Volume 18, Issue 1, June 2023
https://doi.org/10.51153/mf.v18i1.622

Karachi Institute of Economics and Technology
KIET
Collaboration with Pakistan Air Force

Market Forces

Volume 18, Issue 1.
ISSN: 1816-8434(p), 2309-866X(e)

Home Page: https://kiet.edu.pk/marketforces/index.php/marketforces
DOI: https://doi.org/10.51153/mf.v18i1.622
Title: A Systematic Review in the World of the Metaverse

Affiliation:
Salman Hassan, University of Karachi, Karachi University Business School
Sohaib-uz-Zaman, University of Karachi, Karachi University Business School
Syed Hasnain Alam, University of Karachi, Karachi University Business School

Manuscript Information: Retrieved: February 20, 2023. Revised: May 18, 2023. Accepted May 20, 2023. Available online: June 28, 2023.

Citation:
Hassan, S., Zaman, S., Alam, S. A. (2023). A systematic review in the world of the metaverse. *Market Forces 18(1), 135-150.*

Conflict of Interest
The author (s) declared no conflict of interest and have not received any funds for the project.

A Systematic Review in the World of the Metaverse

Salman Hassan
University of Karachi, Karachi University Business School
Sohaib-uz-Zaman
University of Karachi, Karachi University Business School
Syed Hasnain Alam
University of Karachi, Karachi University Business School

Abstract

Metaverse uses "virtual reality" in e-commerce to create immersive virtual spaces. The philosophy behind it is to make people addicted to virtual 3d reality, and with the options of "teleportation, changing environment, and using cryptocurrency to shop," this will be the ultimate future of technology. Apart from the benefits of the metaverse, it has many challenges, including "cyber security." This study has synthesized past literature into nine themes based on a systematic review. All nine themes deal with the potential challenges and opportunities for users, including buyers and sellers. People can live an ideal life in the metaverse, leading to the denial mode of not accepting the real world and prefer living in the metaverse. For example, bald individuals can get a head full of hair in the metaverse. Someone with a disability can walk and fly in the metaverse. All these lucrative features will make virtual life more like heaven and real life like hell.

Keywords: *Virtual commerce; immersive technology; metaverse, cyber security, addiction, regulations.*

Introduction

Multiple users through a single browser can connect to multiple websites. Similarly, the metaverse is an online 3-D virtual space that allows users to interact, socialize, meet, and play games (Mystakidis, 2022). The concept of the metaverse is not new. The science fiction novel "Snow Crash" used this concept in 1992, which is now a reality (Wang et al., 2022). With the advancement of technology, consumers worldwide can connect

[1]Corresponding Author: Salman Hassan. Email: salmanhassankubs@gmail.com

and interact with each other (Kshetri, 2022). Internet-based smart devices, including smartwatches and smart mobiles, allow users to track each other activities and data. Many users collect and sell personal data of others (Buchholz, Oppermann, & Prinz, 2022).

Wang, Lee, Braud, and Hui (2022) assert that consumers are aware of the risks associated with using these devices but continue to use these devises because they offer many benefits. In most cases, the users are unaware that other users might collect their data. For example, when users talk on a smartphone, they don't realize that some users might be recording their conversations, adversely affecting their privacy (Damar, 2021). These devices collect different data types, including consumers' and behavior attitudes. It also collects data on users' physical and cultural values. Many consumers believe that these devices' benefits outweigh the privacy risks. (Al-Suwaidi & Zemerly, 2009). VR, an essential component of the metaverse, can compromise users' privacy. Mozumder et al.(2022) assert that metaverse users must show sensible social behavior. The metaverse duplicates what individuals find in real life, for instance, structures, roads, and people. It has the capability of constructing things that do not exist.

In the following sections, we have discussed the methodology, followed by the literature review and conclusion.

Methodology

Based on a systematic literature review, this research paper gives an overview of the metaverse from a broad perspective. It also focuses on the potential challenges and solutions for the metaverse users. A systematic literature review is considered a rigorous approach. Using it, the authors identify, evaluate, and interpret available literature relevant to the research topics. This paper adopted literature that has examined the attitudes and behaviors of metaverse users and the challenges they face. We have used this approach to study multiple emerging topics in information communication systems, including the application of VR/AR (Duan et al., 2021), usage of blockchain systems to protect the digital twins inside the metaverse (Chen, Lee, Chang, Choo, & Zhang, 2019), privacy concerns of bystanders and non-users (Aditya et al., 2016), and social metaverse (Al-Suwaidi & Zemerly, 2009; Shu, Zheng, & Hui, 2018).

This paper reviewed relevant research papers from eight online scholarly databases, including Emerald, Science Direct, Scopus, EBSCO, Web of Science, Wiley, ProQuest, and SpringerLink. The eligible criteria to review the papers ensured that all included results could contribute to at least one of the four research questions. Furthermore, the methodology of this paper aligns with the guideline of a systematic review previously

used by Kitchenham (2007). It includes preparation, analysis, and reporting. The study specifically addresses the following research questions.

1. How do clients behave towards the metaverse?
2. What are the significant privacy challenges metaverse users face?
3. What are the possible solutions for users in virtual commerce?
4. What are the possible solutions for metaverse users in application design?

Criteria for Selecting Research Papers

Table 1 depicts the criteria we used to exclude and include the research papers.

Table – 1 Criteria for Selecting Each Research Paper

1. Exclusion	2. Inclusion	3. Eligibility	4. Relatedness
We excluded papers whose full-text version is not available.	We Included papers whose full test version is available.	Originally published papers in reputed academic journals were eligible	Answer question Q1 and either Q2 and Q3 or Q4.
Research papers that are not relevant to the metaverse.	Research papers are relevant to the metaverse.	Research papers that were complete in all aspects	--
The language of the papers is not English.	The language of the papers is English.	Address a research topic related to the metaverse.	--

Challenges and Potential Solutions

Challenge 1: Privacy and Identity

In the metaverse, people can make avatars based on their appearance in the real world or use fictitious personal data, including name, age gender. Many users use fictitious data as they do not want to disclose their real identity to other avators (Wang et al., 2022). Players can interact and watch the user's activities using symbols while playing the game. For instance, in the game "Second Life - an open-world social metaverse," the players can use a symbol instead of a real name (Antin, 2020). Far and Rad (2022) assert that one of the limitations of VR technology is the users are not sure who is watching or following them. The literature suggests that the users act in the metaverse in the same manner as they would in real life. Thus, their attitudes and behaviors in the metaverse may resemble their real-life attitudes and behaviors (Leenes, 2008).

As refer above, users are vulnerable to constant observation when their avatar interfaces with different ones in the metaverse. Players can protect themselves from

the threat of security, risk, and vigilance of others by using multiple avatars (Far & Rad, 2022). The users can make different avatars and behave differently in each. This strategy may confuse other avatars as they cannot distinguish between the avators using real or fictitious personal data (Canbay, Utku, & Canbay, 2022). The avatar can have different configurable ways of behaving. For instance, while purchasing a product in the metaverse, the user can create one more avatar that purchases the same product. This strategy may confuse the attackers about who the real avatar is (Ghirmai et al.,2023). Alternatively, the avatar can make temporary and private copies of a piece of the metaverse (e.g., a recreation area). Through this approach, the attacker will not be able to listen to the user (Japar et al., 2023).

API integrates the duplicate copies of the metaverse by merging them with the main metaverse. If the private portion of the metaverse and the main metaverse is not fully aligned and updated, it will create problems for the users in the future (Mitrushchenkova, 2023). A potential solution to the privacy problem is that the users create their invisible avatars in the metaverse. It will allow them to communicate with others without the fear of being monitored (Kalyvaki, 2023). Since private duplicates restrict the sharing of the assets of primary texture, it will be difficult for others to copy them. Tran et al.(2023) assert that in these virtual situations, fakes and substitute portrayals can adversely affect clients' attitudes and behavior.

In the metaverse, the created virtual universes can be dangerous in the context of security. For example, fake portrayals may confuse and deceive users since they may not be able to distinguish between real and fake portrayals (Mitrushchenkova, 2023). The attacker can develop creative ideas that create a fearful sense of urgency. Consequently, the users may disclose their personal and secure information to the attackers leading to scam/fraud in the metaverse. For example, the users may disclose the private key of the cryptocurrency wallet or any other financial or private information, which may eventually hurt the users (Gupta et al., 2023). Users are vulnerable to many security and privacy risks in the virtual world. Many strategies are available for protecting users from unwarranted security risks (Bibri & Allam, 2022). The attackers in the metaverse learn what clients intend to purchase. Using this knowledge, they may develop comparable virtual items which the client may purchase deceptively (Mitrushchenkova, 2023).

Challenge 2: Governance of Ethics and Laws

Alternate aspects, such as deep fakes in the metaverse, can adversely hurt users (Fernandez & Hui, 2022). McStay (2023) asserts a need for regulating and governing in the metaverse. For example, in the US, there are regulations regarding privacy and security in the context of the metaverse (Leenes, 2008). Mitrushchenkova (2023) asserts that the growth and popularity of the metaverse significantly depend on making ethical

laws for users. Thus, regulators must develop codes of conduct to monitor users' chat logs and conversations (Ferebee, 2022).

Such regulations can assist the metaverse developers in banning users reported for using fraudulent means to deceive consumers. The governance aspects may include restrictions and penalties for the banned users (Kasiyanto & Kilinc, 2022). The rules and regulations may vary from one country to another. Therefore, the metaverse may have to align with the rules and regulations of the host country (Qu, 2022). Few authors believe that the gradual implementation of tools and techniques will allow specific groups to control their group members, similar to a federated model. The metaverse users can create specific rules and regulations, like allowing entrance to users with similar affinities (Anshari et al., 2022). Blockchain technologies will also force users to adhere to the rules and regulations. Such rules and regulations will guide users to behave according to rules and regulations, discouraging misbehaviors. The creators of the metaverse can punish users who fail to follow the rules and regulations (Kasiyanto & Kilinc, 2022)

Challenge 3: The Protection of Digital Twins

Digital twins mean creating virtual objects that resemble the original in terms of "physical appearances and behavioral performance" (Far & Rad, 2022). Such objects can clone "real-world objects and systems" (Lv et al., 2022). The interactions in the metaverse are crucial as they improve physical systems, resulting in innovation and enhancing user experience (Jamshidi Ebadpour & Moghani, 2022). Metaverse must protect digital twins by close monitoring and ensuring that created digital twins resemble the original (Rasheed, San, & Kvamsdal, 2020). Thus to protect digital twins, the metaverse must have an effective information system. Blockchain, with a mechanism of a distributed single chain, helps store data inside a cryptographic block (Nofer, Gomber, Hinz, & Schiereck, 2017). Blockchain systems use biometric data to store and protect digital twins (Han et al., 2022). The peer-to-peer network verifies and validates each new block before including the new record in the chain (Reyna, Martín, Chen, Soler, & Díaz, 2018). Recent application development has made it possible to launch non-fungible tokens (NFT), a new form of a digital ecosystem market (Sghaier Omar & Basir, 2020). It allows digital twin creators to classify their products as new, innovative, and unique (Han et al., 2022).

Challenge 4: Safeguarding Biometric Data

Metaverse using data from the physical world, such as hand movements, creates an immersive user experience (Duan et al., 2021). The introduction of gadgets such as "VR head-mounted displays, unique wearables such as gloves and special suits" can provide a more realistic and immersive experience in the metaverse. These devices give users more control over their avatars (Egliston & Carter, 2021). Another example would be

a different sensor attached to the user, such as a gyroscope, to track the user's head movements (Smith et al., 2023). The "biometric integrates input and output data." As a result, users can have a holistic experience interacting with other avatars (Duan et al., 2021). At the same, these biometric data have several disadvantages for users, including more vulnerability to privacy threats (Smith et al., 2023). McSta (2023) asserts that digital twins generate real digital assets in the metaverse using real biometric data. Thus digital twins, on the one hand, need to protect the data from attacks and, on the other hand, ensure its accessibility to digital twins and other related devices.

Challenge 5: Ease of Digital Attacks

Users of the metaverse ecosystem are vulnerable to privacy and leakage issues. Therefore developers must pay attention to it in the earlier stages. If they do not address these issues, the developers may have to redesign it from scratch, resulting in a loss of data and time (Acquisti, Taylor, & Wagman, 2016; Nofer, Gomber, Hinz, & Schiereck, 2017). For example, the "third-party cookies-based advertisement ecosystem" was based on cookies that mainly keep track of users' activities for providing personal advertisements. Since the system had significant privacy concerns, privacy regulators like GDPR had to intervene. Google decided to eliminate third-party cookies from Chrome in 2022, killing the "third-party cookies-based advertisement ecosystem" (Aditya et al., 2016; Shu, Zheng, & Hui, 2018). In recent years the public has protested the ubiquitous presence of technologies in the metaverse. Despite all the good intentions of the devise owners, the users are still unsure about the privacy and security of data. Subsequently, many developers, designers, and users offered a solution to tackling the issues arising from the "ubiquitous presence of technologies" (Aditya et al., 2016; Shu, Zheng, & Hui, 2018). A system with a built-in verifiable mechanism may increase its social acceptability. At the same time, if the users are not worried about sharing their data, the new system will not face any social desirability issues (Dilibal & Tur2022).

Users are not bothered if they know how other parties use their data. However, they protest if they find variations in data's perceived and actual usage. For example, many Facebook users share their data willingly (Canbay, Utku, & Canbay, 2022). However, users strongly protested when they found that Cambridge Analytica Data misused their data. As a result, "The US Congress and the UK parliament" summoned Facebook and Cambridge Analytica. Subsequently, Cambridge Analytica had to file for bankruptcy (Confessore, 2018). Besides many solutions, one suggests not collecting users' data. However, this may be counterproductive in terms of growth and innovation. The German Chancellor Angela Merkel proposed another solution that enables users to sell their data for monetary or non-monetary benefits. Many researchers have also given valuable insight into the "economics of privacy" and the structure for "efficient privacy

trading" (Pal et al., 2018). Implementing the above concepts may enhance the data flow and compensates users adequately for their data (Sen, Joe-Wong, Ha, & Chiang, 2013).

Challenge 6: Addiction

The most important issue with the extensive growth of the metaverse is people spending excessive time in the virtual digital environment leading to addiction (Bojic, 2022). Extant literature suggests numerous people are already addicted to virtual cyberspaces and social networking sites (Liu & Gao, 2022). Like all addictions, metaverse-addicted users will use it to escape "real-world problems" (Dutilleux & Chang, 2022). It's a bitter reality, but user addictions to digital spaces and the virtual world may lead to psychological and mental disorders, including depression, loneliness, and aggression (Kerdvibulvech, 2022).

The COVID-19 pandemic has provided a viable and efficient alternative to physical meetings and social interaction in the form of virtual meetings. Many researchers believe excessive and extensive virtual meetings may lead to abuse or addiction to the Internet (López- García, Sánchez Gómez, & García-Valcárcel Muñoz-Repiso, 2020). Extant literature documents AR/VR platforms are examples of metaverse addiction. Many studies have examined the causes of behavioral addiction in VR and their treatments (Segawa et al., 2020). AR games such as Pokémon Go can also help learn the behavioral changes of mega players, such as spending patterns, group-oriented actions in urban areas, and dangerous actions in the actual world. All these behavior changes can have a destructive impact on society (Colley et al., 2017). The virtual environment allows users to engage in "impossible or immortal" activities. It is highly likely that in the metaverse, users "could experience super-realism," which mainly means that they will engage in activities that"resemble the real world."It may include experiencing racial attacks (Lewis & Taylor-Poleskey, 2021).

Challenge 7: Cyberbullying

Cyberbullying means bullying a person in cyberspace. It may include posting harmful content in cyberspace, posting hate speech, making fun of someone's physical disability, and making jokes about ethnicity (Chatzakou et al., 2019). Metaverse is a humongous cyberspace, and cyberbullying in the metaverse will be inevitable. In the long run, the metaverse will not be able to operate on a full scale without regulations regarding cyberbullying. The authorities will then have to step up and shut down some virtual spaces where they deduct cyberbullying in the metaverse. Using algorithms can help to detect cyberbullying (Yan et al., 2021). The balanced approach of such algorithms (Singh & Hofenbitzer, 2019) will have perceived fairness to all the users in the metaverse. If the metaverse regulator fails to take timely action against cyberbullying

users, it can seriously hurt the customer journey in the metaverse (Qasem et al., 2022; Yıldız & Tanyıldızı, 2023; Tugtekin, 2023; Anshari et al. 2022).

Challenge 8: The Environment

The virtual world records all user activities, like some social media websites that monitor users, record data, and sell it commercially (Sá & Serpa, 2023). The same can happen in the 3D virtual world, where it will record every activity, even the smallest detail, like an avatar looking at the billboard twice or the avatar taking an interest in the virtual shop selling sneakers (Mystakidis, 2022). Subsequently, the virtual environment will show the advertisement/ billboard or the environment related to users' interests.

For instance, if users like flowers, the display will show them a garden full of roses. Keeping a record of users'physical touch is required so the environment can react to their actions (Rillig et al., 2022). For instance, if a user flips a page in a book in the metaverse, the reaction will be a flip of a page. All this will happen through the tracking of the avatar activities so that the environment can respond to the action accordingly (López García, Sánchez Gómez, & García-Valcárcel Muñoz-Repiso, 2020). A highly customized avatar helps the user to escape personality deficiency. The metaverse creates an environment per user liking. For example, bald people can have an avatar full of hair in the metaverse.

Similarly, persons with a physical disability can have an athletic body in the metaverse. The feeling of perfection will make it an inescapable virtual room for the users. (Carter, 2022). It is one reason all the big brands are jumping into the metaverse world. Literature suggests that the metaverse could become a $13 trillion market by the end of 2030 with a whopping 5 billion users. "Metaverse will be a most popular place to buy, trade, and store cryptocurrency" (Metaverse Bitcoin News, n.d.). Continuous improvements in the metaverse environment aim to make it look close to reality (Zauskova, Miklencicova, & Popescu, 2022).

Conclusion and Recommendations

In the present era, consumers' attention has shifted toward social media. The platforms will be more interactive and closer to reality. They aim to ensure people spend time in the metaverse rather than the real world. The investment into the metaverse will promote engaging content just like social media. It will allow forward-thinking brands to display their products or advertisements in the metaverse (Kim, 2021). The primary goal of these brands is to engage customers with interesting content. The more engaging the contents are, the more money the brands will earn (Holsapple & Wu, 2007). All big brands may spend their resources on social media. As a result, the jobs for digital content creators may increase.

The same will go for the metaverse. The idea behind it is to make people addicted to virtual 3d reality, and with the options of teleportation, changing environment, and using cryptocurrency to shop, this will be the ultimate future of technology. People can live a perfect life in the metaverse. They eventually will get into the denial mode of not accepting the real world and prefer to live in the metaverse. For example, bald individuals can get a head full of hair in the metaverse. Someone with a disability can walk and fly in the metaverse. All these lucrative features will make virtual life a dream life more like heaven and real life as hell (Luke & Evelina, 2017; Ding, Xu, Chen, & Xu, 2016).

Reference

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54(2)*, 442–492.

Aditya, P., Sen, R., Druschel, P., Joon Oh, S., Benenson, R., Fritz, M., ... & Wu, T. T. (2016, June). I-pic: A platform for privacy-compliant image capture. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (pp. 235-248)*.

Al-Suwaidi, G. B., & Zemerly, M. J. (2009, May). Locating friends and family using mobile phones with global positioning system (GPS). In *2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 555-558)*. IEEE.

Antin, D. (2020, May 24). How the Virtual World "Second Life" is a Showcase of the Metaverse. {Available}.https://medium.com/super-jump/how-the-virtual-world-second-life-is-a-showcase-of-the-metaverse-5bd9fb67450.

Anshari, M., Syafrudin, M., Fitriyani, N. L., & Razzaq, A. (2022). Ethical Responsibility and Sustainability (ERS) Development in a Metaverse Business Model. *Sustainability*, *14(23)*, 1-17.

Bibri, S. E., & Allam, Z. (2022). The metaverse as a virtual form of data-driven smart cities: The ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society. *Computational Urban Science*, *2(1)*, 22-37

Bojic, L. (2022). Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality? *European Journal of Futures Research*, *10(1)*, 1-24.

Buchholz, F., Oppermann, L., & Prinz, W. (2022). There's more than one metaverse. *i-com*, *21(3)*, 313-324.

Canbay, Y., Utku, A., & Canbay, P. (2022, October). Privacy Concerns and Measures in Metaverse: A Review. In *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)* (pp. 80-85). IEEE.

Carter, D. (2022). Immersive Employee Experiences in the Metaverse: Virtual Work Environments, Augmented Analytics Tools, and Sensory and Tracking Technologies. *Psychosociological Issues in Human Resource Management*, *10(1*), 35-49.

Chatzakou, D., Leontiadis, I., Blackburn, J., Cristofaro, E. D., Stringhini, G., Vakali, A., & Kourtellis, N. (2019). Detecting Cyberbullying and Cyberaggression in Social Media. *ACM Transactions on the Web*, *13(3)*, 1–51.

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, *95*, 420–429.

Colley, A., Wenig, N., Wenig, D., Hecht, B., Schöning, J., Thebault-Spieker, J., Lin, A. Y., Degraen, D., Fischman, B., Häkkilä, J., Kuehl, K., Nisi, V., & Nunes, N. J. (2017). The Geography of Pokémon GO. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17.*

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. {Available} .https://www nytimes.com/2 018 /04/04 /us pol itics cambridge-analytica-scandal-fallout.html

Damar, M. (2021). Metaverse shape of your life for future: A bibliometric snapshot. *Journal of Metaverse*, *1(1)*, 1-8.

Dilibal, C. and Tur, Y., (2022). Implementation of Developed Esantem Smart Healthcare System in Metaverse. In *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1027-1031)*. IEEE.

`Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021, October). Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia (pp. 153-161)*.

Dutilleux, M., & Chang, K. M. (2022). Future Addiction Concerned for Human-Being. *International Multilingual Journal of Science and Technology*, *7(2)*, 4724-4732.

Egliston, B., & Carter, M. (2021). Critical questions for Facebook's virtual reality: Data, power and the Metaverse. *Internet Policy Review*, *10(4)*, 1-23.

Far, S. B., & Rad, A. I. (2022). Applying digital twins in Metaverse: User interface, security and privacy challenges. *Journal of Metaverse*, *2(1)*, 8-15.

Ferebee, S. S. (2022). Metaverse: The Ethical Dilemma. In *Exploring Ethical Problems in Today's Technological World (pp. 315-330)*. IGI Global.

Fernand`ez, C. B., & Hui, P. (2022). Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse. In *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)* (*pp. 272-277)*. IEEE.

Gupta, A., Khan, H. U., Nazir, S., Shafiq, M., & Shabaz, M. (2023). Metaverse Security: Issues, Challenges and a Viable ZTA Model. *Electronics*, *12(2)*, 391.

Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2023). Self-Sovereign Identity for Trust and Interoperability in the Metaverse. *Arxiv. Ahead of Print*.

Holsapple, C. W., & Wu, J. (2007). User acceptance of virtual worlds. *ACM SIGMIS Database*, *38(4)*, 86-102.

Han, Y., Niyato, D., Leung, C., Kim, D. I., Zhu, K., Feng, S., ... & Miao, C. (2022). A dynamic hierarchical framework for d digital twin synchronization in the metaverse. *IEEE Internet of Things Journal*, *10(1)*, 268-284.

Jamshidi, M. B., Ebadpour, M., & Moghani, M. M. (2022, December). Cancer Digital Twins in Metaverse. In *2022 20th International Conference on Mechatronics-Mechatronika (ME) (pp. 1-6)*. IEEE.

Japar, M. H. P. H. M., Anshari, M., & Sumardi, W. H. H. (2023). Privacy and Security Concerns in the Metaverse. In *Metaverse Applications for New Business Models and Disruptive Innovation (pp. 133-149)*. IGI Global.

Kalyvaki, M. (2023). Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*, *3(1)*, 87-92.

Kasiyanto, S., & Kilinc, M. R. (2022). The Legal Conundrums of the Metaverse. *Journal of Central Banking Law and Institutions*, *1(2)*, 299-322.

Kim, J. (2021). Advertising in the Metaverse: Research Agenda. *Journal of Interactive Advertising*, *21(3)*, 1–4.

Kerdvibulvech, C. (2022). Exploring the impacts of COVID-19 on digital and metaverse games. In *HCI International 2022 Posters: 24th International Conference on Human-Computer Interaction, HCII 2022, Virtual Event, June 26-July 1, 2022, Proceedings, Part III (pp. 561-565)*. Cham: Springer International Publishing.

Kshetri, N. (2022). Web 3.0 and the metaverse shaping organizations' brand and product strategies. *IT Professional*, *24(02)*, 11-15.

Leenes, R. (2007). Privacy in the metaverse: Regulating a complex social construct in a virtual world. In IFIP International Summer School on the Future of Identity in the Information Society (pp. 95-112). Boston, MA: Springer US.

Lewis, R., & Taylor-Poleskey, M. (2021). Hidden Town in 3D. *Journal on Computing and Cultural Heritage*, *14(2)*, 1–14.

Liu, J., & Gao, G. (2022, December). The Metaverse: The Essential Characteristics of "Full Body Immersion" and the Risk of Addiction. In *2022 6th International Seminar on Education, Management and Social Sciences (ISEMSS 2022) (pp. 3564-3569)*. Atlantis Press.

López-García, C., Sánchez Gómez, M. C., & García-Valcárcel Muñoz-Repiso, A. (2020). Scales for measuring Internet Addiction in Covid-19 times: Is the time variable still a key factor in measuring this addiction? *ACM International Conference Proceeding Series*, 600–604.

Luke, J. Y., & Evelina, L. W. (2017). Exploring Indonesian young females online social networks (OSNs) addictions. *Proceedings of the 3rd International Conference on Communication and Information Processing*.

Lv, Z., Xie, S., Li, Y., Hossain, M. S., & El Saddik, A. (2022). Building the Metaverse by Digital Twins at All Scales, State, Relation. *Virtual Reality & Intelligent Hardware*, *4(6)*, 459-470.

McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy & Technology*, *36(1)*, 13-27.

Metaverse Bitcoin News. (n.d.). Retrieved March 5, 2023, from news.bitcoin.com website: https://news.bitcoin.com/metaverse-most-popular-place-to-buy-trade-store-cryptocurrenc y/

Mitrushchenkova, A. N. (2023). Personal Identity in the Metaverse: Challenges and Risks. *Kutafin Law Review*, *9(4)*, 793-817.

Mozumder, M. A. I., Sheeraz, M. M., Athar, A., Aich, S., & Kim, H. C. (2022, February). Overview: Technology roadmap of the future trend of metaverse based on IoT, blockchain, AI technique, and medical domain metaverse activity. In *2022 24th International Conference on Advanced Communication Technology (ICACT) (pp. 256-261)*. IEEE.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2(1)*, 486-497.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59(3)*, 183–187.

Pal, R., Crowcroft, J., Kumar, A., Hui, P., Haddadi, H., De, S., Ng, I., Tarkoma, S., & Mortier, R. (2018). *Number 925 Privacy markets in the Apps and IoT age*. https ww w .c l.c am. ac. U k/techreports/UCAM-CL-TR-925.pdf

Qasem, Z., Hmoud, H. Y., Hajawi, D. A., & Al Zoubi, J. Z. (2022). The Effect of Technostress on Cyberbullying in Metaverse Social Platforms. In *Co-creating for Context in the Transfer and Diffusion of IT: IFIP WG 8.6 International Working Conference on Transfer and Diffusion of IT, TDIT 2022, Maynooth, Ireland, June 15–16, 2022, Proceedings (pp. 291-296)*. Cham: Springer International Publishing.

Qu, Y. (2022, December). Analysis of the Realization of the Rule of Law Ethics in Meta-cosmic Relevance. In *2022 6th International Seminar on Education, Management and Social Sciences (ISEMSS 2022) (pp. 2770-2780)*. Atlantis Press.

Rasheed, A., San, O., & Kvamsdal, T. (2020). Digital Twin: values, challenges and enablers from a modeling perspective. {Available}. https://doi.org/10.1109/access.2020.2970143.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190.

Rillig, M. C., Gould, K. A., Maeder, M., Kim, S. W., Dueñas, J. F., Pinek, L., … & Bielcik, M. (2022). Opportunities and risks of the"Metaverse"for biodiversity and the environment. *Environmental Science & Technology*, *56(8)*, 4721-4723.

Sá, M. J., & Serpa, S. (2023). Metaverse as a Learning Environment: Some Considerations. *Sustainability*, *15(3)*, 1-13.

Segawa, T., Baudry, T., Bourla, A., Blanc, J.-V., Peretti, C.-S., Mouchabac, S., & Ferreri, F. (2020). Virtual Reality (VR) in Assessment and Treatment of Addictive Disorders: A Systematic Review. *Frontiers in Neuroscience*, *1-13*.

Singh, V. K., & Hofenbitzer, C. (2019). Fairness across network positions in cyberbullying detection algorithms. *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*.

Sghaier Omar, A., & Basir, O. (2020). Capability-based non-fungible tokens approach for a decentralized AAA framework in IoT. *Advances in Information Security*, 7–31.

Shu, J., Zheng, R., & Hui, P. (2018). Cardea. *Proceedings of the 9th ACM Multimedia Systems Conference*, 304–315.

Smith, C. H., Molka-Danielsen, J., Rasool, J., Webb-Benjamin, J. B., & UK, K. L. (2023, January). The world as an interface: exploring the ethical challenges of the emerging metaverse. In *Proceeding of the Hawaii International Conference System Sciences, Maui, HI (pp. 6045-6054)*.

Tran, N. C., Wang, J. H., Vu, T. H., Tai, T. C., & Wang, J. C. (2023). Anti-aliasing convolution neural network of finger vein recognition for virtual reality (VR) human–robot equipment of metaverse. *The Journal /of Supercomputing*, *79(3)*, 2767-2782.

Tugtekin, U. (2023). The Dark Side of Metaverse Learning Environments: Potential Threats and Risk Factors. In *Shaping the Future of Online Learning: Education in the Metaverse (pp. 57-67)*. IGI Global.

Wang, F. Y., Qin, R., Wang, X., & Hu, B. (2022). Metasocieties in Metaverse: Metaeconomics and metamanagement for metaenterprises and metacities. *IEEE Transactions on Computational Social Systems*, *9(1)*, 2-7.

Wang, Y., Lee, L. H., Braud, T., & Hui, P. (2022, July). Re-shaping Post-COVID-19 teaching and learning: A blueprint of virtual-physical blended classrooms in the metaverse era. In *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW) (pp. 241-247)*. IEEE.

Yan, R., Li, Y., Li, D., Wang, Y., Zhu, Y., & Wu, W. (2021). A Stochastic Algorithm Based on Reverse Sampling Technique to Fight Against the Cyberbullying. *ACM Transactions on Knowledge Discovery from Data*, *15(4)*, 1–22.

Yıldız, İ., & Tanyıldızı, N. İ. (2023). An Analysis of News Containing Cyberbullying in the Metaverse. In *Handbook of Research on Bullying in Media and Beyond (pp. 196-214)*. IGI Global.

Zauskova, A., Miklencicova, R., & Popescu, G. H. (2022). Visual Imagery and Geospatial Mapping Tools, Virtual Simulation Algorithms, and Deep Learning-based Sensing Technologies in the Metaverse Interactive Environment. *Review of Contemporary Philosophy*, *21*, 122-137.