Chapter 10
Future Trends of Cryptography in Cyber Metaverse Security

Shuruq Khalid Abdulredha
http://orcid.org/0009-0003-3138-9426
Directorate Education of Babylon, Ministry of Education, Iraq

Hasanain Mohammed Manji Al-Rzoky
http://orcid.org/0000-0002-4841-2237
Directorate Education of Babylon, Ministry of Education, Iraq

ABSTRACT

The past twenty years have seen the emergence of the metaverse as an interactive virtual world that converges both the physical and virtual world through the digital transformation process. This chapter provides a methodical analysis of recent research on encryption techniques and information security in complex digital environments, especially in the metaverse and related technologies. Based on a review of several scholarly studies, the analysis compares current trends, highlights significant contributions, identifies security concerns, and suggests solutions. Furthermore, the analysis focuses on how advanced encryption, quantum computing-resistant technologies, and the integration of artificial intelligence can enhance privacy and data protection, all of which contribute to a comprehensive understanding of the current state of affairs and possible future directions of scientific research in this field. as well as provide solutions to enhance security in the metaverse.

DOI: 10.4018/979-8-2600-2313-6.ch010

INTRODUCTION

Encryption is a fundamental technical tool in the creation of a metaverse environment. This is because it protects the confidentiality of data, ensures secure identity, and allows for flexible methods of access into those environments. Although encryption can provide protection from many cybersecurity risks and threats. However, it does not provide complete protection for all cybersecurity risks and threats. Therefore, to obtain sufficient levels of security using encryption, it should be utilized in conjunction with other security tools. This will help to minimize the negative effects of performance, key management, and compatibility across multiple environments and networks (Thakur et al., 2023).

Encryption provides for data privacy and provides for integrity, to provide a foundation for cryptographic methods used for securing communications as well as protecting data found within metaverse environments (Zhai et al., 2024). In addition, effective encryption facilitates data-sharing mechanisms that protect privacy and user identity. Encryption has three major components: The first is secure channels that provide secure sessions and transmission encryption to protect real-time audio, video, and sensor data transmitted between users and servers, and mitigate the risk of eavesdropping and replay attacks (Thakur et al., 2023; Zhai et al., 2024). The second is protecting data at rest during idle time, by encrypting the storage of user profiles or other medical or educational content on platforms or storage nodes, thereby limiting unauthorized disclosures if a platform or storage node becomes compromised (Huang et al., 2023). The third component of encryption is its use in providing access control, by utilizing cryptographic keys and schemes to support fine-grained access, such as attribute-based policies and selective attribute disclosure within shared virtual environments (Huang et al., 2023; Liu et al., 2025).

Although encryption protects against data breaches and some forms of data leak, eavesdropping, and unauthorized access to an asset, etc., it only covers the smallest part of the larger threat model, including identity theft, social engineering, and platform vulnerabilities. In addition, studies have shown that encryption can provide confidentiality and selective sharing of data; however, it will only be effective if paired with authentication mechanisms and policy enforcement to protect against identity theft and misuse of access to the encrypted data (Alnuaimi & Alawida, 2024; Huang et al., 2023). However, despite these advantages, there are limits to how much protection that encryption provides. Encryption does not protect against impersonating another user, compromising the endpoint through malware or other means, attacking users based upon the information they send as metadata, and/or tracking the behavior of users, unless it is combined with additional layers of security measures (Bhaskar et al., 2024; Sonkamble et al., 2025).