Chapter 10
Metaverse Forensics:
A Preliminary Analysis of Opportunities and Challenges

Faouzi Kamoun

https://orcid.org/0000-0002-3740-1452
ESPRIT, Tunisia

Farkhund Iqbal
Zayed University, UAE

Siem Zeresenay
Zayed University, UAE

Zainab Khalid
National University of Sciences and Technology, Pakistan

Richard Ikuesan
https://orcid.org/0000-0001-7355-2314
Zayed University, UAE

Sened Abraham
Zayed University, UAE

ABSTRACT

The metaverse is poised to offer an immersive virtual environment for people to meet, socialize, collaborate, play, and conduct business transactions. Although the metaverse has not yet reached its full maturity, it has already been misused to launch illegal activities that can jeopardize the safety and well-being of individuals, and cause harm to organizations. Despite its increased importance, "metaverse forensics" remains an unexplored research topic. This chapter starts by reviewing the state-of-the-art research related to metaverse cybersecurity threats and underlying ethical, privacy, and legal issues. It then presents the results of a forensic investigation analysis performed on the VRChat and AltspaceVR metaverse platforms. The authors present new insights into metaverse forensics in terms of accessing digital containers and retrieving useful information for forensic investigators. Additionally, they highlight the primary obstacles encountered in metaverse digital forensic investigations and put forth recommendations for future research directions.

INTRODUCTION

The metaverse has brought major changes to the way we socialize and interact with each other. It has emerged as a potential new catalyst for innovation bringing a new breed of business models, products, and services into a rich marketplace. During the first ten months of 2021, the metaverse industry received over US$10 billion in venture capital funding (Kunthara, 2021). The public offering by Roblox at the beginning of 2021 signaled the beginning of a new wave of social engagements in the metaverse. In fact, many big events have been organized including birthday parties, concerts, egg hunt contests, and a tie-in with Gucci in celebration of its 100th anniversary, among many others (Garon, 2022). Snapchat's 3D bitmoji feature, introduced in July 2021, enabled users to create avatars for augmented reality, thus uplifting user experience (Garon, 2022). In October 2021, Facebook announced that it was changing its brand name to Meta and declared the metaverse to be the future of an embodied Internet where people will be inside rather than just looking at it (Mackenzie, 2022). This vision reflects a migration of the Internet from Web 2.0 towards Web 3.0 whereby the presence of a decentralized online platform allows users to own and control the assets they create. Microsoft envisages an "enterprise metaverse" where business gatherings and classrooms will take place in the form of immersive avatar-based online interactions. The metaverse offers a perpetual, persistent, and immersive multiuser virtual environment, enabling seamless embodied user interactions in real-time and dynamic trading of artificial artifacts (Mystakidis, 2022). With the premise of mixed reality, the metaverse is poised to perfectly blend the digital and the real worlds so that they become impossible to tell apart (Reid, 2021). As a massive aggregator of technologies, applications, and end-users, the metaverse is on the verge of acquiring the quality of a singleton, an attribute for a fast-emerging technological trend that, at a point in time, seems uncontrollable and irreversible, resulting in unforeseen social and legal ramifications (Di Pietro & Cresci, 2022).

The term metaverse was first introduced in 1992 in a Neal Stephenson novel titled – Snow Crash. Neal presented the metaverse as a Virtual Reality (VR) environment based on the Internet and Augmented Reality (AR), using avatars and software agents (Joshua, 2017). The novel was later portrayed in the science fiction movie Ready Player One (Sparkes, 2021). Today, the metaverse is depicted as an integrated immersive ecosystem from the modern Internet that uses VR headsets, haptic gloves and suits, AR glasses, blockchain technology, holograms, Brain-Computer Interface (BCI) technologies, and avatars to seamlessly bring together the physical and the virtual worlds, enabling people to interact through avatars in the context of 3D virtual shared experiences (Braud et al, 2021). What differentiates the metaverse from traditional online platforms is the immersive user experience where the boundary between the physical and the virtual world is blurred. In other words, the metaverse projects the physical person into a virtual avatar capable of interacting with other persons, embodied into avatars, in various forms of cooperative or competitive activities. Some popular Massively Multiplayer Online Role-Playing games (MMORPGs) such as Second Life (SL) are hosting more than 11 million residents (Leenes, 2007).

The metaverse has ignited innovative business models across diverse application domains such as retail, leisure and hospitality, gaming, tourism, health, education, luxury fashion, marketing, logistics, education, manufacturing, warehouse management, sport, fitness, military, and social networks. An increasing number of tech giants such as Facebook, Microsoft, Amazon, Snap Inc, and NVIDIA have already showcased, via huge investments and many acquisitions, their desire to conquer the world of the metaverse. The adoption and diffusion of metaverse services have also been facilitated by the integration of blockchain and virtual currencies, in addition to the decline in physical social activities during the covid-19 pandemic.

Related Content

Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking
Muhammad Abulaishand Nur Al Hasan Haldar (2018). *International Journal of Digital Crime and Forensics (pp. 95-119).*
www.irma-international.org/article/advances-in-digital-forensics-frameworks-and-tools/201538

The Dynamics of Social Engineering and Cybercrime in the Digital Age
Nabie Y. Contehand DeAngela "Dee" Sword (2021). *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 144-149).*
www.irma-international.org/chapter/the-dynamics-of-social-engineering-and-cybercrime-in-the-digital-age/282231

A Study on Embedding Efficiency of Matrix Encoding
Lifang Yu, Yun Q. Shi, Yao Zhao, Rongrong Niand Gang Cao (2013). *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security (pp. 92-102).*
www.irma-international.org/chapter/study-embedding-efficiency-matrix-encoding/75666

The Security Risks and Challenges of 5G Communications
Young B. Choiand Matthew E. Bunn (2021). *International Journal of Cyber Research and Education (pp. 46-53).*
www.irma-international.org/article/the-security-risks-and-challenges-of-5g-communications/281682

The Impact of Social Engineer Attack Phases on Improved Security Countermeasures: Social Engineer Involvement as Mediating Variable
Louay Karadsheh, Haroun Alryalat, Ja'far Alqatawna, Samer Fawaz Alhawariand Mufleh Amin AL Jarrah (2022). *International Journal of Digital Crime and Forensics (pp. 1-26).*
www.irma-international.org/article/the-impact-of-social-engineer-attack-phases-on-improved-security-countermeasures/286762