Personalized User Experiences in Metaverse through Federated Learning

Alexander Hillisch, Felix Koczan,
Affiliations: Department of Information Systems and Operations Management
Vienna University of Economics and Business

***Abstract*— Although the metaverse has a promising potential to provide personalized experiences driven by AI, the challenge of ensuring security and user privacy within the metaverse arises. In order to make sure, that the metaverse is a safe environment, a robust system architecture is needed. As a result, we leverage a decentralized federated learning (DFL) approach, where machine learning models are deployed, executed, and trained on end-users' devices (edge devices), in order to avoid storing all the data on centralized databases. This paper represents a technical implementation of a federated learning algorithm, which is designed to deliver real-time personalized content, while maintaining user privacy, based on Tensorflows's federated learning framework, within a Python environment. In conclusion, this research aims to enhance the security and privacy of data within the metaverse and therefore tackles one of the potential issues that could hinder the widespread adoption of the metaverse.**

I. Introduction

The metaverse represents a groundbreaking endeavor to transcend the constraints of traditional connectivity, offering a comprehensive and deeply personalized user experience. It seamlessly integrates aspects of our real lives into the digital sphere, enriching our daily existence with concepts like Augmented Reality, Virtual Reality, and Mixed Reality. In this boundless realm, users can effortlessly communicate, play games, or socialize with friends and colleagues in a myriad of imaginative worlds and novel ways, previously unimaginable in the physical world. This immense potential has beckoned tech giants like Meta (formerly Facebook, underscoring their commitment to metaverse leadership), Microsoft, and Nvidia, who have made substantial investments in this fusion of cutting-edge technologies.

However, the quest to deliver such a highly personalized and immersive user experience in the metaverse necessitates the collection of copious amounts of sensitive user data, including payment information, biometric data, device IDs, and user preferences. Given that the metaverse is still in the exploratory and innovative phase, robust privacy policies and data protection mechanisms have yet to be fully established. To address this conundrum, machine learning paradigms, such as federated learning, offer a viable solution.

Federated learning, a decentralized machine learning approach pioneered by Google in 2016 to offer predictive suggestions for user queries in Google's search bar, serves as a promising solution. It entails deploying a global model from a central server to all participants, often referred to as edge devices. These edge devices then train the model on local data, and specific model parameters are transmitted back to the central server. These parameters are aggregated and employed to enhance the global model, iterating until a convergence threshold is reached. The primary advantage of federated learning is that user data remains secure. By distributing the global model to users' edge devices, computational tasks and a substantial portion of the computing power are effectively "outsourced" to users. This not only safeguards user data but also alleviates the central server's computational burden.

Our paper addresses one of the metaverse's principal challenges hindering widespread adoption: the absence of a robust privacy framework and effective security measures. We also delve into the specific types of data that may be vulnerable to interception or compromise. Furthermore, we present a federated learning algorithm that mitigates these privacy and security gaps, offering a plausible solution for enhancing metaverse adoption. Lastly, we identify potential limitations and research opportunities stemming from our implementation, which are crucial for the continued advancement of the metaverse.

This paper unfolds as follows: First, we provide an in-depth exploration of the metaverse concept, emphasizing its potential societal benefits. Second, we offer a detailed examination of the federated learning paradigm, highlighting its advantages compared to centralized approaches. Third, we delve deeply into the intricacies of privacy and data security within the metaverse, showcasing instances where data may be jeopardized by malicious actors. Fourth, we elucidate how our proposed algorithm tackles the security and privacy challenges and compare it to traditional

centralized algorithms. Finally, we encapsulate our findings and extend a glimpse into the realm of future research opportunities within this field.

REFERENCES

- Chen, B. J., Yang, D.-N. User Recommendation in Social Metaverse with VR. In (pp. 148–158). https://doi.org/10.1145/3511808.3557487 (Original work published October, 2022)
- Chen, Y., Huang, S., Gan, W., Huang, G., Wu, Y. (2023, March 23). Federated Learning for Metaverse: A Survey. https://arxiv.org/pdf/2303.17987.pdf
- Qayyum, A., Butt, M. A., Ali, H., Usman, M., Halabi, O., Al-Fuqaha, A., Abbasi, Q. H., Imran, M. A., Qadir, J. (2023). Secure and Trustworthy Artificial Intelligence-Extended Reality (AI-XR) for Metaverses. ACM Computing Surveys, Article 3614426. Advance online publication. https://doi.org/10.1145/3614426
- Yang, T., Andrew, G., Eichner, H., Sun, H., Li, W., Kong, N., Ramage, D., Beaufays, F. (2018, December 7). Applied Federated Learning: Improving Google Keyboard Query Suggestions. https://arxiv.org/pdf/1812.02903.pdf