# Security and Privacy in Metaverse: Issues, Challenges, and Future Opportunities

**AARUSHI SETHI**
National Institute of Technology, Kurukshetra, India (e-mail: sethi.aarushi30@gmail.com)

**ABSTRACT** The advent of the metaverse, a three-dimensional virtual space that mimics the physical world and even surpasses it, with the realization of emerging technologies, has pushed for attention, investment and competition among Tech-giants such as Facebook, Tencent and Microsoft. This development has been concomitant of various jurisdictions conferring upon data, the right to be owned as property. The virtual environments have thus evolved parallelly as both incubators for innovation and breeding grounds for data theft and appropriation. The study of the impact of the Metaverse has, therefore, become paramount to understanding its foundation and evolution in relation to the paradigm it sets for the digital world and how that may manifest into novel security and privacy threats to its users and creators.

**KEYWORDS** Metaverse; security; privacy.

## I. INTRODUCTION

THE Metaverse [1] has come to represent a simulated, immersive environment that facilitates online interaction through Virtual Reality (VR) and Augmented Reality (AR) [2]technology. Virtual and physical spaces are enmeshed to create a hypothetically perpetual experience for its users. Its users create digital avatars that can then explore sub-metaverses, or different worlds created within the Metaverse. The immersive reality generated by the Metaverse helps users tune out the physical world for an artificial one, by creating convincing stimuli that elicit psychological and affective responses to the virtual environment. These worlds often transcend the limitations of the physical world through hyper spatiotemporality, drawing in users and increasing the diversity of experience simultaneously. However, like all technologies in a risk society, there is a flip side to the Metaverse. While it provides creative freedoms, it also has potential for misuse and subversion. This is because concomitant of the rights the Metaverse endows upon its users are some fundamental duties that make the virtual space safe and user-friendly. While most people are more than enthusiastic about exercising their own rights, when it comes to performing the parallel duties with relation to the rights of other users, they shirk off this responsibility. This, along with malicious avatars and hackers who are prone to using illegal means to obtain benefits, allow for a Metaverse that is less than conducive to its enjoyment by all its patrons. These threats [3] within and to the Metaverse are analyzed below. Solutions to the problems they pose are also examined for their efficacy and feasibility.

## II. SECURITY THREATS IN METAVERSE

### *THREAT TO ACCESS, AUTHENTICATION CONTROL AND NETWORKS*

To deliver VR services [4], service providers increasingly rely on devices that facilitate the creation of new data inputs. Biometrics and behavioral patterns feed into the system and create data whose rights may be denied to the user. The massive creation and flow of sensitive information in real time without clear demarcations of access, possession and ownership, may complicate not only the task of safeguarding this information but also identifying from where or whom threats to it may arise. As 'traditional' tools, techniques and methods to recognise and thereafter allocate access are outgrown, the exigency of this concern becomes obvious to the observer. The worst affected are the users who find their privacy breached [5] by methods like identity theft, impersonation attacks etc and their data in the hands of unrelated, often malevolent third parties. This leak of private, sensitive data can cause harm to not only the individual user, but also the bigger corporations and government bodies that may be involved in the supply of data. Once under the access of a malicious party, it is difficult to regain the access and control of a sub-metaverse and the compromised environment may act as an access point for other sub-metaverses. Hence, proper access and authentication must be ensured. Further, metaverse can be prone to malware attacks such as DDoS and sybil attacks which can compromise the network security of the system. Hence, robust security protocols must be established to counter and prevent such attacks.

### IMPACT ON USER GENERATED CONTENT

User Generated Content (UGC) [6] [7] or data created in the Metaverse and through the means to get access to the Metaverse can be manipulated, appropriated and corrupted, if an adequate security network is not invested in. The integrity of the data, if compromised, has deleterious effects on not just the user, but also the service provider. The data thus created may be forged, altered, tampered with and contextually worked in ways that may impact the functioning of the sub-metaverse, the avatar and the user's profile, among others. If the perpetrators remain undetected, the consequences may be compounded. In addition to the modification of existing data, one of the ways in which malicious parties may cause harm is through adding false inputs on their own. Metaverse systems can be misled using false messages and instructions [8]. Since the Metaverse transcends the geographical boundaries of states, implementing data protection laws will also be a hassle in case of such a breach. Additionally, Intellectual Property Rights within and for the sub-metaverses and other elements that comprise them will be harder to enforce than in the physical space. As digital economies gain prominence, this aspect especially will be under scrutiny as the opportunity cost analysis of measurement of IPR protection will determine the contraction, expansion or indifference towards such economies. Increasingly, there will be pressure on the regulators to ensure that not just the rights of the creators and sellers, but also those of the audience and buyers are preserved. This also means adapting the terms and scope of private law, such as in contracts, to suit the virtual world and adapt its functioning to intangible digital assets like Non-Fungible Tokens (NFTs) [9] [10] .

### PRIVACY THREATS

Pervasive data collection in the Metaverse is not limited to just the behavioral and biological aspects of user activity. Besides biometrics (including but not limited to retina, fingerprint, facial and speech features), XR and HCI technologies make physical tracking of the user feasible. The scope to use the Metaverse for political communication, and therefore political profiling and personally identifiable information, is wide. The structure, nature and content of not just individual interaction in and with the environment, but also the selection and creation of the environment itself can be used to analyze the psychology of its user. There is a wide berth to monitor public opinion through the Metaverse, where the digital footprint expands into a digital memoir of an individual's alternate life that very often reflects their actual one. Profiling, pattern detection and social engineering through the data extracted from digital avatars is not only a gross violation of an individual's privacy but also manipulates them into preferring alternatives that this data can then be used to condition them to pick. Even if the active agential role in profiling is minimized, privacy concerns still remain in the form of hacking and inefficiency in storing sensitive data centrally in cloud servers or edge devices. Such inefficiency is not limited to just one end of the process of virtual interactions. It is observed also in VR devices that get compromised and XR and HCI devices [11] that are manipulated to track physical movements, among others. Thus, as a passive enabler of breaches of privacy and confidentiality too, the Metaverse has compounded the problem of pitting someone's profit, through legal, illegal or extra-legal means against someone else's rights. Privacy leakage may occur at numerous stages during an end-to-end data transmission process starting right from data collection to data transfer from edge to centralized cloud and may be prevented by using encryption and distributed transmission techniques to minimize the threat.

### ECONOMIC THREATS

Needless to say, the current economic structures are largely regulating more tangible industries that deal with goods and services whose repercussions are felt in the physical world. To maneuver through the digital landscape, and to balance the needs of the user with an entrepreneurial atmosphere furthering innovation, the economy must be more flexible in terms of antitrust laws and ownership regulations etc. Asset identification through NFTs is a feasible solution to the issue of ownership however multiple other loopholes in the existing rules remain that allow malicious actors to manipulate the economy and tip the balance to an unfair state. The supply and demand status of certain elements especially, is vulnerable to strategic manipulation by avatars and users. This would also inflate or deflate prices depending on the status. Market forces will fall prey to the interests of such players. Free-riding is also an unintended outcome which creates externalities for the creators in the economy. Such externalities allow some users or avatars to exploit the Metaverse markets without compensating for such use and provide benefits to parties not directly involved in the process. The costs arising from such actions are borne by the creators or the service providers. The economic principle of abatement, if transposed to the digital context, may help bring down such externality to a socially acceptable level. The Coase Theorem [12], which grants property rights to avoid the overwhelming nature of negative externalities leading to property failure can be used by adapting it to the virtual systems. A transparent economy goes a long way in minimizing risks and by ensuring that collusive subversive elements are timely identified and neutralized, the economy can be protected from external manipulation that disrupts the normal flow of the forces of demand and supply.

### SOCIAL THREATS

One must acknowledge that the threats that exist within the Metaverse can leach into the physical world, if the adequate safeguards necessary for a safe user experience are not established. As mentioned above, XR and HCI devices can be corrupted and used to monitor the user's physical movements and also their location. The pervasiveness of GPS, for example, makes tracking someone's real time activity possible. Personal safety is also impacted by the potential to misuse the digital space to commit crimes that, though limited in physical injury, can damage one mentally. Reports of sexual abuse and harassment of online avatars have highlighted how online crimes can have great psychological impact on their victims. Cyberstalking, cyberbullying and other cybercrimes also happen to get heightened in the Metaverse. Problems of misinformation, false news and controversial opinions can also spread like wildfire in the digital space. While the digital environment has enough space to accommodate diversity of thoughts and users, it must align with the norms set up to regulate virtual simulations and interactions within them. While it seems like an easy criterion to meet, the overlap of jurisdictions and ambiguity in current regulations make conforming to the requirements difficult. The concentration or centralisation of governance, however, does not seem feasible, given the manner in which the Metaverse is evolving. The maintenance of 'law and order' within the Metaverse and a system of checks and balances for regulators via punishment and reward mechanisms is one way to resolve this quandary. An ethical design is necessary to achieve the same. Additionally, as and when crimes from the physical world get transposed into the virtual world, their magnitude and intensity has become a topic of legal debate. The gray area often eludes a solution, for to compare a crime committed online to one in person has been a controversial subject. This debate has outgrown its hypothetical nature, with cases of digital avatars being raped entering actual courts. These in turn require multiple jurisdictions to address the severity of punishment that can be meted to perpetrators. Since there has been very conservative policy intervention in VR, more engagement is necessary before a conclusive outcome to this problem can be developed.

## III. PREVENTION TECHNIQUES AND FRAMEWORKS

### ROBUST AUTHENTICATION SETUP

As discussed previously, authentication and access to the metaverse or sub-metaverse network [13] [14] needs to be secured in order to ensure security from malicious third parties. There are many methods through which the security of a metaverse network can be preserved. Firstly, it must be ensured that the wearable devices that are used to 'enter' or gain access to the metaverse have proper authentication steps. The authentication should be a multi-step process and must be a combination of biometric and keys for multi-factor authentication. The keys must be regularly rotated after a given span of time. Highly accurate AI systems like face and speech recognition should be built that can detect advanced physical infiltration and impersonation techniques such as using deep fakes and voice simulation.

### BUILDING SOLUTIONS FOR NETWORK ATTACKS

It is imperative that potential cyber attacks like Sybil and DDoS attacks [15] are kept in mind while designing the security protocols and firewalls of a metaverse subsystem. This can be done by integrating traditional antivirus softwares into the metaverse or by using novel machine learning techniques that not only detect and prevent malicious attacks, but also forecast it using the metaverse data trends after analyzing the User Generated Content or UGC. Virtual network functions can be established in virtual reality and can be controlled by an SDN.

### DECENTRALIZED FRAMEWORK

The management of the metaverse should be decentralized [16] [17], right from the authentication and access to the construction and connection of multiple client devices to a centralized network. This can also be incorporated with federated learning which can construct and train AI based metaverse models using federated learning that will increase the privacy of the generated data.

### ESTABLISHING PROTOCOLS

To ensure that there is ethical use and development of the metaverse, it is important that stricter laws and protocols are developed both in the real world and in the metaverse. For the real world IT laws, it should be ensured that the production of mentaverse is done ethically and cybercrimes such as data theft, data forging etc. are not committed. For the metaverse, there must be laws established within the metaverse that protect the users and the virtual 'avatars' as well.

## IV. CONCLUSION

In conclusion, the metaverse is a realm that is yet to be explored but it is not as far distant from reality as it once seemed. That established, it must be ensured that appropriate measures are taken to ensure that this virtual reality is safe, secure and protected. In this paper we discussed some of the major security threats to the metaverse and the possible solutions to it. Further, these solutions can be developed and integrated with each other and the metaverse.

## REFERENCES

[1] S. Mystakidis, "Metaverse," Encyclopedia, vol. 2, no. 1, pp. 486–497, 2022.

[2] R. T. Azuma, "A survey of augmented reality," Presence: teleoperators & virtual environments, vol. 6, no. 4, pp. 355–385, 1997.

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

[4] M. J. Schuemie, P. Van Der Straaten, M. Krijn, and C. A. Van Der Mast, "Research on presence in virtual reality: A survey," CyberPsychology & Behavior, vol. 4, no. 2, pp. 183–201, 2001.

[5] V. Nair, G. M. Garrido, and D. Song, "Exploring the unprecedented privacy risks of the metaverse," arXiv preprint arXiv:2207.13176, 2022.

[6] G. Lastowka, "User-generated content and virtual worlds," Vand. J. Ent. & Tech. L., vol. 10, p. 893, 2007.

[7] L. Evans, J. Frith, and M. Saker, "User generated worlds," in From Microverse to Metaverse. Emerald Publishing Limited, 2022, pp. 41–48.

[8] K. Plangger and C. L. Campbell, "Managing in an era of falsity: Falsity from the metaverse to fake news to fake endorsement to synthetic influence to false agendas," Business Horizons, 2022.

[9] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (nft): Overview, evaluation, opportunities and challenges," arXiv preprint arXiv:2105.07447, 2021.

[10] L. V. Kiong, Metaverse Made Easy: A Beginner's Guide to the Metaverse: Everything you need to know about Metaverse, NFT and GameFi. Liew Voon Kiong, 2022.

[11] Z. Tan, “Metaverse, hci, and its future,” in 2022 3rd International Conference on Mental Health, Education and Human Development (MHEHD 2022). Atlantis Press, 2022, pp. 897–901.

[12] J. Farrell, “Information and the coase theorem,” Journal of Economic Perspectives, vol. 1, no. 2, pp. 113–129, 1987.

[13] P. Kürtünlüoğlu, B. Akdik, and E. Karaarslan, “Security of virtual reality authentication methods in metaverse: An overview,” arXiv preprint arXiv:2209.06447, 2022.

[14] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, “Design of secure mutual authentication scheme for metaverse environments using blockchain,” IEEE Access, vol. 10, pp. 98 944–98 958, 2022.

[15] O. Analytica, “Metaverse adoption will multiply cybersecurity risks,” Emerald Expert Briefings, no. oxan-ga, 2022.

[16] S. Zeng, Z. Li, H. Yu, Z. Zhang, L. Luo, B. Li, and D. Niyato, “Hfedms: Heterogeneous federated learning with memorable data semantics in industrial metaverse,” arXiv preprint arXiv:2211.03300, 2022.

[17] J. Kang, D. Ye, J. Nie, J. Xiao, X. Deng, S. Wang, Z. Xiong, R. Yu, and D. Niyato, “Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal aoi,” in 2022 IEEE International Conference on Blockchain (Blockchain). IEEE, 2022, pp. 71–78.

• • •