Space Authentication in the Metaverse: A Blockchain-Based User-Centric Approach

Mr. Prasanna Kumar M J
Assistant Professor
Computer Science and Engineering
BGS Institute of Technology
Adichunchanagiri University

Monisha H P
20CSE050
Computer Science and Engineering
BGS Institute of Technology
Adichunchanagiri University

Abstract:
As the metaverse continues to gain traction, the importance of research into metaverse security becomes increasingly evident. While there has been notable research on authenticating users within the metaverse, there remains a gap in the authentication of specific spaces within this virtual environment. This paper aims to address this gap by introducing a novel user-centric blockchain-based authentication method that incorporates space authentication. The proposed approach utilizes blockchain smart contracts to authenticate users through cosine similarity metrics. This method offers significant advantages by seamlessly integrating metaverse and blockchain technologies, all without the need for a centralized authority. One notable feature of this approach is its ability to establish user-centric authentication, ensuring security while users navigate different spaces within the metaverse.

Keywords - Blockchain, metaverse, authentication based on blockchain, user authentication, Security

1. INTRODUCTION

The metaverse constitutes a virtual space where individuals interact and conduct various activities using avatars representing their real-life identities. It's characterized by its multidimensional spatial layout and its fusion of digital spaces interconnected through the internet. Often described as an infinite digital realm, it enables diverse experiences for users without constraints like geographical barriers, space, or time. For instance, technologies like medical twins replicate real-world environments to forecast surgical outcomes, while Mesh creates virtual offices for meetings. As interest in the metaverse grows, research has extensively explored its constituent technologies and applications. Authentication of metaverse users has been a focal point, with studies proposing methods like decentralized identifiers and biometric authentication. However, many overlook the spatial aspects of the metaverse, which offer unique authentication opportunities across various interactions. Existing research primarily focuses on authenticating users transitioning into the metaverse environment, overlooking spatial complexities. For instance, in healthcare or office scenarios within the metaverse, there's a need to segregate spaces based on roles or permissions. While traditional methods like rank assignment or password protection are used, they have vulnerabilities like tampering with ranks or password exposure. Recent research explores novel approaches like user role-based or policy-based space authentication, yet they often centralize role assignment or policy establishment. This paper introduces a user-centric authentication technique leveraging blockchain, addressing limitations in existing methods. It prioritizes user security and autonomy, allowing them to manage their authentication data securely.

In this approach, users autonomously generate authentication tokens using blockchain, authenticated through smart contracts for space access. Users manage their credentials, reducing external theft risks, while service providers retain flexibility through smart contracts.

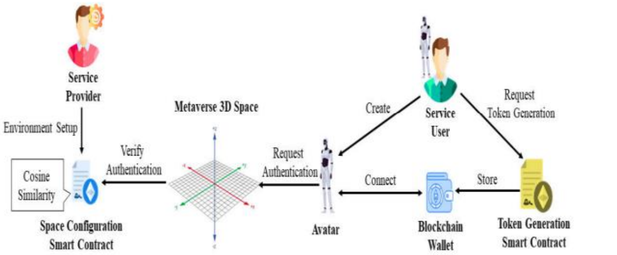
II. RELATED WORK

In the realm of authentication methods for accessing spaces in the metaverse, existing research can be broadly classified into two main categories: user role-based space authentication and policy-based space authentication.

Zhu et al. conducted a study utilizing computer vision algorithms to create a 3D model of physical space, with the aim of enhancing space authentication. Their approach involved mapping 3D space coordinates to the physical real-world space for user location identification. Additionally, user authorization for specific locations was determined by central entities, with access granted based on pre-defined roles.

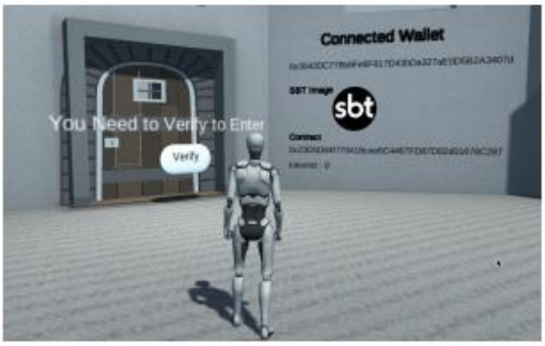
Wright and Madey emphasized the importance of restricting access to spaces and objects, proposing a method that allowed movement within specific spaces and interaction with objects through discretionary access control. Users were categorized into group roles or individual user roles, dictating their access to specific spaces. Wei et al. introduced a study focusing on assigning identity-based capabilities to users, enabling or restricting their access to specific spaces based on these capabilities. This approach utilized identification-based access control technology for access control and user authentication. Sun et al. addressed the lack of appropriate access control authentication mechanisms in 3D virtual environments by proposing a method for authenticating spaces using role-based access control technology. Users could authenticate themselves for accessing objects, assets, and avatars within the space based on their roles. Despite the effectiveness of these approaches in assigning roles to users for authentication when accessing particular spaces, a common limitation is the centralization of role assignment, which may lead to vulnerabilities such as a single point of failure and potential theft of user-assigned roles and information by malicious actors. Lehaman and Tan introduced a study suggesting authenticating users by enforcing specific rules within a given space, utilizing GPS data from their cell phones to determine the user's physical location within the real-world environment. User authentication relied on predefined policies associated with that space. Tsankov et al. proposed a study that divided the physical environment into distinct spaces and established global requirements for each of these spaces. User authentication was carried out based on the policies assigned to each individual space. Adrian Bullock, Steve Benford, and their colleagues explored user authentication through the creation of an access graph defined by space boundaries. This research involved assigning policies to various spaces, determining which users could access each space. The common theme among these studies is the application of policies to spaces for user authentication, seeking to categorize spaces and establish fine-grained policies for each space. However, like those that assign roles to users, they face limitations such as centralization and potential vulnerabilities.

III. The System's Architecture

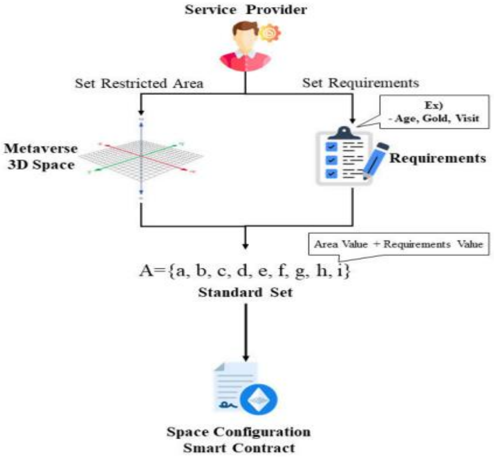


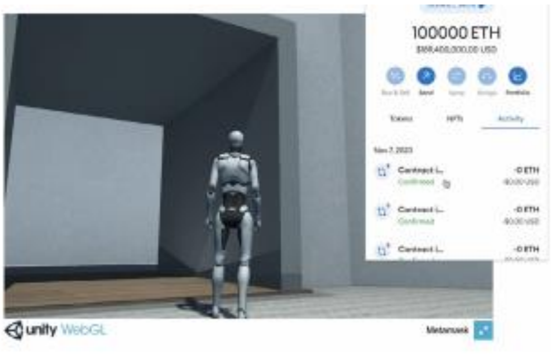
proposes a novel system architecture for space authentication in the metaverse, focusing on user-centricity and leveraging blockchain technology. Traditional authentication methods often overlook the intricate spatial aspects of the metaverse, leading to vulnerabilities and limitations. Our approach addresses these challenges by introducing a decentralized and user-centric authentication system, ensuring secure access to specific spaces within the metaverse environment. By harnessing the immutability and transparency of blockchain technology, users maintain control over their authentication credentials, mitigating risks associated with centralized authorities. This paper outlines the architecture, mechanisms, and benefits of our proposed approach, emphasizing its feasibility and effectiveness through experimental validation.

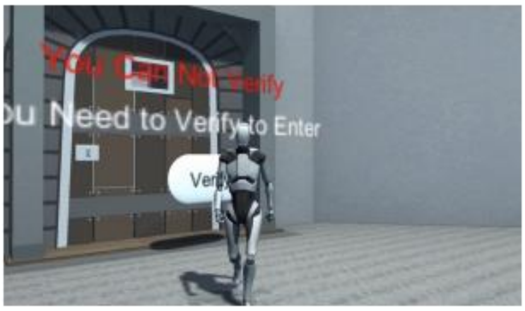
IV. IMPLEMENTATION



(a) Authentication Request







(c) Authentication Failure

V. EXPERIMENTS

This experiment aims to validate the effectiveness and feasibility of a blockchain-based user-centric approach for space authentication in the metaverse environment. The proposed approach leverages blockchain technology to ensure secure access to specific spaces within the metaverse while prioritizing user autonomy and security. The experiment involves simulating user interactions within a virtual environment, generating authentication tokens using blockchain, and validating space authentication based on user attributes. Through rigorous experimentation and analysis, the experiment aims to demonstrate the practical applicability and advantages of the proposed approach in enhancing authentication mechanisms within the metaverse..

VI. CONCLUSIONS

In this paper, we proposed a user-centric authentication scheme leveraging blockchain technology to secure access to specific spaces within a metaverse environment. Our approach comprises three main components: a methodology for metaverse and smart contract design by service providers, an authentication token generation method for service users, and a space authentication method relying on authentication tokens. We demonstrated the effectiveness of our approach in utilizing user attributes for authentication, employing cosine similarity to measure attribute similarity.

A notable strength of our work is the introduction of user-centric authentication, achieved through the seamless integration of metaverse and blockchain technologies without relying on a centralized authority. This approach enhances security and autonomy for users navigating the metaverse environment.

In future research, we intend to explore extending our approach to apply access control techniques to individual objects within the metaverse. Additionally, we aim to optimize network communication costs between blockchain and metaverse systems during the authentication process, further enhancing efficiency and scalability.

REFERENCES

[1] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, ‘‘Fusing blockchain and AI with metaverse: A survey,’’ IEEE Open J. Comput. Soc., vol. 3, pp. 122–136, 2022.
[2] L. Young, ‘‘A study on metaverse hype for sustainable growth,’’ Int. J. Adv. Smart Converg., vol. 10, no. 3, pp. 72–80, 2021.
[3] R. Cheng, N. Wu, S. Chen, and B. Han, ‘‘Will metaverse be NextG Internet? Vision, hype, and reality,’’ IEEE Netw., vol. 36, no. 5, pp. 197–204, Sep. 2022.
[4] M. Wright, H. Ekeus, R. Coyne, J. Stewart, P. Travlou, and R. Williams, ‘‘Augmented duality: Overlapping a metaverse with the real world,’’ in Proc. Int. Conf. Adv. Comput. Entertainment Technol. ACM, Dec. 2008, pp. 263–266.
[5] T. Erol, A. F. Mendi, and D. Dogan, ‘‘The digital twin revolution in healthcare,’’ in Proc. 4th Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT), Oct. 2020, pp. 1–7.
[6] (2023). Microsoft Mesh, Virtual Office. Accessed: Dec. 20, 2023. [Online].
[7] M. A. I. Mozumder, M. M. Sheeraz, A. Athar, S. Aich, and H.-C. Kim, ‘‘Overview: Technology roadmap of the future trend of metaverse based on IoT, blockchain, AI technique, and medical domain metaverse activity,’’ in Proc. 24th Int. Conf. Adv. Commun. Technol. (ICACT), 2022, pp. 256–261.
[8] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, ‘‘A survey on the metaverse: The state-of-theart, technologies, applications, and challenges,’’ IEEE Internet Things J., vol. 10, no. 6, pp. 14671–14688, May 2023.
[9] S. Bhattacharya, S. Varshney, and S. Tripathi, ‘‘Harnessing public health with ‘metaverse’ technology,’’ Frontiers Public Health, vol. 10, p. 4452, Dec. 2022. 18712 VOLUME 12, 2024 J. Seo et al.: Space Authentication in the Metaverse: A Blockchain-Based User-Centric Approach
[10] S. E. Bibri and S. K. Jagatheesaperumal, ‘‘Harnessing the potential of the metaverse and artificial intelligence for the Internet of City Things: Cost-effective XReality and synergistic AIoT technologies,’’ Smart Cities, vol. 6, no. 5, pp. 2397–2429, Sep. 2023.
[11] 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.
[12] K. Yang, Z. Zhang, T. Youliang, and J. Ma, ‘‘A secure authentication framework to guarantee the traceability of avatars in metaverse,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 3817–3832, 2023.
[13] 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,’’ Comput. Commun., vol. 211, pp. 271–285, Nov. 2023.