北京科技大学

硕士学位研究生
选题报告及文献总结

论文题目 **Privacy-Preserving Scheme For The Virtual Reality Avatars In Metaverse.**

指导教师： 黄旗明副教授

单　　位：计算机与通信工程学院通信工程系

学　　号： M202161029

作　　者： Alec Mabhiza Chirawu 亚历克上

专业名称： 信息与通信工程

入学时间： 2021 年 9 月

2024 年 07 月 04

Table of Contents

1. ABSTRACT

Metaverse services pose strong security and privacy requirements on client side due to the fact that a lot of user data is collect with and without their concern. Since without client data is almost impossible for metaverse to come to live so the only way is to collect client data and protect it by all means, we propose an efficient and reliable Differential privacy (DP) and Fully Homomorphic encryption (FHE) preserving schemes using cryptographic approach. It can preserve users' privacy data by making their identity be anonymity for data mining companies and metaverse server. For communication, both (DP) publicly sharing information and (FHE) allows analysts to perform computations on encrypted data without having to decrypt it first, are employed to guarantee confidentiality and integrity of request and response data. Besides, we also provide other preserving-privacy scheme which can resist internal attack, external attack and colluding attack.

2. INTRODUCTION

The proliferation of digital data[2] has resulted in a greater demand for data sharing and exchange, as doing so is vital to get crucial and previously unrecognized information. Data was predominantly collected online in recent years for a number of purposes, including marketing and developing better models to enhance systems. Web cookies were used to capture a variety of data that was so vast that new protection regulations were required. However, compared to data gathered via websites, the amount of client data transferred to the cloud has expanded by more than 200 percent as the metaverse has developed. This is true since the metaverse offers pathways and direct usage of sensors that can gather all relevant data about a client, from name to health information. Due to the importance of this client information to the metaverse[1], it necessitates high-tech security measures to guard against unauthorized access. While sharing sensitive information became important to the developers[9].

Virtual reality (VR) is set to continue collecting data, which was always going to happen. Even though virtual reality (VR) technology has been in some form since the dawn of the internet, it has only lately come to light that major corporations are really interested in transforming these technologies into vastly networked social "metaverse" platforms. These platforms' fundamental architecture transforms every user's sight, movement, and speech into a stream of data that is instantaneously broadcast to users

all over the world in order to allow real-time engagement[4],[7]. This study aims to highlight the unrivaled privacy dangers of the metaverse and provide comprehensive security and privacy architecture for VR environments.

However, owing to the fact that a lot of data is collected from the user, from their surroundings to their heartbeat rate, and every movement is recorded, making it a massive data source in the metaverse, safeguarding the privacy and security of metaverse data remain significant challenges[12],[13]. Developers may find additional data valuable, such as the response of the iris in VR when exposed to near light, which is collected through data sharing because user data is regularly posted every time a user visits the metaverse in order to link the private information obtained from users.

3. RELATED WORK

The study of privacy protection has drawn a lot of interest in recent years. The majority of the suggested protocols concentrated data across several servers. Some of the ways are based on secret sharing mechanisms, while many of the others depend on a reliable third party. The work of the author in [3], whose framework introduced two secure linear regression algorithms, serves as a good illustration. These techniques [7],[13] are based on safe multi-party computing and secure data integration. The technique in [7] implying that no party may discover another party's data, which suggests that privacy preservation is the primary objective. The technique in [13] employs the secure summation protocol, which makes it easier for each participant to exchange local statistical data for calculating global regression coefficients.

Numerous recent studies highlight how contemporary machine learning algorithms violate privacy. We will only describe the confidentiality attacks among the three major kinds of ML attacks (namely, confidentiality, integrity, and availability attacks [6]), as privacy-preserving strategies are the focus of our study. These attacks may be divided into two categories: model extraction attacks and data extraction attacks.

Cryptographic tools are frequently included in several cryptography-based procedures in order to preserve and provide privacy for the dataset[7]. Even in the case of two parties, secure multiparty computing is typically not practicable due to the extremely high communication and processing complexity. In principle, secure multiparty computation can be highly helpful to resolve multi-party

privacy-preserving deep learning. [5] take a somewhat different tack in their publication. In order to prevent privacy leaks throughout the data collection process, it used secure scalar and secret sharing. It is significant to note that this strategy has its own drawbacks because it is difficult to adapt to multi-party models and only works in a two-party scenario. The author of [8] proposes a privacy-preserving method based on homomorphic encryption [11] that uses a back-propagation algorithm and is appropriate for multi-party deep learning over arbitrarily partitioned datasets. To decrypt the ciphertext of the intervening parameters in each of the rounds, this system necessitates that all parties be online, unlike the other schemes.

One of the current research methods that poses a lot of threat to metaverse companies is going incognito [3]. The author uses a technique that leverages local " ε-differential privacy" to quantifiably obscure sensitive user data attributes, with a focus on intelligently adding noise when and where it is needed most to maximize privacy while minimizing usability impact. This method has proven to be effective at protecting user data by restricting the types of data that metaverse companies can collect. This method is excellent, but it slows the metaverse's growth in the sense that metaverses rely heavily on real user data, and in order for them to meet all ethical, social, and religious differences, all types of data must be collected and used for training by researchers and metaverse companies in order to extend the metaverse's greatness and quality.

4. METHODOLOGY

In this section, I will discuss the proposed methodology to accomplish the work as follows:

4.3. FULLY HOMOMORPHIC ENCRYPTION(FHE)

This proposal's primary goal is to shield user information from collection and public disclosure. A cryptographic technique (FHE)[8] enables computation on encrypted data. In a traditional client-server architecture, data is safely kept on both the user and server sides. In a traditional client-server architecture, data is safely kept on both the user and server sides. Data is encrypted using a variety of techniques during communication exchanges across an untrusted network[9],[10],[11]. However, the server must decrypt the client's private data and process it in clear text when providing the service to which the client has subscribed. With FHE, the server may continue to provide its services while the data is end-to-end encrypted. Key_generation, encryption, and decryption are the three algorithms that make up a general public key_encryption method. Let pk be a public key produced by key_generation, and let m be a plain message. We refer to the encrypted data as the ciphertext [[m]]pk (m, pk). We will ignore the second option and use [[m]]

as we will only be utilizing one public key for the duration of this endeavor lefting the room for (DP).

4.4. DIFFERENTIAL PRIVACY (DP)

The (DP) ensures that the original data of the user is not disclosed during the data collection process by adding predetermined random noises to the original data and sending the noisy data to a data collector. It is a viable method of ensuring personal privacy during the data collection process but doesn't guarantee data safety from user to developer servers. Using group privacy method allows the control and analysis of privacy loss acquired by groups[14]. This gives large room to protection of one uses collected since it will be be grouped all together in (DP) process on user local computer before being shared to the internet where it will require (FHE).

5. RESEARCH CONTENT & OBJECTIVITY

6.1. RESEARCH OBJECTIVES

- Danger, significant concern, and subject
- To meet the requirement for avatar privacy protection in the metaverse.
- There are new problems in protecting sensitive data.
- Discover a simple method to limit unwanted data access.
- Streamline the transfer of information between metaverse users and meta servers.
- Investigate metaverse data privacy-preserving schemes.

6.2. WORKING PROPOSAL

Based on the above problems and the current research progress, the main research contents and the exact solution that this research is aimed to address is as follows.:

I. Combining a fully homomorphic encryption scheme with a differential privacy scheme to form a new scheme that is capable of protecting user data starting from the collection process to the developer's servers.

II. Cryptovoxels is the development platform that we are going to use.

6.4. LIMITATIONS

We will probably encounter several blocks while conducting our research. Combining (DP) and (FHE) may appear simple, but there are several restrictions that make it difficult to combine the two schemes into a single efficient scheme. We must disregard certain approaches and concentrate solely on those that are relevant in order to address this issue. It will be challenging if pre-paid data is necessary for the success of this research because all of the data utilized in it comes from open-source sites. We have previously examined every piece of equipment needed for this issue, and as of today, every necessity is within reach.

- Naturally, there are two main issues with the system:
- It is computationally highly costly (DP).

Naturally, (FHE) is extremely slow since it makes use of big keys to achieve the required level of security. This has been accepted as a trade-off for the successful completion of this research.

6.4. RESEARCH SIGNIFICANCE

Data protection from unscrupulous partners and data miners is becoming an increasingly urgent problem. The most delicate data that has to be preserved is that which has been gathered as a result of the so-called metaverse. No matter whether the information is supplied voluntarily or not, it is necessary for the metaverse technology to operate properly, since without it, it would be a waste. Users' equipment will be less effective if metaverse corporations are prevented from collecting user data; hence, the only way to be secure is to take every precaution to maintain optimum data protection. Finding fresh approaches to protecting privacy in the metaverse was the goal of this study. Researchers and metaverse businesses will be able to access a wide variety of data for their jobs more readily and without breaking any privacy laws in this way. Users won't be reluctant to offer sensitive information if an appropriate privacy-preserving strategy is used since they won't have to worry about their personal information being compromised. The public also gains from this since it provides an excessive amount of assurance.

The problem mentioned in the preceding section can be mitigated by a number of publicly available, but more has to be done. We know how (DP)’s Group Privacy works, and we also know how (FHE) works. Therefore, it is necessary to create a different strategy that can withstand

privacy breaches from both malevolent attackers and computational nodes at the same time, and combining (DP) and (FHE) to form a new privacy-preserving scheme might be the best solution for both data users(collection) and metaverse companies.

6. REFERENCES

1. Nair, Vivek & Garrido, Gonzalo & Song, Dawn. (2022). Exploring the Unprecedented Privacy Risks of the Metaverse. 10.48550/arXiv.2207.13176.
2. wang, yuntao; Su, Zhou; Zhang, Ning; xing, rui; Liu, Dongxiao; Luan, Tom H.; et al. (2022): A Survey on Metaverse: Fundamentals, Security, and Privacy. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.19255058.v3
3. Nair, Vivek, et al. Going Incognito in the Metaverse. doi.org/10.48550/arXiv.2208.05604.
4. Sun, J., Gan, W., Chen, Z., Li, J., & Yu, P.S. (2022). Big Data Meets Metaverse: A Survey. *ArXiv, abs/2210.16282*.
5. Kaur, Deepti & Singh, Narinder & Banerjee, Bonny. (2022). A review of platforms for simulating embodied agents in 3D virtual environments. Artificial Intelligence Review. 10.1007/s10462-022-10253-x.
6. J. Pang, Y. Huang, Z. Xie, J. Li and Z. Cai, "Collaborative city digital twin for the COVID-19 pandemic: A federated learning solution," in Tsinghua Science and Technology, vol. 26, no. 5, pp. 759-771, Oct. 2021, doi: 10.26599/TST.2021.9010026.

7. Z. Lv and R. Lou, "Edge-Fog-Cloud Secure Storage with Deep-Learning-Assisted Digital Twins," in IEEE Internet of Things Magazine, vol. 5, no. 2, pp. 36-40, June 2022, doi: 10.1109/IOTM.002.2100145.
8. M. Brabant, O. Pereira and P. Méaux, "Homomorphic Encryption for Privacy-Friendly Augmented Democracy," 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON), 2022, pp. 18-23, doi: 10.1109/MELECON53508.2022.9843009.
9. E. Bozkir, D. Geisler and E. Kasneci, "Person Independent, Privacy Preserving, and Real Time Assessment of Cognitive Load using Eye Tracking in a Virtual Reality Setup," 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), 2019, pp. 1834-1837, doi: 10.1109/VR.2019.8797758.
10. Torkzadehmahani R, Nasirigerdeh R, Blumenthal DB, Kacprowski T, List M, Matschinske J, Spaeth J, Wenke NK, Baumbach J. Privacy-Preserving Artificial Intelligence Techniques in Biomedicine. Methods Inf Med. 2022 Jun;61(S 01):e12-e27. doi: 10.1055/s-0041-1740630. Epub 2022 Jan 21. PMID: 35062032; PMCID: PMC9246509.
11. Hamza, Rafik & Dao, Minh. (2022). Privacy-preserving deep learning techniques for wearable sensor-based big data applications. Virtual Reality & Intelligent Hardware. 10.3724/SP.J.2096-5796.21.00047.
12. Bailenson J. Protecting Nonverbal Data Tracked in Virtual Reality. JAMA Pediatr. 2018 Oct 1;172(10):905-906. doi: 10.1001/jamapediatrics.2018.1909. PMID: 30083770.
13. Bye, Kent & Hosfelt, Diane & Chase, Sam & Miesnieks, Matt & Beck, Taylor. (2019). The ethical and privacy implications of mixed reality. 1-2. 10.1145/3306212.3328138.
14. X. Yao, R. Zhang and Y. Zhang, "Differential Privacy-Preserving User Linkage across Online Social Networks," 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS), 2021, pp. 1-10, doi: 10.1109/IWQOS52092.2021.9521333.