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.

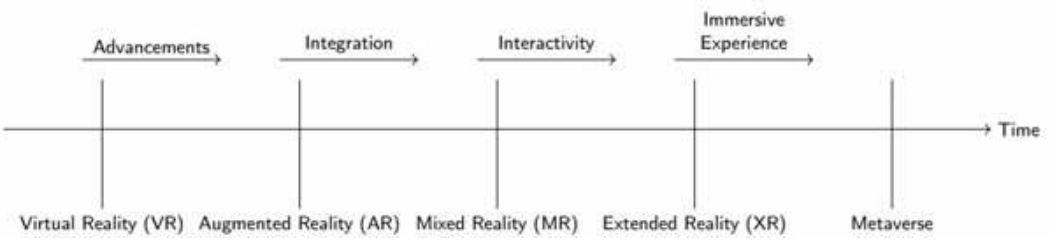
This study aims to scrutinize access control models and techniques specifically tailored for the Cloud-based Metaverse, an immersive virtual reality environment. The investigation encompasses an in-depth exploration of the distinctive characteristics inherent to the Metaverse, encompassing its dynamic 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



- Exploring access control technologies and models designed for the Cloud-based Metaverse.
- Identifying and assessing the potential threats and risks associated with access control and providing effective mitigation strategies and countermeasures to address access control threats in the Cloud-based Metaverse.

This study bears significant implications for diverse stakeholders in the Metaverse ecosystem. Developers and designers of virtual environments stand to gain profound insights into access control challenges, principles, and technologies, enabling the creation of secure and user-friendly experiences (Bu et al., 2021; Singh, G. et al., 2022). Policymakers and regulators can capitalize on these findings to formulate suitable guidelines and regulations, ensuring the privacy and security of Metaverse users (Wang et al., 2022). Users themselves can acquire valuable knowledge regarding potential risks and best practices for safeguarding personal information and exerting control over digital identities (Krasnova et al., 2009; Gupta S.P. et al., 2022). This research contributes to the broader realms of cybersecurity and privacy in virtual environments by illuminating the intricate nature of access control in the Metaverse. It provides indispensable perspectives for researchers, practitioners, and industry professionals keen on developing robust access control measures within the Metaverse, thereby fostering the growth of a secure and trustworthy virtual ecosystem.

The remainder of this manuscript is organized as follows: Section 2 examines the unique characteristics of the Metaverse that pose challenges for access control, including the dynamic nature of virtual environments, user diversity, privacy concerns, and regulatory compliance. Section 3 discusses the access control principles and criteria specific to the Cloud-based Metaverse, encompassing principles like least privilege, separation of duties, RBAC, defense-in-depth, and auditability/accountability. The criteria of integrity, confidentiality, and availability are also explored. Section 4 focuses on identity verification and authorization methods for secure user access in the Cloud-based Metaverse, including biometrics, multi-factor authentication, and role-based/attribute-based authorization. Section 5 analyzes various access control technologies and models for the Cloud-based Metaverse, such as SSO solutions, blockchain-based access control, ABAC, adaptive access control, and VMI for isolation. Section 6 investigates potential threats to access control in the Metaverse, including DoS attacks, malware and exploits, and social engineering techniques. Mitigation strategies such as IDS/IPS, SIEM, and user education and awareness programs are explored. Section 7 summarizes the findings, contributions of the research, limitations, and future research directions, concluding with final remarks. By delving into each section, this manuscript aims to provide a comprehensive understanding of access control models and techniques tailored for the Metaverse, ultimately facilitating the creation of secure and trustworthy virtual environments.

ACCESS CONTROL CHALLENGES IN THE CLOUD-BASED METAVERSE

The Metaverse introduces many unique characteristics and intricacies, which in turn give rise to significant challenges in access control. This section delves deep into these challenges, thoroughly examining the dynamic nature of virtual environments, the diverse user population, privacy concerns that emerge within a shared space, and the critical need for addressing regulatory compliance and legal implications. To comprehensively understand the disparities, Table 1 compares access control challenges encountered in traditional digital environments and those specific to the Metaverse. This comparative analysis underscores the distinctions, encompassing user diversity and scalability, the ever-changing nature of virtual environments, privacy concerns within a shared space, and the intricate landscape of regulatory compliance and legal implications that demand attention. By navigating through these complexities, we aim to shed light on the nuances of access control in the Metaverse, enabling the establishment of robust and adaptive security measures.

Unique Characteristics of the Metaverse

The Metaverse presents many access control challenges as a vast, interconnected virtual space comprising diverse platforms, applications, and user-generated content (Weinberger, 2022) (Tang et al., 2022; Barthwal, V, 2022). This intricate landscape, which integrates physical and digital realms, real-time interactions, and immersive experiences, demands careful consideration of access control mechanisms (Duan et al., 2022; Kumar et al., 2022). One such challenge involves balancing open collaboration, creativity, and the imperative to uphold security and privacy. The Metaverse fosters an environment where users are encouraged to generate and share their virtual experiences (Duan et al., 2022; Priyanka et al, 2021). However, this openness inherently risks unauthorized access, malicious activities, and intellectual property theft.

Consequently, access control measures must navigate the fine line between nurturing creativity and safeguarding sensitive information. Another crucial challenge involves ensuring interoperability and compatibility among diverse platforms and applications within the Metaverse (Lin & Latoschik, 2022; Bisht V. S et al., 2022; Ali, R., 2022). Given the diverse virtual environments users may traverse, each equipped with distinct access control mechanisms and authentication processes, harmonizing these mechanisms and enabling seamless access across platforms without compromising security is an intricate undertaking.

Dynamic Nature of Virtual Environments

Virtual environments within the Metaverse exhibit dynamic and ever-evolving characteristics, constantly changing (Davis et al., 2009; Noueihed, H., et al, 2022). These dynamic aspects pose significant challenges in effectively managing access control. Adding new resources, functionalities, and users and potential modifications or removals of existing elements further complicates the access control landscape. One primary challenge lies in the prompt provisioning and revocation of access rights. As virtual environments continue to evolve, user roles may undergo alterations, and access requirements may fluctuate. To address this, access control mechanisms must be flexible to swiftly accommodate such changes (Dionisio, III, and Gilbert, 2013; 4. Wahab, O. A. et al. 2017). Any delays in granting or revoking access can result in unauthorized access or hinder users' ability to fulfill their tasks efficiently. Hence, the dynamic nature of the Metaverse demands continuous monitoring and adjustment of access control policies. Regular assessments and updates are imperative to ensure

Table 1. Comparison of traditional digital environments and the metaverse in terms of access control challenges

Access Control Challenges	Traditional Digital Environments	The Metaverse
User Diversity and Scalability	Access control policies and mechanisms are primarily designed for a specific organization or system, accommodating a limited number of users.	The Metaverse encompasses a vast and diverse user population, requiring scalable access control solutions to manage permissions and privileges for millions of users across different virtual environments.
Dynamic Nature of Virtual Environments	Digital environments are relatively static, with predefined access control rules that do not change frequently.	The Metaverse is dynamic, with virtual environments constantly evolving, requiring adaptive access control mechanisms to handle the dynamic allocation of resources and changing permissions based on user activities.
Privacy Concerns in a Shared Space	Privacy concerns primarily revolve around personal data protection within a specific digital environment.	The Metaverse is a shared virtual space where users interact and exchange data, posing challenges in ensuring privacy, data segregation, and preventing unauthorized access to personal information across interconnected virtual worlds.
Regulatory Compliance and Legal Implications	Traditional digital environments must often comply with specific industry regulations or legal requirements within a limited jurisdiction.	The Metaverse operates globally, necessitating compliance with multiple jurisdictions and diverse regulatory frameworks, leading to complex challenges in access control enforcement, data privacy, and cross-border data transfers.

access permissions align with evolving security requirements and user roles (Pearlman et al., 2021; Possik, J et al., 2022). Organizations must prioritize the adaptability of access control mechanisms to effectively cater to the dynamic nature of virtual environments, thereby upholding both security and operational efficiency.

User Diversity and Scalability

The Metaverse embraces a vast user populace characterized by various roles, diverse backgrounds, and varying access requirements (Roesner et al., 2012; Deveci, M et al., 2022). In this subsection, we delve into the intricacies presented by user diversity and the imperative for scalable access control mechanisms. Users assume multifarious roles within the Metaverse, such as casual participants, content creators, or administrators, each necessitating distinct access privileges. Effectively managing access control for this diverse user base poses challenges in determining appropriate access levels across different user categories while ensuring alignment with their intended activities within the virtual environment. The task of access control in the Metaverse is further compounded by the need for scalability (Campbell et al., 2002). As the user population rapidly expands, access control mechanisms must adeptly accommodate the growing number of users and their diverse access needs without compromising security or performance. Traditional access control models may encounter hurdles in efficiently handling the assignment and revocation of privileges within such a dynamic and rapidly evolving environment.

Consequently, scalable access control solutions that can seamlessly adapt to evolving access requirements while accommodating the burgeoning user base become indispensable. Central to this challenge is managing user identities and authentication within the Metaverse (Windley, 2005; Gokasar, I., et al., 2023). Users may possess multiple digital identities or personas within the virtual realm, necessitating precise verification and authentication procedures to enforce appropriate access control. Striking the delicate balance between robust identity verification, user convenience, and privacy emerges as critical in establishing an effective access control framework within the Metaverse.

Privacy Concerns in a Shared Space

Privacy is a paramount concern within the Metaverse, owing to its interconnected and communal nature (Chiu et al., 2006). Users engage in social interactions, share personal information, and participate in virtual communities, necessitating robust access control mechanisms to address privacy concerns (Qamar et al., 2023). The protection of users' data poses a significant challenge. Access control mechanisms must guarantee that personal information shared within the Metaverse remains accessible solely to authorized individuals or entities (Qamar et al., 2023; Singla, A. et al., 2022). It necessitates the implementation of robust authentication protocols, data encryption techniques, and privacy-preserving measures to safeguard sensitive user data against unauthorized access or disclosure.

Furthermore, managing privacy preferences and consent presents another challenge. In the Metaverse, users exhibit diverse privacy preferences regarding the visibility of their activities, interactions, or personal information (Strater & Lipford, 2008; Upadhyay, U. et al., 2023). Access control mechanisms should provide fine-grained controls over privacy settings, enabling users to define their desired levels of privacy and grant consent for collecting and utilizing their data. Additionally, organizations operating within the Metaverse must adhere to pertinent privacy regulations and legal frameworks within their jurisdictions. Hence, access control mechanisms should incorporate privacy-by-design principles, ensuring the integration of privacy requirements into the system architecture and access control processes from the outset.

Regulatory Compliance and Legal Implications

The evolution of the Metaverse introduces a range of regulatory and legal considerations regarding access control (Mecozzi et al., 2022). In this subsection, we delve into the challenges associated with regulatory compliance and the legal landscape within the Metaverse. Adhering to data protection

regulations, such as the GDPR and other jurisdictional requirements (Kalyvaki, 2023; Stergiou, C. L. et al. 2020), becomes crucial as user data collection and processing occur in the Metaverse. Access control mechanisms must ensure compliance with privacy and security standards, incorporating user consent, data transparency, and user rights management (Lorch et al., 2003). Transparently informing users about data collection, usage, and sharing within the Metaverse while empowering them to control their personal information is essential. Legal implications arise in situations involving unauthorized access, data breaches, or malicious activities within the Metaverse (Shackelford et al., 2015). Establishing liability and accountability frameworks becomes challenging, necessitating clear policies and legal structures to address such incidents. Auditability and accountability mechanisms within access control enable tracking and attribution of actions, mitigating legal risks and fostering user trust (Gadekallu et al., 2022; Chopra, M. et al., 2022). Researchers, developers, and policymakers can lay the groundwork for robust and effective access control models and techniques by addressing these Metaverse-specific access control challenges. It, in turn, establishes a secure, privacy-respecting, and legally compliant virtual environment that empowers users to explore and engage with confidence.

ACCESS CONTROL PRINCIPLES AND CRITERIA IN THE CLOUD-BASED METAVERSE

Access control ensures secure interactions within the Cloud-based Metaverse, necessitating a strong foundation built upon established principles and criteria (Ning et al., 2023). This section explores the fundamental principles that steer access control within virtual environments. Additionally, we delve into the specific criteria contributing to the effectiveness of access control mechanisms specifically tailored for the Cloud-based Metaverse. Figure 2 depicts the interrelationships and describes the Access Control Principles to provide visual clarity. The intricate nature of access control in the Cloud-based Metaverse demands a comprehensive understanding of these principles and criteria to establish a robust and reliable security framework.

Principle of Least Privilege

The principle of least privilege (PoLP) (Steiner et al., 2018) is a fundamental tenet in access control within the Metaverse. Its essence lies in granting users only the minimal privileges required to fulfill

Figure 2. Understanding the relationship between access control principles

their authorized tasks. By adhering to this principle, the risk of unauthorized access is mitigated, and the potential impact of malicious activities is curtailed. Achieving the least privilege necessitates a comprehensive analysis of access rights and formulating access control policies aligned with user roles, responsibilities, and tasks (Ferraiolo et al., 1999). This approach effectively thwarts privilege escalation, limits the attack surface, and constrains unauthorized actions by both users and malicious entities. The adoption of the least privilege principle enhances the security and integrity of access control mechanisms in the dynamic realm of the Metaverse.

Implementing fine-grained access control frameworks is crucial to ensure robust access control in the Metaverse (Damiani et al., 2002). These frameworks guarantee that users are granted access only to the specific resources and functionalities essential for their designated tasks. Upholding the principle of least privilege necessitates regular reviews and audits of access permissions, aligning them with evolving user roles and responsibilities. However, in the dynamic realm of the Cloud-based Metaverse, organizations should consider embracing dynamic least-privilege approaches. These approaches enable the adjustment of access permissions based on contextual information, such as the user's ongoing activity, location, or device integrity. By dynamically tailoring privileges, users are equipped with the necessary access rights in real time while minimizing the potential exploitation of unnecessary privileges. This adaptive mechanism enhances security in the Metaverse while promoting efficient resource allocation and mitigating potential risks.

Principle of Separation of Duties

The principle of separation of duties (Joshi et al., 2001) underscores the distribution of crucial tasks and responsibilities among multiple individuals to prevent fraudulent activities or unauthorized actions. By fragmenting sensitive operations into distinct steps and assigning them to different users, organizations establish a system of checks and balances within the Metaverse. Implementing this principle necessitates a comprehensive understanding of the requisite tasks, associated risks (Fenton & Wolfe, 2019), and potential impact. By identifying critical actions and ensuring that no single user possesses independent control over them, organizations can effectively mitigate the risks of malicious activities or inadvertent errors that may compromise the security and integrity of virtual environments. For instance, in the context of the Metaverse, granting administrative privileges or modifying access control policies might require the involvement of multiple authorized individuals, each responsible for a specific step in the process. This approach significantly diminishes the likelihood of unauthorized modifications or misuse of privileges.

Applying the separation of duties principle extends to user roles and responsibilities in the Metaverse (Baracaldo & Joshi, 2013). Organizations establish a system of checks and balances by assigning distinct roles to users and ensuring that no single user possesses all the privileges necessary to engage in malicious activities. However, achieving an effective implementation of this principle requires striking a balance between efficiency and productivity considerations in the Cloud-based Metaverse. It becomes essential for organizations to thoroughly analyze operational requirements and the potential impact on user experience when distributing tasks among multiple users.

Principle of Role-Based Access Control (RBAC)

The access control model known as Role-Based Access Control (RBAC) has gained widespread adoption due to its ability to organize access permissions according to predefined roles (Sandhu et al. et al., 2000). Within the Metaverse, RBAC offers a structured and scalable approach to access control management by assigning permissions to user roles rather than individual users. In this context, RBAC involves the establishment of user roles based on job functions, responsibilities, or other relevant criteria. Access control policies are then employed to associate specific permissions with each role, enabling users to inherit the appropriate access rights associated with their assigned roles (Shen & Dewan, 1992). Consequently, this approach simplifies the access management process and reduces administrative overhead.

Organizations can implement RBAC in the Metaverse by defining a hierarchical role structure and mapping user roles to specific resources and functionalities. It allows for efficient and consistent access control management, especially in large-scale virtual environments with numerous users and resources. RBAC can also facilitate compliance with the principle of least privilege by ensuring that users are granted only the necessary permissions for their roles (Kern & Anderl, 2018). By periodically reviewing and updating role assignments, organizations can maintain the principle of least privilege as user responsibilities evolve. RBAC can also be combined with other access control models, such as attribute-based access control, to provide more fine-grained and context-aware access control in the Cloud-based Metaverse. This hybrid approach allows organizations to leverage the strengths of different models to meet specific access control requirements.

Principle of Defense-in-Depth

The defense-in-depth principle underscores the importance of deploying multiple layers of security controls to safeguard the Metaverse against diverse threats and vulnerabilities (Mughal, 2022). It acknowledges that relying solely on a single security measure cannot guarantee absolute protection, necessitating a cohesive blend of complementary security measures for establishing a resilient defense strategy. In the context of access control within the Metaverse, defense-in-depth entails implementing various security controls across different levels to ensure resource confidentiality, integrity, and availability (May, Hammerstein, Mattson, and Rush, 2006). These controls encompass network firewalls, intrusion detection systems, encryption mechanisms, secure authentication protocols, and monitoring and auditing systems. By adopting defense-indepth, the Metaverse can fortify its security posture and mitigate potential risks through a layered and comprehensive approach.

Incorporating a multi-layered framework of access control mechanisms within organizations is instrumental in effectively mitigating risks associated with unauthorized access, data breaches, and prevalent security incidents within the Metaverse (Mughal, 2018). These interconnected layers of defense contribute collectively to the overall security posture, serving as robust barriers against diverse threats. The concept of defense-in-depth entails continuous monitoring and evaluation of security controls, ensuring persistent effectiveness in addressing emerging threats and vulnerabilities encountered within the Metaverse (ÇİFCİ, 2023). It encompasses user education as a vital aspect, fostering a culture of heightened security awareness that fortifies the overall resilience of the virtual environment. Organizations should adopt a risk-based approach when implementing defense-in-depth measures in the Cloud-based Metaverse. This approach involves conducting comprehensive risk assessments, identifying critical assets, and proactively recognizing potential threats. Such an approach enables organizations to prioritize resource allocation and fortify the most vulnerable areas within the virtual environment.

Principle of Auditability and Accountability

The principle of auditability and accountability, as highlighted within the context of the Metaverse, assumes a paramount role in ensuring transparent access control mechanisms and holding users accountable for their actions within the virtual environment (Spears & Barki, 2010). Auditability entails the capacity to track and document access control events, such as login attempts, access requests, and modifications to access permissions (Maesa et al., 2019). By maintaining comprehensive audit logs, organizations can effectively trace the chronology of access activity, identify potential security incidents, and facilitate forensic investigations in the face of breaches or unauthorized activities. Conversely, accountability revolves around establishing unambiguous user identification and authentication mechanisms within the Metaverse (Gajanayake et al., 2011). It guarantees that access control activities can be ascribed to specific individuals, discouraging malicious behaviors, fostering responsible conduct, and enabling compliance with legal and regulatory obligations.

To ensure auditability and accountability within the Cloud-based Metaverse, organizations must implement robust logging mechanisms, monitoring tools, and centralized SIEM systems (Isa et al., 2021). These SIEM systems are crucial in collecting, analyzing, and securely storing access control logs, generating comprehensive reports, and issuing real-time alerts for suspicious activities. Simultaneously, organizations must establish well-defined access control policies that outline acceptable behavior, delineate expected responsibilities, and clearly articulate the consequences of policy violations. By fostering a culture of accountability and prioritizing user awareness and education, organizations can fortify the overall security posture of the Metaverse.

Criteria for Effective Access Control in the Cloud-Based Metaverse

In conjunction with the fundamental principles, many specific criteria enhance the efficacy of access control mechanisms within the Cloud-based Metaverse. These criteria are instrumental in ensuring that access control solutions adequately address the distinctive challenges and requirements posed by the virtual environment (Popović & Hocenski, 2010). Table 2 presents an array of diverse criteria, each playing a crucial role in facilitating effective access control within the Cloud-based Metaverse. The table encompasses a comprehensive description of the significance of each criterion, accompanied by an exploration of the associated challenges and the corresponding mitigation techniques employed to address them. By meticulously examining these criteria, a deeper understanding of access control mechanisms tailored specifically for the Cloud-based Metaverse can be attained, fostering secure and robust virtual environments.

Integrity

Integrity, an essential criterion in Cloud-based Metaverse access control, is pivotal in maintaining the accuracy, consistency, and unaltered data, information, and resources within virtual environments (Ratnasingham, 1998). Unauthorized modifications or tampering with data can have severe consequences, including privacy breaches, dissemination of misinformation, or compromised system functionality. Organizations must implement robust mechanisms to safeguard data integrity that prevent unauthorized modification. These mechanisms involve access controls, data encryption, and integrity checks (Wei et al., 2020). Only authorized individuals can modify data by employing these measures while ensuring that any alterations are appropriately logged and audited. Additionally, establishing data backups and disaster recovery strategies is crucial for mitigating data integrity incidents and addressing system failures in the Metaverse (Shen et al., 2020). Regular backups and verification processes enable data restoration to its original state, thereby minimizing the impact of potential data integrity breaches.

Confidentiality

Confidentiality is a crucial criterion within Cloud-based Metaverse access control, safeguarding sensitive information and restricting its accessibility solely to authorized entities (Zissis & Lekkas, 2012). A breach of confidentiality may result in unauthorized data disclosure, privacy infringements, or intellectual property theft. Upholding confidentiality demands implementing encryption techniques, access controls, and secure communication protocols (Abouelmehdi et al., 2017). Such measures prevent unauthorized data access and safeguard information against interception or eavesdropping. In the Metaverse, fostering a culture of confidentiality necessitates user awareness and education programs (Bertino & Takahashi, 2010). Users should receive education on the significance of protecting sensitive information, comprehend the risks posed by data breaches, and adopt optimal practices for handling confidential data.

Availability

Availability is a critical criterion within access control, guaranteeing the timely accessibility of resources and services in the Cloud-based Metaverse (El Sibai, Gemayel, Bou Abdo, and Demerjian,

2020). Any denial of access or interruptions in service can yield significant consequences, spanning loss of productivity, reputational harm, or financial setbacks. Organizations, therefore, must establish resilient or malicious attacks; high-availability architectures, load balancing, and failover mechanisms can be employed. Furthermore, the Metaverse necessitates proactive monitoring systems alongside robust alerting mechanisms to promptly detect and respond to any availability issues (Khorshed et al., 2012). Regular testing, performance optimization, and capacity planning are also crucial, ensuring that the access control mechanisms can effectively handle the anticipated workload and user demands.

To achieve a secure and dependable virtual environment in the Cloud-based Metaverse, it is imperative to consider and tackle the criteria outlined previously carefully. By doing so, access control mechanisms can effectively safeguard the integrity, confidentiality, and availability of resources and interactions. It, in turn, ensures the protection and preservation of crucial elements within the Cloud-based Metaverse, fostering an environment that users can trust and rely on.

IDENTITY VERIFICATION AND AUTHORIZATION IN THE CLOUD-BASED METAVERSE

The effective identification and authorization of users within the Cloud-based Metaverse play a pivotal role in upholding the virtual environment's security and trustworthiness (Gunduz and Das (2020). This section explores diverse methodologies encompassing identity verification and authorization techniques applicable to the Metaverse. Considering virtual environments' distinctive demands and challenges, a comprehensive analysis of these methods is essential. By addressing the intricacies of user authentication and access control within the Cloud-based Metaverse, this research seeks to facilitate the establishment of a secure and reliable virtual realm.

Identification and Authentication Methods

Identity verification in the Cloud-based Metaverse involves establishing the authenticity of users and ensuring their claimed identities (Lim et al., 2017). This process safeguards against unauthorized access, impersonation, and fraudulent activities within virtual environments. To achieve robust and

Table 2. Criteria for effective access control in the cloud-based metaverse: Integrity, confidentiality, and availability

Criteria	Description	Challenges	Mitigation Techniques
Integrity	Ensures that data and resources in the Metaverse are accurate, complete, and unaltered.	• Unauthorized modifications or tampering of data • Integrity violations during data transmission • Protection against data corruption or manipulation	• Cryptographic techniques (e.g., digital signatures, hashing) • Data validation and checksum mechanisms • Access control policies and enforcement mechanisms
Confidentiality	Preserves the privacy and confidentiality of sensitive information in the Metaverse.	• Unauthorized access to sensitive data • Data breaches or leaks • Protection against eavesdropping or interception	• Encryption algorithms and protocols • Secure communication channels (e.g., SSL/TLS) • Access control mechanisms (e.g., role-based, attribute-based) • Data classification and labeling
Availability	Ensures that data and services in the Metaverse are accessible and usable when needed.	• Service disruptions or outages • Distributed denial of service (DDoS) attacks • Resource exhaustion or contention	• Redundancy and fault-tolerant architectures • Load balancing and traffic management • Intrusion prevention systems (IPS) and firewalls • Incident response and disaster recovery plans

reliable identity verification, various identification and authentication methods can be employed (Yousefi et al., 2019). Table 3 provides a comprehensive overview of these methods, highlighting their benefits and potential applications in verifying user identities and enhancing access control. Utilizing such techniques fosters a secure and trustworthy environment in the Metaverse.

Biometrics

Biometric authentication methods leverage individuals' distinctive physical or behavioral characteristics to ascertain their identities (Jain et al., 2000). In the Cloud-based Metaverse, these methods find application through technologies like fingerprint recognition, iris scanning, voice recognition, and facial recognition. Utilizing such methods yields heightened precision and delivers a seamless user experience. Within the Cloud-based Metaverse, biometric authentication necessitates users to register their biometric data, which is securely stored and employed for subsequent identity verification (Vallabhu & Satyanarayana, 2012). Incorporating biometrics enhances access control security by ensuring that only authorized individuals can authenticate themselves and gain entry to virtual resources.

Privacy considerations arise when employing biometric authentication in the Cloud-based Metaverse (Habibu et al., 2021). Users express concerns regarding the storage and potential misuse of their biometric data. Implementing robust encryption and data protection measures to address these concerns and safeguard biometric information is crucial. Despite their effectiveness, biometric authentication methods are not immune to vulnerabilities and attacks (Martin et al., 2010). For instance, presentation attacks, such as employing a high-resolution photograph to deceive a facial recognition system, can compromise the integrity of biometric authentication. Mitigating such risks requires the implementation of countermeasures like liveness detection and anti-spoofing techniques to ensure the reliability of biometric identification.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a robust security measure utilized in the Cloud-based Metaverse (Dasgupta et al., 2017). It combines multiple authentication factors to verify user identity. These factors encompass something the user knows (e.g., a password or PIN), something the user has (e.g., a physical token or mobile device), and something the user is (e.g., biometric data). By requiring users to present multiple pieces of evidence, MFA strengthens identity verification and reduces the risk of unauthorized access (Ogbanufe & Baham, 2023). Even if one factor is compromised, using multiple factors ensures enhanced security. In the context of the Cloud-based Metaverse, an illustrative scenario involves users providing a password, followed by a one-time password generated on their mobile device, and verifying their biometric data. This layered approach contributes to higher assurance and safeguards against potential threats to user identities.

Implementing Multi-Factor Authentication (MFA) in the Cloud-based Metaverse is pivotal in bolstering access control mechanisms by significantly raising the barriers for attackers attempting to impersonate legitimate users (Alahmad et al., 2022). However, striking a delicate balance between security and user convenience is crucial, as excessively intricate authentication processes might deter users or engender frustration. Organizations must meticulously assess the selection of authentication factors based on the sensitivity of the accessed resources and the associated risk levels within the virtual environment (Kumar & Goyal, 2019). Leveraging adaptive MFA techniques, wherein authentication factors dynamically adapt in response to contextual information, can further fortify the security posture of the Cloud-based Metaverse.

Behavioral Biometrics

Behavioral biometrics involve the analysis of distinct patterns of user behavior to verify their identities. Within the Metaverse context (Bo et al., 2013), behavioral biometrics can be leveraged to assess user interactions, such as typing patterns, mouse movements, or touch gestures. By employing machine

Table 3. Identification and authentication methods in the cloud-based metaverse

Method	Description	Advantages	Challenges	Use Cases
Biometrics	To verify their identity, biometric authentication utilizes individuals' unique physical or behavioral characteristics, such as fingerprints, iris patterns, or voice recognition.	• High accuracy and uniqueness • Difficult to forge or spoof • Convenient and userfriendly	• Privacy concerns • False acceptance or rejection rates • Technological limitations in certain environments	• Access control to highly sensitive virtual spaces • User verification in virtual financial transactions
Multi-Factor Authentication	Multi-factor authentication (MFA) combines multiple authentication factors, such as passwords, biometrics, tokens, or one-time passcodes, to enhance security and reduce the reliance on single-factor authentication.	• Increased security • Defense against stolen credentials • Flexibility in choosing authentication factors	• User inconvenience • Management complexity • Integration challenges with different systems	• Virtual platforms with sensitive user data • Secure remote access to virtual networks
Behavioral Biometrics	Behavioral biometrics leverage unique behavioral patterns, such as keystroke dynamics, mouse movement, or touch gestures, to verify user identities based on their distinctive behavioral traits.	• Non-intrusive and Continuous authentication • Difficult to replicate or imitate • User-friendly experience	• Variability and adaptability of user behavior • Accurate behavioral profiling • User acceptance and understanding	• Continuous user authentication in virtual environments • Monitoring and detecting suspicious activities

learning algorithms, these behavioral patterns can be scrutinized to generate user profiles and identify anomalies that might indicate unauthorized access attempts (Krishnamoorthy et al., 2018). Behavioral biometrics play a vital role in the Metaverse by offering a non-intrusive and continuous authentication mechanism. By continuously monitoring user behavior, access control systems can detect suspicious activities or deviations from established behavioral norms, triggering additional authentication steps or access restrictions and bolstering overall security measures.

However, adopting behavioral biometrics in the Metaverse presents potential privacy concerns, as it involves constantly monitoring and analyzing user actions (Kakarlapudi & Mahmoud, 2021). Organizations must maintain transparency regarding collecting and utilizing behavioral data, ensuring compliance with privacy regulations, and obtaining explicit user consent. Anonymization techniques can be implemented to safeguard user privacy while enabling behavioral biometric analysis. For successful implementation within the Cloud-based Metaverse, sophisticated machine learning algorithms must accurately discern genuine user behavior from potential masquerade attacks or anomalies. These algorithms need continuous training and updates to adapt to evolving user behavior and emerging attack techniques.

Authorization Techniques

After users have undergone successful identification and authentication processes, the subsequent vital step involves determining their access permissions within the Metaverse. Authorization techniques are significant in bestowing appropriate access levels, considering user roles, attributes, and contextual information (Bertino et al., 2005). This subsection delves into distinct authorization models suitable for the Metaverse. To gain a comprehensive understanding, Table 4 presents an overview of these techniques, highlighting their associated benefits and potential applications in granting permissions and managing access control. This valuable resource aids in navigating the intricacies of authorization within the Cloud-based Metaverse, facilitating informed decision-making and effective access control management.

Role-Based Authorization

Role-based authorization (RBA) is a widely adopted approach in access control that assigns permissions based on predefined user roles (Rathi et al., 2022). In the context of the Metaverse, RBA offers a structured and manageable means of granting access privileges according to user responsibilities and functions. RBA aligns with the principle of least privilege, ensuring that users are only granted the minimum necessary permissions required for their tasks. User roles are established based on job functions, organizational hierarchy, or other pertinent criteria (Ferraiolo et al., 2001). Access control policies link specific permissions to each role, restricting users to resources relevant to their designated roles. Adopting RBA in the Cloud-based Metaverse allows access control mechanisms to effectively balance user access with the need for security and privacy, promoting a controlled and regulated virtual environment.

RBA offers a streamlined approach to managing access control by categorizing users into predefined roles based on their access requirements (Nuss, Puchta, and Kunz, 2018). This approach brings advantages like scalability and simplified access grant or revocation processes, accommodating evolving user responsibilities and access needs. Nevertheless, in the context of the Cloud-based Metaverse, role-based authorization alone may not provide the level of granular control necessary for intricate scenarios. Complementary authorization models might be required to address specific access requirements more effectively. Exploring such models can enhance the overall access control framework in the Metaverse.

Attribute-Based Authorization

Attribute-based authorization is an adaptable authorization model that considers various attributes of users, resources, and the context to determine access permissions (Lang et al., 2009). Within the Metaverse, this approach enables dynamic and context-aware access control decisions based on user attributes, resource attributes, environmental conditions, and other contextual information. It follows a policy-based methodology, wherein access control policies specify the conditions under which access should be granted or denied (Hu et al. et al., 2013). These policies may encompass attributes like user

Table 4. Authorization techniques in the cloud-based metaverse

Technique	Description	Key Features	Advantages	Use Cases
Role-Based Authorization	Role-based authorization assigns permissions to users based on their predefined roles and responsibilities within an organization or system.	• Hierarchical role structures • Role assignment and management • Simplified access control administration	• Easy administration and maintenance • Scalability in large organizations • Simplicity in access control management	• Virtual worlds with predefined user roles and responsibilities • Access control in organizational environments
Attribute-Based Authorization	Attribute-based authorization assigns permissions based on user attributes, environmental conditions, and contextual information, providing more fine-grained access control decisions.	• Policies based on user attributes • Context-aware access control • Dynamic access decisions based on attributes	• Granular access control • Flexible and adaptable access policies • Efficient management of user access	• Virtual environments with diverse user attributes and dynamic access requirements • Access control in regulated industries with specific attribute-based policies
Risk-Based Authorization	Risk-based authorization evaluates the risk associated with access requests and adjusts authorization decisions based on risk levels, enabling adaptive and context-aware access control.	• Risk assessment and scoring • Context-driven access decisions • Dynamic policy enforcement based on risk levels	• Enhanced security posture • Real-time adaptation to changing risk conditions • Improved user experience	• Virtual environments with varying risk levels and dynamic access requirements • Access control in scenarios with high-risk sensitivity

roles, location, time of day, and device characteristics. By leveraging attribute-based authorization, the Metaverse can establish a flexible and nuanced access control framework, accommodating the diverse requirements of its virtual ecosystem.

Implementing attribute-based authorization in the Metaverse necessitates establishing a comprehensive attribute management system capable of collecting, storing, and evaluating attributes to facilitate access control decisions. This approach offers a higher granularity and flexibility in governing access permissions, empowering organizations to define precise access policies that align with their specific requirements. By considering additional attributes and context in access control decisions, attribute-based authorization can effectively overcome the limitations of role-based authorization (Rajpoot et al., 2015). For instance, within the Cloud-based Metaverse, granting users access to sensitive financial information may involve their assigned role and factors such as their geographical location, device integrity, and recent user behavior patterns. Such a multi-dimensional approach allows for a more nuanced and context-aware access control mechanism, bolstering security and enhancing fine-grained access management capabilities in the Cloud-based Metaverse.

Risk-Based Authorization

Risk-based authorization considers the risk level of granting access to specific users or resources in the Metaverse (Atlam et al., 2018). It entails assessing risk factors like user behavior, location, or device security posture and dynamically adjusting access permissions based on the risk level. Risk-based authorization models in the Metaverse leverage algorithms and machine learning techniques to calculate the risk associated with access requests. Access control mechanisms evaluate the risk score and make access decisions accordingly (Smari et al., 2014). For instance, if a user's access request originates from an unrecognized location or an untrusted device, the system may require additional authentication steps or restrict access to sensitive resources.

Implementing risk-based authorization in the Cloud-based Metaverse necessitates continually monitoring user behavior, contextual information, and threat intelligence (Dunning & Friedman, 2014). Leveraging machine learning algorithms, historical data can be scrutinized to uncover patterns and anomalies, thereby unveiling potential risks. By dynamically calculating risk scores based on the evaluated risk factors, access control systems can adapt to evolving conditions and emerging threats. This integration of risk-based authorization into the access control framework empowers organizations to prioritize security measures and allocate resources following the level of risk associated with diverse access scenarios within the Cloud-based Metaverse.

ACCESS CONTROL TECHNOLOGIES AND MODELS FOR THE CLOUD-BASED METAVERSE

The Metaverse requires robust access control technologies and models to ensure secure and controlled access to virtual environments Kürtünlüoğlu, Akdik, and Karaarslan (2022). This section explores various access control solutions and their applicability in the context of the Cloud-based Metaverse. It discusses technologies such as SSO, blockchain-based access control, ABAC, adaptive access control, and VMI for isolation. Table 5 provides an overview of the technologies, their benefits, and their potential applications in securing virtual environments.

Single Sign-On (SSO) Solutions

As highlighted in the literature (Derek et al., 2013), SSO solutions play a pivotal role in the Metaverse by streamlining the authentication process. They enable users to access multiple virtual environments or applications using a single set of credentials. In the dynamic landscape of the Metaverse, where users traverse diverse platforms and applications, the significance of SSO cannot be overstated. It simplifies user authentication, contributing to an enhanced user experience. With SSO, users no longer

Table 5. Access control technologies in the cloud-based metaverse

Technique	Description	Key Features	Advantages	Use Cases
Single Sign-On Solutions	SSO allows users to authenticate once and access multiple applications or services without needing separate login credentials.	• Centralized authentication • Federated identity management • Seamless user experience	• Improved user convenience • Simplified user access management • Reduced password fatigue and security risks	• Virtual worlds with multiple interconnected services • Cross-platform applications and services in the Metaverse
Blockchain-based Access Control	Access control mechanisms based on blockchain technology provide decentralized and tamperproof authorization and authentication processes, enhancing security and transparency.	• Distributed ledger technology • Smart contracts for access control rules • Immutable audit trails	• Enhanced security and privacy • Elimination of central authorities • Auditable and transparent access control	• Virtual marketplaces and transactions • Cross-domain access control in the Metaverse
Attribute-Based Access Control (ABAC)	ABAC assigns access permissions based on user attributes, environmental conditions, and contextual information, offering fine-grained control over access decisions.	• Policies based on user attributes • Context-aware access control • Dynamic access decisions based on attributes	• Granular access control • Flexible and adaptable access policies • Efficient management of user access	• Virtual environments with diverse user roles and attributes • Access control in highly regulated industries
Adaptive Access Control	Adaptive access control dynamically adjusts access permissions based on user behavior, risk assessments, and real-time context, balancing security and usability.	• Continuous user authentication and risk assessment • Context-driven access decisions • Dynamic policy enforcement	• Improved security posture • User-friendly experience • Real-time adaptation to changing conditions	• Virtual environments with varying risk levels • Access control in dynamic and unpredictable scenarios
Virtual Machine Introspection (VMI)	VMI enables monitoring and control of virtual machines at the hypervisor level, offering visibility into system activities and the ability to enforce access policies.	• Hypervisor-level monitoring • Detection and prevention of malicious activities • Real-time introspection of virtual machines	• Enhanced visibility and control • Efficient detection and response to security incidents • Isolation and protection of virtual machines	• Securing virtualized infrastructures in the Metaverse • Protection against malware and exploits in virtual environments

need to remember and manage multiple usernames and passwords, mitigating the risks associated with weak passwords or password reuse (Scarfone & Souppaya, 2009).

Furthermore, SSO enhances security through centralized user authentication, wherein authentication is conducted once at a trusted identity provider. Once authenticated, users can seamlessly navigate through authorized resources without needing re-authentication. This robust approach bolsters security and fosters a seamless and efficient user experience within the Cloud-based Metaverse. SSO solutions can seamlessly integrate with access control frameworks, facilitating the enforcement of fine-grained access control policies rooted in user attributes or roles (Zhang et al., 2007). This integration augments the overall access control capabilities within the Metaverse, capitalizing on SSO as an authentication foundation. However, it is imperative for organizations to meticulously assess the security and privacy dimensions associated with SSO solutions. Robust protocols and encryption techniques must be implemented to safeguard user credentials throughout the authentication process. Additionally, sound authorization mechanisms must be established to

ensure that users are granted access solely to authorized resources, contingent upon their authenticated identity and designated privileges.

Blockchain-Based Access Control

Blockchain technology has garnered considerable attention due to its potential to revolutionize access control across various domains, including the Metaverse (Javaid et al., 2021). By offering decentralized and tamper-resistant mechanisms, blockchain presents a promising solution for managing access rights and enforcing access control policies. In the Metaverse context, blockchain-based access control holds several advantages. Firstly, it enables the creation of immutable access control logs, ensuring transparency and auditability (Ahmad et al., 2019). Every access control event, encompassing user authentication, authorization, and permission changes, can be securely recorded on the blockchain, promoting accountability and traceability. Secondly, blockchain-based access control enhances user privacy (Ma, Shi, & Li, 2019). Leveraging techniques like zero-knowledge proofs or selective disclosure, users can verify their identity or access rights without compromising sensitive personal information. This integration of blockchain technology within access control systems presents an intriguing avenue for establishing secure and privacy-enhanced access control mechanisms in the Metaverse.

Blockchain technology can potentially facilitate the development of decentralized identity management systems in the Metaverse (Belchior et al., 2020). This innovative approach empowers users with control over their identities, allowing them to selectively disclose attributes or credentials for access control purposes. By reducing reliance on centralized identity providers, users gain enhanced privacy control. However, integrating blockchain-based access control into the Cloud-based Metaverse necessitates careful consideration of scalability and performance. Given the high-volume activities within virtual environments, blockchain networks must efficiently handle many access control transactions. To address these challenges, scalability solutions such as off-chain processing or layer-two protocols can be implemented. These measures mitigate the potential bottlenecks and ensure the smooth operation of access control mechanisms in the Cloud-based Metaverse.

Attribute-Based Access Control (ABAC)

ABAC is a highly flexible access control model that assesses access decisions by considering attributes linked to users, resources, and environmental conditions (Yuan & Tong, 2005). ABAC is particularly suitable in the context of the Cloud-based Metaverse, characterized by its dynamic and diverse nature. This model enables access control policies to incorporate many attributes, such as user roles, group memberships, access time, location, and various contextual factors (Gupta et al., 2019). The ability to accommodate such granular control empowers organizations to establish intricate access rules and policies that precisely align with the specific requirements of the Metaverse. By leveraging ABAC, organizations can achieve a robust and adaptable access control framework within the dynamic virtual environments of the Metaverse.

ABAC offers dynamic policy enforcement capabilities, enabling real-time access decisions based on current attributes and conditions (Zhu et al., 2019). This adaptability becomes particularly critical in virtual environments where user roles, resource permissions, and contextual factors change frequently. To successfully implement ABAC in the Cloud-based Metaverse, organizations must establish a robust infrastructure for attribute management. It involves defining attribute schemas, establishing attribute authorities, and ensuring consistency across diverse virtual environments and platforms. Effective design of access control policies becomes essential, leveraging attributes to make access decisions while considering the dynamic nature and diversity of the Cloud-based Metaverse.

Adaptive Access Control

Adaptive access control mechanisms continually monitor user behavior, environmental conditions, and risk factors to adjust access decisions dynamically (Bellavista & Montanari, 2017). These

mechanisms are vital in enhancing security within the Cloud-based Metaverse by adapting access control based on real-time context and evolving risk levels. Leveraging techniques such as risk-based authentication, anomaly detection, and behavior profiling (Almehmadi & El-Khatib, 2015), adaptive access control ensures the assessment of users' trustworthiness and access requests. This approach analyzes user behavior patterns, including login times, access patterns, and interaction behaviors, to identify anomalies or suspicious activities effectively. By leveraging real-time context and behavioral insights, adaptive access control reinforces the security posture in the Metaverse, bolstering the overall protection of virtual environments.

In the Metaverse realm, adaptive access control is crucial in detecting and thwarting unauthorized access attempts, compromised accounts, and suspicious activities within virtual environments. Through the continuous evaluation of access requests and user behavior, adaptive access control dynamically enforces more robust authentication measures or restricts access in situations where risk levels surpass pre-established thresholds (Ryutov et al., 2003). Organizations implementing adaptive access control within the Cloud-based Metaverse must cautiously strike a balance between security and user experience. Excessively stringent adaptive controls may yield false positives, inconveniencing users, while excessively lenient controls may expose vulnerabilities to potential security breaches. The achievement of effective and user-friendly adaptive access control mechanisms necessitates incorporating continuous monitoring, feedback loops, and meticulous fine-tuning processes.

Virtual Machine Introspection (VMI)

VMI is an advanced technique that offers comprehensive visibility and precise control over the execution of virtual machines (Hebbal et al., 2015). Within the Metaverse context, VMI is a valuable asset for access control, as it ensures robust isolation and thwarts unauthorized activities within virtual environments. By facilitating real-time monitoring of critical aspects like virtual machine memory, disk operations, network activity, and process execution (Roberts et al., 2013), VMI empowers security professionals to promptly detect and respond to malicious actions, unapproved alterations, and exploit attempts targeting vulnerabilities present in virtual environments. This dynamic capability is a reliable defense mechanism, enhancing the security and integrity of the Metaverse within virtual environments.

By employing VMI, access control mechanisms gain the ability to proactively detect and respond to security incidents occurring within virtual environments. These incidents encompass unauthorized access attempts, malware infections, and suspicious network traffic (Chung et al., 2013). Policies can be defined to trigger automated responses, such as the isolation or quarantine of compromised virtual machines, effectively preventing further damage. Nevertheless, implementing VMI for access control in the Cloud-based Metaverse demands meticulous consideration of performance and compatibility aspects. Minimizing the overhead introduced by VMI techniques is imperative to ensure that the overall performance of virtual environments remains unaffected. Moreover, guaranteeing compatibility with diverse virtualization platforms and environments is vital to facilitate widespread adoption.

ACCESS CONTROL THREATS AND MITIGATION IN THE CLOUD-BASED METAVERSE

The Metaverse, being a digital ecosystem, remains vulnerable to an extensive array of access control threats. Illintentioned individuals may seek to exploit vulnerabilities, compromise user accounts, gain unauthorized access to valuable resources, or employ deceptive social engineering techniques (Siddiqi et al., 2022). This section explores the prevailing access control threats encountered within the Metaverse, accompanied by a comprehensive examination of effective mitigation strategies. Table 6 presents a detailed overview of access control threats, outlining their potential impact on the Cloud-based Metaverse.

Table 6. Access control threats in the cloud-based metaverse

Threat	Description	Potential Impact	Prevalence in the Metaverse
Denial of Service (DoS) Attacks	DoS attacks aim to disrupt or suspend access to services or resources, overwhelming them with requests and rendering them unavailable to legitimate users.	• Service unavailability • Business disruption • Revenue loss • Reputation damage	DoS attacks are prevalent in the Metaverse due to the high concentration of services, virtual environments, and users, making it an attractive target for malicious actors seeking to cause disruptions or gain an advantage.
Malware and Exploits in Virtual Environments	Malicious software and exploits target vulnerabilities within virtual environments, compromising systems and data security and enabling unauthorized access or control.	• Data breaches • Unauthorized access • Information theft • System compromise • Financial losses	With the increasing complexity and interconnectedness of virtual environments in the Metaverse, the risk of malware and exploits is elevated. Malicious actors exploit vulnerabilities in virtual infrastructure, software, and user interactions to gain unauthorized access or extract sensitive information.
Social Engineering Techniques	Social engineering involves psychological manipulation to deceive individuals and trick them into divulging sensitive information or granting unauthorized access.	• Identity theft • Unauthorized access • Fraudulent activities • Compromised accounts • Data breaches	Social engineering techniques are prevalent in the Metaverse due to the vast user base, diverse interactions, and the potential for impersonation, phishing, and social manipulation within virtual communities. Malicious actors exploit human psychology to exploit trust and extract sensitive information.

Denial of Service (DoS) Attacks

DoS attacks in the Metaverse are aimed at disrupting the availability of services or resources by overwhelming them with a high volume of requests or exploiting vulnerabilities (Anyanwu et al., 2022). These attacks target various components, including authentication servers, resource servers, and communication channels. One common form is the Distributed Denial of Service (DDoS) attack, wherein botnets and compromised devices flood the target with traffic, challenging distinguishing legitimate requests from malicious ones. As a result, the availability and performance of virtual environments can be significantly impacted, rendering them inaccessible or unusable for legitimate users (Gupta & Badve, 2017). The disruptive nature of DoS attacks poses a considerable threat to the seamless operation of the Cloud-based Metaverse, demanding robust defense mechanisms to safeguard against such attacks. Organizations must adopt resilient network infrastructure with load balancing and traffic filtering capabilities.

To counteract DoS attacks within the Cloud-based Metaverse. Deploying Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) becomes imperative to identify and thwart suspicious network traffic. Furthermore, implementing rate limiting and throttling mechanisms proves vital in preventing overwhelming resource exhaustion caused by excessive requests. By incorporating these measures, organizations can fortify their defense against DoS attacks and safeguard the uninterrupted functioning of their systems and services in the Cloud-based Metaverse.

Malware and Exploits in Virtual Environments

Virtual environments within the Cloud-based Metaverse are susceptible to the infiltration of malware and the exploitation of vulnerabilities, leading to potential compromises of user accounts, extraction of sensitive information, and disruption of platform functionality (Abraham & Chengalur-Smith, 2010). Malware can be introduced through malicious downloads, infected virtual assets, or compromised user interactions. Organizations should adopt a multi-layered approach to malware protection to counter these threats. It entails the implementation of antivirus and antimalware solutions specifically designed for virtual environments. Additionally, it is essential to regularly update software and apply security patches to mitigate known vulnerabilities. Furthermore, promoting user awareness regarding

safe browsing practices and downloading habits is crucial in preventing malware incidents. Following these measures can establish a robust defense against malware within virtual environments in the Cloud-based Metaverse.

Virtual environments must prioritize robust isolation measures between user accounts and virtual assets to restrict the potential impact of malware infections. Adopting sandboxing techniques becomes imperative to confine potentially malicious code or activities within contained boundaries, effectively mitigating their ability to propagate throughout the wider virtual environment (Sikorski & Honig, 2012). To ensure a high level of security, it is essential to implement secure coding practices and conduct regular security assessments while developing virtual platforms and applications. By leveraging vulnerability scanning and penetration testing, organizations can proactively identify and address security vulnerabilities before they are exploited by malicious actors (Shah & Mehtre, 2015). These practices are vital for establishing a resilient and secure virtual environment.

Social Engineering Techniques in the Cloud-Based Metaverse

Social engineering techniques encompass manipulating users to divulge sensitive information or engage in actions that compromise their security (Workman, 2008). In the vast realm of the Metaverse, social engineering attacks manifest in diverse forms, including phishing, impersonation, and deceptive communication. Phishing attacks within the Cloud-based Metaverse exploit deceptive messaging or the creation of counterfeit websites that closely emulate legitimate virtual platforms. These insidious tactics dupe unsuspecting users into unintentionally revealing their login credentials, personal data, or financial particulars, which can be exploited for unauthorized access or identity theft (Irshad & Soomro, 2018).

Organizations are advised to implement user education and awareness programs to counteract the detrimental impact of social engineering attacks (Saleem & Hammoudeh, 2018). Such programs aim to equip users with essential knowledge regarding prevalent social engineering techniques, effective identification of phishing attempts, and the significance of validating the genuineness of communications and requests. Virtual platforms can enhance security by incorporating two-factor authentication (2FA) or email/SMS verification, fortifying defenses against impersonation and unauthorized account access. It is imperative to establish clear and accessible communication channels that enable users to promptly report any suspicious activities or potential security incidents.

Mitigation Strategies for Access Control Threats

A comprehensive approach blending technical measures, user education, and proactive security practices is paramount to mitigate access control threats in the Cloud-based Metaverse effectively. Table 7, presented below, outlines the key mitigation strategies for addressing access control threats in the Cloud-based Metaverse. By adopting the following strategies, organizations can fortify their defenses against potential access control breaches:

Intrusion Detection Systems (IDS)

In access control, IDS stands as vigilant guardians, continuously monitoring network traffic and system logs to uncover signs of unauthorized access attempts, malicious activities, or policy violations. IDS harnesses the power of signature-based detection, anomaly detection, and behavior-based detection techniques to identify potential security breaches. Regarding the ever-evolving landscape of the Cloud-based Metaverse, IDS is pivotal in detecting and responding to access control threats, including unauthorized access attempts, suspicious network traffic, and atypical user behavior. With its real-time alert generation capabilities and the ability to trigger automated responses, IDS becomes an indispensable asset in mitigating security incidents and proactively preventing further harm (Liao et al., 2013).

Intrusion Prevention Systems (IPS)

IPS surpasses the detection capabilities offered by Intrusion Detection Systems (IDS) through their proactive measures for blocking or mitigating identified threats. IPS leverages diverse techniques to thwart unauthorized access, exploits, and malware infections, including packet filtering, protocol validation, and traffic redirection. Within the virtual environments of the Cloud-based Metaverse, IPS can play a pivotal role by providing active protection against access control threats. IPS is a robust deterrent by upholding access control policies, scrutinizing network traffic, and impeding suspicious activities, significantly minimizing the likelihood of successful attacks and unauthorized access (Chakraborty, 2013).

Security Incident and Event Management (SIEM)

SIEM systems play a critical role in the Metaverse by collecting, correlating, and analyzing security events and logs from diverse sources (Bhatt et al., 2014). By providing a centralized view of security events, SIEM systems facilitate efficient incident response and enable proactive threat detection. Analyzing access logs, authentication events, and user behavior by SIEM systems can help identify access control threats in the Cloud-based Metaverse. Leveraging event correlation and pattern detection, SIEM systems offer early warning signs of potential security breaches or policy violations. Organizations should integrate SIEM systems into their access control infrastructure to enhance threat detection, incident response, and compliance monitoring in the Cloud-based Metaverse. The real-time alerts, automated incident handling, and forensic analysis capabilities of SIEM systems

Table 7. Mitigation strategies for access control threats in the cloud-based metaverse

Mitigation Strategy	Description	Key Features	Benefits
Intrusion Detection Systems (IDS)	IDS monitors network traffic and system activities to detect and alert potential security breaches or policy violations.	• Real-time monitoring and analysis of network traffic • Signature-based detection • Anomaly detection • Behavior-based detection	• Early detection and alerting of unauthorized access attempts • Identification of suspicious patterns or activities • Enhanced incident response capabilities
Intrusion Prevention Systems (IPS)	IPS goes beyond IDS by actively blocking or mitigating detected threats to prevent unauthorized access and exploits.	• Packet filtering • Protocol validation • Traffic redirection • Automatic blocking or isolation of malicious activities	• Proactive prevention of unauthorized access and exploits • Reduction of successful attacks and unauthorized access • Enhanced network security and integrity
Security Incident and Event Management (SIEM)	SIEM systems collect, correlate, and analyze security events and logs from various sources to facilitate efficient incident response and proactive threat detection.	• Centralized log and event collection • Event correlation and analysis • Real-time alerting • Forensic analysis capabilities	• Comprehensive visibility into security events and incidents • Early detection of access control threats • Efficient incident response and mitigation • Compliance monitoring and reporting
User Education Programs	User education and awareness programs aim to educate users about access control best practices, safe browsing habits, and identifying and reporting suspicious activities.	• Security awareness campaigns • Interactive training sessions • Simulated phishing exercises • Clear guidelines and reporting mechanisms	• Development of a security-conscious mindset among users • Informed decision-making while navigating virtual environments • Active participation in maintaining a secure Metaverse environment • Reduction of successful social engineering attacks

effectively contribute to mitigating access control threats (González-Granadillo, González-Zarzosa, and Diaz, 2021).

User Education and Awareness Programs

User education and awareness are pivotal in averting access control threats within the Metaverse (Jensen et al., 2017). Organizations must impart training and furnish resources to enlighten users about best practices for access control, fostering safe browsing habits and enabling them to recognize and report suspicious activities. Regular security awareness campaigns, interactive training sessions, and simulated phishing exercises can instill a security-conscious mindset and enable users to make well-informed decisions while navigating virtual environments. Effective communication of clear guidelines, policies, and reporting mechanisms ensures active user engagement in upholding a secure Cloud-based Metaverse environment. By fostering a culture of security awareness and empowering users with knowledge and tools to safeguard themselves, organizations can proficiently mitigate access control threats and establish a safer and more secure experience for all stakeholders.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This section presents a concise summary encompassing the key findings and significant contributions from extensive research on access control models and techniques tailored for the Metaverse. The manuscript has explored the distinct challenges presented by the Cloud-based Metaverse and delved into various access control principles and criteria. An in-depth analysis of diverse technologies and models designed for access control in the Cloud-based Metaverse has also been conducted. Furthermore, common access control threats and the corresponding mitigation strategies have been identified. The culmination of this research emphasizes the paramount importance of robust access control mechanisms to ensure the utmost security, privacy, and trustworthiness of virtual environments within the dynamic realm of the Cloud-based Metaverse. This research offers insights into access control models and techniques tailored to the Cloud-based Metaverse. However, it is essential to acknowledge the limitations encountered and propose future research directions. Recognizing these constraints can pave the way for further advancements in securing virtual environments.

- **Dynamic nature of the Metaverse:** The Metaverse continuously evolves, with emerging technologies, platforms, and use cases necessitating adaptable access control models. Future research should prioritize accommodating the dynamic nature of the Metaverse and addressing evolving security challenges.
- **Scalability and interoperability:** As the Cloud-based Metaverse expands to encompass diverse virtual environments, ensuring scalable and interoperable access control mechanisms becomes paramount. Further research should explore approaches for seamless integration and management of access control across different virtual platforms and environments.
- **Privacy and data protection:** With growing concerns about privacy and data protection, research should delve into privacy-enhancing access control mechanisms for the Cloud-based Metaverse. It entails exploring techniques like differential privacy, secure data sharing, and user-centric access control to balance security and privacy requirements.
- **Trust and reputation management:** Trust plays a pivotal role in the Cloud-based Metaverse, where users engage and interact extensively. Future research should investigate trust and reputation management mechanisms for access control, enabling users to assess the trustworthiness of virtual entities, platforms, and interactions.
- **Ethical considerations:** With the Cloud-based Metaverse's increasing integration into people's lives, ethical considerations surrounding access control demand attention. Future research should explore the ethical implications of access control models and techniques in the Metaverse, including fairness, bias, and user consent issues.

This manuscript has delved into access control models and techniques for the Cloud-based Metaverse, addressing the unique challenges, principles, criteria, technologies, threats, and mitigation strategies associated with access control in virtual environments. The research findings underscore the significance of robust access control mechanisms in ensuring the security, privacy, and trustworthiness of the Cloud-based Metaverse. Organizations and users can confidently navigate the Cloud-based Metaverse by understanding and implementing effective access control measures, fostering a secure and immersive digital experience. As the Cloud-based Metaverse continues to evolve, further research is needed to adapt access control approaches, address emerging challenges, and explore ethical considerations to create a sustainable and inclusive Metaverse ecosystem.

REFERENCES

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A review. *Procedia Computer Science*, *113*, 73–80. doi:10.1016/j.procs.2017.08.292

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196. doi:10.1016/j.techsoc.2010.07.001

Ahmad, A., Saad, M., & Mohaisen, A. (2019). Secure and transparent audit logs with blockaudit. *Journal of Network and Computer Applications*, *145*, 102406. doi:10.1016/j.jnca.2019.102406

Alahmad, Alkandari, & Alawadhi. (2022). Survey of broken authentication and session management of web application vulnerability attack. *Journal of Engineering Science and Technology, 17*, 874–882.

Ali, R. (2022). The video gamer's dilemmas. *Ethics and Information Technology*, *24*(2), 18. doi:10.1007/s10676-022-09638-x

Almehmadi, A., & El-Khatib, K. (2015). On the possibility of insider threat prevention using intent-based access control (ibac). *IEEE Systems Journal*, *11*(2), 373–384. doi:10.1109/JSYST.2015.2424677

Anyanwu, G. O., Nwakanma, C. I., Lee, J.-M., & Kim, D.-S. (2022). Optimization of rbf-svm kernel using grid search algorithm for ddos attack detection in sdn-based vanet. *IEEE Internet of Things Journal*.

Atlam, H. F., Alenezi, A., Hussein, R. K., & Wills, G. B. (2018). Validation of an adaptive risk-based access control model for the internet of things. *International Journal of Computer Network and Information Security*, *12*, 26. doi:10.5815/ijcnis.2018.01.04

Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security*, *39*, 237–254. doi:10.1016/j.cose.2013.08.001

Barrera, K. G., & Shah, D. (2023). Marketing in the metaverse: Conceptual understanding, framework, and research agenda. *Journal of Business Research*, *155*, 113420. doi:10.1016/j.jbusres.2022.113420

Barthwal, V., Rauthan, M. S., & Varma, R. (2022). SMA-LinR: An Energy and SLA-Aware Autonomous Management of Virtual Machines. *International Journal of Cloud Applications and Computing*, *12*(1), 1–24. doi:10.4018/IJCAC.2022010103

Belchior, R., Putz, B., Pernul, G., Correia, M., Vasconcelos, A., & Guerreiro, S. (2020). Ssibac: self-sovereign identity based access control. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* 1935–1943. doi:10.1109/TrustCom50675.2020.00264

Bellavista, P., & Montanari, R. (2017). *Context awareness for adaptive access control management in iot environments, Security and Privacy in CyberPhysical Systems: Foundations*. Principles and Applications.

Bertino, E., & Takahashi, K. (2010). *Identity management: Concepts, technologies, and systems*. Artech House.

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security and Privacy*, *12*(5), 35–41. doi:10.1109/MSP.2014.103

Bisht, J., & Vampugani, V. S. (2022). Load and cost-aware min-min workflow scheduling algorithm for heterogeneous resources in fog, cloud, and edge scenarios. *International Journal of Cloud Applications and Computing*, *12*(1), 1–20. doi:10.4018/IJCAC.2022010105

Bo, C., Zhang, L., Li, X.-Y., Huang, Q., & Wang, Y. (2013). Silentsense: silent user identification via touch and movement behavioral biometrics. *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, 187–190. doi:10.1145/2500423.2504572

Bu, L., Chen, C.-H., Ng, K. K., Zheng, P., Dong, G., & Liu, H. (2021). A user-centric design approach for smart product-service systems using virtual reality: A case study. *Journal of Cleaner Production*, *280*, 124413. doi:10.1016/j.jclepro.2020.124413

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., & Dennis Mickunas, M. (2002). Towards security and privacy for pervasive computing. *International Symposium on Software Security*, 1–15.

Chakraborty, N. (2013). Intrusion detection system and intrusion prevention system: A comparative study. *International Journal of Computing and Business Research*, *4*, 1–8.

Chiu, C.-M., Hsu, M.-H., & Wang, E. T. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision Support Systems*, *42*(3), 1872–1888. doi:10.1016/j.dss.2006.04.001

Chopra, M., Singh, S. K., Gupta, A., Aggarwal, K., Gupta, B. B., & Colace, F. (2022). Analysis & prognosis of sustainable development goals using big data-based approach during COVID-19 pandemic. *Sustainable Technology and Entrepreneurship*, *1*(2), 100012. doi:10.1016/j.stae.2022.100012

Chung, C.-J., Khatkar, P., Xing, T., Lee, J., & Huang, D. (2013). Nice: Network intrusion detection and countermeasure selection in virtual network systems. *IEEE Transactions on Dependable and Secure Computing*, *10*(4), 198–211. doi:10.1109/TDSC.2013.8

Çifci. (2023). *Cybersecurity risks of emerging technologies: An analysis on mitigation strategies*. CONGRESS ID.

Damiani, E., De Capitani di Vimercati, S., Paraboschi, S., & Samarati, P. (2002). A finegrained access control system for xml documents. *ACM Transactions on Information and System Security*, *5*(2), 169–202. doi:10.1145/505586.505590

Dasgupta, D., Roy, A., Nag, A., Dasgupta, D., Roy, A., & Nag, A. (2017). *Multifactor authentication: More secure approach towards authenticating individuals*. Advances in User Authentication.

Davis, A., Murphy, J., Owens, D., Khazanchi, D., & Zigurs, I. (2009). Avatars, people, and virtual worlds: Foundations for research in metaverses. *Journal of the Association for Information Systems*, *10*(2), 1. doi:10.17705/1jais.00183

Derek Halling, T., & Hahn, D. C. (2013). Bringing interlibrary loan services under a single sign-on umbrella. *Library Hi Tech*, *31*(1), 76–86. doi:10.1108/07378831311303949

Deveci, M., Pamucar, D., Gokasar, I., Köppen, M., & Gupta, B. B. (2022). Personal Mobility in Metaverse With Autonomous Vehicles Using Q-Rung Orthopair Fuzzy Sets Based OPA-RAFSI Model. *IEEE Transactions on Intelligent Transportation Systems*, 1–10. doi:10.1109/TITS.2022.3186294

Dionisio, J. D. N. (2013). 3d virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*, *45*, 1–38. doi:10.1145/2480741.2480751

Duan, H., Huang, Y., Zhao, Y., Huang, Z., & Cai, W. (2022). User-generated content and editors in video games: Survey and vision. 2022 IEEE conference on games (CoG), 536–543.

Dunning, T., & Friedman, E. (2014). *Practical machine learning: a new look at anomaly detection*. O'Reilly Media, Inc.

El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, *31*(2), e3720. doi:10.1002/ett.3720

Fenton, J. H., & Wolfe, J. M. (2019). Organizing for success: Some human resources issues in information security. In *Information Security Management* (pp. 441–460). Auerbach Publications. doi:10.1201/9781351073547-30

Ferraiolo, D. F., Barkley, J. F., & Kuhn, D. R. (1999). A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and System Security*, *2*(1), 34–64. doi:10.1145/300830.300834

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed nist standard for role-based access control. *ACM Transactions on Information and System Security*, *4*(3), 224–274. doi:10.1145/501978.501980

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with care: An information accountability perspective. *IEEE Internet Computing*, *15*(4), 31–38. doi:10.1109/MIC.2011.51

Gokasar, I., Pamucar, D., Deveci, M., Gupta, B. B., Martinez, L., & Castillo, O. (2023). Metaverse integration alternatives of connected autonomous vehicles with self-powered sensors using fuzzy decision making model. *Information Sciences*, *642*, 119192. doi:10.1016/j.ins.2023.119192

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors (Basel)*, *21*(14), 4759. doi:10.3390/s21144759 PMID:34300500

Gou, Z., Yamaguchi, S., & Gupta, B. B. (2017). Analysis of various security issues and challenges in cloud computing environment: a survey. *Identity Theft: Breakthroughs in Research and Practice*, 221-247.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. doi:10.1016/j.comnet.2019.107094

Gupta, B. B., & Badve, O. P. (2017). Taxonomy of dos and ddos attacks and desirable defense mechanism in a cloud computing environment. *Neural Computing & Applications*, *28*(12), 3655–3682. doi:10.1007/s00521-016-2317-5

Gupta, M., Benson, J., Patwa, F., & Sandhu, R. (2019). Dynamic groups and attributebased access control for next-generation smart cars. *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, 61–72.

Gupta, T., & Panda, S. P. (2022). Cloudlet and virtual machine performance enhancement with CLARA and evolutionary paradigm. *International Journal of Cloud Applications and Computing*, *12*(1), 1–16. doi:10.4018/IJCAC.298322

Habibu, Luhanga, & Sam. (2021). A study of users' compliance and satisfied utilization of biometric application system. *Information Security Journal: A Global Perspective, 30*, 125–138.

Hebbal, Y., Laniepce, S., & Menaud, J.-M. (2015). Virtual machine introspection: Techniques and applications. *2015 10th international conference on availability, reliability and security*, 676–685.

Hu, Ferraiolo, Kuhn, Friedman, Lang, Cogdell, Schnitzer, Sandlin, Miller, & Scarfone. (2013). *Guide to attribute based access control (abac) definition and considerations* (draft). NIST special publication 800.

Hu, B., Gaurav, A., Choi, C., & Almomani, A. (2022). Evaluation and comparative analysis of semantic web-based strategies for enhancing educational system development. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–14. doi:10.4018/IJSWIS.302895

Hu, V. C., Ferraiolo, D., & Kuhn, D. R. (2006). *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology. doi:10.6028/NIST.IR.7316

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *International Journal of Computer Science and Network Security*, *18*, 43–55.

Isa, Khairuddin, Sulaiman, Ismail, Shukran, & Sajak. (2021). Siem network behaviour monitoring framework using deep learning approach for campus network infrastructure. *International Journal of Electrical and Computer Engineering Systems*, 9–21.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, *43*(2), 90–98. doi:10.1145/328236.328110

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for industry 4.0: A literature-based review, Blockchain. *Research and Applications*, *2*(4), 100027. doi:10.1016/j.bcra.2021.100027

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597–626. doi:10.1080/07421222.2017.1334499

Joshi, J., Ghafoor, A., Aref, W. G., & Spafford, E. H. (2001). Digital government security infrastructure design challenges. *Computer*, *34*(3), 66–72. doi:10.1109/2.901169

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). A systematic review of blockchain for consent management. Healthcare, 9, 137. doi:10.3390/healthcare9020137

Kalyvaki, M. (2023). Navigating the metaverse business and legal challenges: Intellectual property, privacy, and jurisdiction. *Journal of Metaverse*, *3*(1), 87–92. doi:10.57019/jmv.1238344

Kern, A., & Anderl, R. (2018). Using rbac to enforce the principle of least privilege in industrial remote maintenance sessions. *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, 107–114. doi:10.1109/IoTSMS.2018.8554805

Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6), 833–851. doi:10.1016/j.future.2012.01.006

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. doi:10.1007/s12394-009-0019-1

Krishnamoorthy, S., Rueda, L., Saad, S., & Elmiligi, H. (2018). Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning. *Proceedings of the 2018 2nd international conference on biometric engineering and applications*, 50–57. doi:10.1145/3230820.3230829

Kumar, K., & Thaman, J. (2022). Improving Virtual Machine Migration Effects in Cloud Computing Environments Using Depth First Inspired Opportunity Exploration. *International Journal of Cloud Applications and Computing*, *12*(1), 1–22. doi:10.4018/IJCAC.314209

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1–48. doi:10.1016/j.cosrev.2019.05.002

Lang, B., Foster, I., Siebenlist, F., Ananthakrishnan, R., & Freeman, T. (2009). A flexible attribute based access control method for grid computing. *Journal of Grid Computing*, *7*(2), 169–180. doi:10.1007/s10723-008-9112-1

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. doi:10.1016/j.jnca.2012.09.004

Lim, S. Y., Kiah, M. M., & Ang, T. F. (2017). Security issues and future challenges of cloud service authentication. *Acta Polytechnica Hungarica*, *14*, 69–89.

Lin, J., & Latoschik, M. E. (2022). Digital body, identity and privacy in social virtual reality: A systematic review. *Frontiers in Virtual Reality*, *3*, 974652. doi:10.3389/frvir.2022.974652

Lorch, M., Adams, D. B., Kafura, D., Koneni, M., Rathi, A., & Shah, S. (2003). The prima system for privilege management, authorization and enforcement in grid environments. *Proceedings. First Latin American Web Congress*, 109–116. doi:10.1109/GRID.2003.1261705

Lungu, A. J., Swinkels, W., Claesen, L., Tu, P., Egger, J., & Chen, X. (2021). A reviewon the applications of virtual reality, augmented reality and mixed reality in surgical simulation: An extension to different kinds of surgery. *Expert Review of Medical Devices*, *18*(1), 47–62. doi:10.1080/17434440.2021.1860750 PMID:33283563

Ma, M., Shi, G., & Li, F. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 34045–34059. doi:10.1109/ACCESS.2019.2904042

Maesa, D. D. F., Mori, P., & Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. *Computers & Security*, *84*, 93–119. doi:10.1016/j.cose.2019.03.016

Martin, M. V., Jóhannsdóttir, K., Reynaga, G. B., & Tashiro, J. (2010). Unconscious mind: Authenticating with something you don't know? or just an infallible liveness test? In *CCECE 2010* (pp. 1–6). IEEE. doi:10.1109/CCECE.2010.5575164

May, C. J., Hammerstein, J., Mattson, J., & Rush, K. (2006). *Defense in depth: foundation for secure and resilient it enterprises, Technical Report*. Carnegie-Mellon Univ. doi:10.21236/ADA460375

Mecozzi, R., Perrone, G., Anelli, D., Saitto, N., Paggi, E., & Mancini, D. (2022). Blockchain-related identity and access management challenges:(de) centralized digital identities regulation. *2022 IEEE International Conference on Blockchain (Blockchain),* 443–448. doi:10.1109/Blockchain55522.2022.00068

Mughal, A. A. (2018). The art of cybersecurity: Defense in depth strategy for robust protection. *International Journal of Intelligent Automation and Computing*, *1*, 1–20.

Mughal, A. A. (2022). Well-architected wireless network security. *Journal of Humanities and Applied Science Research*, *5*, 32–42.

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet of Things Journal*.

Noueihed, H., Harb, H., & Tekli, J. (2022). Knowledge-based virtual outdoor weather event simulator using unity 3D. *The Journal of Supercomputing*, *78*(8), 10620–10655. doi:10.1007/s11227-021-04212-6

Noueihed, H., Harb, H., & Tekli, J. (2022). Simulating Weather Events on a Real-world Map using Unity 3D. In SMARTGREENS (pp. 86-93). Academic Press.

Nuss, M., Puchta, A., & Kunz, M. (2018). Towards blockchain-based identity and access management for internet of things in enterprises. *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15*, 167–181. doi:10.1007/978-3-319-98385-1_12

Ogbanufe, O. M., & Baham, C. (2023). Using multi-factor authentication for online account security: Examining the influence of anticipated regret. *Information Systems Frontiers*, *25*, 897–916.

Pearlman, K., Initiative, X., Visner, S., Magnano, M., & Cameron, R. (2021). *Securing the metaverse-virtual worlds need real governance*. Simulation Interoperability Standards Organization–SISO.

Popović, K., & Hocenski, Ž. (2010). Cloud computing security issues and challenges. *The 33rd international convention mipro*, 344–349.

Possik, J., Azar, D., Solis, A. O., Asgary, A., Zacharewicz, G., Karami, A., . . . Wu, J. (2022, September). A distributed digital twin implementation of a hemodialysis unit aimed at helping prevent the spread of the Omicron COVID-19 variant. In *2022 IEEE/ACM 26th international symposium on distributed simulation and real time applications (ds-rt)* (pp. 168-174). IEEE.

Priyanka, H., & Cherian, M. (2021). Effective Utilization of Resources through Optimal Allocation and Opportunistic Migration of Virtual Machines in Cloud Environment. *International Journal of Cloud Applications and Computing*, *11*(3), 72–91. doi:10.4018/IJCAC.2021070105

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. doi:10.1016/j.cose.2023.103127

Rajpoot, Q. M., Jensen, C. D., & Krishnan, R. (n.d.). Integrating attributes into role-based access control. Data and Applications Security and Privacy XXIX: 29th Annual IFIP WG 11.3 Working Conference. doi:10.1007/978-3-319-20810-7_17

Rathi, N., Singla, R., & Tiwari, S. (2022). Towards a role-based authentication system based on ssvep-p300 hybrid brain–computer interfacing. *Behaviour & Information Technology*, *41*(15), 3301–3317. doi:10.1080/0144929X.2021.1979655

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet Research*, *8*(4), 313–321. doi:10.1108/10662249810231050

Roberts, A., McClatchey, R., Liaquat, S., Edwards, N., & Wray, M. (2013). Poster: Introducing pathogen: a real-time virtualmachine introspection framework. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 1429–1432.

Roesner, F., Kohno, T., Moshchuk, A., Parno, B., Wang, H. J., & Cowan, C. (2012). Userdriven access control: Rethinking permission granting in modern operating systems. *2012 IEEE Symposium on Security and Privacy*, 224–238. doi:10.1109/SP.2012.24

Ryutov, T., Neuman, C., Dongho, K., & Li, Z. (2003). Integrated access control and intrusion detection for web servers. *IEEE Transactions on Parallel and Distributed Systems*, *14*(9), 841–850. doi:10.1109/TPDS.2003.1233707

Saleem & Hammoudeh. (2018). Defense methods against social engineering attacks. *Computer and network security essentials*, 603–618.

Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The nist model for role-based access control: towards a unified standard. ACM Workshop on Role-Based Access Control, 10. doi:10.1145/344287.344301

Scarfone & Souppaya. (2009). *Guide to enterprise password management* (draft). NIST special publication 800, 800–118.

Schmidt, K. (2006). *High availability and disaster recovery: concepts, design, implementation* (Vol. 22). Springer Science & Business Media.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27–49. doi:10.1007/s11416-014-0231-x

Shen, B., Tan, W., Guo, J., Cai, H., Wang, B., & Zhuo, S. (2020). A study on design requirement development and satisfaction for future virtual world systems. *Future Internet*, *12*(7), 112. doi:10.3390/fi12070112

Shen, H., & Dewan, P. (1992). Access control for collaborative environments. *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, 51–58.

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences (Basel, Switzerland)*, *12*(12), 6042. doi:10.3390/app12126042

Sikorski & Honig. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software.* No Starch Press.

Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–43. doi:10.4018/IJSWIS.297143

Singh, G., Malhotra, M., & Sharma, A. (2022). An adaptive mechanism for virtual machine migration in the cloud environment. *International Journal of Cloud Applications and Computing*, *12*(1), 1–10. doi:10.4018/IJCAC.311504

Singla, A., Gupta, N., Aeron, P., Jain, A., Garg, R., Sharma, D., & Arya, V. et al. (2022). Building the Metaverse: Design Considerations, Socio-Technical Elements, and Future Research Directions of Metaverse. *Journal of Global Information Management*, *31*(2), 1–28. doi:10.4018/JGIM.315283

Smari, W. W., Clemente, P., & Lalande, J.-F. (2014). An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system. *Future Generation Computer Systems*, *31*, 147–168. doi:10.1016/j.future.2013.05.010

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *Management Information Systems Quarterly*, *34*(3), 503–522. doi:10.2307/25750689

Steiner, S., de Leon, D. C., & Jillepalli, A. A. (2018). Hardening web applications using a least privilege dbms access model. *Proceedings of the Fifth Cybersecurity Symposium*, 1–6. doi:10.1145/3212687.3212863

Stergiou, C. L., Plageras, A. P., & Psannis, K. E. (2020). Secure machine learning scenario from big data in cloud computing via internet of things network. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, 525-554. doi:10.1007/978-3-030-22277-2_21

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *People and Computers XXII Culture, Creativity*, *Interaction*, *22*, 111–119.

Tang, F., Chen, X., Zhao, M., & Kato, N. (2022). The roadmap of communication and networking in 6g for the metaverse. *IEEE Wireless Communications*.

Uddin, M., Manickam, S., Ullah, H., Obaidat, M., & Dandoush, A. (2023). Unveiling the metaverse: Exploring emerging trends, multifaceted perspectives, and future challenges. *IEEE Access : Practical Innovations, Open Solutions*, *11*, 87087–87103. doi:10.1109/ACCESS.2023.3281303

Upadhyay, U., Kumar, A., Sharma, G., Gupta, B. B., Alhalabi, W. A., Arya, V., & Chui, K. T. (2023). Cyberbullying in the Metaverse: A Prescriptive Perception on Global Information Systems for User Protection. *Journal of Global Information Management*, *31*(1), 1–25. doi:10.4018/JGIM.325793

Vallabhu, H., & Satyanarayana, R. (2012). Biometric authentication as a service on cloud: Novel solution. *International Journal of Soft Computing and Engineering*, *2*, 163.

Wahab, O. A., Bentahar, J., Otrok, H., & Mourad, A. (2017). Optimal load distribution for the detection of VM-based DDoS attacks in the cloud. *IEEE Transactions on Services Computing*, *13*(1), 114–129. doi:10.1109/TSC.2017.2694426

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys and Tutorials*.

Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, *102*, 902–911. doi:10.1016/j.future.2019.09.028

Weinberger, M. (2022). What is metaverse? A definition based on qualitative meta-synthesis. *Future Internet*, *14*(11), 310. doi:10.3390/fi14110310

Windley, P. J. (2005). *Digital Identity: Unmasking identity management architecture (IMA)*. O'Reilly Media, Inc.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. doi:10.1002/asi.20779

Xu, M., Ng, W. C., Lim, W. Y. B., Kang, J., Xiong, Z., Niyato, D., Yang, Q., Shen, X. S., & Miao, C. (2022). A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *IEEE Communications Surveys and Tutorials*.

Yuan, E., & Tong, J. (2005). Attributed based access control (abac) for web services. *IEEE International Conference on Web Services (ICWS'05)*. doi:10.1109/ICWS.2005.25

Zhang, N., Yao, L., Nenadic, A., Chin, J., Goble, C., Rector, A., Chadwick, D., Otenko, S., & Shi, Q. (2007). Achieving fine-grained access control in virtual organizations. *Concurrency and Computation*, *19*(9), 1333–1352. doi:10.1002/cpe.1099

Zhu, Y., Yu, R., Ma, D., & Chu, W. C.-C. (2019). Cryptographic attribute-based access control (abac) for secure decision making of dynamic policy with multiauthority attribute tokens. *IEEE Transactions on Reliability*, *68*(4), 1330–1346. doi:10.1109/TR.2019.2948713

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. doi:10.1016/j.future.2010.12.006

Alok Kumar is working as a Professor in the Department of Computer Science Engineering, at Sir Padampat Singhania University, Udaipur, India. He is also the Founder of Raccord IT Solutions, Jaipur, which is involved in advanced application and software development. Dr. Kumar has rich professional experience in Data Science Consulting, Developing Data Products, Big Data Implementation, Big Data Visualization, Data management and maintenance for Banking, Healthcare, Manufacturing, Scientific Research, and Data-Driven Marketing Sectors. He worked as a researcher at Ghent University, Belgium, and was involved in industrial consultancy. He was a post-doctoral researcher at the Department of Mathematical Engineering of Universite Catholique de Louvain, Belgium and associated with the "Large Graphs and Networks" research group and involved in an EU-FP7 FIRE Project "EULER" with Prof. Jean-Charles Delvenne and Prof. Vincent Blondel. Prior to that, he worked briefly at the Department of Computer Science and Engineering of the National Institute of Technology Patna, India as an Assistant Professor. He obtained PhD in Information Technology from the Indian Institute of Information Technology Allahabad, India in Internet architecture and IoT. He completed a Bachelor of Engineering in Information Technology from MBM Engineering College, Jai Narain Vyas University, Jodhpur, India, and a Master of Technology in Computer Engineering from the Center for Development of Advanced Computing, Noida, India. He has published several research articles in international journals and conferences of repute. Dr. Kumar delivered many technical talks at various prestigious academic and industrial events.

Kwok Tai Chui received the B.Eng. degree in electronic and communication engineering - Business Intelligence Minor and Ph.D. degree from City University of Hong Kong. He had industry experience as Senior Data Scientist in Internet of Things (IoT) company. He is an Assistant Professor at the School of Science and Technology, Hong Kong Metropolitan University. He was the recipient of 2nd Prize Award (Postgraduate Category) of 2014 IEEE Region 10 Student Paper Contest. Also, he received Best Paper Award in IEEE The International Conference on Consumer Electronics-China, in both 2014 and 2015. He has more than 100 research publications including edited books, book chapters, journal papers, and conference papers. His research interests include computational intelligence, data science, energy monitoring and management, intelligent transportation, smart metering, healthcare, machine learning algorithms and optimization.