Digital Identity Theft and Privacy Concerns in the Metaverse

Dr. Syed Asad Ali Shah

Abstract:

The rise of the metaverse has introduced unprecedented opportunities for digital interaction while also amplifying concerns around identity theft and privacy risks. This paper examines the challenges through a systematic review of the literature and interviews with metaverse experts and users. The findings reveal three critical themes regarding risks such as; security flaws in digital identity frameworks, privacy issues emanating from improper consent processes, and delayed implementation of cybersecurity practices as influenced by users and technological deficits. The findings of the thematic analysis concern the insufficiency of the present mechanisms of authentication, the absence of strict normalisation and the absence of stable norms for regulating it. The necessity of the application refers to the privacy and security through integrating design models and, at the same time, increasing the awareness of users. One of the major design issues identified in metaverse platforms is the issue of usability and security and balancing between the two. In this study, experts are sampled and interviewed to offer information and perspective on budding issues such as usability and security in metaverse. This research calls for a multi-pronged approach, combining technological innovation, regulatory oversight, and behavioural interventions, to mitigate risks and foster trust in the metaverse. The findings contribute to a deeper understanding of securing digital identities in virtual spaces.

Keywords: Digital Identity Theft, Privacy Concerns, Metaverse, Cybersecurity, Personal Information in Digital Platforms.

1. Introduction:

The constant development of IT technologies has given rise to the appearance of metaverse, that is collective virtual space through which the users can interact through digital identities. This environment captures elements of augmented reality, virtual reality and the internet to enable users to socialize, work and transact business (Canbay et al., 2022). The metaverse offers vast potential in such areas as the development of new connections and collaboration because it also uncovers new forms of risks, including digital identity theft and privacy violation. Thus, as users integrate with these spaces primarily through their avatars, or their personal data, potential adversaries may be targeting weaknesses in identity and privacy frameworks or infrastructure (Shahriar, 2024). Therefore, this research focuses on the existence of identity theft and privacy violations in the metaverse and the importance of implementing security measures to protect individuals' and digital data.

Digital identity theft refers to a situation where one uses an individual's or a company's information or data to deceive or impersonate an illicit advantage. When examining the identities integrated in the metaverse, this study is not only speaking of username and password type information but more complex things like avatars, biometrics, and transaction histories (Atlam et al., 2024). It is made worse by the fact that personal interaction and discrete data are consistently shared across the metaverse in the manner that is inherent with this virtual universe. Information crimes in metaverse platforms and threats, such as hacking, phishing and data leaks have raised concerns on security weaknesses of metaverse. Still, corresponding threats and protective measures necessary to prevent such risks are unknown to most users (Wang and Wang, 2023). Privacy issues increase the intensity of the problems. Individuality in Metaverse applications is acquired through large amounts of data gathering from which user experiences are improved as well as the platform of obtaining its revenues through precisely targeted advertising. Though this data collection process presents some questions about consent, ownership of data and misuse. The rules and laws established for data protection in the physical world, like GDPR, do not cover well the fast and fluid nature of the digital world (Chen et al., 2022).

1.1. Problem Statement:

Despite all the in-depth understanding regarding the metaverse, there is still limited understanding regarding how digital identity threats and privacy problems manifest in these virtual environments (Dwivedi, 2022). The current security and safety protocols often

fail to appropriately indicate the sophisticated threats that are imposed by malicious actors. This gap in the past literature knowledge leaves users vulnerable to exploitation and undermines trust in metaverse platforms. Moreover, the lack of proper regulation for cyber threats and absence of standardised privacy practices, exacerbates the risk of identity theft and data breaches, disrupting the integrity and safety of users' digital experiences (Huang, Li and Cai, 2023).

1.2. Research Aim:

The core aim of the study is to examine the risks posed to digital identity thefts and privacy concerns in the metaverse and also to evaluate the emerging challenges and how they are managed through the existing security frameworks. This research tends to propose actionable and relevant recommendations to foster digital identity privacy and protection in virtual spaces.

1.3. Research Objectives:

- To examine the scope and nature of digital identity theft and privacy concerns in the metaverse.
- To assess the current privacy and security interventions integrated by metaverse platforms.
- To determine the perspectives of cybersecurity users and experts regarding the effectiveness of these measures.
- To introduce strategies to enhance digital identity security and privacy practices in the metaverse.

2. Literature Review:

The conversion of the physical universe into the digital or virtual space (metaverse), also changes the style of people to connect, meet new friends, search the job market, and do business (Chawki, Basu and Choi, 2024). However, these advantages also come with great risks, specifically of identity theft and the violation of privacy rights. Users are creating accounts or digital avatars that resemble themselves and also input their various personal information in these interactive virtual platforms which increases the concerns about the security of the identity and misuse of data (Dwivedi, 2022). This study aims to review the existing literature component in academic articles on digital identity theft as well as privacy issues in a metaverse environment with an emphasis on risks of the virtual environment as well as the steps taken towards implementation in tackling such challenges.

2.1. Metaverse Identity Theft:

Cyber identity theft is best described as the unauthorized and criminal use of someone's details or virtual persona (Chawki, Basu and Choi, 2024). In the context of the metaverse, it goes well beyond one's common identity theft since users communicate with one another through distinctive platforms and are not just confined to personal details such as just name and address. Some virtual assets may be avatars, or a person's personal likes and dislikes and purchasing history, or biometric features such as facial recognition or tracking the way a person moves in the metaverse (Shahriar, 2024). The presence of multiple diversified avatars in the metaverse environment enhances the rates of theft risk. The first one is Virtual Avatars Security Concerns. These avatars, the study found, are used by cybercriminals in impersonation, financial fraud, or social engineering attacks (Rashid and Khan, 2024). Quite often such avatars contain a rich data payload that belongs to the user themselves, including their preferences and social connections. Thieves can capture these avatars virtually, they take control of private social networks or engage in monetary procedures using fake identification.

Another significant reason that the authors identified for digital identity theft in virtual environments is the weak authentication processes. Research conducted says that most of the existing metaverse applications still use traditional security measurements like Single Factor Authentication (SFA) or merely simple security models (Awadallah et al., 2023). The reliance on easily by passable security measures, like usernames and passwords, puts users at high risk of exploitation. In addition, due to the decentralised approach of many of the pliant metaverse platforms, there is no single authority charged with the protection of user data and this makes the possibility of exploitation of the existing weaknesses by bad actors (Pooyandeh, Han and Sohn, 2022).

2.2. Privacy concerns in the Metaverse:

One of the significant issues in metaverse is privacy, as these virtual environments often require users to share a wide range of personal information to improve their experience. This leads to sensitive and critical information like brewing history, biometric data, location data and even emotional responses (Chen et al., 2022). Most metaverse sites gather this sort of data for advertising, tracking users' behaviours and similar tasks. Many people consider the huge collection of data to be harmful to privacy especially given other well-known problems of data vulnerability in other social media platforms. A 2022 report by the European Union Agency for Cybersecurity (ENISA) highlighted the privacy risks posed by the growing presence of the metaverse. The drawback highlighted that users may remain unaware of the amount and kinds of personal information that those contexts gather, there is no transparency regarding the utilization and distribution of that data. Most platforms have inconspicuous and unintelligible consent models, which disregards users' legitimate rights created by information protection provisions such as General Data Protection Regulation (GDPR) (Enisa, 2016). Moreover, the given laws remain rather challenging to enforce on the globe and across jurisdictions as many platforms fit into the metaverse are launched on the international level, not connected to the national legislation systems (Canbay et al., 2022).

A study conducted by Zhang and Wu (2023) reveals that the metaverse platforms mostly prioritises user experience but neglects the users' anonymity by monetizing the privacy protections. These environments are supposed to be as realistic as possible, and the main parameters which define this kind of realism are based on the constant monitoring of the user's activity and interests. The first problem stems from the absence of established rules governing most regions and the relatively low standards of privacy protection that users are offered as a result. Secondly, it has been pointed out that biometric data deployment in virtual worlds pose possible intrusions to privacy (Wang and Wang, 2023). In most of the cases, integrated metaverse platforms apply such high-tech components as advanced facial recognition, eye-tracking, and, sometimes, voice recognition. Although these technologies improve user experience but also create new opportunities for privacy invasion. For instance, facial recognition data can be influenced to monitor or utilized to control the user (Zhang and Wu, 2023). This means that the storing of such firm's data without user consent or even regulation is a big issue of privacy.

2.3. Security Measures and Solutions:

The metaverse presents several unique security challenges, but various measures have been proposed to address digital identity theft and privacy risks. One of the most significant solutions is to enhance the current forms of authentication and identity check. Authors such as Chen et al. (2021) have classified MFA as an adequate way of minimizing identity theft in virtual contexts. This is because MFA demands the use of several factors, they include password, fingerprint, face recognition or tokens hence reducing the chances of another person accessing the users' accounts.

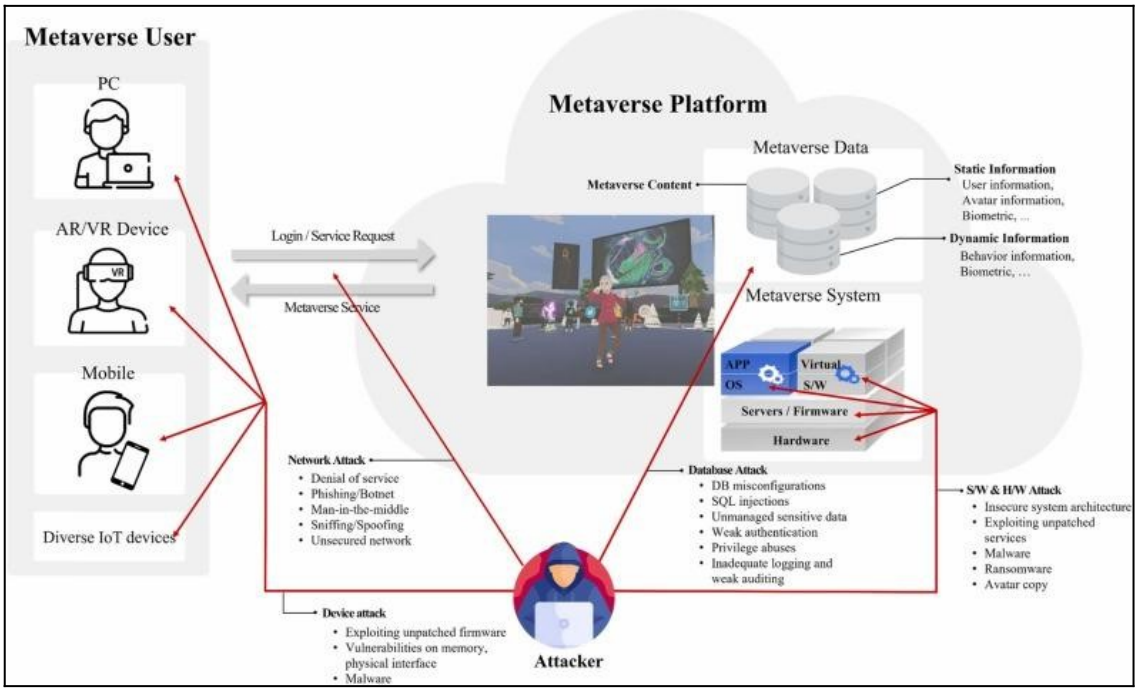

Figure 1 Metaverse Platforms (Dwivedi, 2022)

Technology of blockchain has also been recognized as a feasible solution for the identity management in metaverse. Termination of transactions and ownership of identities on blockchain is distributed and once data is recorded, it cannot be altered or deleted, thus adding more value to its applicability in cyberspace (Atlam et al., 2024). This means that, using the blockchain, consumers are able to retain their measures of privacy concerning their personal information and prevent abusing or unauthorised use of it by third parties by encoding it in smart contracts. In recent works of Habib et al. (2022), blockchain appears to be a nearly fault-free communication medium to document the user engagements and purchasing activities due to zero chance of cyber-attacks and scams. Some of the proposed solutions to prevent losing privacy in metaverse are Privacy-enhancing technologies (PETs), including end-to-end encryption, anonymity of data manipulation. Such technologies make it impossible for third parties to access user information while in transit or in storage (Chen et al., 2021). Also, as a continuation of the metaverse, decentralized VPNs effectively keep users' locations and activity in the metaverse anonymous.

Based on the same argument, procedures of adequate privacy policies and techniques of user consent should also be developed. For users to be able to regulate their data, the current privacy policies that organizations implement should state clearly the purpose for collecting data and ask for the users' permission for the collection of their data in simple language. Others have recommended the adoption of special data protection laws relevant to metaverse much as the GDPR but implemented in virtually-real environments (Lee, Zankl and Chang, 2016).

3. Methodology:

3.1. Research Design:

This study adopts a qualitative research design, combining a systematic literature review and semi-structured interviews to explore digital identity theft and privacy concerns in the metaverse. Thus, the current study best suits a qualitative investigation, as it focuses on providing a deeper understanding of the structures of perception and attitudes of metaverse users as well as new themes that arose during the study of safety and privacy in virtual environments. The quantitative analysis of existing research will allow identifying the existing knowledge on the subject while the qualitative data collected from cybersecurity specialists and Metaverse users will offer the contemporary view on the problem and actual experiences (Bryda and Costa, 2023).

3.2. Data Collection Tool:

Data for this study has been collected from two main sources: scientific secondary articles from the authentic databases and semi-structured interviews. The secondary has been collected from scholarly articles in these journals retrievable from Google Scholar, EBSCO, and JSTOR database. These sources give a wide list of articles discussing such topics as digital identity theft, privacy-related threats, and security measures in the context of virtual spaces and metaverse.

Primary data has been collected through semi-structured interviews with cybersecurity experts and metaverse users who had personal experiences or possess knowledge regarding the identity theft and other privacy issues in these areas. The interview includes an initial reading of certain questions to maintain a kind of openness, however, the interviewer sticks to certain topics that are of interest to the research including digital identity theft, privacy risks as well as potential solutions. Such an interviewing style allows for the subject expression of their ideas, and thus affords good quality qualitative data that can supplement the results of the literature analysis.

3.3. Data Collection Method:

The data collection process is segmented into two steps. The first step is a systematic literature review to identify peer-review data sources which leads to defining the theoretical background of digital identity theft and privacy issues in metaverse. Scientific articles from regional and international peer-reviewed journals, presentations at conferences, and official documents that are retrieved from Google Scholar, EBSCO, JSTOR. These articles give an understanding of the previous research works, models, and security measures in virtual ecosystems.

The second stage is carried out through the use of semi structured interviews with a purposive sampling from experts and users. The experts are the cyber security personnel while the users are those that have been involved in the metaverse. All interviews are virtual and have taken place via video conferencing tools, namely Zoom or Skype and then recorded for transcription.

3.4. Data Analysis Technique:

In this study thematic analysis technique is used to analyse data from secondary sources and interviews. This approach enables the researcher to search, code, and summarize observed Patterns (Themes) in the qualitative data. Thematic analysis has been conducted in a systematic manner: This method enables the current knowledge on these phenomena of digital identity theft and privacy risks in the metaverse gleaned through the literature review together with the first-hand data (Naeem et al., 2023).

3.5. Ethical Considerations:

The general principle of ethics is important for the protection of this research. The primary data was collected from the participants through a semi-structured questionnaire by initially taking their consent form while the secondary data collected from the peer-reviewed articles and secondary sources are used in a manner that are consistent with academic ethical standards by properly citing the authors' works. About the interviews, the subjects have read and signed informed consent, and they were told about their rights to leave the study at any time. All the answers given by participants were anonymised and the 'Collecting sensitive data' procedures were deployed to also ensure that nothing identifying about the participant. Additionally, participants were informed about the purpose of the study, the voluntary nature of their participation, and how the data will be used. All interview data was securely stored and only accessible to the research team. The study also ensures compliance with ethical guidelines related to data protection and confidentiality, in line with ethical review board requirements.

4. Results:

4.1. Analysis of the Extracted Findings:

After going through the interviews collected from Metaverse experts and users along with the data obtain from the systematic literature review, few patterns and themes were emerge, revealing that there are critical cybersecurity and privacy issues in the metaverse predominantly on how one can protect his or her identity (Pooyandeh et al., 2022). In a broader descriptive approach, many of the past studies have identified a general threat in AI-based metaverse and emphasize on the two-sided nature of AI as a security

tool and as the tool for threats exploitation. According to one of the participants there are numerous threats in regards to personal information and cybercrime. Moreover, one of the recent studies broadens the concept by identifying specific security gaps, including inadequate encryption and weak user authentication protocols, which leave digital identities susceptible to theft (Huang et al., 2023).

Garg (2024) also highlighted some significant findings by providing a detailed review of metaverse security frameworks arguing for an increased emphasis on creating privacy standards for the metaverse as well as developing a stronger system of authentication due to the high risk of identity theft. According to Mostafa et al. (2024) a behavioural approach shows that weakness of cybersecurity and the barriers resulted from technological factors as well as awareness levels of users also hindering situations in the metaverse. According to their results, efforts to improve cybersecurity and user interfaces are still possible.

In concern of this specific issue, almost all the participants discuss virtual operational; systems where poor identity verification or security walls jeopardises the operations in metaverse. However, Chen et al. (2022) suggests using both blockchain and biometric to serve the purpose of highly secure user identification. Taken together, all these studies foreground the interaction between technology, behaviour, and policy issues in tackling identity theft and other privacy issues in the metaverse.

4.2. Systematic Literature Review:

No	Study Title	Study Design	Population	Methods	Results	Sources (References)
1	Cybersecurity in the AI-Based Metaverse: A Survey	Quantitative Method	Cybersecurity Professionals	Descriptive method is applied and an anonymous survey. Open end survey was done to collect data.	The findings highlight that a cyber-situation management system based on artificial intelligence should be able to analyse data of any volume.	Pooyandeh, M., Han, K.-J. and Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences*, 12(24), p.12993. doi:https://doi.org/10.3390/app122412993
2	Metaverse Security and Privacy: An Overview	Quantitative Method	Metaverse users	Survey, adapted Digital reality and metaverse 2014 nationwide	This survey provides an in-depth review of the security and privacy issues raised by key technologies in Metaverse application.	Chen, Z., Wu, J., Gan, W. and Qi, Z. (2022). Metaverse Security and Privacy: An Overview. doi:https://doi.org/10.1109/bigdata55660.2022.10021112.
3	Security and Privacy in Metaverse: A Comprehensive Survey	Quantitative study	Users from different economic sectors	Open ended Survey was conducted to gather data and cause-and-effect relationships and probabilities.	The findings Metaverse is targeting to build a digital copy mapped from our real world with imaginary extension	Huang, Y., Li, Y.J. and Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Mining and Analytics*, 6(2), pp.234–247. doi:https://doi.org/10.26599/bdma.2022.9020047.
4	Evaluating the barriers affecting cybersecurity behaviour in the Metaverse using PLS-SEM and fuzzy set	Quantitative Method	395 Metaverse users	Open ended survey was conducted and regression analysis was used to analyse data.	The Metaverse, in essence, is not just a technological marvel; it heralds a transformative phase in the evolution of digital human interaction and experience	Mostafa Al-Emran, Al-Sharafi, M.A., Foroughi, B., Iranmanesh, M., Alsharida, R.A., Noor Al-Qaysi and Ali, N. (2024). Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and
5	Digital identities in the metaverse: Privacy, security, and user authentication in virtual financial	qualitative approach	Cross- case analysis	3 Case studies of different users were used to analyse the findings of the study. Thematic analysis	The successful cases examined demonstrate that a user-friendly experience and scalability are integral to the adoption of advanced security technologies.	Garg, K. (2024). Digital identities in the metaverse: Privacy, security, and user authentication in virtual financial systems. *International*

	systems			technique was used.		*Journal of Financial Engineering*. doi:https://doi.org/10.1142/s242478632442009x.

4.3. Thematic Analysis:

4.3.1. Theme 1: Security Vulnerabilities in Digital Identity Management:

The findings through the systematic literature review, and experts' interviews currently expose considerable security issues in the metaverse, including the nature and management of digital identities. The existing literature has revealed that there are certain gaps in encryption technologies, inadequate authentication mechanisms, and insufficient regulatory policies (Pooyandeh et al., 2022). These results are consistent across responses from metaverse specialists, who highlighted the threats of functioning in decentralized environments as well as the case of identity cloning. As for the basic concerns, users' remarks suggested that they fear that their avatars may be hacked and the information distorted or stolen. They agree that sound technological techniques like block chain and biometric authentication are necessary for strengthening identity protection.

4.3.2. Theme 2: Privacy Concerns and User Awareness:

Privacy concerns such as privacy intrusion with uncontrolled tracking, data collection from Web users, and poor compliance with users' consents became a recurrent issue. As expressed in (Chen et al., 2022; Huang et al., 2023), users exacerbate distrust due to the lack of transparency in the data usage and increased rate of cybercrimes. Interviews revealed a dichotomy: while experts from all disciplines advocated for policy actions and privacy by design, users often expressed minimal awareness and attention to existing privacy settings and protections. This points to an important gap of customer-oriented educational interventions that can equip people with information on how to protect their data in the metaverse.

4.3.3. Theme 3: Behavioural and Technological Barriers to Cybersecurity Adoption:

Barriers to cyber security adoption have been categorized as behavioural and technological and their integration is hindered. The literature (Garg, 2024; Mostafa et al., 2024) presented a concept of users' resistance caused by an overly intricate interface and inconvenience. Concerning the choice between user experience and security, experts stated that the platforms are designed by keeping users in mind, leaving little to security, meaning that security has become a trade-off for user experience. People complained about complicated security designs that do not allow the user to engage freely. This theme serves to stress the unmatched efficacy of creating easy-to-navigate applications and consciousness-raising in the sphere of the metaverse's cyber-safety.

5. Discussion:

The paper explores the two risks, namely, identity theft and privacy violation concerns in the metaverse through a systematic literature review and interviews. The research identifies critical gaps and opportunities for improving security and privacy frameworks in this rapidly evolving virtual ecosystem. Moreover, the findings of the study, extracted through collected data, identified the digital identity management risks as a concern and cybercrime issues that are significantly emerging in the world. The present encryption systems and authentication methods were criticized as inadequate techniques to deal with identity theft schemes in metaverse, which was shown in the research conducted by Chen et al. (2022). Such fears were supported with reference to cases across different countries, which was described as being both decentralised and centralised operations as the virtual platforms had too much power and the platform's structure was too decentralised. While decentralization strengthens user autonomy, it fails to provide general rules for implementing more secure solutions.

Another theme that was addressed in the study is privacy risks and threats, seen in both the literature of the field and user interviews regarding the insufficient processes involved in gaining consent and lack of clarity in how data is utilised. They complained about unauthorized tracking and the absence of rules regarding the use of collected data by companies behind metaverse platforms. It is (Pooyandeh et al., 2022) further suggested that the privacy-by-design principles could help to decrease risks but their implementation is still uneven. This calls for better regulation by governments and NPCAs and more drastic sensitisation of users on management of their privacy.

Behavioural and technological barriers to adopting cybersecurity measures present an additional layer of complexity. Whereas literature (Mostafa et al., 2024) in the study discussed the hesitance and fear of users when it comes to such complicated procedures, the interviews showed that the majority of them prefer convenience to security. This tension between usability and security indicates a critical design challenge for metaverse developers: designing processes that can implement and incorporate effective and deep cylinder-security protocols without complicating or ossifying the interface.

6. Conclusion:

In conclusion, this study reveals that despite technological innovations that might have fostered the development of the metaverse, there are enormous security and privacy issues resulting from the significant advancement that requires consideration and high attention. The synthesis of systematic literature and interview data highlights three interconnected themes like risks posed to security, privacy issues and challenges that organisations face in implementing and practicing cybersecurity. Accordingly, it is evident that none of these challenges can be best solved with a single approach of using technology, adjusting the laws, or educating the users.

Future studies could also look at the effectiveness of specific technological solutions like decentralized identity systems and biometric security in the decentralised environments that constitute metaverse and scan how well they are implemented across different metaverse spaces. Furthermore, further exploration of user behaviour and awareness can provide actionable insights for designing more intuitive and secure virtual environments. By such measures, the metaverse can become a safety-oriented, open, and people-oriented method of interaction in the management of the digital world.

References:

Atlam, H.F., Ndifon Ekuri, Muhammad Ajmal Azad and Harjinder Singh Lallie (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics*, [online] 13(17), pp.3568–3568. doi:https://doi.org/10.3390/electronics13173568.

Awadallah, A.M., Damiani, E., Mohamed Jamal Zemerly and Chan Yeob Yeun (2023). Identity Threats in the Metaverse and Future Research Opportunities. doi:https://doi.org/10.1109/icbats57792.2023.10111122.

Bryda, G. and Costa, A.P. (2023). Qualitative Research in Digital Era: Innovations, Methodologies and Collaborations. *Social Sciences*, [online] 12(10), p.570. doi:https://doi.org/10.3390/socsci12100570.

Canbay, Y., Utku, A. and Canbay, P. (2022). *Privacy Concerns and Measures in Metaverse: A Review*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ISCTURKEY56345.2022.9931866.

Chawki, M., Basu, S. and Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, [online] 13(3), p.33. doi:https://doi.org/10.3390/laws13030033.

Chen, Z., Wu, J., Gan, W. and Qi, Z. (2021). *Metaverse Security and Privacy: An Overview*. [online] Available at: https://arxiv.org/pdf/2211.14948.

Chen, Z., Wu, J., Gan, W. and Qi, Z. (2022). Metaverse Security and Privacy: An Overview. doi:https://doi.org/10.1109/bigdata55660.2022.10021112.

Dwivedi, Y.K. (2022). Metaverse beyond the hype: Multidisciplinary Perspectives on Emerging challenges, opportunities, and Agenda for research, Practice and Policy. *International Journal of Information Management*, [online] 66(66), p.102542. doi:https://doi.org/10.1016/j.ijinfomgt.2022.102542.

Enisa (2016). *ENISA*. [online] Europa.eu. Available at: https://www.enisa.europa.eu/.

Garg, K. (2024). Digital identities in the metaverse: Privacy, security, and user authentication in virtual financial systems. *International Journal of Financial Engineering*. doi:https://doi.org/10.1142/s242478632442009x.

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. and Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, [online] 14(11). doi:https://doi.org/10.3390/fi14110341.

Shahriar, H. (2024). Into the Metaverse: Technological Advances Shaping the Future of Consumer and Retail Marketing. *The Future of Consumption*, pp.55–75. doi:https://doi.org/10.1007/978-3-031-33246-3_4.

Huang, Y., Li, Y.J. and Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Mining and Analytics*, 6(2), pp.234–247. doi:https://doi.org/10.26599/bdma.2022.9020047.

Lee, W., Zankl, W. and Chang, H. (2016). *An Ethical Approach to Data Privacy Protection*. [online] ISACA. Available at: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection.

Mostafa Al-Emran, Al-Sharafi, M.A., Foroughi, B., Iranmanesh, M., Alsharida, R.A., Noor Al-Qaysi and Ali, N. (2024). Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA). *Computers in human behavior*, 159, pp.108315–108315. doi:https://doi.org/10.1016/j.chb.2024.108315.

Naeem, M., Ozuem, W., Howell, K.E. and Ranfagni, S. (2023). A step-by-step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, 22(1), pp.1–18. doi:https://doi.org/10.1177/16094069231205789.

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

Rashid, M. and Khan, M. (2024). Metaverse as Medium: Understanding the Revival of McLuhan's Notion 'Medium is the Message' in the Emergent Virtual Reality Landscape. *Journal of Communication and Cultural Trends*, [online] 6(1), pp.87–108. doi:https://doi.org/10.32350/jcct.61.05.

Wang, S. and Wang, W. (2023). A review of the application of digital identity in the Metaverse. *Security and Safety*, [online] 2, p.2023009. doi:https://doi.org/10.1051/sands/2023009.

Zhang, W. and Wu, H. (2023). Digital Identity, Privacy Security and their Legal Safeguards in the Metaverse. doi:https://doi.org/10.1051/sands/2023011.

Appendices:

Appendix A: Interview Questionnaire:

1. What do you think are the most prominent challenges users encounter when establishing and managing their digital identities in the metaverse?

2. In your opinion, how well do current metaverse platforms address privacy concerns, such as data protection and user consent?

3. How effective do you think the existing authentication and security protocols (e.g., passwords, biometrics) in the metaverse are in preventing identity theft?

4. How do you perceive the role of regulations and policies in ensuring digital identity protection and privacy in the metaverse?

5. How knowledgeable do you think the average user is about potential risks such as identity theft and privacy violations in the metaverse?

6. What innovative strategies or technologies do you believe could be implemented to enhance digital identity security and privacy in the metaverse in the future?

Appendix B: Informed Consent Form:

Objective and Procedure: I understand the purpose of this research and that I am voluntarily participating. The procedures have been explained clearly.

Name: _____

Date: _____

Research Title: _____

Researcher's Name: _____

Confidentiality and Data Use: I consent to the collection and storage of data as described, with my confidentiality being protected at all times.

Data Collected:

1. _____
2. _____
3. _____

Risks and Benefits: The potential risks and benefits of this research have been explained, and I agree to participate under these conditions.

Signature: _____

Researcher's Signature: _____

Date: _____