Journal of Advances and Scholarly Researches in Allied Education
Vol. 21, Issue No. 7, October-2024, ISSN 2230-7540

DOI: https://doi.org/10.29070/9zdvqv35

Check for updates

Developing Effective Mitigation Strategies for Data Privacy in the Metaverse

B V N Prasad Paruchuri [1] * , Dr. Anoop Sharma [2]

1. Research Scholar, Department of Computer Science & Engineering, University of Technology, Jaipur, Rajasthan, India
bvnprasadparuchuri@gmail.com ,
2. Professor, Department of Computer Science & Engineering, University of Technology, Jaipur, Rajasthan, India

Abstract: As powerful head-mounted displays (HMDs) have become widely available, virtual reality (VR) has entered the mainstream and the concept Delivering fully immersive virtual reality adventures inside the Metaverse, a system that permanent and communal virtual world, has been proposed. Businesses are rushing to purchase virtual reality (VR) gear in the hopes of becoming early adopters and capitalizing on the industry's enthusiasm for VR and the Metaverse. Virtual reality (VR) applications and peripherals collect data, which raises unique privacy and security issues. Now that virtual reality head-mounted displays (HMDs) with intrusive sensors are available, it is more important than ever to include security and privacy considerations into the application development lifecycle to prevent the collection of sensitive biometric data, such as eye movements and facial expressions. As this case study shows, we assume that a tech company has lately turned its focus to the Metaverse, and that a group of cybersecurity specialists and programmers have been assigned the duty of creating new virtual reality apps for this company. This case study takes a page out of the development, security, and operations (DevSecOps) playbook by having participants think about how to build virtual reality (VR) applications securely, model potential threats, and implement privacy and security measures. By highlighting possible privacy and security concerns linked to this quickly developing technology, The findings of this study contribute to the existing literature on IS education. It also demonstrates how DevSecOps methods may deal with software development security challenges.

Keywords: Virtual reality, privacy, DevSecOps, threat modelling, metaverse

X

INTRODUCTION

A continuous digital domain that allows users to connect with virtual settings and interact via avatars or digital representations, The term "Metaverse" describes a future when the actual and virtual worlds combine. In its broadest sense, this idea incorporates a wide range of technologies, platforms, and uses, including AR, VR, MR, and 3D virtual worlds. Fixing issues with access control within the Metaverse is becoming more important as the ecosystem grows in popularity. Everything having to do with a system's or environment's entrance, permissions, and activities is part of the access control policy and system. Protecting the Metaverse's users' privacy, data, and interactions setting is the job of access control. With the advent of the Metaverse, a new age of virtual reality has begun, one in which people may engage in a wide variety of pursuits, from gaming to socialising to doing business, while simultaneously engaging in extensive virtual worlds and communicating with people in real-time. The Metaverse's access control concepts and processes examined in depth is required since, as this virtual world grows, it poses unique problems with access control.

An immersive virtual reality environment called the Cloud-based Metaverse is the target of this study's

examination of access control models and procedures. This study delves deeply into the unique features of the Metaverse, including its ever-changing structure, varied user base, communal areas, and the ramifications for security measures. Also covered in depth are the rules and guidelines that need be in place for efficient access control in a Metaverse hosted on the cloud. Included in these concepts are well-established notions like as least privilege, defense-in-depth, auditability/accountability, and role-based access control (RBAC). Access control in the complicated Metaverse relies on three pillars that the article stresses: availability, secrecy, and integrity.

LITERATURE REVIEW

Chen (2022) The metaverse is a hybrid cyberspace and living room that brings the idea of digitalizing and virtualizing the physical world to fruition. In an effort to map the actual world and beyond it incorporates a myriad of current technology. The future of metaverse is bright, and it will likely find numerous uses in many different contexts. As a number of associated technologies reach maturity, the Metaverse will be able to continue operating. Therefore, it's safe to say that the security concerns associated with building the Metaverse might be more significant and intricate. We go over a few technologies that are connected to the Metaverse and discuss some possible concerns with privacy and security in the Metaverse. Based on these technologies, we provide present-day solutions for privacy and security in the Metaverse. Furthermore, we also bring up certain open-ended questions about the prospective Metaverse. All things considered, this study examines the privacy and security concerns brought up by important technologies used in Metaverse applications in great detail. When it comes to the safety and confidentiality of Metaverse users' information, we are hoping that this poll can point researchers in the right direction and give some exciting new possibilities for the future of the Metaverse.

ZHAO (2023) Since its inception in the 1990s, the phrase "metaverse"—a virtual reality (VR) environment that mimics the actual world in three dimensions—has sparked endless speculation. Thanks to the ongoing development of several technologies, the metaverse has recently regained a great deal of interest as a potential reality. It may cause a great deal of good to happen to human society. including less prejudice, the eradication of individual distinctions, and more socialization. The metaverse is not immune to the usual worries about data privacy and security. First, we take a look at what the metaverse is and how it works. We think it's a VR ecosystem that's even better than the ones out there. Following a thorough examination of the four angles—user data, communication, scenario, and goods—we provide prospective solutions to the security and privacy issues that may arise. At the same time, we think the metaverse community has to use the new buckets effect to solve privacy and security issues holistically from a philosophical standpoint.

Parlar, Tuba. (2023) The metaverse is an idealized notion that bridges the gap between the real and virtual worlds. Concerns about user privacy and data security are rising to the surface as the Metaverse grows in popularity. As the number of users grows, so does the quantity of personally identifiable information gathered about them. Users' physiological reactions, facial expressions, voice tones, and vital qualities make up biometric information, which is a part of metaverse data. Data security and privacy are major issues with AI algorithms that use biometric data. The quantity, kind, and use of personally identifiable information that is gathered must be strictly limited. Wearable gear also opens up new avenues for the already-existent dangers in the virtual world to have a greater impact. The security procedures in

place for apps in the Metaverse are inadequate at the moment. This section introduces the concerns and risks associated with data privacy and security in Metaverse applications and then analyses the solutions that have been created to address these core issues.

Bhongade (2024) Many more cyber threats may emerge as a result of the Social Metaverse's unique architectural base. Encrypting and anonymizing user data is the bedrock of privacy protection in the metaverse. Within the Social Metaverse, users may freely exchange information and conduct commerce using these interoperable, decentralized networks. Phishing, data hacking, identity theft, ransomware, and virus assaults are social cyber hazards that the Social Metaverse is susceptible to. Servers, databases, the edge, the fog, and cloud computing platforms are all viable options for data storage in the metaverse. We spoke about the many uses and platforms of the social metaverse. Throughout the paper, we also make reference to possible future research areas. Not only is it an impressive piece of work in and of itself, but we also believe that we covered possible ways to lessen danger in the metaverse in our discussion of cyber threats in the social metaverse and mitigation techniques (PDF).

Pietro (2021) Numerous promising prospects exist in the metaverse for commerce, finance, and society as a whole. However, there are still many important factors that need to be thought about, and their potential effects have been little examined. Several contributions are included in this publication. Initially, we examine the metaverse's underlying principles; subsequently, we zero in on the unique privacy and security concerns brought about by this paradigm shift; and lastly, we expand the contribution's scope to emphasize the metaverse's far-reaching and logical implications across various domains, not limited to technology. We also cover potential future study paths throughout the report. We think that the offered comprehensive perspective on the metaverse's underpinnings, technologies, and problems with an emphasis on privacy and security could lead to some fascinating interdisciplinary study directions in addition to being an intriguing contribution in and of itself.

THE METAVERSE AND VIRTUAL REALITY TECHNOLOGY

Virtual reality A virtual reality (VR) environment is one that is computer-generated but otherwise looks and feels very much like the real thing. One example is VR. has been around since the 1960s, when it was mostly used for research purposes. The first VR applications were prototypes of VR gear and virtual settings. Interest in virtual reality was reignited in 2012 with the release of the Oculus Rift device via Kickstarter. Not only did the widespread availability The emergence of robust consumer-grade head-mounted displays (HMDs) has popularised virtual reality (VR), while advancements in the technology have also facilitated many applications for consumers and enterprises. From affordable smartphone accessories to advanced, tethered and untethered standalone devices models, customers have had their pick of a vast array of HMDs throughout the last decade, as shown in Figure 1.

Figure 1: Different Types of VR HMDs (Samsung Gear VR, Oculus Quest, and Valve Index)

Through head-mounted displays (HMDs) and other related accessories, modern virtual reality technology allows for a very immersive experience with a level of sensory reality that is objective (Slater, 2003). on-the-go screens, including HMDs and other related hardware are critical to the development of the Metaverse because they provide the sensory illusion of a real-world environment (Slater & Wilbur, 1997). When one is fully immersed in a virtual world, they feel more present, as described by Steuer (1992). Users are more prone to act realistically in virtual reality (VR) when their degrees of presence are high (Slater & Wilbur, 1997). Successful immersion requires the collection and use of invasive personal data, including using head-mounted displays and other peripherals, such as those for the eyes and the face.

Figure 2: Virtual Reality Peripherals (e.g., WorldViz, bHaptics, HP Reverb, and Manus)

Companies are aiming to further dissolve the distinctions between the physical and digital realms via the Metaverse, regardless of the fact that virtual reality has been used to create standalone applications. The Metaverse deviates from traditional app models by fusing VR with emerging technologies such as blockchain and nonfungible currencies. (NFTs) to create a shared and durable virtual realm (Dincelli & Yayla, 2022). Several sectors, including healthcare, education, retail, and travel, stand to benefit from the new disruptive organizational potential made possible by the Metaverse (French et al., 2020).

Threat Modeling in Software Development

To further improve security, DevSecOps teams may use threat modeling all the way through the development and operation cycles. Software architects may find security concerns early on and fix them via threat modeling. As an example, according to Shevchenko et al. (2018), One of the most comprehensive threat models is Microsoft's STRIDE model that can be found. DevSecOps teams are given an organized way to methodically evaluate and handle any security risks via STRIDE, which classifies threats into seven different types, as shown in Table 2. Teams that use DevSecOps may identify vulnerable areas in their software projects and implement safeguards while the project is still in the planning stages.

By concentrating on common software security threats during threat modeling, DevSecOps teams may make sure that strong security solutions are in place. One example is the Open Web Application Security Project (OWASP), which lists the ten most pressing web application security issues on a regular basis in an effort to bring attention to new dangers (OWASP, 2021). An invaluable resource for enterprises looking to address major security problems, As Glaisson and Welland (2014) point out, there is general agreement among OWASP members on the top ten security holes in web applications. Web app security as ranked by OWASP is shown in the third table. threats.

Table 1: NIST Secure Software Development Framework Practices (NIST, 2022)

Practices	Tasks
Prepare the organization	- Define security requirements - Implement roles and responsibilities - Implement supporting toolchains - Define and use criteria for security checks - Implement and maintain secure software development environments
Protect software	- Protect all forms of code from unauthorized access and tampering - Provide a mechanism for verifying software release integrity - Archive and protect each software release
Produce well-secured software	- Design software to meet security requirements and mitigate potential security risks - Review software design to ensure compliance with security requirements and risk information - Reuse existing, well-secured software when feasible instead of duplicating functionality - Create source code by adhering to secure coding practices - Configure the compilation, interpreter, and build processes to improve executable code - Review human-readable code to identify vulnerabilities and ensure compliance with security requirements - Conduct comprehensive testing on executable code to identify vulnerabilities and ensure compliance with security requirements - Establish secure default settings for software configuration
Respond to vulnerabilities	- Identify and confirm vulnerabilities on an ongoing basis - Assess, prioritize, and remediate vulnerabilities promptly - Analyze vulnerabilities to identify their root causes

Table 2. Threat Types and Descriptions from STRIDE

(used by Microsoft as of 2022)

Category	Description
Spoofing	Unauthorized access and use of a user's authentication credentials, such as username and password
Tampering	Malicious modification of data, such as unauthorized changes made to data within a database or network
Repudiation	Performing an action without other parties having any way to prove otherwise, such as performing unauthorized actions in a system that lacks the ability to trace operations
Information disclosure	Exposure of information to unauthorized individuals, such as reading a file without appropriate permissions
Denial of service	Denial of service to valid users, such as making a Web server temporarily unavailable
Elevation of privilege	Gaining increased privileged access, such as switching from a standard system user to an administrator level

Table 3: OWASP's 2021 Risk Assessment for Web Application Security

Rank	Web Application Security Risk
1	Broken Access Control
2	Cryptographic Failures
3	Injection
4	Insecure Design
5	Security Misconfiguration
6	Vulnerable and Outdated Components
7	Identification and Authentication Failures
8	Software and Data Integrity Failures
9	Security Logging and Monitoring Failures
10	Server-Side Request Forgery

Common Weakness Enumeration (CWE) issued a list of the 25 most critical software vulnerabilities that developers may use as a reference (CWE, 2021). Based on the most prevalent and serious mistakes that might cause software vulnerabilities, this list has been produced. These vulnerabilities are often simple to spot and exploit, giving hackers the opportunity to gain control of a system or access sensitive information. To rank vulnerabilities in order of severity, CWE uses a scoring methodology that gives each vulnerability a numerical score. Weaknesses in the CWE's software are listed in Table 4. Helping developers, administrators, and cybersecurity experts understand how to properly manage security threats, these lists provide crucial information. As said by Mahmood in 2021.

NIST Cybersecurity Framework

Of the United States Department of Commerce, NIST is an agency that does not regulate. The goal of the National Institute of Standards and Technology (NIST) is to increase American economic competitiveness and innovation via the creation and use of standards. The importance of cybersecurity in safeguarding the country's critical infrastructure led NIST to create the Framework for Cybersecurity (CSF) in 2014. By adhering to the CSF's optional criteria, organisations may enhance their comprehension, handling, and reduction of cybersecurity risks (NIST, 2018). Both big and small enterprises have embraced the redesigned framework as a recommended practice for cybersecurity readiness (Tracy, 2020).

As shown in Table 5, the CSF lays out five essential duties that, when followed, will ensure the availability, integrity, and confidentiality of information technology assets. A strategic perspective on cybersecurity threats is offered by a framework that consists of these five ongoing and simultaneous functions. In order to operationalize cybersecurity activities, the linked 23 categories and 110 subcategories provide a detailed perspective. It is recommended that organizations tackle all five functions at once and choose actions from the many categories and subcategories based on their unique cybersecurity requirements. The CSF does not prescribe the relative significance or sequence of tasks. Organizational cybersecurity risk management plans are already in place; this program only augments them (NIST, 2022).

Table 4: The most dangerous flaws in software (CWE, 2021).

Rank	Software Weakness
1	Out-of-bounds write
2	Improper neutralization of input during web page generation (“cross-site scripting”)
3	Out-of-bounds read
4	Improper input validation
5	Improper neutralization of special elements used in an OS command (“OS command injection”)
6	Improper neutralization of special elements used in an SQL command (“SQL injection”)
7	Use after free
8	Improper limitation of a pathname to a restricted directory (“path traversal”)
9	Cross-site request forgery (CSRF)
10	Unrestricted upload of file with dangerous type
11	Missing authentication for critical function
12	Integer overflow or wraparound
13	Deserialization of untrusted data
14	Improper authentication
15	NULL pointer dereferences
16	Use of hard-coded credentials
17	Improper restriction of operations within the bounds of a memory buffer
18	Missing authorization
19	Incorrect default permissions
20	Exposure of sensitive information to an unauthorized actor
21	Insufficiently protected credentials
22	Incorrect permission assignment for critical resource
23	Improper restriction of XML external entity reference
24	Server-side request forgery (SSRF)
25	Improper neutralization of special elements used in a command (“command injection”)

Framework for NIST Privacy

Security and privacy aren't the same thing, despite the common misconception to the contrary. Security aims to safeguard information technology assets, which may include personally identifiable information, whereas privacy concerns the gathering and application of such data. In the same way, there are two separate privacy concerns associated with data acquired by businesses and governments. To start, there is an abundance of personal data due to Social media use, data Digitisation, reliance on smart devices, and increased monitoring. In the last 20 years, businesses have discovered a plethora of methods to profit on this data. But privacy breaches have resulted from data exploitation (Wall et al., 2015), and businesses don't always realize the full scope of the privacy concerns when they acquire data. The effects of these infractions on individuals might include humiliation, prejudice, and monetary loss (NIST, 2020). One case in point is when Target inadvertently informed a parent that his pregnant teenage daughter had been exposed by the company's poor data management procedures (Duhigg, 2012). Organizations risk losing customers, damaging their brand, and incurring noncompliance costs as a consequence of privacy breaches caused by improper data processing or excessive data gathering (NIST, 2020).

Secondly, hackers would want to get their hands on the acquired data. Hacked data often includes sensitive personal information (PII) including protected health information (PHI), credit card details, and social security numbers. like medical records, insurance details, and payment information. Because of the severe consequences of private information theft, cybersecurity has become a mainstream concern after the 2013

and 2015 prominent data breaches at Anthem and Target, respectively, brought this issue to light. Personal information and health records are still the target of targeted assaults. Over three billion records were exposed the first six months of this year as a result of many data breaches (Winder, 2019). The number of persons impacted by healthcare data breaches peaked in 2021 with 250 million affected (Seh et al., 2020; Landi, 2022).

Organizations confront cybersecurity and privacy threats as seen in Figure 3. Concerns about privacy and cybersecurity are shown by the right and left circles, respectively. Security events that compromise keeping information private, intact, and readily available information technology assets are included in cybersecurity risk category (a). However, these occurrences (for example, a DoS attack assault on a website) do not compromise user privacy. Area (b), the intersection, encompasses the second privacy concern mentioned earlier: the threats to privacy that arise from cybersecurity events. As the Venn graphic demonstrates, not all threats to privacy fall within the purview of cybersecurity. What this means is that security can assist companies in protecting private information in area (b), but it won't solve the initial privacy challenge—the danger of domain (c) for data collecting and processing.

To assess how their systems, goods, and services affect users' privacy, businesses might refer to the National Institute of Standards and Technology's (NIST) recently published Privacy Framework (NIST, 2020). Although the framework's primary tasks are comparable to the CSF, they are developed with privacy in mind. The functions and their primary categories are summarized in Table 6.

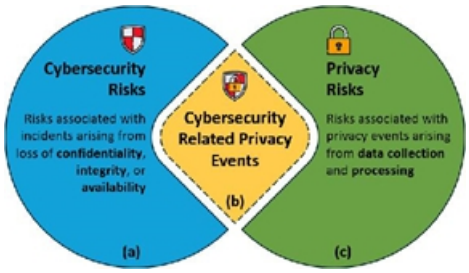

Figure 3: Cybersecurity and Privacy Risk Relationship (NIST, 2020)

CONCLUSIONS

Our research shows that the software development lifecycle would benefit greatly from the inclusion of cybersecurity professionals. To guarantee privacy and security standards and promote continuous development by identifying and monitoring related indicators over time, we present an interesting example that proposes using industry best practices and frameworks. With a focus on virtual reality (VR) and metaverse application development, this case study seeks to pique students' interest in DevSecOps and help them build their abilities in this area. This research offers valuable insights on securing user data and developing VR applications in the Metaverse in a secure and privacy-conscious manner by analyzing the relationship between new VR technologies, privacy, security, and DevSecOps.

References

1. Pietro, Roberto & Cresci, Stefano. (2021). Metaverse: Security and Privacy Issues. 10.1109/TPSISA52974.2021.00032.

2. Bhongade, Ashvini & Dargad, Sweta & Dixit, Asheesh & Mali, Yogesh & Kumari, Barkha & Shende, Ashwini. (2024). Cyber Threats in Social Metaverse and Mitigation Techniques. 10.1007/978-981-97-3690-4_34.

3. Parlar, Tuba. (2023). Data Privacy and Security in the Metaverse. 10.1007/978-981-99-4641-9_8.

4. ZHAO, Ruoyu & Zhang, Yushu & ZHU, Youwen & LAN, Rushi & Hua, Zhongyun. (2023). Metaverse: Security and Privacy ConcernsMetaverse: Security and Privacy Concerns. Journal of Metaverse. 3. 93-99. 10.57019/jmv.1286526.

5. Chen, Zefeng & Wu, Jiayang & Gan, Wensheng & Qi, Zhenlian. (2022). Metaverse Security and Privacy: An Overview. 2950-2959. 10.1109/BigData55660.2022.10021112.

6. 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

7. 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

8. 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

9. 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.

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