Cyber Threats and Safeguarding Strategies in Metaverse Libraries: A Systematic Review

Bolaji David Oladokun
https://orcid.org/0000-0002-7826-9187
Federal University of Technology, Ikot Abasi, Nigeria

Ebiere Diana Orubebe
https://orcid.org/0009-0003-1491-7098
Rivers State University, Nigeria

Yusuf Ayodeji Ajani
https://orcid.org/0000-0002-2786-4461
Al-Hikmah University, Ilorin, Nigeria
trustusouph@gmail.com

Yinka Martins Omoniyi
https://orcid.org/0009-0004-4450-1429
Federal University, Lokoja, Nigeria

Edidiong Nyong Ben
https://orcid.org/0009-0008-2933-4203
Federal University of Technology, Ikot Abasi, Nigeria

Abstract

The study explores cyber threats in metaverse libraries, focusing on the challenges these institutions face as they integrate immersive technologies into their services. The rationale for this study stems from the increasing popularity of the metaverse across various sectors, including libraries, where it enhances user engagement through immersive experiences. However, the integration of these technologies introduces new vulnerabilities that necessitate robust cybersecurity measures. The study employed a systematic review methodology, sourcing relevant literature from Scopus, Web of Science, and Google Scholar published between 2020 and 2024. The findings were categorised into three main themes: the conceptual framework of cybersecurity in the metaverse, cyber threats specific to metaverse libraries, and potential cybersecurity strategies. The findings reveal significant risks for metaverse libraries, particularly concerning data privacy, avatar impersonation, intellectual property theft, and the security of virtual interactions. The study also underscores the need for compliance with global data protection regulations and for libraries to establish transparent privacy policies.

Keywords: cyber threats; data protection; identity theft; metaverse libraries; virtual environments

https://doi.org/10.25159/3005-4222/17806
ISSN 3005-4222 (Online)

Introduction

The rapid evolution of digital technologies has led to the emergence of immersive environments, with the metaverse being one of the most significant developments. The metaverse refers to a virtual space where users can interact with digital environments and with one another in real time, using avatars and technologies such as augmented reality (AR), virtual reality (VR), and other immersive tools (Dionisio et al. 2013; Dwivedi et al. 2022). This convergence of the physical and digital worlds presents unprecedented opportunities for communication, learning, and information sharing. As institutions traditionally responsible for information dissemination and knowledge sharing, libraries are now exploring ways to integrate the metaverse into their services to create dynamic, immersive, and personalised user experiences (Ajani et al. 2024). By doing so, libraries aim to transcend the limitations of traditional digital platforms and offer more engaging and interactive experiences for users.

The integration of the metaverse into library services represents a shift from static digital resources to fully interactive and immersive environments (Subaveerapandiyan et al. 2024). In these virtual spaces, users can not only access digital books, journals, and other materials but also attend events, collaborate with peers, and interact with librarians in real time, as if they were physically present in the same space. Libraries have already been experimenting with virtual environments, such as VR tours of library spaces, online research consultations, and virtual exhibits, as ways to extend their services beyond physical boundaries (Noh 2015). With the rise of the metaverse, these experiences are expected to become even more interactive and engaging, further transforming how users engage with library collections and resources.

Currently, digital libraries rely on online tools and platforms to provide access to e-books, e-journals, and research databases (Verma and Dwivedi 2023). Meanwhile, virtual environments are becoming essential for distance learning and collaboration, with platforms like online classrooms and webinars already widely used (Childs et al. 2023). Ng (2022) argues that the introduction of metaverse libraries takes these trends a step further by offering users a more immersive and interactive space to engage with content. In these virtual environments, users can explore and interact with resources in ways that replicate real world experiences, but with the added benefits of digital enhancements. These trends highlight the growing acceptance of technology as a tool to enhance access to information and foster collaboration. However, this integration also presents significant challenges, particularly in the realm of cybersecurity.

While the potential of metaverse libraries is undeniable, the integration of metaverse technologies introduces unique and significant cyber threats. Pooyandeh et al. (2022) note that cybersecurity in metaverse libraries must safeguard not only the virtual world's infrastructure but also the personal data of users interacting within these environments. In the metaverse, users often share vast amounts of personal information, including their preferences, behaviours, and, in some cases, even biometric data. This creates new vulnerabilities that cybercriminals can exploit, leading to risks such as identity theft

through avatar impersonation, data breaches within virtual spaces, and unauthorised access to sensitive information.

The need for robust cybersecurity measures in metaverse libraries cannot be overstated. As libraries adopt digital and virtual services, they are responsible for safeguarding users' data and ensuring the security of information accessed within the metaverse. In a space where users engage in real time interactions and collaborate across vast digital networks, the risk of security breaches is amplified. Personal data, intellectual property, and library resources become vulnerable to malicious attacks if cybersecurity is not prioritised (Dawson et al. 2014). Moreover, the immersive nature of the metaverse can make users less aware of the cyber threats they may face, increasing their susceptibility to attacks. This highlights the urgent need for libraries to implement advanced cybersecurity protocols to protect both users and digital assets. Despite the growing interest in the metaverse, there is limited peer-reviewed empirical research specifically addressing cybersecurity in metaverse libraries (Ajani et al. 2024; Gao et al. 2024; Oladokun et al. 2023a; Subaveerapandiyan et al. 2024). While cyber threats in digital environments have been extensively explored in fields such as computer science, information security, and digital literacy, a significant research gap remains in examining these issues within the context of metaverse libraries. This article bridges that gap by synthesising insights from these diverse fields to provide a comprehensive overview of cybersecurity concerns unique to metaverse libraries, including potential threats, vulnerabilities, and strategies for safeguarding user data and digital resources.

Purpose of the Study

The purpose of this article is to explore the cyber threats faced by metaverse libraries. This article sheds light on the risks that libraries face as they integrate immersive technologies into their services. The following subtopics were reviewed:

1. Examine the cybersecurity framework in the metaverse

2. Determine cyber threats in metaverse libraries

3. Explore cybersecurity strategies for metaverse libraries

Literature Review

Cybersecurity Framework in the Metaverse

The rise of the metaverse marks a significant shift in how digital spaces are used for interaction, learning, and service delivery. The metaverse transcends the limitations of the physical world by offering immersive virtual environments where users can interact, communicate, and collaborate. Its adoption in libraries represents an innovative leap in information service delivery, providing users with an engaging space to access, explore, and interact with both traditional and digital resources in real time (Oladokun and

Gaitanou 2024). However, this shift also introduces critical cybersecurity concerns, as the metaverse becomes a vast network of interconnected digital assets, personal data, and user activities that are increasingly vulnerable to cyber-attacks.

The metaverse is a collective virtual space that merges digital and physical realities through immersive technologies such as virtual reality (VR), augmented reality (AR), and 3D simulations (Kye et al. 2021). Unlike traditional digital environments with limited user interactivity, the metaverse offers dynamic, immersive, and interconnected experiences (Oladokun et al. 2023a). In this virtual world, users interact with digital objects, avatars, and environments as if they were engaging with the physical world. This immersive interaction is made possible by advanced hardware (e.g., VR headsets, haptic devices) and software systems that simulate physical presence, enabling users to perform tasks and activities within a 3D environment. In the context of libraries, these features of the metaverse present exciting opportunities to enhance user engagement with and access to resources (Oladokun et al. 2023a). However, the defining characteristics of the metaverse—immersion, real-time interaction, and personalisation—also introduce significant cybersecurity challenges. The use of avatars to represent users raises concerns about identity theft and impersonation (Oladokun and Gaitanou 2023). Cybercriminals may exploit these vulnerabilities to manipulate digital identities, steal personal data, or gain unauthorised access to sensitive information stored in metaverse libraries. Thus, understanding the key features of the metaverse is crucial for identifying the cybersecurity risks that libraries may face as they adopt this technology.

Cybersecurity, the practice of protecting digital systems, networks, and data from unauthorised access, attacks, and damage, becomes increasingly critical in this context (Fadziso et al. 2023).

In the context of digital spaces such as the metaverse, cybersecurity encompasses a range of measures aimed at safeguarding user information, securing communication channels, and ensuring the integrity of digital assets (Borky and Bradley 2019). Foundational cybersecurity principles—confidentiality, integrity, and availability (commonly known as the CIA triad)—serve as the basis for most cybersecurity frameworks (Samonas and Coss 2014). The cybersecurity principles are outlined below:

1. Confidentiality refers to the protection of sensitive information from unauthorised access (Singh et al. 2014). In metaverse libraries, this might involve ensuring that users' personal information, such as their log-in credentials, reading preferences, and interaction history, is kept secure from external threats. Given that users in the metaverse generate significant amounts of data as they interact with the environment, maintaining confidentiality is crucial to prevent data breaches.

2. Integrity involves ensuring that digital information remains accurate, consistent, and free from unauthorised alteration (Harley and Cooper 2021). In a metaverse

library, this means protecting the integrity of both the digital collections and the user-generated data. For example, a hacker could tamper with virtual books and resources, or even modify interactions within a virtual learning space, compromising the quality and trustworthiness of the information provided by the library.

3. Availability ensures that systems, data, and services are accessible when needed (Kang et al. 2014). For libraries in the metaverse, this means guaranteeing that users can access library resources, virtual environments, and services without disruption. Cyberattacks, such as distributed denial-of-service (DDoS) attacks, can threaten the availability of these services, rendering a metaverse library temporarily or permanently inaccessible.

In addition to the CIA triad, other key cybersecurity concepts such as encryption, user authentication, and secure communication protocols play a vital role in safeguarding metaverse environments (Kaur et al. 2023). Encryption is the process of encoding data so that only authorised parties can access it. In metaverse libraries, encryption ensures that data transferred between users and the library system remains confidential and secure, even if intercepted by malicious actors. User authentication also refers to the process of verifying the identity of a user before granting access to a system or service (Olabanji et al. 2024). In a metaverse library, advanced authentication methods, such as multifactor authentication (MFA) or biometric verification, can help prevent unauthorised access to user accounts (Sharma et al. 2024). Finally, secure communication protocols ensure that data transmitted across the network is protected from interception or tampering by hackers.

The integration of metaverse technology into library services offers a wealth of opportunities for expanding access to information, improving user engagement, and enhancing the overall library experience. Tella et al. (2023) state that one of the primary opportunities presented by metaverse libraries is the ability to create highly immersive and interactive learning environments. Unlike traditional digital libraries, which offer limited user interaction, metaverse libraries provide users with a rich, 3D virtual space where they can explore, manipulate, and engage with digital resources in real time. Metaverse libraries also have the potential to make information services more accessible and inclusive. Libraries can reach a wider audience, including users who may face physical, geographical, or socio-economic barriers to accessing traditional library services. For instance, individuals with disabilities can benefit from customisable avatars, personalised navigation tools, and accessible content that accommodates their needs in the virtual environment.

Despite these exciting opportunities, the metaverse also introduces several cybersecurity challenges that libraries must contend with. One of the most significant challenges is the protection of user privacy and data security. As users interact with metaverse libraries, they generate vast amounts of personal data, including behavioural

data, biometric data (if using AR/VR technologies), and interaction histories (Saxena et al. 2023, 3). Cybercriminals can exploit vulnerabilities in the system to steal sensitive information or impersonate users in the virtual environment. Another challenge is the potential for identity theft and avatar impersonation in the metaverse (Awadallah et al. 2024). Users in the metaverse are represented by avatars, which can be customised to reflect their identities. However, if an unauthorised person gains access to a user's avatar, they can impersonate the user, potentially leading to malicious actions, such as spreading misinformation or gaining access to sensitive information.

Additionally, libraries must address the risk of intellectual property theft in metaverse environments (Longshak et al. 2023). Digital content and resources, including books, research papers, and multimedia materials, are often subject to intellectual property laws. In a metaverse library, unauthorised users may attempt to copy or distribute these materials without proper attribution or permission (Khalaf 2025). Libraries must implement digital rights management (DRM) technologies and copyright protection measures to prevent the unauthorised use and distribution of their collections. Lastly, ensuring the availability and reliability of library services in the metaverse is a key concern. Zainuddin et al. (2024) observe that cyberattacks, such as DDoS attacks, can disrupt the functionality of metaverse libraries, rendering them inaccessible to users. Libraries must invest in robust cybersecurity infrastructure, including firewalls, intrusion detection systems, and disaster recovery plans to ensure that their services remain available and functional, even in the face of cyber threats.

Cyber Threats in Metaverse Libraries

As metaverse libraries become an integral part of the digital landscape, offering immersive and interactive environments for accessing and engaging with library resources, they also introduce significant cybersecurity risks. These threats stem from the complex and interconnected nature of the metaverse, where users interact with both digital content and other users in real time. The challenges to ensuring cybersecurity in this environment are multifaceted, ranging from data privacy and identity theft to phishing, malware, and hacking.

One of the most pressing cybersecurity concerns in metaverse libraries is data privacy (Saracoglu 2023). Wang et al. (2023) indicate that users in the metaverse generate vast amounts of personal information as they navigate virtual spaces, interact with digital objects, and communicate with other users. This data includes not only traditional personal identifiers, such as usernames, passwords, and contact information, but also behavioural data, biometric data (in cases of VR/AR), and interaction histories. The immersive nature of the metaverse means that users are constantly producing data that can be analysed and exploited if not properly secured. Data privacy in metaverse libraries becomes a critical issue when considering how personal information is stored, shared, and potentially misused by malicious actors (Sharma et al. 2024). A data breach in a metaverse library could expose users' personal details, including their reading habits, virtual activities, and even sensitive biometric data collected by AR/VR devices.

Hackers could use this data for identity theft, creating fraudulent accounts or manipulating users' virtual identities. In the metaverse, identity theft takes on a new dimension, as users are represented by avatars that can be impersonated by cybercriminals if access is gained to their accounts. If an unauthorised person assumes control of a user's avatar, they could engage in activities that harm the user's reputation, steal valuable data, or deceive others within the metaverse environment (Oladokun and Gaitonou 2024).

In addition to the foregoing, phishing, malware, and hacking remain significant cybersecurity threats in the metaverse. Phishing attacks involve cybercriminals sending deceptive messages designed to trick users into revealing sensitive information, such as log-in credentials or financial details (Nyasvisvo and Chigada 2023). In the metaverse, phishing can take on new forms, such as fraudulent avatars or virtual objects that appear to be legitimate but are designed to deceive users into sharing personal data. For example, a hacker might create a fake avatar that impersonates a library staff member and asks users to provide their login information or other sensitive details.

Malware is another critical threat, as malicious software can be embedded in virtual objects or digital content within the metaverse (Vondráček et al. 2023). Users who interact with infected objects may unknowingly download malware that compromises their personal devices, steals data, or gains unauthorised access to their accounts. Malware can also spread through virtual spaces, affecting multiple users and systems within the metaverse library. Hacking, on the other hand, involves unauthorised access to the metaverse library's servers or databases, potentially allowing cybercriminals to manipulate or steal data, disrupt services, or cause widespread damage to the virtual infrastructure (Elshenraki 2023, 15). With users interacting through avatars, there is a heightened risk of unauthorised access if authentication protocols are weak or easily circumvented. In a metaverse library, user authentication refers to the process of verifying a user's identity before granting access to the virtual space or specific digital resources. This further implies that traditional password-based systems are often inadequate in securing metaverse environments, as cybercriminals can easily exploit weak passwords or use social engineering tactics to gain access to user accounts.

In addition to personal data, metaverse libraries house a wealth of digital content, including books, research papers, multimedia materials, and other intellectual property (Oladokun et al. 2023b). This is to say protecting this content from unauthorised use and distribution is another significant cybersecurity challenge. In the metaverse, users can easily replicate, modify, or share digital resources without proper attribution or permission, leading to copyright infringement and intellectual property theft.

Cybersecurity Strategies for Metaverse Libraries

The integration of metaverse technologies into library services marks a significant shift in how users engage with information and digital content. Data protection and privacy are central to the cybersecurity framework of metaverse libraries, where users generate

vast amounts of personal and interaction data (Fiaz et al. 2023). One of the primary measures for enhancing data protection in metaverse libraries is the use of encryption technologies. In addition to encryption, libraries must adopt comprehensive privacy policies that clearly outline how user data is collected, stored, and used within the metaverse environment. Transparency is key to fostering trust among users, who may be concerned about how their data is handled in virtual spaces. These policies should comply with global data protection regulations, such as the General Data Protection Regulation (GDPR) and local privacy laws, ensuring that libraries adhere to legal standards for data protection.

One of the most effective strategies for preventing cybersecurity threats in metaverse libraries is empowering users with the knowledge and tools to protect themselves (Sharma et al. 2024). User education and awareness campaigns play a crucial role in helping library patrons recognise potential risks and take proactive steps to safeguard their virtual identities and personal information. Metaverse libraries must invest in creating comprehensive cybersecurity training programmes tailored to their user base. These programmes should cover common cybersecurity threats, such as phishing, malware, and identity theft, as well as best practices for navigating virtual environments securely. In addition to formal training programmes, libraries can use digital signage and virtual tutorials within the metaverse to remind users of key security practices. Interactive workshops, webinars, and gamified learning experiences can also engage users in a more immersive and enjoyable way, making it easier to grasp complex cybersecurity concepts.

User authentication is a critical element in ensuring the security of metaverse libraries, where users interact through avatars and access a wide range of digital resources (Sharma et al. 2024). Traditional password-based authentication methods are often inadequate for the metaverse, as they can be easily compromised through weak passwords, social engineering, or brute-force attacks. MFA is one of the most effective authentication strategies for metaverse environments (Hasan et al. 2024). MFA requires users to provide multiple forms of verification, such as something they know (a password), something they have (a one-time code sent to their phone), or something they are (biometric data). By combining these factors, libraries can significantly reduce the risk of unauthorised access, even if a user's password is compromised. For instance, a user attempting to log in to a metaverse library would need to enter their password and then verify their identity through a second method, such as a fingerprint scan or a code sent to their mobile device.

Biometric authentication, including fingerprint recognition, facial recognition, and even voice authentication, can provide an additional layer of security in metaverse libraries (Kuru and Kuru 2024). Biometric data are unique to each user, making it more difficult for hackers to replicate or bypass. However, metaverse libraries must implement biometric authentication responsibly, ensuring that biometric data are securely stored and processed to prevent misuse. In addition to MFA and biometrics, libraries can

employ behaviour-based authentication, which uses machine learning algorithms to analyse user behaviour and detect anomalies (Folino et al. 2023). For example, if a user's avatar begins to exhibit unusual behaviours, such as logging in from an unfamiliar location or engaging in activities inconsistent with their usual patterns, the system can flag the account for review and require additional authentication before allowing access. This dynamic approach to authentication enhances security by adapting to changes in user behaviour and detecting potential threats in real time.

Methodological Approach

Given the evolving nature of metaverse technologies and the relatively nascent stage of their integration into library services, a systematic review approach is the most suitable method for exploring cyber threats in this context. Therefore, this study applied a systematic review approach to explore cyber threats in metaverse libraries. Relevant literature was sourced from the Scopus, Web of Science, and Google Scholar databases. Scopus and Web of Science were chosen because they are highly reputable databases that offer access to peer-reviewed articles, ensuring the quality and credibility of the sources. Google Scholar was included to broaden the search and capture grey literature and emerging research that might not yet be indexed in the other databases. Articles published between 2020 and 2024 were considered to ensure the inclusion of up-to-date studies, given the rapid advancements in metaverse technologies. Keywords such as "metaverse libraries," "cybersecurity threats," "virtual reality," and "data privacy" were used to filter the most relevant literature. Following the search, duplicates were removed, and only peer-reviewed articles directly addressing cybersecurity in metaverse environments, particularly within libraries, were selected. Thematic analysis was employed to analyse the literature. This involved coding the data and categorising it into themes based on the three research objectives: the conceptual framework of cybersecurity in the metaverse, cybersecurity threats in metaverse libraries, and cybersecurity strategies for metaverse libraries. This approach enabled the identification of patterns and key themes related to cybersecurity concerns, risks, and mitigation strategies.

Discussion of the Findings

Cybersecurity Framework in the Metaverse

The conceptual framework of cybersecurity in the metaverse highlights the growing integration of immersive digital environments with real world applications, particularly in libraries. The metaverse, defined by technologies such as virtual reality (VR) and augmented reality (AR), offers libraries dynamic, interactive spaces where users can access digital resources in a virtual, 3D setting (Oladokun et al. 2023a). While this presents opportunities for improved access and user engagement, it introduces significant cybersecurity challenges. These challenges stem from the immersive nature of the metaverse, where users' digital identities, personal data, and interactions become

vulnerable to cyberattacks. A critical aspect of cybersecurity in the metaverse is the CIA triad: confidentiality, integrity, and availability. Confidentiality ensures the protection of sensitive user data such as login credentials and interaction histories (Singh et al. 2014). Integrity protects digital collections and user-generated content from unauthorised modification, ensuring the reliability of the resources within the metaverse (Harley and Cooper 2021). Availability focuses on keeping library services accessible without disruption, even in the face of cyber threats such as distributed denial-of-service (DDoS) attacks (Kang et al. 2014).

In addition to the CIA triad, concepts like encryption, user authentication, and secure communication protocols are vital to safeguarding metaverse environments. Encryption ensures that data transmitted between users and systems remains secure (Kaur et al. 2023), while advanced authentication methods, such as multi-factor authentication (MFA), prevent unauthorised access to user accounts (Olabanji et al. 2024). These measures are crucial for maintaining the security of the metaverse, where users' avatars and identities could be impersonated by malicious actors.

Cyber Threats in Metaverse Libraries

The study explored a range of complex challenges that emerge from the nature of immersive virtual environments. One of the foremost concerns is data privacy, as users in the metaverse generate significant personal data, including behavioural and biometric information, which cybercriminals can exploit if not adequately secured (Saracoglu 2023). Wang et al. (2023) stress that the collection of such data introduces a heightened risk of privacy breaches, making personal information vulnerable to theft, fraud, and unauthorised manipulation. Data breaches may expose users' virtual activities and even sensitive biometric data collected by AR/VR devices, leading to identity theft (Sharma et al. 2024). In the metaverse, identity theft is particularly concerning, as users are represented by avatars which can be impersonated, leading to reputational harm and data exploitation (Oladokun and Gaitonou 2024). Additionally, phishing, malware, and hacking pose significant threats to the security of metaverse libraries. Nyasvisvo and Chigada (2023) point out that phishing in the metaverse can take the form of deceptive avatars or virtual objects, tricking users into revealing sensitive information. Malware can be embedded in virtual objects or digital content, spreading through virtual spaces and affecting multiple users and systems (Vondráček et al. 2023). Hacking further compounds these risks, as cybercriminals may gain unauthorised access to servers or databases, allowing them to steal data or disrupt services (Fnraki 2023).

Cybersecurity Strategies for Metaverse Libraries

The findings on cybersecurity strategies for metaverse libraries highlight the importance of safeguarding user data and ensuring secure access to virtual environments. A key strategy is the use of encryption to protect personal and interaction data, ensuring that information is securely transmitted and stored (Fiaz et al. 2023). Comprehensive privacy policies that comply with regulations like GDPR are essential for fostering transparency

and user trust. These policies clarify how data is collected, stored, and shared, offering a legal framework for data protection. User education is another critical component of cybersecurity in metaverse libraries. Training programmes that inform users about common threats, such as phishing and malware, empower them to take proactive measures (Sharma et al. 2024). Interactive learning experiences, like workshops and gamified tutorials, can help users grasp complex cybersecurity concepts more effectively. MFA is emphasised as an effective method for preventing unauthorised access, requiring users to provide multiple forms of verification (Hasan et al. 2024). Biometric authentication, including fingerprint and facial recognition, adds an extra layer of security but must be implemented responsibly to protect sensitive biometric data (Kuru and Kuru 2024). Additionally, behaviour-based authentication, which detects anomalies in user behaviour, offers dynamic protection against potential security breaches (Folino et al. 2023).

Implications of the Study

The findings of this study have important implications for both policy and practice. In terms of policy implications, libraries must establish clear policies on data protection and privacy, aligning with global regulations. These policies should outline how user data is collected, stored, and utilised in the metaverse environment. Additionally, libraries must adopt cybersecurity frameworks that prioritise secure user authentication and access control, while ensuring compliance with intellectual property laws. In practice, libraries should implement advanced security measures, including MFA, encryption, and behavioural authentication systems. Continuous user education programmes are crucial for promoting a cybersecurity-aware culture within the metaverse. Moreover, collaboration with cybersecurity professionals can aid in developing standardised protocols and response strategies to mitigate potential threats.

Conclusion

The study established that cyber threats are fundamental and cannot be undermined in this era of the Fourth Industrial Revolution. As a result, this article has explored key cyber threats in metaverse libraries, focusing on the protection of user data, safeguarding digital content, and preventing cyberattacks. Among the most pressing threats are data privacy breaches, identity theft, phishing attacks, malware, hacking, and intellectual property violations. Ensuring secure user authentication and access control, as well as protecting users' personal information, are critical components in addressing these vulnerabilities. One of the primary cyber threats in metaverse libraries is the vast amount of data generated by users and the potential misuse of this information. Libraries must implement strong data protection measures, including encryption, anonymisation, and compliance with privacy regulations, to prevent breaches and unauthorised access. Equally important are strategies to prevent phishing, malware, and hacking, which can disrupt library services and compromise user accounts. Advanced authentication techniques, such as MFA and biometric verification, are essential in securing user identities and maintaining the integrity of virtual interactions within the metaverse.

The role of libraries in promoting a safe metaverse cannot be overstated. As stewards of knowledge and information, libraries must lead the way in creating secure virtual environments that protect both users and content. This involves not only implementing robust cybersecurity measures but also educating users on best practices for navigating the metaverse safely. User education and awareness programmes can empower library patrons to recognise and avoid potential threats, such as phishing attempts and suspicious digital objects. Moreover, libraries must collaborate with cybersecurity experts to stay ahead of emerging threats and adopt the latest technologies and best practices. In so doing, libraries can develop standardised security protocols and create a safer metaverse experience for all users.

References

Ajani, Y. A., B. D. Oladokun, R. T. Enakrire, et al. 2024. "Metaverse Adventures into Libraries: What Librarians and Information Users Need To Know." *Reference Services Review* 52 (3). https://doi.org/10.1108/RSR-05-2024-0025

Awadallah, A., K. Eledlebi, J. Zemerly, et al. 2024. "Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities." *IEEE Communications Surveys and Tutorials*. https://doi.org/10.1109/COMST.2024.3442475

Borky, J. M., and T. H. Bradley. 2019. "Protecting Information with Cybersecurity." In *Effective Model-Based Systems Engineering*, edited by J. M. Borky and T. H. Bradley, 345–404. Springer Nature. https://doi.org/10.1007/978-3-319-95669-5_10

Childs, E., F. Mohammad, L. Stevens, et al. 2023. "An Overview of Enhancing Distance Learning Through Emerging Augmented and Virtual Reality Technologies." *IEEE Transactions on Visualization and Computer Graphics* 30 (8): 4480–4496. https://doi.org/10.1109/TVCG.2023.3264577

Dawson, M., M. Omar, J. Abramson, and D. Bessette. 2014. "The Future of National and International Security on the Internet." In *Information Security in Diverse Computing Environments*, edited by Anne Kayem, 149–178. IGI Global. https://doi.org/10.4018/978-1-4666-6158-5.ch009

Dionisio, J. D. N., W. G. Burnes III, and R. Gilbert. 2013. "3D Virtual Worlds and the Metaverse: Current Status and Future Possibilities." *ACM Computing Surveys* 45 (3): 1–38. https://doi.org/10.1145/2480741.2480751

Dwivedi, Y. K., L. Hughes, A. M. Baabdullah et al. 2022. "Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice, and Policy." *International Journal of Information Management* 66: 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Elshenraki, H. N. 2023. *Forecasting Cyber Crime in the Metaverse Era: Future Criminal Methods*. IGI Global. https://doi.org/10.4018/979-8-3693-0220-0

Fadziso, T., U. R. Thaduri, S. Dekkati, V. K. R. Ballamudi, and H. Desamsetti. 2023. "Evolution of the Cybersecurity Threat: An Overview of the Scale of Cyber Threat." *Digitalization and Sustainability Review* 3 (1): 1–12.

Fiaz, F., S. M. Sajjad, Z. Iqbal, M. Yousaf, and Z. Muhammad. 2024. "MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms." *Future Internet* 16 (5): 176. https://doi.org/10.3390/fi16050176

Folino, G., C. Otranto Godano, and F. S. Pisani. 2023. "An Ensemble-Based Framework for User Behaviour Anomaly Detection and Classification for Cybersecurity." *The Journal of Supercomputing* 79 (11): 11660–11683. https://doi.org/10.1007/s11227-023-05049-x

Gao, H., A. Y. L. Chong, and H. Bao. 2024. "Metaverse: Literature Review, Synthesis, and Future Research Agenda." *Journal of Computer Information Systems* 64 (4): 533–553. https://doi.org/10.1080/08874417.2023.2233455

Harley, K., and R. Cooper. 2021. "Information Integrity: Are We There Yet?" *ACM Computing Surveys* 54 (2): 1–35. https://doi.org/10.1145/3436817

Hasan, M. F., F. M. Ashfaq, A. A. Chowdhury, S. I. Hamim, and M. Rahmani. 2024. "Dynamic Authentication Protocols For Advanced Security In Federated Metaverse Systems." BSc thesis, Brac University.

Kang, S., B. Veeravalli, K. M. M. Aung, and C. Jin. 2014. "An Efficient Scheme to Ensure Data Availability for a Cloud Service Provider." In *2014 IEEE International Conference on Big Data*, 15–20. IEEE. https://doi.org/10.1109/BigData.2014.7004378

Kaur, D., B. Singh, and S. Rani. 2023. "Cyber Security in the Metaverse." In *Handbook of Research on AI-Based Technologies and Applications in the Era of the Metaverse*, edited by A. Khang, V. Shah, and S. Rani, 418–435. IGI Global. https://doi.org/10.4018/978-1-6684-8851-5.ch023

Khalaf, A. 2025. "Copyright Law and Metaverse: A Comparative Study of Challenges and Opportunities of the Egyptian Copyright Law Entering the Virtual Era." MA diss., the American University in Cairo.

Kuru, K., and K. Kuru. 2024. "Blockchain-Based Decentralised Privacy-Preserving Machine Learning Authentication and Verification with Immersive Devices in the Urban Metaverse Ecosystem." Preprints. https://doi.org/10.20944/preprints202402.0317.v1

Kye, B., N. Han, E. Kim, Y. Park, and S. Jo. 2021. "Educational Applications of Metaverse: Possibilities and Limitations." *Journal of Educational Evaluation for Health Professions* 18: 32. https://doi.org/10.3352/jeehp.2021.18.32

Longshak, J. E., S. A. Oyeboade, M. S. Abdullahi, and K. M. Chanai. 2023. "Intellectual Property Rights (IPR) in the Blockchain Era." In *Global Perspectives on Sustainable Library Practices*, edited by Victoria Okojie, and Magnus Osahon Igbinovia, 263–296. IGI Global. https://doi.org/10.4018/978-1-6684-5964-5.ch020

Ng, D. T. K. 2022. “What is the Metaverse? Definitions, Technologies, and the Community of Inquiry.” *Australasian Journal of Educational Technology* 38 (4): 190–205. https://doi.org/10.14742/ajet.7945

Noh, Y. 2015. “Imagining Library 4.0: Creating a Model for Future Libraries.” *The Journal of Academic Librarianship* 41 (6): 786–797. https://doi.org/10.1016/j.acalib.2015.08.020

Nyasvisvo, B., and J. M. Chigada. 2023. Phishing Attacks: A Security Challenge for University Students Studying Remotely.” *The African Journal of Information Systems* 15 (2): 3.

Olabanji, S. O., Y. Marquis, C. S. Adigwe, S. A. Ajayi, T. O. Oladoyinbo, and O. O. Olaniyi. 2024. “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection.” *Asian Journal of Research in Computer Science* 17 (3): 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Oladokun, B. D., D. O. Yahaya, and R. T. Enakrire. 2023a. “Moving Into the Metaverse: Libraries in Virtual Worlds.” *Library Hi Tech News* 40 (9): 18–21. https://doi.org/10.1108/LHTN-08-2023-0147

Oladokun, B. D., R. T. Enakrire, and Y. A. Ajani. 2023b. “Metaliteracy Advocacy: The Need for Libraries to Engage Users in the Metaverse.” *Business Information Review* 40 (4): 167–172. https://doi.org/10.1177/02663821231209602

Oladokun, B. D., and P. Gaitanou, P. 2024. “Avatars and Their Players–Art in the Libraries.” *Library Hi Tech News*, ahead of print, published 25 June 2024. https://doi.org/10.1108/LHTN-04-2024-0055

Pooyandeh, M., K. J. Han, and I. Sohn. 2022. “Cybersecurity in the AI-based Metaverse: A Survey.” *Applied Sciences* 12 (24): 12993. https://doi.org/10.3390/app122412993

Samonas, S., and D. Coss. 2014. “The CIA Strikes Back: Redefining Confidentiality, Integrity, and Availability in Security.” *Journal of Information System Security* 10 (3).

Saracoglu, D. 2023. “Metaverse and New Cybersecurity Threats.” In *Metaverse: Technologies, Opportunities and Threats*, edited by Fatih Sinan Esen, Hasan Tinmaz, and Madhusudan Singh, 99–121. Springer Nature Singapore. https://doi.org/10.1007/978-981-99-4641-9_7

Saxena, A. C., A. Ojha, D. Sobti, and A. Khang. 2023. “Artificial Intelligence (AI)-Centric Model in the Metaverse Ecosystem.” In *Handbook of Research on AI-Based Technologies and Applications in the Era of the Metaverse*, edited by A. Khang, V. Shah, and S. Rani, 1–24. IGI Global. https://doi.org/10.4018/978-1-6684-8851-5.ch001

Sharma, S., J. Singh, A. Gupta, F. Ali, F. Khan, and D. Kwak. 2024. “User Safety and Security in the Metaverse: A Critical Review.” *IEEE Open Journal of the Communications Society* 5: 5467–5487. https://doi.org/10.1109/OJCOMS.2024.3397044

Singh, A., A. Vaish, and P. K. Keserwani. 2014. “Information Security: Components and Techniques.” *International Journal of Advanced Research in Computer Science and Software Engineering* 4 (1).

Subaveerapandiyan, A., A. Baiju, N. Ahmad, M. K. Verma, and P. Sinha. 2024. “Exploring Metaverse Literacy: Immersive Technologies in Library Environments.” *Journal of Web Librarianship* 18 (2): 39–63. https://doi.org/10.1080/19322909.2024.2382688

Tella, A., Y. A. Ajani, and U. V. Ailaku. 2023. “Libraries in the Metaverse: The Need for Metaliteracy for Digital Librarians and Digital Age Library Users.” *Library Hi Tech News* 40 (8): 14–18. https://doi.org/10.1108/LHTN-06-2023-0094

Verma, S., and U. Dwivedi. 2023. “Optimizing Digital Knowledge Repositories: Leveraging Electronic Resources in University Libraries for Enhanced Academic Advantages.” *Perspectives in Social Work* 37 (3): 112–132.

Vondráček, M., I. Baggili, P. Casey, and M. Mekni. 2023. “Forensic Readiness and Analysis of Metaverse Platforms: A Novel Metaverse Forensic Artefact Classification And Data Extraction Approach.” *Forensic Science International: Digital Investigation* 42: 301607.

Wang, H., H. Ning, Y. Lin, et al. 2023. “A Survey on the Metaverse: The State-Of-The-Art, Technologies, Applications, and Challenges.” *IEEE Internet of Things Journal* 10 (16): 14671–14688. https://doi.org/10.1109/JIOT.2023.3278329

Zainuddin, A. A., A. Othman, N. A. M. Zahid, N. A. S. K. Zaman, A. N. M. A. Razmi, and M. H. A. K. Zaman. 2024. “A Comprehensive Analysis of IoT Security and Privacy in Smart City Applications.” *Bulletin of Social Informatics Theory and Application* 8 (1): 37–58.