On the privacy and security for e-education metaverse

Sofia Sakka, Vasiliki Liagkou, Chrysostomos Stylios, Afonso Ferreira

On the privacy and security for e-education metaverse

1st Sofia Sakka
Department of Informatics and Telecommunications
University of Ioannina
Arta, Greece
0009-0003-9206-9936

2nd Vasiliki Liagkou
Department of Informatics and Telecommunications
University of Ioannina
Arta, Greece
0000-0002-1162-5490

3rd Chrysostomos Stylios
Department of Informatics and Telecommunications
University of Ioannina
Arta, Greece
Industrial Systems Institute, Athena RC
Patra, Greeece
0000-0002-2888-6515

4th Afonso Ferreira
CNRS – Institut de Recherches en Informatique de Toulouse
Toulouse, France
afonso.ferreira@irit.fr

***Abstract*—Metaverse brings a new era of digital networking, blurring the lines between the physical and digital realms, enabling users to engage in social, educational, commercial and entertainment activities in a distributed environment. Especially in the field of education, this innovation brings various facilities and benefits, empowering all involved in a new world of learning. However, like the physical world, metaverse raises security and privacy issues that generate concerns among users, hampering its integration especially into everyday life, such as education. Therefore, in this work we identify security and privacy challenges associated with e-education metaverse environments, posing a series of research questions encompassing a wide spectrum of concerns. We also analyse protocols intended to create a trustworthy metaverse environment.**

Keywords— metaverse, education, security, privacy, authentication, blockchain

I. Introduction

From chalkboards to projectors and textbooks to tablets, education has always evolved alongside technology. The latest technological frontier in education are metaverses, which are interconnected, virtual shared spaces created by the convergence of virtually augmented physical reality and interactive digital spaces. This innovation brings about changes in the traditional forms of communication of individuals and traditional teaching methods, providing new perspectives and a wide range of new teaching and learning areas.

The metaverse is more than just an online environment; it serves as a portal to possibilities that were previously unthinkable in the physical world. With its immersive features, it regularly places students in mental or practical scenarios that would be too risky or hazardous to reproduce in reality. Additionally, it makes simpler to understand something that needs extensive practice and effort and motivates students to attempt to produce or investigate something that they would otherwise be unable to undertake due to practical considerations like cost or a lack of genuine resources. Also, it enables learners to perceive, experience, or observe things from different perspectives or roles and learn to interact and collaborate with individuals they might not have opportunities to work with in the real world [1].

To take advantage of all these opportunities, metaverse-enabled education systems are expected to efficiently utilise an unprecedented amount of data, with the risk of disclosing sensitive or private information of individuals during data collection, communications, and learning-based processing [2]. Therefore, using the metaverse for educational purposes has the potential to offer a useful learning mode, but it may also bring up significant moral concerns such violating people's privacy, bullying, cheating, and educational inequality [1].

In this work, we identify security and privacy challenges associated with e-education metaverse environments, particularly concerning data collection, communication, and processing, while preserving the anonymity and privacy of users. As we delve further into our exploration, we pose a series of research questions encompassing a wide spectrum of concerns and analyse protocols intended to create a trustworthy metaverse environment.

II. Research Methodology

It is important to set some research questions that could serve as a guide to our research. These questions will shed light on challenges at different levels of the metaverse environment and help identify possible holistic solutions for this innovative landscape. These are the following:

RQ1: What are the potential privacy and security risks for accessing the metaverse for educational services?

RQ2: Artificial Intelligence (AI) algorithms are employed in the metaverse for personalized and intelligent educational experiences. However, can they ensure the privacy of users, especially for students? What are the potential security threats to AI algorithms used for educational purposes in the metaverse?

RQ3: What is the role of blockchain technology in enhancing privacy, security, and trust among users in educational metaverse applications?

Addressing these issues can pave the way for a trustworthy e-education metaverse, otherwise the metaverse may become a lawless digital space [3].

III. Security and Privacy Issues

A wide variety of personal data, including biometric and behavioural data is collected and stored in the metaverse. In an educational metaverse environment, the risk of unauthorized access, impersonation, or harassment can lead to privacy violations and emotional distress. Personal data, academic records, and even the actual location of students/educators may be at risk. Wearables or Augmented/Virtual Reality (AR/VR) devices act as a

"gateway" to the metaverse era, collecting this data, potentially providing adversaries with a broad attacking surface [2]. Furthermore, the Machine Learning models help to personalize learning experience and recommend customised learning activities that suit to each student's needs, or to early detect and prevent potential risks, such as inappropriate content, by analysing patterns of behaviour and content [4]. However, the utilised learning algorithms are still vulnerable to privacy and security risks [2].

IV. Related works

Research on security and privacy challenges in metaverse environments is still in its infancy [3], [5]. Although there are several research works that identify these challenges, such as [6]–[9], the quest for comprehensive solutions remains a relatively uncharted territory. Most of these papers offer solutions based on blockchain technology promising transparent, decentralised, and reliable services that protect users' privacy creating a sustainable ecosystem [3]. Unfortunately, there are no specific solutions for providing a trustworthy environment in metaverse educational settings, so we are examining existing solutions that could be applied to our requirements.

Ryu et al. [10], designed a mutual authentication scheme for metaverse relying on blockchain technology that ensures secure communication and transparency in the management of user identification data. Despite the building of secure communication between platform servers and users, their scheme also implements secure interactions between avatars. However, avatars need to demonstrate their real-world user details to other avatars in certain circumstances (e.g., age, gender). Thus, the avatar authentication phase developed by Ryu et al. could expose users' private information to providers of metaverse services [11]. In addition, their scheme had high computational cost [12].

Therefore, Kim et al. [11], proposed a secure authentication scheme between avatars that allows users to protect their privacy during avatar interactions without relying on the service provider. However, after our security analysis we found out that their protocol was vulnerable to private key disclosure providing an adversary with multiple advantages. Thakur et al. [12], proposed a secure mutual authentication scheme for safer user-server and avatar–avatar interactions utilizing Elliptic Curve Cryptography (ECC) and fuzzy extractor. Nevertheless, they assume that their scheme is vulnerable against physical implementation attacks including differential side-channel analysis and deep learning-based side-channel analysis.

Although these schemes aim to build a trustworthy metaverse environment, security vulnerabilities of the ML models are not conveniently addressed [13]. Therefore, we also have to consider such issues, justifying research question 2. Finally, research works such as [14]

V. Conclusions

The integration of metaverse in education heralds a new era of learning. However, there is a need for balancing this innovation with strict security and privacy safeguards to create a trustworthy educational environment. In this work we identified security and privacy challenges associated with e-education metaverses and discovered vulnerabilities in existing solutions, shedding the light on open issues within the educational field of metaverses.

References

[1] G.-J. Hwang and S.-Y. Chien, "Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective," *Computers and Education: Artificial Intelligence*, vol. 3, p. 100082, 2022, doi: 10.1016/j.caeai.2022.100082.

[2] M. Letafati and S. Otoum, "On the privacy and security for e-health services in the metaverse: An overview," *Ad Hoc Networks*, vol. 150, p. 103262, Nov. 2023, doi: 10.1016/j.adhoc.2023.103262.

[3] X. Zhang, Y. Chen, L. Hu, and Y. Wang, "The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics," *Front. Psychol.*, vol. 13, p. 1016300, Oct. 2022, doi: 10.3389/fpsyg.2022.1016300.

[4] Q. Zhang, "Secure Preschool Education Using Machine Learning and Metaverse Technologies," *Applied Artificial Intelligence*, vol. 37, no. 1, p. 2222496, Dec. 2023, doi: 10.1080/08839514.2023.2222496.

[5] C. Zhang, S. Feng, R. He, Y. Fang, and S. Zhang, "Gastroenterology in the Metaverse: The dawn of a new era?," *Front. Med.*, vol. 9, p. 904566, Aug. 2022, doi: 10.3389/fmed.2022.904566.

[6] A. M. Awadallah, E. Damiani, J. Zemerly, and C. Y. Yeun, "Identity Threats in the Metaverse and Future Research Opportunities," in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates: IEEE, Mar. 2023, pp. 1–6. doi: 10.1109/ICBATS57792.2023.10111122.

[7] A. Gupta, H. Khan, S. Nazir, M. Shafiq, and M. Shabaz, "Metaverse Security: Issues, Challenges and a Viable ZTA Model," *Electronics*, vol. 12, no. 2, p. 391, Jan. 2023, doi: 10.3390/electronics12020391.

[8] K. Ghamya, C. C. Yadav, D. V. S. Pranav, K. Reddy Madhavi, and A. Patel, "Metaverse: The Potential Threats in the Virtual World," in *Proceedings of Fourth International Conference on Computer and Communication Technologies*, vol. 606, K. A. Reddy, B. R. Devi, B. George, K. S. Raju, and M. Sellathurai, Eds., in Lecture Notes in Networks and Systems, vol. 606. , Singapore: Springer Nature Singapore, 2023, pp. 59–67. doi: 10.1007/978-981-19-8563-8_6.

[9] Y. Huang, Y. J. Li, and Z. Cai, "Security and Privacy in Metaverse: A Comprehensive Survey," *Big Data Min. Anal.*, vol. 6, no. 2, pp. 234–247, Jun. 2023, doi: 10.26599/BDMA.2022.9020047.

[10] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain," *IEEE Access*, vol. 10, pp. 98944–98958, 2022, doi: 10.1109/ACCESS.2022.3206457.

[11] M. Kim, J. Oh, S. Son, Y. Park, J. Kim, and Y. Park, "Secure and Privacy-Preserving Authentication Scheme Using Decentralized Identifier in Metaverse Environment," *Electronics*, vol. 12, no. 19, p. 4073, Sep. 2023, doi: 10.3390/electronics12194073.

[12] G. Thakur, P. Kumar, C.-M. Chen, A. V. Vasilakos, Anchna, and S. Prajapat, "A Robust Privacy-Preserving ECC-Based Three-Factor Authentication Scheme for Metaverse Environment," *Computer Communications*, vol. 211, pp. 271–285, Nov. 2023, doi: 10.1016/j.comcom.2023.09.020.

[13] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, "On the Design of a Privacy-Preserving Communication Scheme for Cloud-Based Digital Twin Environments Using Blockchain," *IEEE Access*, vol. 10, pp. 75365–75375, 2022, doi: 10.1109/ACCESS.2022.3191414.

[14] S. Badruddoja, R. Dantu, Y. He, M. Thompson, A. Salau, and K. Upadhyay, "Trusted AI with Blockchain to Empower Metaverse," in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, San Antonio, TX, USA: IEEE, Sep. 2022, pp. 237–244. doi: 10.1109/BCCA55292.2022.9922027.