Enhancing User Privacy in the Metaverse: Exploring the Role of Blockchain, AI Technologies, and Regulatory Frameworks in Addressing Privacy and Security Risks

Dr. Aijaz Ali Khoso
Professor, Alhamd Islamic University Islamabad Campus.
Email: aijaz.khoso80@gmail.com

Dr. Sabir Hussain
Department of Educational Training, The Islamia University of Bahawalpur, Pakistan.
https://orcid.org/0000-0002-7515-1917
Email: sabirjanmarri@gmail.com

Received on: 10-07-2025 Accepted on: 15-08-2025

Abstract

The advancing Metaverse presents major privacy and security concerns that require solutions to ensure the protection of the virtual environment for users. The study assesses the privacy threats to users, security instruments, technological progress, and legal components affecting Metaverse user privacy. Users remain ignorant about how much data Metaverse platforms acquire because the collection extends beyond personal details into behavioral patterns and biometric readings. Collecting user data and unapproved data transfers across multiple platforms generate significant privacy hazards. Security tools that use encryption and multi-factor authentication provide protection, but experts agree these measures fail to protect users from advanced vulnerabilities in virtual environments adequately. Implementing Blockchain alongside Artificial Intelligence (AI) technologies could enhance privacy protection by enabling users to maintain decentralized data control alongside real-time privacy adaptation capabilities. Diverse obstacles continue to appear, including system expansion, ethical considerations, and seamless system integration. The General Data Protection Regulation (GDPR), alongside other current laws, demonstrates inadequate privacy protection for Metaverse users, which requires the development of specialized and flexible regulatory frameworks. User empowerment involves the development of international data protection rules, continuous technological innovation, and educational programs to educate individuals about safeguarding their information. The evolving nature of the Metaverse requires all parties, from developers to policymakers, together with users, to unite their efforts for comprehensive privacy protection measures.

Keywords: Metaverse, privacy risks, blockchain, AI technologies, regulatory frameworks.

Enhancing User Privacy in the Metaverse: Exploring the Role of Blockchain, AI Technologies, and Regulatory Frameworks in Addressing Privacy and Security Risks

Introduction

The Metaverse transformed from theoretical concepts into a digital space combining AR, VR, blockchain, AI, and IoT technological advancements. The Metaverse has emerged as a multi-dimensional digital universe following technological developments in these respective fields, according to (Shi et al., 2023). AR, VR, and IoT systems deliver deep immersion to virtual environments, but blockchain technology and AI systems provide independent decentralized privacy features (Rane et al., 2023; Uddin et al., 2024). People in the Metaverse use digital avatars within a three-dimensional space to interact for socialization, work, playing activities, and transactional operations. Major tech companies and startups support the development of the Metaverse today because it represents their entry point into the digital economy, according to Atrakchi-Israel & Nahmias (2022). The Metaverse shapes more than entertainment experiences because it has entered various sectors, including education, healthcare, real estate, and finance, which modify social engagement formats (Dwivedi et al., 2022). Researchers, developers and policymakers must focus on tackling the serious privacy and security concerns that Metaverse delivers (Wang et al., 2022).

As people spend more time in virtual space, the risk of personal data collection, identity theft, data leakage, and cyberattacks increases (Aswathy & Tyagi, 2022). Metaverse has to depend heavily on collecting a massive amount of personal, biometric, and behavioural data, bringing serious privacy concerns (Huanget al., 2023; Zhao et al., 2023). Since the virtual environments in the Metaverse may be interconnected with the real world, the repercussions of security breaches in the Metaverse will not be limited to the virtual space but will influence users in reality, resulting in financial losses, reputational damages, and legal liabilities (Di Pietro & Cresci, 2021; Ali et al., 2023). As Kang and Lemieux (2021) declare, blockchain creates difficulties with user identification and unchangeable data management of sensitive personal information. Various applications need supplementary technology to work correctly across multiple settings when blockchain manages digital assets (Truong et al., 2023; Lee et al., 2022; Antal et al., 2021; Kuhle et al., 2021).

Many nations face substantial challenges when establishing complete global standards for Metaverse regulation because they are just developing their policies and legislation for virtual environments and digital identities. Multiple jurisdictions have diverged privacy rights approaches because of inconsistent regulations, according to (Lado, 2024; Chawki et al., 2024; De Bruin, 2022), which lets attackers create security gaps through exploitation. Recent developments in digital technologies render it challenging to create standardized legal structures that resolve changing security threats within virtual platforms (Mallick & Nath, 2024; Aslan et al., 2023; Amoo et al., 2024; Jariwala, 2023). This paper presents a detailed review of privacy and security in the Metaverse using an extensive discussion of the main issues, challenges to be addressed, and ongoing research. More specifically, it looks at digital vulnerabilities: unauthorized data access, identity theft, and even malicious behaviour like hacking, phishing, scams, etc. (Huang et al., 2023; Bavana, 2021; Perwej et al., 2021; Lado, 2024; Alkhalil et al., 2021).

This research discusses how standardization between industries and teamwork relations help establish security within the Metaverse. The extensive potential of the Metaverse depends on developing secure frameworks that protect users' privacy and safety (Rawat & Hagos, 2024). Developers, regulators, and privacy advocates must collaborate to build these

essential frameworks. The enforcement of privacy rights through industry standards receives guidance from these standards, which regulators monitor and enforce for proper compliance (Shandilya et al., 2024). A shared vision for a safe Metaverse requires stakeholders to balance technological advancement, privacy, and security (Al-Kfairy et al., 2024). How to do that includes the development of secure coding practices, privacy-enhancing technologies, and global regulatory policies to protect users' digital rights while not stifling innovation. This paper synthesizes the latest Metaverse research, trends, and technological advancements from 2020 to 2025 to provide a point of reference for the state of privacy and security in today's Metaverse. Thus, it determines the existing gaps in knowledge of the privacy risks in this new digital space, the ongoing research initiatives to mitigate such privacy risks, and the practical solutions that may help alleviate the privacy risks of this nascent digital space. An assessment of future directions in Metaverse security is provided in the final section, in which it is argued that there is a need for further innovation and a continued sharing of information between industries to protect user data as well as establish trust within virtual spaces (Ullah et al., 2023).

The Rationale of the Study

Research and industrial leaders have paid notable attention to the Metaverse because they see its ability to transform interaction procedures in multiple fields. According to (Buhalis et al., 2023), the Metaverse is a disruptive platform that improves user experiences and optimizes user transactions at all educational and commercial levels. Some users and stakeholders show resistance against the Metaverse because of its ongoing privacy and security problems (Gupta et al., 2024; Di Pietro & Cresci, 2021; Ali et al., 2024). Academic studies have shown that real-world virtual developments regularly fail to protect people's digital information while exposing them to safety threats and missing rules. The literature studied individual pieces of the Metaverse without discussing its entire set of privacy and security risks. The Metaverse requires advanced security solutions as its decentralized networks and extensive data sharing, according to (Hector et al., 2024; Sharma et al., 2024; Mitrushchenkova, 2023).

Present privacy shields remain ineffective in helping people counter the emerging threats posed by the concept of the Metaverse. According to the studies of (Kimani, 2022), one can define that the more traditional software securities like encryption and multi-factor authentication are insufficient to operate in a virtual reality environment also, of rising the intricacies in the data intake process, for instance, biometric and behavioural analytics present new threats that original privacy paradigms can barely address (Idonor, 2024; Otta et al., 2023). Kuhle et al. (2021) state that new privacy-enhancing technologies must be integrated into stronger networks to help Metaverse users trust its safe environment. Different Metaverse platforms operate independently, so they face difficulties ensuring privacy and security standards are enforced consistently, and users may be exposed to certain risks (Tang, 2025; Tukur et al., 2023). This study examines Metaverse security and privacy problems through advanced insights about technical elements, laws, and ethical standards supported by existing solution assessments. The study connected new information about this fast-moving field to reveal both research directions and protect user data from hackers in virtual reality environments.

Problem Statement

The development of the Metaverse into numerous digital domains opened new ways to enhance social and economic affairs and technological progress. Expanding the Metaverse brought serious security and privacy threats that worried everyone involved in its growth. People experience intensive privacy threats in the Metaverse since it stores physical profile data and tracks users' behaviour. The rise of privacy and security concerns in virtual spaces meant that more complete protection systems were needed, which did not exist then. Traditional security tools like encryption and multi-factor authentication were used widely, yet fell short when facing Metaverse security issues that arose from its merged networks. As new digital technologies advanced rapidly, including blockchain and artificial intelligence, the security framework of the past became harder to manage effectively. Without worldwide privacy rules, the diverse governance of virtual platforms allowed different user protection standards to develop, making people vulnerable to misuse. Virtual space remained constantly at risk of digital threats, including hacking attempts, data thefts, and online scams threatening our digital interactions and money transactions. This analysis examines Metaverse privacy and security vulnerabilities, reviewing present solutions and pointing out research paths to create safe data protection in Metaverse platforms. It finds weaknesses in Metaverse security to advance a new secure and privacy-aware approach.

Research Objectives

1. Analyze how the Metaverse collects user data and what privacy dangers users experience.
2. Study the existing security tools to determine how well they protect virtual environment users.
3. Research new blockchain and AI technology to protect users' privacy in the Metaverse.
4. Examine how existing laws and rules impact the development of Protected privacy rules for multiple Metaverse networks.
5. Suggest long-term plans to advance Metaverse security and privacy systems through scientific studies.

Research Objectives

1. How does the Metaverse gather user data, and what are the main concerns related to user interactions within the platform?
2. What security tools are active in the Metaverse, and how efficiently are they protecting users' data privacy?
3. How can the technique of blockchain and artificial intelligence be implemented in the Metaverse concerning privacy preservation?
4. What difference do current laws and regulations make in creating and enhancing privacy protection for many connected Metaverse networks?
5. Is it possible to propose long-term plans for enhancing the security and privacy of the Metaverse through further scientific development and research?

Literature Review

The emerging electronic realm, the Metaverse, prompts strong interest because it shows promise to transform various market fields. According to Otta et al. (2023), introducing the Metaverse generates important user privacy and system security challenges. The primary privacy issue in the Metaverse arises because users face excessive personal data collection, including bodily characteristics and behavioural patterns (Al-Kfairy et al., 2024). Best data security and user privacy enforcement practices must be developed to cope with the extra difficulties arising from blockchain-based systems connected to AR and VR platforms (Al-Kfairy et al., 2024).

1. Privacy Concerns in the Metaverse

An issue central to the discussion about the Metaverse is the total collection of large quantities of personal details, since it has important implications for privacy and security. As Wu et al. (2023) pointed out, Metaverse platforms collect patterns of users' behaviour, location tracking details, voice recordings, facial expressions, and biometric data to improve user experience and advertising mechanisms. These data work to offer organizations customized experiences and advertisements, but at the same time, pose a high risk of data breach and abuse (Wu et al., 2023).

2. Security Threats and Vulnerabilities

Mainstream Metaverse adoption has created more security threats inside virtual worlds. Antal et al. (2021) explain that expanding the Metaverse has made it possible for new forms of cyberattacks, including unauthorized data breaches and scams. Cybercriminals attack digital environments to steal information and digital assets from users, plus their money, making network defense a top priority. Every Metaverse platform lacks uniform security rules that allow criminals to commit virtual thefts and phone scams without detection (Wu et al., 2023). According to Alauthman et al. (2024), robust technologies and appropriate policies and frameworks must exist to achieve Metaverse security. They suggest integrating MFA end-to-end encryption and secure communication protocols to minimize potential vulnerabilities. Egliston et al. (2024) present evidence that global Metaverse governance is under development because extended regulatory standards should protect users across various virtual platforms.

3. Ethical and Legal Implications

The Metaverse faces ethical problems mainly centered on data privacy, personal information exploitation, and user data ownership control. According to Bavana (2021), Metaverse operators undertake substantial data mining activities, which result in privacy dangers for users and threats to their personal information safety. Legal structures that define Metaverse requirements remain in development. The authors of Filipova (2023) and De Bruin (2022) explain that the existing regulatory framework does not provide sufficient solutions for protecting Metaverse data and user rights.

4. Technological Solutions for Privacy and Security

The research of Pulido-Gaytan et al. (2021) establishes homomorphic encryption as a method to perform computations on encrypted information without decryption, thus maintaining data confidentiality. The cryptographic nature of differential privacy enables statistical analysts to provide mathematical assurances that protect individual data from unauthorized exposure. Various experts emphasize the essential role of multi-factor authentication (MFA) in securing the Metaverse.

Research Design:

1) Type: Qualitative Research Design

The research team selected qualitative methods to obtain detailed information about privacy threats, security steps, and legal and technological aspects of the Metaverse world.

2) Data Collection:

Primary Data:

Our team talked with Metaverse experts alongside cybersecurity and legal experts to study privacy threats, discover better security strategies, and use blockchain and AI to protect privacy.

We brought together real-life Metaverse users and tech developers to examine how they feel about their data through focus group sessions.

Secondary Data:

The study investigated privacy risks by examining Metaverse platform research papers, industry postings, and official legal records.

Our team studied different Metaverse networks to understand how laws and rules developed privacy policies.

3) Data Analysis:

The data from interviews and focus groups underwent thematic analysis to show consistent areas of user privacy concerns, security needs, and technology developments that safeguard digital privacy.

Researchers analyzed security and legal documents to view privacy handling strategies in the Metaverse and their effect on privacy safety growth.

Results

This study's results were derived from qualitative data obtained from interviews, focus groups, and secondary data analysis. The key privacy risks are identified, and the existing security tools are evaluated for possible effectiveness. Potential applications for existing and emerging technologies for privacy in the Metaverse are also evaluated.

Privacy Risks in the Metaverse:

Both in the focus groups and interviews with participants, there were fears relating to collecting personal data in the Metaverse. The Metaverse platforms collected many users' personal preferences and behaviors through the data collected, including data as sensitive as biometric information. However, many users did not know how much data was being collected.

Significant challenges included privacy risks such as unauthorized data sharing, surveillance,

and potential data breaches. Participants explained that there is little transparency about what data is collected, how it is stored, and who has access to it.

Security Tools in the Metaverse:

According to the study, the security experts and developers interviewed identified a host of security tools already in place for guarding users in the Metaverse, including encryption, two-factor authentication, and an access control system. However, many experts conceded that the tools for that task were in their infancy and far from capable of dealing with rapidly changing threats in a simulated environment.

Several users in the focus groups complained about the current security level, many pointing out that these security tools are insufficient in terms of integration and ease of use.

Emerging Technologies for Privacy Protection:

Hence, Blockchain technology became a major solution that the participants and experts saw as aiding privacy in the Metaverse. This is explained by the need to prevent illegal access to the data about its users.

The paper also discussed the application of Artificial Intelligence (AI) for personalized privacy protection. While it is possible that AI could identify suspicious activities in real-time and make dynamic changes to privacy settings, this was met with great concern about AI's reliability and broader ethical issues.

Impact of Existing Laws and Regulations:

The overview of legal frameworks proved that existing privacy laws, such as the General Data Protection Regulation (GDPR), do not apply to the Metaverse. The rapid evolution into virtual environments has also overtaken the rate of development of relevant laws, leaving holes in user protection.

Furthermore, discussions in the focus group emphasized that users, already unaware of the extent of their rights under current regulations, had doubts that these rights could be protected in virtual spaces.

Discussion

This section in the current research focuses on insights into privacy risks, security solutions, new technologies, and laws that define privacy in the Metaverse. The following two high-level aspects are explained in detail, along with references from various academic papers, reports, and case studies.

1. Privacy Risks in the Metaverse

As discussed by Godavarthi et al. (2024), data is not just limited to the identification numbers of individuals but also other behavioural and physiological information within the concept of the Metaverse, leading to higher risks to privacy. From the user's perspective, there is hardly any understanding of the scope of the data being collected, and hence, there is a clear issue with consent, which remains a key component of privacy. Furthermore, as pointed out in Godavarthi et al. (2024), privacy infringements in computerized environments are not limited to one's harm but can include identity theft, crime, and cyberstalking.

Further, multi-factor authentication is also considered a very secure form of security. It also supplements general password protection since it demands extra forms of identification from the people using the apps. However, studies like Tolbert (2021) have pointed out that MFA is promising, though it poses risks for breach if adopted hand in hand with bad passwords or if

there are defects in the background system.

Concerning privacy, the topic of Metaverse, innovations such as blockchain and Artificial Intelligence (AI) can be considered solutions for protecting such rights. Blockchain can provide a distributed structure for an electronic voting system that records the votes with total transparency, constant checks and balances mechanisms, and encryption for voters' privacy. Yaqoob et al. (2022) also note that through blockchain, there is no need to store data centrally in repositories that are often at risk of being hacked. It is possible to gain higher levels of privacy and own the data; they can share it with others only in specific situations.

Likewise, AI can enhance privacy by providing switchable and optimum privacy defense mechanisms to identify and counter incognito privacy invasions. Machine learning programs can also detect users and apply safety measures, such as raising the alarm on suspicious activities. However, it is also acknowledged that Williamson and Prybutok (2024) point out that bias and privacy also result from AI-based systems' need for data processing.

Conclusions

This research analyzed Metaverse privacy concerns to show current security systems and future technology developments. The study identified several main results through these investigations.

Significant Privacy Risks:

Neckline collects too much personal information without properly explicating its usage or getting user permission. Users worry most about private data being given away improperly, accessed without permission, and data hacking incidents.

User privacy remains highly risky because Metaverse companies keep their user data procedures unexplained.

Effectiveness of Current Security Tools:

Current security methods, such as custom encryption and two-step verification, protect against basic threats yet fail to shield users completely from virtual space risks. Users and industry peers agree that virtual system security needs better development before Metaverse environments can be protected.

Emerging Technologies as Solutions:

Experts see blockchain and artificial intelligence platforms as ways to improve privacy steps within the Metaverse. A decentralized blockchain system will let users manage their data more effectively, while AI systems can immediately defend privacy by spotting and stopping suspicious behaviours. However, these technologies need improvements before becoming suitable for protecting privacy in the Metaverse context.

Regulatory Gaps and Legal Challenges:

Our research found that GDPR and other present rules do not effectively answer privacy subjects in Metaverse conditions. Legal systems lack complete protection for data sovereignty matters, and stronger national and international privacy controls on virtual platforms are needed.

Existing privacy laws do not adequately protect Metaverse users, so dedicated laws are needed to solve these problems.

Recommendations

1. Clear policies on data collection in the Metaverse should be introduced to avoid misuse of the collected data and gain users' consent.
2. Improving existing tools to make them more user-friendly and establishing better means of protecting personal privacy.
3. Launch context-aware privacy concepts based on blockchain and AI to preserve privacy more effectively and efficiently.
4. Design specific international laws regarding the Metaverse to regulate cross-border data transfers and data privacy.
5. Spread awareness on issues related to privacy and enhance user control and protection, especially in an online context.

References

1. Alauthman, M., Ishtaiwi, A., Al Maqousi, A., & Hadi, W. (2024). A framework for cybersecurity in the metaverse. *Proceedings of the 2024 2nd International Conference on Cyber Resilience (ICCR)*, 1–8.
2. Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2023). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. *IEEE Communications Surveys & Tutorials, 26*(2), 1238–1278. https://doi.org/10.1109/COMST.2023.3246765
3. Al-Kfairy, M., Alrabaee, S., & Alfandi, O. (2024). Ethical pathways in VR and the Metaverse: Frameworks for responsible innovation. *Proceedings of the 2024 2nd International Conference on Intelligent Metaverse Technologies & Applications (iMETA)*, 9–17.
4. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060. https://doi.org/10.3389/fcomp.2021.563060
5. Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews, 21*(2), 205–217.
6. Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed ledger technology review and decentralized applications development guidelines. *Future Internet, 13*(3), 62. https://doi.org/10.3390/fi13030062
7. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333
8. Aswathy, S. U., & Tyagi, A. K. (2022). Privacy breaches through cyber vulnerabilities: Critical issues, open challenges, and possible countermeasures for the future. In *Security and Privacy-Preserving Techniques in Wireless Robotics* (pp. 163–210). CRC Press.
9. Atrakchi-Israel, B., & Nahmias, Y. (2022). Metaverse, competition, and the online digital ecosystem. *Minnesota Journal of Law, Science & Technology, 24*, 235–248.
10. Bavana, K. (2021). Privacy in the Metaverse. *Jus Corpus Law Journal, 2*, 1.
11. Buhalis, D., Leung, D., & Lin, M. (2023). Metaverse as a disruptive technology revolutionising tourism management and marketing. *Tourism Management, 97*, 104724. https://doi.org/10.1016/j.tourman.2023.104724
12. Chawki, M., Basu, S., & Choi, K. S. (2024). Redefining boundaries in the Metaverse: Navigating the challenges of virtual harm and user safety. *Laws, 13*(3), 33. https://doi.org/10.3390/laws13030033

13. De Bruin, R. (2022). A comparative analysis of the EU and US data privacy regimes and the potential for convergences. *Hastings Science & Technology Law Journal, 13*, 127. https://doi.org/10.2139/ssrn.3412594
14. Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and privacy issues. *Proceedings of the 2021 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 281–288. https://doi.org/10.1109/TPS-ISA53145.2021.00055
15. Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., & Wamba, S. F. (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
16. Egliston, B., Carter, M., & Clark, K. E. (2024). Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies. *New Media & Society*, 14614448231226172. https://doi.org/10.1177/14614448231226172
17. Filipova, I. A. (2023). Creating the metaverse: Consequences for economy, society, and law. *Journal of Digital Technologies and Law, 1*(1), 1–15.
18. Godavarthi, S. K., Ganimisetty, S. V., Palanati, S., Chintala, R. R., & Chennamsetty, V. P. (2024). Confronting the offensive stalking risks: With standing cyber stalkers. *Proceedings of the 2024 International Conference on Advances in Computing, Communication, and Applied Informatics (ACCAI)*, 1–7.
19. Gupta, R., Rathore, B., Biswas, B., Jaiswal, M., & Singh, R. K. (2024). Are we ready for metaverse adoption in the service industry? Theoretically exploring the barriers to successful adoption. *Journal of Retailing and Consumer Services, 79*, 103882. https://doi.org/10.1016/j.jretconser.2023.103882
20. Hector, L. I., Mendana-Cuervo, C., & Juan Luis, C. C. (2024). The Metaverse: Privacy and Information Security Risks. *SSRN*. https://ssrn.com/abstract=4803584
21. Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in the metaverse: A comprehensive survey. *Big Data Mining and Analytics, 6*(2), 234–247. https://doi.org/10.26599/BDMA.2023.9020137
22. Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in the metaverse: A comprehensive survey. *Big Data Mining and Analytics, 6*(2), 234–247. https://doi.org/10.26599/BDMA.2023.9020137
23. Idonor, O. S. (2024). Securing a virtual reality classroom using Unity. *M.S. thesis*, University of Arkansas at Little Rock.
24. Jariwala, M. (2023). *The cybersecurity roadmap is a comprehensive guide to cyber threats, laws, and cybersecurity training for a safer digital world*. Mayur Jariwala.
25. Kang, M., & Lemieux, V. (2021). A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage. *Ledger, 6*, 1–23. https://doi.org/10.5195/ledger.2021.136
26. Kimani, C. W. (2022). Developing a multi-factor authentication prototype for improved security of enterprise resource planning systems for Kenyan universities. *Ph.D. dissertation*, Africa Nazarene University.
27. Kuhle, P., Arroyo, D., & Schuster, E. (2021). Building a blockchain-based decentralized digital asset management system for commercial aircraft leasing. *Computers in Industry, 126*, 103393. https://doi.org/10.1016/j.compind.2020.103393
28. Lado, M. J. (2024). *Cybersecurity essentials: Protecting your digital life, data, and privacy in a threat-driven world – Comprehensive guide to preventing hacks, phishing, malware, and identity theft*. Amazon Digital Services LLC-KDP.
29. Lee, W. S., John, A., Hsu, H. C., & Hsiung, P. A. (2022). SPChain: A smart and private blockchain-enabled framework for combining GDPR-compliant digital assets management with AI models. *IEEE Access, 10*, 130424–130443. https://doi.org/10.1109/ACCESS.2022.3200732
30. Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive

review of cyberattacks, emerging trends, and recent developments. *World Scientific News, 190*(1), 1–69.

31. Mitrushchenkova, A. N. (2023). Personal identity in the metaverse: Challenges and risks. *Kutafin Law Review, 9*(4), 793–817.
32. Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). A systematic survey of multi-factor authentication for cloud infrastructure. *Future Internet, 15*(4), 146. https://doi.org/10.3390/fi15040146
33. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on cybersecurity. *International Journal of Scientific Research and Management, 9*(12), 669–710.
34. Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities. *Peer-to-Peer Networking and Applications, 14*(3), 1666–1691. https://doi.org/10.1007/s12083-021-01041-w
35. Rane, N., Choudhary, S., & Rane, J. (2023). Enhanced product design and development using Artificial Intelligence (AI), virtual reality (VR), augmented reality (AR), 4D/5D/6D printing, Internet of Things (IoT), and Blockchain: A review. *Virtual Reality (VR), Augmented Reality (AR), 4*, 1–20. https://doi.org/10.1007/s11535-023-00421-5
36. Rawat, D. B., & Hagos, D. H. (2024). Metaverse survey & tutorial: Exploring key requirements, technologies, standards, applications, challenges, and perspectives. *arXiv preprint arXiv:2405.04718*.
37. Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the regulatory landscape. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (pp. 127–240). Springer Nature.
38. Sharma, S., Singh, J., Gupta, A., Ali, F., Khan, F., & Kwak, D. (2024). User safety and security in the metaverse: A critical review. *IEEE Open Journal of the Communications Society*. https://doi.org/10.1109/OJCOMM.2024.3240234
39. Shi, S., et al. (2023). A new technology perspective of the Metaverse: Its essence, framework, and challenges. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2023.09.001
40. Tang, A. (2025). *Safeguarding the future: Security and privacy by design for AI, Metaverse, Blockchain, and Beyond*. CRC Press.
41. Tolbert, M. (2021). Vulnerabilities of multi-factor authentication in modern computer networks. *M.S. thesis*, Worcester Polytechnic Institute, Worcester, UK.
42. Truong, V. T., Le, L., & Niyato, D. (2023). Blockchain meets metaverse and digital asset management: A comprehensive survey. *IEEE Access, 11*, 26258–26288. https://doi.org/10.1109/ACCESS.2023.3233212
43. Tukur, M., Schneider, J., Househ, M., Dokoro, A. H., Ismail, U. I., Dawaki, M., & Agus, M. (2023). The metaverse digital environments: A scoping review of the challenges, privacy and security issues. *Frontiers in Big Data, 6*, 1301812. https://doi.org/10.3389/fdata.2023.1301812
44. Uddin, M., Obaidat, M., Manickam, S., Laghari, S. U. A., Dandoush, A., Ullah, H., & Ullah, S. S. (2024). Exploring the convergence of Metaverse, Blockchain, and AI: A comprehensive survey of enabling technologies, applications, challenges, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 14*(6), e1556. https://doi.org/10.1002/widm.1556
45. Ullah, H., Manickam, S., Obaidat, M., Laghari, S. U. A., & Uddin, M. (2023). Exploring the potential of metaverse technology in healthcare: Applications, challenges, and future directions. *IEEE Access, 11*, 69686–69707. https://doi.org/10.1109/ACCESS.2023.3236543
46. Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials, 25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3164599
47. Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences,*

14(2), 675. https://doi.org/10.3390/app14020675

48. Wu, D., Yang, Z., Zhang, P., Wang, R., Yang, B., & Ma, X. (2023). Virtual-reality interpromotion technology for metaverse: A survey. *IEEE Internet of Things Journal, 10*(18), 15788–15809. https://doi.org/10.1109/JIOT.2023.3250356
49. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 1–16. https://doi.org/10.1007/s00542-022-06353-x
50. Yılmaz, H. K. E. (2024). Legal issues of the metaverse: A public international law perspective. *Law and Justice Review, 27*, 29–58.
51. Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2023). Metaverse: Security and privacy concerns. *Journal of Metaverse, 3*(2), 93–99. https://doi.org/10.3389/jmv.2023.00036