devices.

4 User Awareness

Educating students, teachers, and staff on cybersecurity best practices.

Ensuring robust security and privacy is paramount for an educational environment to effectively fulfill its mission of educating users.

Lack of confidence among users.

Fail to achieve its intended objectives.

Students, teachers, and other stakeholders expect that their personal information and data are adequately protected.

This trust forms the foundation for a productive and conducive educational atmosphere.

Security and Privacy Issues on educational metaverses

To ensure that the advantages of the metaverse are utilized effectively, we investigate the vulnerabilities of utilized technologies that promise evolving educational experiences.

The pros and cons of main utilized metaverse technologies.

These categories involve:

- Edge devices
- Access control and identity management processes
- Machine Learning model
- Artificial Intelligence models

Edge Devices

Pros

Immersive Learning Experience:

- Realistic Learning Environments
- Real-world Simulations
- Safe Experimentation in Dangerous or Expensive Scenarios
- Practice in Medical Procedures and Skills Training

Inclusivity and Accessibility:

- Overcoming Sensory or Cognitive Barriers
- Integration of Participants with Special Needs in Mainstream Education
- Fostering Inclusive Educational Practices

Cons

Passive and Active Attacks

- Eavesdropping, MitM Attacks

Similar Challenges to IoT Devices with Limited Security Measures

- Risk of Personal Data Leakage: Name, Age, Academic Records, Location

Threats of Unauthorized Access, Impersonation, and Harassment

Denial-of-Service Attacks

Access Control & Identity Management Scheme

Pros

Enhanced Security:

- Prevents Unauthorized Access
- Mitigates Data Breaches

Role Definition and Credibility:

- Defines User Roles: distinguishes between educators, students, and other stakeholders
- Ensures Credibility: Establishes trust in degrees and certifications by authenticating user identities

Tailored Policies:

- Customized User Policies: Provides different access levels and permissions based on user roles
- Flexible Management: Allows for dynamic adjustment of policies to accommodate changing user needs

Cons

Avatar Identity Ambiguity:

- Challenges in Identifying Users: Raises questions about the true identity behind avatars
- Lack of clarity in avatar identity may lead to privacy violations

Privacy and Equality Concerns:

- Risks of Privacy Offending: Potential for Bullying and Cheating: Ambiguity in user roles can facilitate unethical behavior
- Educational Inequality: Inconsistent enforcement of identity policies may create disparities in educational experiences

Machine Learning Model

Pros

Personalized Learning Experiences:

- ML models analyze interaction patterns
- Recommends Customized Activities
- Engagement and motivation in the learning process.

Risk Detection and Prevention:

- Identifies Potential Risks: detect and prevent inappropriate content consumption or behavior within the metaverse.
- Safeguards Student Well-being

Enhanced Efficiency:

- Automates Learning Processes
- Analyzes Vast Data

Cons

Privacy Risks:

- Collection and storage of biometric and behavioral data pose privacy risks to users.
- Data processing on third-party servers exposes information to malicious actors
- Data poisoning attacks

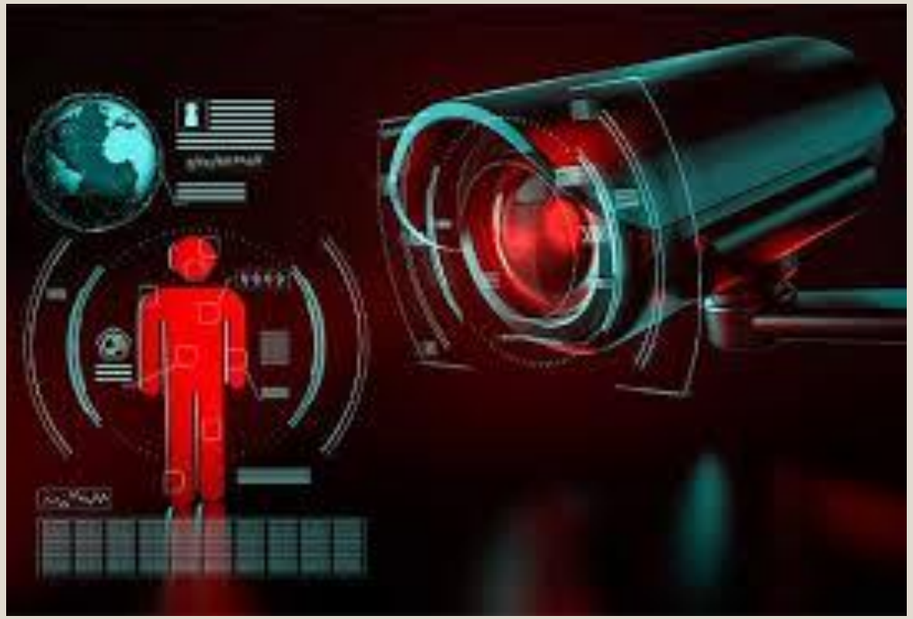
Threats to Model Integrity:

- Privacy Attacks: Adversaries exploit vulnerabilities to gain insights into model decisions, parameters, or architectures.
- Black-box and White-box Access: Intruders seek varying levels of access, from inference results to full model parameters

Misuse of Behavioral Data:

- Exploitation for Non-Educational Purposes
- Ethical Concerns

Artificial Intelligence Model



Pros

Instant Feedback and Recommendations

Supportive Roles in Education:

- Intelligent Non-player Characters (NPCs
- NPC Tutors
- NPC Tutees
- Intelligent Learning Tools
- Policy-making Advisor

Cons

Data Governance and Ethical Concerns:

- Adverse Human Rights Impacts
- Monitoring of student behavior raises privacy concerns and the potential for unfair targeting or discrimination.
- Acoustic side channel attacks

Authentication Challenges:

- Biometric Authentication Risks: vulnerable to replication or manipulation, compromising user security.
- Authentication systems in the metaverse must account for the presence of AI technolo

Related Work

- Existing literature reveals numerous security and privacy challenges within educational metaverse environments.
- Notably, proposed solutions are notably scarce, indicating a significant gap in addressing these concerns.
- Research in this domain is still in its early stages, leaving the pursuit of solutions largely uncharted.
- Challenges include decentralized authentication, securing avatar communication, and countering malicious behaviors.
- Urgent attention is needed to develop robust solutions, ensuring a trustworthy educational metaverse environment.

Unlocking Educational Potential: Metaverse Platforms and Their Features (1/2)

	Features	Compatibility	Website/Repository
Vircardia	• Open source platform • Full self – hosted • 3D Virtual Environment • Multi - user interaction using web - based clients • Full world editor • Auth policy: username & password	• Desktop • Mobile • VR (through web)	• https://vircadia.com/ • https://github.com/vircadia
Sansar	• Closed source platform • No self - hosted • 3D Virtual Environment • Full world editor • Auth policy: username & password	• Desktop • VR (HTC Vive, Oculus Quest 2)	• https://www.sansar.com/ • https://github.com/Wookey-Technologies
Second Life	• Closed source platform • No self - hosted • 3D Virtual Environment • Interaction with other users and content within a multi-user online virtual world • Full world editor • Auth policy: username & password	• Desktop • VR (through third party app)	• https://secondlife.com/ • https://github.com/secondlifePlatform

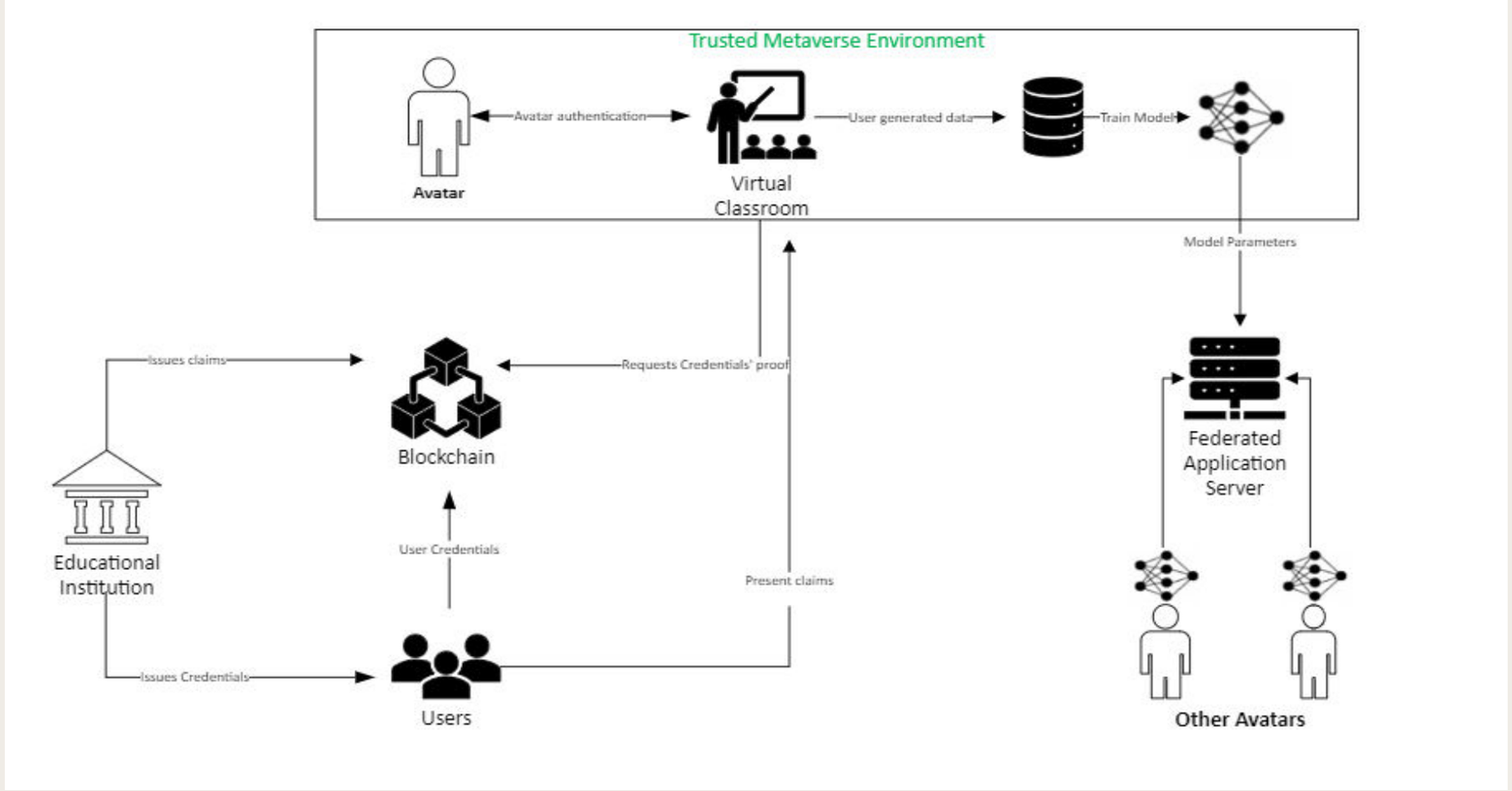
Unlocking Educational Potential: Metaverse Platforms and Their Features (2/2)

Platform	Features	Compatibility	Website/Repository
OpenSimulator	• Open source platform • Full self – hosted • 3D Virtual Environment • Interaction with other users and content within a multi-user online virtual world • Full world editor • Auth policy: username & password	• Desktop • VR (through third party app)	• http://opensimulator.org/wiki/Main_Page • https://github.com/opensim
Vortex School	• Open source platfom • Full self – hosted • 3D Virtual Environment • Deployment of the virtual classroom to end-users on cloud servers or local • Creation of virtual classroom without additional programming skills • Auth policy: Biometric data (face and voice recognition)	• Desktop (Beta - Prototype) • VR (through Desktop)	• https://github.com/Aca1990/VoRtex-School

Countermeasures-Propositions

Attack Target	Flaws	Technology-Potential Solutions
User	Unauthorised Access	Blockchain-based Access Control
	Impersonation	Multifactor authentication, NFTs
Avatar	Identity Theft- Identity Linkability	Blockchain-based Identity Management Scheme
	Authentication	Decentralised authentication protocols
Application	Privacy Leakage of ML/AI models	Decentralised Federated Learning, Differential Privacy
	Network Vulnerabilities	Intrusion Detection System (IDS)
	Data integrity	Verification through blockchain, NFTs

A Resent Work



- Blockchain-based access control to counter metaverse's decentralization challenge.
- Enables decentralized governance and data ownership.
- Avatar authentication
- Federated Learning to data privacy concerns in data training procedure.

Additional Countermeasures

- Non-fungible tokens (NFTs) to validate college diplomas and transcripts e.t.c

Integration of Intrusion Detection System (IDS):

- Network Intrusion Detection system (NIDs)
- Host-based Intrusion Detection system (HIDs)

Secure AI Platforms: Enhancing Learning Experiences

Personalized Instruction

- AI-powered platforms can adapt learning content and methods to individual student needs.

Secure AI Platforms: Enhancing Learning Experiences

Personalized Instruction

- AI-powered platforms can adapt learning content and methods to individual student needs.

Limitations

Blockchain &ML/AI

Integrating blockchain with ML/AI models also brings several limitations:

- time-consuming, increasing transaction verification costs
- low latency requirements of VR/AR services in the metaverse may conflict with blockchains' processing power

Intrusion Detection Systems

Employing an IDS in the metaverse could affect its effectiveness:

- Lack of metaverse datasets for adequate training.
- ML-based IDS rely heavily on labelled network data for training, making it difficult for models to accurately identify and respond to emerging threats without sufficient metaverse-specific datasets.
- Other current approaches train without validating performance on another data sets exposing the model to overfitting and attacks on the aggregation algorithm

Educational Institutions

- Educational institutions have budgetary challenges associated with the necessary hardware and personne costs to implement the metaverse.
- Participants involve students, educators, and diverse employees who are not technologically qualified

non-fungible tokens

- NFTs may not fully address all security concerns, such as potential vulnerabilities in their implementation.

Vulnerabilities

Categorization of potential vulnerabilities based on attack targets to aid in developing holistic solutions

Research

Lack of research, especially in educational settings, underscoring the need for tailored solutions

Educational Environments

Stressed the importance of investigating proposed solutions adapted to educational environments' architecture and vulnerabilities

The Future of Education: Blending Physical and Digital Spaces

Hybrid Classrooms

Seamless integration of physical and virtual elements, enabling remote and in-person learning.

1

Collaborative Platforms

Cloud-based tools that facilitate real-time interaction and collaboration among students and teachers.

2

Lifelong Learning

Personalized, on-demand educational resources that support continuous skill development.

3