International Journal of Cloud Applications and Computing
Volume 14 • Issue 1

Mitigating Risks in the Cloud-Based Metaverse Access Control Strategies and Techniques

Utsav Upadhyay, Sir Padampat Singhania University, India

Alok Kumar, Sir Padampat Singhania University, India

Gajanand Sharma, JECRC University, Sitapura, India

Ashok Kumar Saini, Manipal University Jaipur, India

Varsha Arya, Department of Business Administration, Asia University, Taiwan, & Department of Electrical and Computer Engineering, Lebanese American University, Beirut, Lebanon, & Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun, India, & Chandigarh University, Chandigarh, India

Akshat Gaurav, Ronin Institute, USA*

Kwok Tai Chui, Hong Kong Metropolitan University, Hong Kong

ABSTRACT

The advent of the metaverse has revolutionized virtual interactions and navigation, introducing intricate access control challenges. This paper addresses the need for effective access control models in the cloud-based metaverse. It explores its distinct characteristics, including its dynamic nature, diverse user base, and shared spaces, highlighting privacy concerns and legal implications. The paper analyzes access control principles specific to the cloud-based metaverse, emphasizing least privilege, separation of duties, RBAC, defense-in-depth, and auditability/accountability. It delves into identity verification and authorization methods, such as biometrics, multi-factor authentication, and role-based/attribute-based authorization. Advanced access control technologies for the cloud-based metaverse are examined, including SSO solutions, blockchain-based access control, ABAC, adaptive access control, and VMI for isolation. Risk mitigation strategies encompass IDS/IPS, SIEM, and user education programs.

KEYWORDS

Access Control, Authorization, Blockchain, Cloud, Metaverse, Verification

INTRODUCTION

The Metaverse signifies the fusion of virtual and physical realities, manifesting as a seamless digital realm enabling user engagement with virtual environments and interaction through avatars or digital representations (Barrera & Shah, 2023). This encompassing concept encompasses diverse platforms,

DOI: 10.4018/IJCAC.334364 *Corresponding Author

applications, and technologies, such as virtual reality (VR), augmented reality (AR), mixed reality (MR), and 3D virtual worlds (Lungu et al., 2021). As the Metaverse gains traction, addressing access control challenges becomes pivotal within this virtual ecosystem. Access control encompasses mechanisms and policies governing user entry, permissions, and actions within a given system or environment (Hu et al., 2006; Singh et al., 2022). Access control ensures user interactions and data security, privacy, and integrity in the Metaverse context. The emergence of the Metaverse ushers in a novel era of virtual reality, enabling individuals to immerse themselves in expansive digital landscapes, real-time interaction with others, and a diverse range of activities spanning from gaming to socializing to conducting business (Uddin et al., 2023; Hu, B et al. 2022). As this virtual realm ascends, it presents distinctive challenges concerning access control, thereby necessitating a comprehensive exploration of access control models and techniques specifically tailored for the Metaverse (Xu et al., 2022). Figure 1 delineates the evolution of virtual environments leading up to the Metaverse.

This study aims to scrutinize access control models and techniques specifically tailored for the Cloud-based Metaverse, an immersive virtual reality environment. The investigation encompasses an in-depth exploration of the distinctive characteristics inherent to the Metaverse, encompassing its dynamic nature, diverse user population, shared spaces, and the consequential implications on access control. Additionally, the study delves into the fundamental principles and criteria governing effective access control within the Cloud-based Metaverse. These principles include well-established tenets such as least privilege, separation of duties, role-based access control (RBAC), defense-in-depth, and auditability/accountability. Moreover, the study emphasizes the pivotal aspects of integrity, confidentiality, and availability as vital access control components within the intricate Metaverse realm.

This research investigates the deployment of identity verification and authorization methods within the Cloud-based Metaverse to ensure robust user access. It delves into diverse techniques like biometrics, MFA, and RBAC/ABAC, examining their applicability and effectiveness in the Metaverse context. Furthermore, the study explores access control technologies and models tailored for the Cloud-based Metaverse, such as SSO systems, blockchain-based AC, ABAC, adaptive AC, and VMI for isolation. These solutions' advantages, limitations, and suitability for addressing unique challenges in the Metaverse are analysed. Moreover, the research explores potential threats and risks associated with Cloud-based Metaverse access control, including DoS attacks, malware, exploits, and social engineering. Effective mitigation strategies encompass IDS/IPS, SIEM, and user education programs to counter these threats adequately.

The core objective of this study is to deliver a comprehensive understanding of access control challenges specific to the Cloud-based Metaverse and to explore suitable models and techniques to tackle those challenges. The specific aims encompass:

- Examining the access control principles and criteria applicable to the Cloud-based Metaverse environment and investigating identity verification and authorization methods tailored for secure user access.

Figure 1. Timeline illustrating the progression of virtual environments, from virtual reality (VR) to augmented reality (AR), mixed reality (MR), extended reality (XR), and ultimately culminating in the metaverse