International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 7, pp. 1125-1132
doi: 10.25147/ijcsr.2017.001.1.122
https://stepacademic.net

Short Paper *

A Review of Metaverse and Cybersecurity in the Digital Era

Parichat Jaipong
Manipal GlobalNxt University, Malaysia
iam.parichatt@gmail.com
ORCID ID: orcid.org/0000-0002-9249-3169
(corresponding Author)

Sutithep Siripipattanakul
Kasetsart University, Thailand
fedustt@ku.ac.th
ORCID ID: orcid.org/0000-0002-5477-6723

Patcharavadee Sriboonruang
Kasetsart University, Thailand
fagrpds@ku.ac.th
ORCID ID: orcid.org/0000-0002-2171-2387

Tamonwan Sitthipon
University of Geomatika, Malaysia
tamonwan.f@gmail.com
ORCID ID: orcid.org/0000-0002-2280-7871

Date received: August 21, 2022
Date received in revised form: October 3, 2022*;* November 3, 2022
Date accepted: November 4, 2022

Recommended citation:

Jaipong, P., Siripipattanakul, S., Sriboonruang, P., & Sitthipon, T. (2023). A Review of Metaverse and Cybersecurity in the Digital Era. *International Journal of Computing Sciences Research*, *7*, 1125-1132. https://doi.org/10.25147/ijcsr.2017.001.1.122

**Special Issue on Metaverse and Cybersecurity in the Digital Economy. Guest Editor: Supaprawat Siripipatthanakul, Ph.D. Supervisor & Lecturer at University of Geomatika, Malaysia; DBA Researcher at Manipal GlobalNxt University, Malaysia.*

ABSTRACT

Purpose – Adoption of the metaverse may increase cybersecurity risks. This study evaluates the literature on metaverse and cybersecurity in the digital era.

Method – A narrative synthesis was used in this review article. The literature and information were reviewed systematically to explore metaverse and cybersecurity in the digital era from various books and research articles on EBSCO, Google Scholar, Scopus, Web of Science, and ScienceDirect. The inclusion criteria were studies that clearly defined metaverse and cybersecurity in the digital era, were published and written in English and were peer-reviewed. Moreover, content analysis was employed.

Results – The results reveal that the metaverse is a crucial future innovation of digital technology in the digital era. The metaverse adoption may multiply cybersecurity risks. Furthermore, the importance of financial cybercrime in the metaverse for authorities, corporations, and individuals to address has grown, necessitating new regulatory and compliance frameworks and novel cybersecurity mechanisms. As a result, cybersecurity is considered necessary.

Conclusion – The metaverse is an essential technology with both advantages and disadvantages. The metaverse concept is expected to be central to future development and will provide significant benefits. However, its adoption may cause cybersecurity risks. Cybersecurity is essential to reduce those risks.

Recommendations – The recommendation is to consider a quantitative study, such as surveys, regarding metaverse and cybersecurity in the digital era. Also, a qualitative approach, such as interviews, could give a clear view of insight results for further study.

Research Implications – This review article contributed to the literature on metaverse and cybersecurity in the digital era. Therefore, it could guide future research on metaverse and cybersecurity in the digital age. It may also aid academics in broadening their research by incorporating more potential elements.

Keywords – metaverse, cybersecurity, digital economy, technology, digitalisation

INTRODUCTION

The metaverse is the vital future iteration of the internet (Nath, 2022). The metaverse's basic principle is to blur the boundaries between the virtual and real worlds, allowing users to accomplish everything in the real world using technological devices in virtual space. It began with human-computer interaction and has since evolved into an online network of virtual worlds. Moreover, the metaverse's characteristics make it suitable for use in massively multiplayer online scenarios such as multiplayer games, multiplayer video chat, distance learning, remote work, and so on (Tan, 2022). In addition, the metaverse is currently conceptualised in various sections and parts, but an entire metaverse is seen as the next computing platform and internet extension. The first

metaverse concept was implemented successfully in the game Second Life. Second Life is a video game or website launched in 2003 that allows users to join and experience a second life in the virtual world. In the virtual world, they can assume any identity and play any role. Web3D enables people to play the role of an avatar in a virtual world, where they can explore, meet other residents, participate in individual, group, or both activities, and so on, just as they would in real life (Nath, 2022).

Much of people's lives in the twenty-first century are spent communicating via technology. It has become a part of human existence. Moreover, since the COVID-19 pandemic, it has become more prevalent in work, study, and leisure (Noronha-Sousa et al., 2022). If looking for meaning in the communication message, it can refer to the entire communication technology as cyberspace. Cyberspace is a new combination of mass media and technology. Complete with its practices, behaviours, and manifestos, working cyberspace can be considered a global basis of human existence in the same way that clean air or the absence of a pandemic is. While cyberspace is resistant to total control, it is still fragile and needs to be protected if humans reap its benefits (Adamson, 2021). Furthermore, financial cybercrime in the metaverse has grown in importance for authorities, corporations, and individuals to address, necessitating new regulatory and compliance frameworks and novel cybersecurity mechanisms. Financial cybercrime has increased significantly in the metaverse, with either massive stealing of cryptocurrencies from exchanges or the sale of fake or dubious non-fungible tokens (NFT) and other financial products that have lost significant value in a short period. Cybercrime has occurred on a large scale in the metaverse. Still, due to the infancy of regulations and the virtual nature of these activities, only a few crimes have been prosecuted (Katterbauer et al., 2022). Hence, cybersecurity is necessary because it simply protects the immediate, practical, and ongoing technological elements (Adamson, 2021). Thus, this review article evaluates the literature on metaverse and cybersecurity in the digital era.

LITERATURE REVIEW

Metaverse

Since 2021, businesses and individuals have been paying close attention to metaverse platforms and services. Metaverse is a compound word that combines meta, which means transcendence, beyond, virtual, or abstract, and the universe, which means the world (Lee & Kim, 2022). The metaverse is a virtual reality that combines social media, online gaming, augmented reality (AR), virtual reality (VR), and cryptocurrencies. Augmented reality enhances the user experience by superimposing visual elements, sound, and other sensory input onto real-world settings. Virtual reality, on the other hand, is entirely virtual and enhances fictional realities (Folger, 2022). Metaverses, embedded in our lives, create virtual experiences within the physical world. Moving towards metaverses in aircraft maintenance, mixed reality (MR) opens enormous possibilities for interaction with virtual aeroplanes (digital twins) that provide a near-real experience while maintaining physical distance during pandemics. 3D twins of modern machines exported to MR can be easily manipulated, shared, and updated, creating enormous benefits for aviation colleges that still use retired models for practice (Siyaev & Jo, 2021). Metaverse has distinguishing features that distinguish it from other tools in a variety of

environments, such as education (Akour et al., 2022), business (Enache, 2022), and digital medicine (Sun et al., 2022). In an educational environment, users can interact with one another through a virtual learning platform within the virtual world. The interactivity feature that makes the world more dynamic creates an innovative educational scenario of autonomous and collaborative learning, allowing access to all available resources. The metaverse system operates without requiring users to move in the real world while maintaining a continuous, time-limited connection with the virtual world. Similarly, the corporeality feature introduces the avatar, which has no limits in the virtual world, resulting in a more realistically defined environment, as avatar shapes are on par with or superior to those found in 3D games. The persistence feature is critical because it saves conversations, data, and objects even after users leave the virtual world (Akour et al., 2022).

The metaverse has been identified as one of today's most promising technologies in the digital economy. Some may regard the metaverse as merely a new term for VR or AR. It is much more than AR or VR (Hwang & Chien, 2022). Facebook, one of the largest online communities and the most well-known social media platforms, is capable of successfully connecting billions of people worldwide (Limsakul & Kraiwanit, 2020). In an ambiguous move, Facebook changed its name to Meta in October 2021, ushering in a new era of social interaction enabled by metaverse technology, which appears poised to become the future centre of gravity for online social interactions. At first glance, the communicated change indicates a radically new business model based on an unprecedented configuration of the three components: value creation, value proposition, and value capture (Kraus et al., 2022). As a relatively new topic, metaverse has been popular for several years, and technology companies worldwide have devoted some, if not all, of their resources to Metaverse development. Microsoft and other large corporations have invested hundreds of millions of dollars in Metaverse development projects. This demonstrates a growing belief that the metaverse concept, a virtual world, will be at the heart of future development and can provide significant benefits (Tan, 2022).

Cybersecurity

The advancement of information and communication technologies (ICT), the spread of the Internet, and mobile communications have all contributed to globalisation entering a qualitatively new stage of development. The computer and newly created ICTs are the main technological attributes of the current stages of globalisation, uniting the world into a single communication system and creating an integrated financial and information space (Limna et al., 2022). In the digital era, many people rely on ICT in all aspects of cyber-physical society, resulting in the need for cybersecurity to become increasingly important. Although most people appear to regard the Internet as a safe environment and use it daily via smartphones, tablets, and computers, numerous attacks occur daily. Cyberattacks, hacks, and security breaches on the Internet are no longer unusual. Hence, cybersecurity is critical for individuals and public and private organisations, but ensuring security is often difficult. (de Bruijn & Janssen, 2017; Spremić & Šimunic, 2018). Cybersecurity is a set of technologies and processes designed to protect computers, networks, programs, and data from attack, damage, or unauthorised access. In recent days, cybersecurity has undergone massive shifts in technology. Its operations

in computing and data science are driving the change, where machine learning, a core component of artificial intelligence (AI), can play a vital role in discovering insights from data. Machine learning has the potential to significantly alter the cybersecurity landscape, and data science is paving the way for a new scientific paradigm (Sarker et al., 2020). Furthermore, cybersecurity threats are increasing as the next generation of internet technology emerges, and metaverse adoption may multiply cybersecurity risks (Oxford Analytica, 2022). Millions of cyber-attacks occur daily, and data security in the metaverse will continue to be challenging. As a result of the augmented reality (AR) and the virtual reality (VR) technologies that power the metaverse, many privacy and security concerns, such as network credential theft, identity theft, social engineering attacks, and ransomware attacks, may arise. Hackers may be able to steal a user's identity in the metaverse by exploiting security flaws in these devices (Nath, 2022). Therefore, the need for cybersecurity is becoming increasingly important (de Bruijn & Janssen, 2017).

RESEARCH METHODOLOGY

This systematic review employed a narrative synthesis. Narrative synthesis is the process of conducting a systematic review and synthesis of findings from multiple studies that heavily rely on words and text to summarise and explain the synthesis's findings (Limna, 2022). Purposive sampling occurs when researchers use their knowledge to select the most beneficial sample. This method is frequently used in qualitative research. The goal is to gain comprehensive knowledge (Limna et al., 2021; Siripipatthanakul et al., 2022). Content analysis is a qualitative method for systematically and objectively describing and quantifying specific phenomena by drawing valid inferences from verbal, visual, or written data (Limna & Kraiwanit, 2022). The researchers conducted a systematic documentary review in this study and analysed the data using content analysis. English-language, peer-reviewed articles from ScienceDirect, PubMed, Google Scholar, Scopus, and Web of Science were included for data collection and analytics. Moreover, five independent reviewers examined search results, extracted data, and evaluated the quality of studies to summarise and report the findings. Data collection and analysis were between May 15 and July 30, 2022.

DISCUSSION

Hwang and Chien (2022) and Tan (2022) stated that the metaverse had been identified as one of today's most popular and promising technologies in the digital age. Moreover, Akour et al. (2022), Enache (2022), and Sun et al. (2022) indicated that the metaverse plays a pivotal role and has distinguishing characteristics that set it apart from other tools in several environments, including education, business, and digital medicine. Additionally, Tan (2022) stated that the metaverse concept is expected to be central to future development and provide substantial benefits. However, Oxford Analytica (2022) argued that using the metaverse may increase cybersecurity threats. Nath (2022) also indicated that millions of cyber-attacks occur daily, and data security in the metaverse will remain a challenge. Many privacy and security concerns may arise due to the AR and VR technologies that power the metaverse, such as network credential theft, identity theft, social engineering attacks, and ransomware attacks. By exploiting security flaws in these devices, hackers may be able to steal a user's identity in the metaverse. To combat these

risks, de Bruijn and Janssen (2017) and Spremi and Šimunic (2018) advocated for cybersecurity.

RESULTS AND CONCLUSIONS

Digital technologies play a critical role in many people's lives. The metaverse is a critical future innovation of digital technology in the digital era. The basic principle of the metaverse is to blur the frontiers between the virtual and real worlds, allowing users to fulfil everything in the real world using technological devices in virtual space. It began with human-computer interaction and has since evolved into an online network of virtual worlds. Furthermore, the characteristics of the metaverse make it suitable for use in massively multiplayer online scenarios such as multiplayer games, video chat, distance learning, remote work, and so on. However, the metaverse adoption may multiply cybersecurity risks. The importance of financial cybercrime in the metaverse for authorities, corporations, and individuals to address has grown, necessitating new regulatory and compliance frameworks and novel cybersecurity mechanisms to combat. As a result, cybersecurity is considered necessary because it simply protects the immediate, practical, and ongoing technological elements.

In the digital age, the metaverse has been identified as one of the most popular and promising technologies. In various contexts, including education, business, and digital medicine, it plays a pivotal role and has distinguishing characteristics that set it apart from other tools. In addition, the metaverse concept is anticipated to be central to future development and offer substantial benefits. Nevertheless, the use of the metaverse may increase cybersecurity risks. Every day, millions of cyberattacks are launched, and data security in the metaverse will continue to be challenging. Due to the AR and VR technologies that power the metaverse, many privacy and security concerns may arise, such as network credential theft, identity theft, social engineering attacks, and ransomware attacks. By exploiting these devices' security flaws, hackers may be able to steal a user's identity in the metaverse.

LIMITATIONS AND RECOMMENDATIONS

This review article employed a narrative synthesis. The recommendation is to consider a quantitative study, such as online surveys, regarding metaverse and cybersecurity in the digital era. Also, a qualitative approach, such as online interviews or focus groups, could give a clear view of insight results for further study.

RESEARCH IMPLICATIONS

This systematic review contributed to the literature on metaverse and cybersecurity in the digital era. Therefore, it could guide future research on metaverse and cybersecurity in the digital era. Moreover, it may assist academics in broadening their research by incorporating more potential elements.

DECLARATION

Conflict of Interest

All authors declared that there is no conflict of interest.

Inform Consent

It may not be applicable because this paper is a review article, and no respondents are involved.

Ethics Approval

It may not be applicable because this paper is a review article, and no respondents are involved.

REFERENCES

Adamson, G. (2021). Cybersecurity as the Protection of Cyberspace. In *2021 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-8). IEEE.

Akour, I. A., Al-Maroof, R. S., Alfaisal, R., & Salloum, S. A. (2022). A Conceptual Framework for Determining Metaverse Adoption in Higher Institutions of Gulf Area: An Empirical Study using Hybrid SEM-ANN Approach. *Computers and Education: Artificial Intelligence*, *3*, 100052. https://doi.org/10.1016/j.caeai.2022.100052.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly*, *34*(1), 1-7.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M., & Conboy, K. (2022). Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy. *International Journal of Information Management (IJIM)*, 66, Article 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542.

Enache, M. C. (2022). Metaverse Opportunities for Businesses. *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics*, *28*(1), 67-71.

Folger, J. (2022). Alternative Investments: Metaverse Definition. *Investopedia*. Retrieved from https://www.investopedia.com/metaverse-definition-5206578.

Hwang, G. J., & Chien, S. Y. (2022). Definition, Roles, and Potential Research Issues of the Metaverse in Education: An Artificial Intelligence Perspective. *Computers and Education: Artificial Intelligence*, 100082. https://doi.org/10.1016/j.caeai.2022.100082.

Katterbauer, K., Syed, H., & Cleenewerck, L. (2022). Financial cybercrime in the Islamic Finance Metaverse. Journal of Metaverse, Preprint, 1-6.

Kraus, S., Kanbach, D. K., Krysta, P. M., Steinhoff, M. M., & Tomini, N. (2022). Facebook and the Creation of the Metaverse: Radical Business Model Innovation or Incremental Transformation? *International Journal of Entrepreneurial Behavior & Research*, 28 (9), 52-77. https://doi.org/10.1108/IJEBR-12-2021-0984.

Lee, U. K., & Kim, H. (2022). UTAUT in Metaverse: An "Ifland" Case. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*(2), 613-635.

Limna, P. (2022). Artificial Intelligence (AI) in the Hospitality Industry: A Review Article. *International Journal of Computing Sciences Research, 6*, 1-12.

Limna, P., & Kraiwanit, T. (2022). Service Quality and Its Effect on Customer Satisfaction and Customer Loyalty: A Qualitative Study of Muang Thai Insurance Company in Krabi, Thailand. *Journal for Strategy and Enterprise Competitiveness, 1*(2), 1-16. https://so07.tci-thaijo.org/index.php/STECOJournal/article/view/912.

Limna, P., Kraiwanit, T., & Siripipatthanakul, S. (2022). The Growing Trend of Digital Economy: A Review Article. *International Journal of Computing Sciences Research, 6*, 1-11. https://doi.org/10.25147/ijcsr.2017.001.1.106.

Limna, P., Siripipatthanakul, S., & Phayaphrom, B. (2021). The Role of Big Data Analytics in Influencing Artificial Intelligence (AI) Adoption for Coffee Shops in Krabi, Thailand. *International Journal of Behavioral Analytics*, *1*(2), 1-17.

Limsakul, A., & Kraiwanit, T. (2020). Libra as a Digital Currency and its Impacts on the Thai Economy. *AU eJournal of Interdisciplinary Research*, *5*(2), 110-118. Retrieved from http://www.assumptionjournal.au.edu/index.php/eJIR/article/view/4807.

Nath, K. (2022). Evolution of the Internet from Web 1.0 to Metaverse: The Good, The Bad and The Ugly. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.19743676.v1.

Noronha-Sousa, D., Costa, E., Mateus, C., Noronha, A. R., & Vasquez-Justo, E. (2022). Contemporary Education, Technologies, and Human Connectivity: From Native Generations to Digital Immigrants. In *Perspectives and Trends in Education and Technology* (pp. 973-986). Springer, Singapore.

Oxford Analytica. (2022). Metaverse Adoption Will Multiply Cybersecurity Risks. *Emerald Expert Briefings, (Oxan-Ga)*. https://doi.org/10.1108/OXAN-GA266968.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity Data Science: An Overview from Machine Learning Perspective. *Journal of Big data*, *7*(1), 1-29.

Siripipatthanakul, S., Limna, P., Siripipattanakul, S., & Auttawechasakoon, P. (2022). The Impact of TPB Model on Customers' Intentions to Buy Organic Foods: A Qualitative Study in Angsila-Chonburi, Thailand. *Psychology and Education Journal*, *59*(2), 419-434. Retrieved from SSRN: 4109868.

Siyaev, A., & Jo, G. S. (2021). Towards Aircraft Maintenance Metaverse Using Speech Interactions with Virtual Objects in Mixed Reality. *Sensors*, *21*(6), 2066.

Spremić, M., & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. In *Proceedings of the World Congress on Engineering*, 1, 341-346. Hong Kong, China: International Association of Engineers.

Sun, M., Xie, L., Liu, Y., Li, K., Jiang, B., Lu, Y., Yang, Y., Yu, H., Song, Y., Bai, C. and Yang, D. (2022). The Metaverse in Current Digital Medicine. *Clinical eHealth, 5*, 52-57. https://doi.org/10.1016/j.ceh.2022.07.002.

Tan, Z. (2022). Metaverse, HCI, and Its Future. In *2022 3rd International Conference on Mental Health, Education and Human Development,* pp. 897-901. Atlantis Press.