Chapter 3
A Framework for Quantifying Privacy Risks in the 6G Metaverse: A Hybrid AI Attack

Qais Al-Na'amneh
http://orcid.org/0009-0008-3034-7693
Department of Cybersecurity and Cloud Computing, Faculty of Information Technology, Applied Science Private University, Amman, Jordan

ABSTRACT

The metaverse is being heralded as the next stage in the evolution of the internet and promises to provide every individual on Earth with a fully immersive digital reality. The emerging ecosystem, based on the advent of 6G networks and a host of enablers, will challenge existing trends in socialization and commerce, along with industry. However, with this ambition comes new and perhaps the most serious challenges for privacy in creating a universe that is persistent and rich in data. In this chapter, we propose an additional novel kind of hybrid AI-attack vector that synergizes with membership inference and reconstruction attacks, posing threats to user anonymity. The chapter will also look for counteractive measures with the feasibility of advanced cryptographic protocols, differential privacy, and federated learning architectures as the bedrock toward a trustworthy and secure metaverse. These findings express the urgent need for privacy-by-design to be the guiding principle of creating these new virtual worlds, rather than an afterthought.

DOI: 10.4018/979-8-2600-2313-6.ch003

INTRODUCTION

Digital is the edge of a paradigm shift; the line between the physical and the virtual worlds washes out. This is the metaverse, which previously existed only in fiction, and yet it is no longer fanciful; rather, it is the desired destination for making things become real by proving technology's worth in the modern age. It is not just a step forward in today's internet, but also a whole metamorphosis—a universal space that is virtually shared and created by the convergence of virtually enhanced physical reality and physically persistent virtual space, with the promise of multitudes of presence, multisensory full immersion real-time experiences to enable social connectivity, professional collaboration, educational endeavor, and fully-fledged digital economies (Tang et al., 2022).

Indeed, the completion of the 6th generation wireless networks hastens momentum towards reality. 5G is expected to boost mobile broadband and minimize latency, while it is expected that 6G will enable terahertz frequency communications, sub-millisecond latency, and AI integration at the edge of the network, its backbone, and enable this immersive internet. These are not luxuries, but a sine qua non for the outrageous data throughput and computational demands born out of hundreds of thousands of users interacting within high-fidelity, holographic environments simultaneously comprising all types of interrelations beyond the isolated application of the metaverse: Fabric of extended reality (XR), blockchain, cloud computing, and AI into a 6G high-capacity and low-latency backbone (Christopoulou et al., 2025).

But the sunny story of a technotopia soon turns to a darker, deeper story about the loss of privacy. Interestingly, the very vessel designed to bring the value proposition of the metaverse becomes a real panoptic on. Immersive experience demands in-depth, ceaseless collection and processing of highly personal data: more than just click-stream and click history, they encompass biometric cues related to subtle differences in eye gaze and facial expression, and inflections of voice; haptic response that gives an idea about one's physical responses; and precision motion capture tracking a user's virtual existence with sub-millimeter accuracy (Muhajjar & Shihabe, 2024). This data set is a digital representation of the self-high-resolution avatar of one's consciousness and corporeality. What could be imagined with the possibility of misuse, profiling, and manipulation?

The specter of these shadowy threats could be illustrated with a particular effect if a user enters a virtual meeting. The gaze-tracking data could be used not only to ascertain what they were looking at, but also whether they were engaged or distracted, which could then be used for performance evaluation. Later, while hanging out at a virtual lounge, their slightest physiological responses to advertisements could be gauged via subtle biometric cues and put together to create a psychological profile of the user for the purpose of hyper-targeted marketing. Once their gait and interaction