Optimizing the realization of fully homomorphic encryption, building a digital twin digital human (avatar), and using fully homomorphic encryption and other technologies to protect the privacy of sensitive data.

Definition of Terms:

Homomorphic encryption =>  is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form. Homomorphic encryption enables complex mathematical operations to be performed on encrypted data without compromising the encryption.

Fully homomorphic encryption => (FHE) is an encryption scheme that enables analytical functions to be run directly on encrypted data while yielding the same encrypted results as if the functions were run on plaintext.

digital twin =>

digital twin digital human (avatar) =>

privacy of sensitive data =>

If the data is not recorded then its safe , but then without the data technology won’t evolve so the only way out is to protect. Technology companies are facing scrutiny over privacy concerns as the public and lawmakers realize that the free services they enjoyed for years come at a cost— access to personal data. Now, many of these same companies are selling virtual reality (VR) devices to consumers. As of 2018, there have beenmillions of systems sold in the United States.1

Title

Abstract

Research Background

Research Questions

Research method

Limitations

Significance

We know this thing, I am going to be building this thing and this is going to help this in future work.

Timeline

This may not go to plan , so this might happen, else this might not happen.

Ref

5-10

Comparison

1. Exploring the Unprecedented Privacy Risks of the Metaverse.
2. A Survey on Metaverse: Fundamentals, Security, and Privacy.
3. Going Incognito in the Metaverse.
4. Big Data Meets Metaverse: A Survey.
5. A review of platforms for simulating embodied agents in 3D virtual environments.
6. Collaborative city digital twin for the COVID-19 pandemic: A federated learning solution,
7. Z. Edge-Fog-Cloud Secure Storage with Deep-Learning-Assisted Digital Twins,"
8. Homomorphic Encryption for Privacy-Friendly Augmented Democracy,
9. Person Independent, Privacy Preserving, and Real Time Assessment of Cognitive Load using Eye Tracking in a Virtual Reality Setup
10. Privacy-Preserving Artificial Intelligence Techniques in Biomedicine.
11. Privacy-preserving deep learning techniques for wearable sensor-based big data applications.
12. Protecting Nonverbal Data Tracked in Virtual Reality.
13. The ethical and privacy implications of mixed reality.

Many privacy-preserving techniques have been developed to protect user data. The most famous remarkable method that has proven to be quite safe is going unnoticed in the metaverse. It's a nice notion, but there's a problem: the metaverse represents a digital twin, a "clone of the user," and individuals naturally don't behave in the same way, necessitating the need for the real user's daily data. The aforementioned technique restricts the information that metaverse enterprises may gather, and it's crucial for the businesses to have access to this information, such as heart rate, eye movements, and facial expression. This aids businesses in improving their metaverse platforms, which, if not improved, can be dangerous to people.

This helps the companies upgrade their metaverse platforms since they can be harmful to humans if not properly upgraded. without leaking any personal information by combining fully homomorphic encryption with differential privacy.