Chapter 20
Data Privacy in the Metaverse Ecosystem

Sibanjan Debeeprasad Das
https://orcid.org/0000-0002-2437-0482
Indian Institute of Management, Ranchi, India

Pradip Kumar Bala
Indian Institute of Management, Ranchi, India

Rajat Kumar Behera
KIIT University, India

ABSTRACT

This chapter introduces data privacy and its significance in the metaverse to the readers. It introduces several data privacy policies, privacy enhancing techniques (PET), and discusses some existing literatures on data privacy issues in the metaverse. This chapter seeks to educate readers on the various methods and technologies available to protect personal and sensitive data throughout the entire data lifecycle (collection, storage, use, and transmission). In addition, it discusses how these privacy-preserving techniques can be used to secure metaverse data and describes the most recent findings from studies conducted on the PET methods to improve these practices. The chapter also includes suggestions for additional research and development that will help readers take the first step toward enhancing data privacy techniques in the metaverse or incorporating existing technologies into privacy-enhancing metaverse applications.

INTRODUCTION

The metaverse which is a complex immersive 3D digital space with collapsed virtual and real realms, is set to become the next major evolution in the web (Dwivedi et al., 2022; Fernandez and Hui, 2022; Lee et al., 2021; Zhang et al., 2022). The potential application of such cross-platform physical-virtual reality interactions is huge and includes usage in such disciplines as education, healthcare, marketing, and tourism (Dwivedi et al., 2022). But despite the transformative nature of the continued evolution of the

DOI: 10.4018/978-1-6684-8851-5.ch020

metaverse and how it is set to positively impact people in their occupational, social, and leisure interaction, transforming, in the process, the way we conduct business, interact with ourselves and others. It is leading to develop shared experiences by the progressive blurring the gap between physical and digital world. However, this results in extensive data sharing, which raises fundamental privacy and security concerns that has attracted mounting scholarly and public policy scrutiny.

Fernandez and Hui (2022), for instance, discussed the challenges the metaverse faces in terms of security, privacy, and with regard to ethics and governance. The study also explored and provided arguably one of the most comprehensive explanation of the trends and approaches that connected virtual worlds are devising in their solutions and research pathways to enable a more safe, more inclusive, and more sustainable metaverse. It is noted that although extended reality (XR) gears (e.g., head-mounted displays or HMDs) provide users a more immersive, realistic, and superior metaverse experience, the devices capture vast amounts of information from users, including biometrical data. Most of this information is sensitive to both users and bystanders and can present a range of privacy, security, and even ethical problems. Fernandez and Hui (2022) argue as an example that head movement and eye tracking collected by HMDs can provide gaze data that give away the users' sexual preferences, thus putting the most personal or private aspects of our persona and psyche at risk.

Uberti (2022) echoed near-similar sentiments noting that as new meta-versa technologies gathers personal and intimate information at an increasingly granular level such as a person's eye movement, gait, voice, emotions, and other biometrics, the continued use of the immersive worlds in the metaverse will put greater strain on existing security safeguards, exposing people to a host and deadly privacy infringements. This is compounded by the seeming lack of controls in the metaverse, which by its very nature cannot be limited to a single or select data privacy regimes (e.g., the EU GDPR or California Consumer Privacy Act) given its global reach and use (Weingarden, 2022). In most instances, multiple legislations are applicable, and this raises the question about whether or not there is any data safeguard and privacy protection responsibility in the metaverse at all (Todd, 2022).

As we see, data privacy is a major concern in the metaverse. To deal with this problem, it requires a combination of clear regulations, secure storage and transfer solutions, user control and education, and responsible use of data by metaverse platforms. Protecting users' privacy in the metaverse's melting pot of regulatory regimes is thus critical. A number of studies (De Guzman, Thilakarathna, & Seneviratne, 2019; Lebeck et al., 2017) have proposed solutions for safeguarding users' privacy and ensuring their security in such scenarios. Some of these privacy-enhancing technologies (PETs) include intrinsic protection, data aggregation, protected rendering and sharing, and authentication. These PETs can collectively work to obfuscate any of the users' sensible or private data from the sensors before being uploaded or shared online (Fernandez & Hui, 2022). However, creating a tailored privacy policy is perhaps the most effective way of mitigating privacy and security concerns in the metaverse. Thus this chapter will delve into these details on the current challenges, current research and potential solutions related to data privacy in Metaverse.

Literature Review

World has been some high profile data privacy breach that had lead to serious consequences such as identity theft and financial frauds. Equifax, one of the largest credit reporting agencies in the US, suffered a data breach that exposed the personal information of 143 million consumers, including Social Security numbers, birth dates, and addresses (Gressin, 2017). Hackers stole credit and debit card information