Privacy Concerns and Measures in Metaverse: A Review

Yavuz CANBAY
Department of Computer Engineering
Faculty of Engineering and Architecture,
Sutcu Imam University
Kahramanmaras, Türkiye
yavuzcanbay@ksu.edu.tr
0000-0003-2316-7893

Anıl UTKU
Department of Computer Engineering
Faculty of Engineering,
Munzur University
Tunceli, Türkiye
anilutku@munzur.edu.tr
0000-0002-7240-8713

Pelin CANBAY
Department of Computer Engineering
Faculty of Engineering and Architecture,
Sutcu Imam University
Kahramanmaras, Türkiye
pelincanbay@ksu.edu.tr
0000-0002-8067-3365

2022 15th International Conference on Information Security and Cryptography (ISCTURKEY) | 978-1-6654-5603-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISCTURKEY56345.2022.9931866

***Abstract*—Metaverse is the new buzzword in today's digital world. It is a new internet application and a new form of the social world that integrates new technologies such as; Artificial Intelligence (AI), Virtual Reality (VR), Augmented Reality (AR), Extended Reality (XR), Blockchain (BC), etc. The metaverse can be seen as a virtual world that mimics the real world. Most things that can be done in the real world, such as shopping, making new friends, attending concerts, playing games, and so on, can be done differently in Metaverse. While a person who represents himself with his presence in the real world realizes this representation in the digital world with his personal data. Hence, the Metaverse exploits personal data to create and maintain this virtual world. At this point, privacy concerns of users in Metaverse occur, and Metaverse Service Providers (MSP) should take these concerns into account. This paper focuses on privacy concerns in Metaverse, presents some measures in order to minimize these concerns, and provides a comprehensive list of personal data collected and processed in Metaverse.**

Keywords—Metaverse, privacy concerns, personal data protection

I. INTRODUCTION

Metaverse is a new digital world combining technology, social life, and hyper spatiotemporality. It enables people to have an immersive experience based on AI, AR, VR, BC, etc. As a parallel world to the real world, Metaverse seamlessly integrates the physical world with the virtual world. It allows digital copies of persons to carry out rich activities such as making friends, rearing virtual pets, designing virtual fashion items, buying virtual estate, attending concerts, creating and selling digital art, etc [1].

Avatar is the 3d digital representation of a real person in the Metaverse. It can be said that what you have in the real world is what you will have in the Metaverse, for instance, mother, father, brother, sister, car, pet, properties, skills, etc. But, the most crucial having can be said that your personal data, such as gender, sexuality, name, age, height, religious belief, health data, and more. In addition to those, think that your avatar has a heartbeat, gender, skin color, etc. Furthermore, it will have your behaviors, emotions, reactions, and more. Although your avatar is a non-living asset, it has your own data, which was collected from you via wearable devices [2, 3].

Data privacy is the self-control of any person over determining to share his data with whom, for what purposes, and at which level. Privacy is a big concern for people. Because disclosure of privacy may cause people to be exposed to discrimination, loss of reputation, be excluded from society and be exposed to unfair treatment. Hence, personal data privacy should be crucial for technology developers and suppliers [4].

In this study, we aimed to pay attention that privacy in Metaverse is a big problem and a growing concern in the near future. When Metaverse becomes widespread, more personal data will feed the MSP, and then maybe the technology companies will collect the most amount of personal data ever. Note that through these data, some groups or maybe marginal MSP can easily direct people according to an opinion or an idea. In addition, we briefed some measures for privacy concerns available in the literature. Then, we provided a comprehensive list of personal data collected and processed in Metaverse.

This paper is organized as follows. In Section II, the definition, ecosystem, technology, and personal data used in Metaverse are given. Section III presents personal data privacy. Section IV includes some related works considering privacy concerns in Metaverse. Section V presents some measures in order to minimize privacy concerns in Metaverse, and finally, Section VI concludes the study.

II. METAVERSE

A. Definition and Ecosystem

Metaverse is a combination of the words meta and verse, meaning a new field created by the convergence of VR and AR [5]. It refers to a realm beyond the physical world, in other words, beyond the physical world or the universe. Metaverse is a network where users can interact with each other and with digital objects through their virtual representations of avatars [6]. Metaverse can be thought of as a combination of virtual reality, multiplayer online gaming, and the web.

Metaverse provides a three-dimensional virtual world experience to users [7]. This three-dimensional virtual world allows users to interact with tools such as VR glasses and AR glasses [8]. Metaverse connects users through avatars in the virtual universe. In order for users to perceive the virtual universe physically, senses such as sight, hearing, touch, and even smell are tried to be simulated through interface technologies. Metaverse allows users to overcome their physical limitations as much as possible [6]. It enables users to communicate concretely with each other and virtual objects through real-time interactions.

Metaverse has three main aspects; presence, interoperability, and standardization. Presence is the feeling of being in a virtual space with other users, embodied by real

people. Feeling embodied allows users to interact more comfortably. The sense of presence is carried out through technologies such as virtual reality glasses. Interoperability refers to the ability to switch between sandboxes and the same virtual assets, such as avatars and digital assets. Standardization refers to the interoperability of platforms and services in the Metaverse [9].

According to Lee et al. [5], various technologies and an ecosystem are required for the interaction between the physical world and the Metaverse. AI, BC, computer vision, network infrastructures such as 5G/6G, AR, Internet of Things (IoT), and robotics are the technologies in which the Metaverse interacts in the real world [10].

Trust in the system, accountability, security, privacy, and social acceptability in the virtual world are other essential parts of the ecosystem which are indispensable to every computer system. In addition, content and avatars, which are elements of real existence in the virtual world, are the most critical components of the ecosystem [11].

B. Enabling Technologies

Metaverse is a combination of physical reality, AR, and VR in a shared online space [6]. It is associated with VR, AI, AR, BC, Brain-Computer Interfaces (BCI), IoT, Mixed Reality (MR), Web 3.0, and Mobile Device Processors technologies [1].

VR is an experience that simulates realistic situations such as gaming, social networking, and education. It is associated with the Metaverse as an experience that allows users to come together to communicate in the same virtual environment regardless of physical distance [12].

AI supports computers to think like humans and solve complex problems like humans. AI technologies will interact with the Metaverse in various ways. For example, AI software can interact with humans or each other and be programmed according to their purposes. AI technologies also have facilitated character creation with the help of Unreal Engines [13]. The results of the created characters having AI and acting intelligently can be surprising and surreal. AI automates software development processes enabling the creation of more complex characters. AI can be used to create, supervise and maintain smart contracts in BC technologies [14]. The usage areas of AI technologies in the Metaverse can be exemplified as avatar creation with artificial intelligence, multilingual accessibility, the expansion of the virtual reality world, and intuitive interface.

AR refers to enriching the real world of users with computer-generated content. AR glasses and lenses can be used to enrich the real world with the help of AI technologies. In this way, it becomes possible to interact with both the real world and the virtual world [15].

BC technology will be a currency that is used for making digital transactions quickly and securely. BC was developed to use some options, such as cryptocurrencies. It is a technology that enables multiple access to data and verification of data in real-time. BC technology allows digital property ownership, digital payment, governance, accessibility, and interoperability in the Metaverse [16].

BCI allows people to manipulate avatars, objects, and digital operations using brain signals. Using technologies such as Neuralink, BCI aims to acquire the senses of touch and smell in the Metaverse with the help of devices implanted in the brain [17].

The most common application of IoT in the Metaverse is to collect and provide data. The effective use of the Metaverse with IoT will provide significant developments in the field of economy. IoT enables data generated in the virtual world in the Metaverse to be transferred to real-world devices [1].

MR is created when users interact directly with the Metaverse in a real-world physical environment. It is a combination of the physical and digital worlds [18].

Social media platforms, which have become popular thanks to Web 2.0, service users with dynamic infrastructure. Blockchain and AI concepts form the basis of Web 3.0. It is also associated with the Metaverse universe, which has become popular recently and was put forward to solve security and centralization problems today. Web 3.0, which aims to minimize monopoly activities with decentralized platforms, is very assertive in security thanks to blockchain technology [19].

In order for AR technologies to be accessible to everyone, high-speed microprocessors must be integrated into devices. With this way, improvements in subjects such as refresh rate, delay time, realistic graphics, and transferred image speed will be achieved [20].

C. Personal Data in Metaverse

Social media platforms, which entered our lives with Web 2.0, allow users to interact with other users by offering profiles they can manage. But on the backside, users' metadata is also stored by social media platforms. Much metadata is stored in the background, including family members, colleagues, locations visited, and future plans that users do not share directly [21].

Social media applications access such information with the help of location services, cameras, contact lists, reminders, and microphones on mobile devices [22]. Privacy violation of personal biometric data such as face recognition information, retina information, and fingerprint obtained in Metaverse is handled in some studies [23].

It is known that MSP is able to collect data such as user interactions through wearable technologies, microphones, cameras, heart, and respiratory monitors for advertising and user tracking purposes. They use these data to develop their products and services according to user expectations [24]. As the digital traces of users in Metaverse increase, it is predicted that users will become more vulnerable to cyber-attacks.

In the Metaverse, data will be generated when users personalize their avatars in the virtual universe or contact other avatars to socialize [25]. With the increase in digital user data in the Metaverse, it is predicted that companies will even process data such as pulse, heartbeat, and brain waves in order to provide users with a more attractive experience. When such data is leaked or misused, it is likely that the user is faced with a situation that puts their identity and real-world life at risk.

III. Personal Data Privacy

Any data belonging to a person and directly or indirectly identifying the data owner can be accepted as personal data. For instance, name, surname, age, height, weight, gender, social security number, passport number, income, and health

are some of the personal data. In [26, 27], personal data is classified as;

- general personal data; name, surname, social security number, IP address, email address, passport number, race, age, gender, location data, finance, phone number, date of birth, professional, education information, and so on.
- special personal data; racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and sexual orientation or activity.

While general personal data protection may be done with regular measures, special personal data requires a high level of protection. Fig. 1 shows personal data collected and processed in Metaverse.

IV. Privacy Concerns In Metaverse

While Metaverse is a personal data-driven world, privacy-focused attacks inevitably occur.

Yang et al. [28] emphasized that personal data on Metaverse, such as digital assets, the identity of virtual items, and cryptocurrency spending records should be protected against disclosure attacks. Guaranteeing the privacy of Metaverse users is a challenging problem, and some solutions should be provided.

Nguyen et al. [29] reported that interactions between users and Metaverse could be leaked. Hence, the interaction between service providers and users can be done by employing BC technology, which provides users privacy and anonymity.

Wang et al. [2] discussed the privacy aspects of the Metaverse. They emphasized that Metaverse systems require personal data-intensive functionalities. Hence, it performs a pervasive data collection method. In order to interact with the avatar, user profiling activities collect data at the most granular level, such as facial expressions, eye movements, iris movements, hand movements, speeches, biometrics, and brain wave patterns. They claim that with the help of XR and human-computer interaction (HCI), MSP will enable the collection of data about physical movements, user attributes, and user tracking. They also referred that in the virtual office meetings, interactions between employees and biometric data of employees, such as voices, can be monitored and analyzed by the managers. In addition, they emphasized that personal data collected from some wearable devices are moved from device to platform via wireless or wired communication. In this transformation process, though the communication is encrypted, an attacker may perform an eavesdropping attack and obtain some sensitive information. The authors also expressed that an avatar is created using data collected from human bodies. These data are transferred to a central platform in order to train personalized avatar appearances that may contradict regulations such as General Data Protection Rule (GDPR). They also declared that private data stored in the cloud and edge storage might be disclosed by hacking. Some privacy risks about unauthorized data access, misuse of user data, and digital footprints are provided in detail. Lastly, it is worth underlining that data of wearable devices enabling MSP to collect some information to infer behaviors of users by using their eye movements, hand gestures, facial expressions, and so on will be a primary risk for users. Because MSP may model your sense of who you are and how you talk, behave, feel and express yourself.

Zhao et al. [30] analyzed privacy concerns in Metaverse. User information such as related physiological, physical, biometric, and social should be protected since they are personal data. Communication also should be private since it should include sensitive data. In addition, personal privacy should be considered even in situations such as insulting, tracking, or even sexual harassment. Transactions of goods, such as character modeling, appearance, costumes, buildings, and artworks, belonging to an avatar may be disclosed. So these kinds of transactions should also be protected.

Gadekallu et al. [16] expressed that privacy laws in the real world may not be accountable in the digital world. Hence, privacy laws compatible with Metaverse should be created with the collaboration of decision-makers and MSP.

Fernandez and Hui [31] reported that sensors used in Metaverse collect a vast amount of biometric data and spatial data, including surroundings. Sensors in XR technologies commonly scan and monitor users' surroundings. Head-mounted displays can collect biometric data such as head movement and eye tracking data. Authors declared that users' habits, choices, and activities in Metaverse are another valuable piece of data for service providers. Because users' moods can be obtained via these data, hence privacy of them should be provided.

Nair et al. [32] presented how an adversary can obtain any personal data from Metaverse. They developed a VR application and used some data sources such as geospatial telemetry, device specifications, network, and behavioral observations. In the experimental studies, they obtained some biometrics data about anthropometrics, vision, fitness, and reaction time with minimum error rates. In addition, geolocation, device specifications, demographic and acuity data are also obtained with high accuracy.

Park and Kim [3] expressed that privacy in Metaverse is a big issue because it collects data on behavior that is more detailed than user conversations and internet history.

Pietro and Cresci [33] noted that everything and everyone would be the product of Metaverse. The platform collects lots of personal data such as body movements, physiological responses, brainwaves, and virtual interactions with the surrounding environment. Social networking platforms are already collecting more sensitive data about users. The fusion of data collected in social networking platforms and MSP will give more opportunities to data holders to extract sensitive data about users. Some unwanted situations could occur in the Metaverse, such as doxing, spying, and stalking. Additionally, privacy concerns about communication should be considered in Metaverse. If an interaction or communication between users is disclosed, it may harm the users. They are open issues for Metaverse.

Far and Rad [34] reported that users' activities in Metaverse should be private in order not to be obtained by an adversary. In addition, they warned users about thinking that their privacy may be broken by authorities and governments.

Lee et al. [5] specified that wearable devices in Metaverse collect lots of personal data, including physical data, cultural data, economic data, habits, choices, and communications. In many cases, users may accept that there are always privacy risks while using Metaverse. Users in Metaverse can be exposed to extortion, continuous monitoring, or eavesdropping.

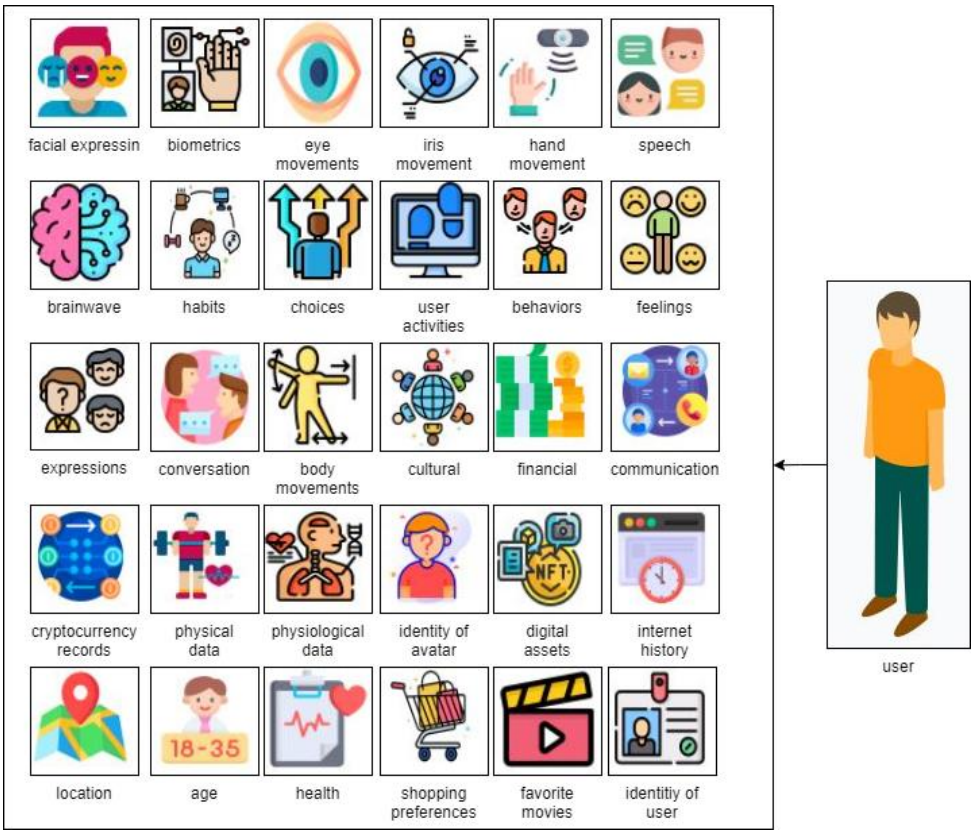

Fig 1. Personal data collected and processed in Metaverse

Falchuk et al. [35] noticed that digital footprints and digital breadcrumbs allow service providers to not only track people but also get more information about identity, location, age, shopping preferences, friends, favorite movies, credit card numbers, social security numbers, social security identity, mother's maiden name, medical history, bank account information, and much more.

In addition to those, companies are in the search of how to turn personal data into cash. For instance, a big social media platform patented its eye and face tracking technology [36].

All of these mentioned privacy risks are significant issues that MSP should take into account and minimize.

V. Privacy Protection Measures in Metaverse

This chapter briefs some measures for privacy preservation in Metaverse provided in the literature.

The authors of the study [37] have proposed some measures for corporations operating in Metaverse. Since HCI devices collect many personal data, including biometrics, users should be educated about privacy implications. In addition, the consent mechanism of the Metaverse should be clear and straightforward enough. Regulations and laws about data protection are not consistent around the world. For instance, European Union has its own GDPR, the UK has its version of GDPR, and Turkey has its own data protection rule. This inconsistency should be eliminated in Metaverse. As a separate territory or world, a strict data protection rule dedicated to Metaverse should be created. Users should be warned if they allow their data to be collected by the MSP for ads. Additionally, privacy protection and ease of use could cause conflict in Metaverse. But, MSP should persist on renewal of consent when data re-entry.

Fernandez and Hiu [31] expressed that privacy-enhanced technologies (PET) should be used in Metaverse. PET obfuscates sensitive data from sensors before being shared with cloud services. They also proposed that users should use second avatars to avoid leaking any sensitive data such as demographics, cultural and economic background. Finally, they suggested that users should have the opportunity to configure their personal spaces, such as visual access via privacy bubbles [31].

Park and Kim [3] remarked that Metaverse collects behavioral data that is more detailed than user conversations and internet history. Avatar two-factor authentication and protection of transmitted data should be used by the service providers.

Pietro and Cresci [33] emphasized that a privacy setting should be made available to the users so that the users can choose their desired level of privacy.

Yang et al. [28] declared that Metaverse-oriented cryptography mechanisms are some proposals that could be seen as privacy protection measures.

Lee et al. [5] support that a solution to privacy threats is the use of multiple avatars and privacy copies in the Metaverse. The technique focuses on creating different avatars with different behavior and freedom according to user preferences. These avatars can be placed in the Metaverse to confuse attackers as they will not know which avatar is the actual user. The avatars can have different configurable behaviors.

Funck et al. [35] proposed two plans to ensure privacy. The first plan is about the cloud of clones. This plan's purpose is to obfuscate user location, activities, beliefs, desires, and/or

intentions. In this plan, the system creates one or more avatar "clones" that have the same or similar appearance to the user's avatar. Plan B is about creating a private copy of some part of the virtual world. The requested part of the Metaverse is the main fabric that continues to exist in parallel and unaffected by the actions of the user in the temporary Private Copy. This will give comfort about untraceability to users in private copy. For instance, think that a user may want a private virtual shopping experience. At this time, the user requests a Private Copy of a virtual store. This store may sell personal items for which the user does not want to be observed shopping.

The measures mentioned above are some solutions that try to minimize privacy concerns. However, since technology is developing at a dizzying pace, these measures will be aged. Hence new measures should be proposed in order to catch the speed of technology. In addition, with the spread of technology, different types of personal data may be targeted by the MSP; hence new measures will always be required.

VI. Conclusion

Metaverse is a personal data-centric platform. As shown in Fig. 1, it collects and processes lots of personal data such as; biometrics, facial expressions, eye movements, iris movements, hand movements, speech, brain wave patterns, habits, choices, activities of users, behaviors, feelings, expressions, user conversations, internet history, body movements, cultural data, financial data, communications, location, age, shopping preferences, favorite movies, identities, medical data, digital assets, the identity of virtual items, cryptocurrency spending records, physiological data, physical data and much more.

Privacy concerns should not be ignored in a personal data-intensive platform like Metaverse. The concerns existing in the literature can be summarized as follows;

- personal data on the Metaverse such as digital assets, the identity of virtual items, and cryptocurrency spending records can be disclosed by the adversaries,
- interactions between user and Metaverse can be leaked,
- users may be profiled according to their habits and preferences,
- some attacks such as eavesdropping in communication may be performed, and in addition, data storage, which stores personal data, may be hacked, and all data may be disclosed,
- privacy laws in the real world may not be accountable in the digital world,
- behavioral data is more valuable than classical personal data since it defines how a person acts. Hence collecting such data should require more efforts to defeat disclosures,
- privacy of users may be broken by authorities and governments,
- the fusion of data collected in social networking and data contained in Metaverse may compromise user privacy at a higher level. Because such fusion may emerge unpredictable deeper information about a user.

Some countermeasures provided in the literature for privacy concerns are listed below;

- MSP should educate the users about privacy implications and present a clear consent mechanism,
- an agreed regulation considering personal data protection in Metaverse should be created,
- privacy-supported devices and privacy-enabled technology should be used in Metaverse,
- users should have the authority of privacy configurations for their personal space in Metaverse,
- two-factor authentication for avatars should be used,
- MSP should enable users to have multiple avatars for privacy concerns,
- private copies of some parts of Metaverse should be provided if a user request an anonymous interaction.

As it can be clearly seen from the literature that privacy is a big concern for Metaverse platforms. While it provides lots of opportunities to people, by considering the motto of "if any product or service is free, you are the product", a great number of personal data will be consumed on these platforms. And this situation will benefit service providers, such as making more money. But the important thing for the users is that they are modeled in Metaverse, and their real personal data is mostly transferred to MSP. Hence, users should consider this trade-off.

References

[1] H. Ning *et al.*, "A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges," *arXiv preprint arXiv:2111.09673,* 2021.

[2] Y. Wang *et al.*, "A survey on metaverse: Fundamentals, security, and privacy," *arXiv preprint arXiv:2203.02662,* 2022.

[3] S.-M. Park and Y.-G. Kim, "A Metaverse: Taxonomy, components, applications, and open challenges," *Ieee Access,* vol. 10, pp. 4209-4251, 2022.

[4] Y. Canbay, S. Sagiroglu, and Y. Vural, "A Mondrian-based Utility Optimization Model for Anonymization," International Conference on Computer Science and Engineering (UBMK), 2019.

[5] L.-H. Lee *et al.*, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," *arXiv preprint arXiv:2110.05352,* 2021.

[6] S. Mystakidis, "Metaverse," *Encyclopedia,* vol. 2, no. 1, pp. 486-497, 2022.

[7] A. Davis, J. Murphy, D. Owens, D. Khazanchi, and I. Zigurs, "Avatars, people, and virtual worlds: Foundations for research in metaverses," *Journal of the Association for Information Systems,* vol. 10, no. 2, p. 1, 2009.

[8] S. Balakrishnan, M. S. S. Hameed, K. Venkatesan, and G. Aswin, "Interaction of Spatial Computing In Augmented Reality," *International Conference on Advanced Computing and Communication Systems* 2021, vol. 1, pp. 1900-1904.

[9] M. E. Latoschik, F. Kern, J.-P. Stauffert, A. Bartl, M. Botsch, and J.-L. Lugrin, "Not alone here?! scalability and user experience of embodied ambient crowds in distributed social virtual reality," *IEEE transactions on visualization and computer graphics,* vol. 25, no. 5, pp. 2134-2144, 2019.

[10] Q.V. Pham, X.Q. Pham, T. T. Nguyen, Z. Han, and D.S. Kim, "Artificial Intelligence for the Metaverse: A Survey," *arXiv e-prints,* arXiv: 2202.10336, 2022.

[11] P. A. Rauschnabel, B. J. Babin, M. C. tom Dieck, N. Krey, and T. Jung, "What is augmented reality marketing? Its definition, complexity, and future," vol. 142, ed: Elsevier, 2022, pp. 1140-1150.

[12] B. Kye, N. Han, E. Kim, Y. Park, and S. Jo, "Educational applications of metaverse: possibilities and limitations," *Journal of Educational Evaluation for Health Professions,* vol. 18, 2021.

[13] A. Jungherr and D. B. Schlarb, "The Extended Reach of Game Engine Companies: How Companies Like Epic Games and Unity Technologies Provide Platforms for Extended Reality Applications and the Metaverse," *Social Media+ Society,* vol 8, no 2, 2022.

[14] B. D. Deebak and A.-T. Fadi, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements," *Journal of Information Security and Applications,* vol. 58, 2021.

[15] P. A. Rauschnabel, "Virtually enhancing the real world with holograms: An exploration of expected gratifications of using augmented reality smart glasses," *Psychology & Marketing,* vol. 35, no. 8, pp. 557-572, 2018.
[16] T. R. Gadekallu *et al.*, "Blockchain for the Metaverse: A Review," *arXiv preprint arXiv:2203.09738,* 2022.
[17] G. Boddington, "The Internet of Bodies—alive, connected and collective: the virtual physical future of our bodies and our senses," *AI & society,* 2021.
[18] M. Speicher, B. D. Hall, and M. Nebeling, "What is mixed reality?," *CHI conference on human factors in computing systems*, 2019, pp. 1-15.
[19] K. Nath, "Evolution of the Internet from Web 1.0 to Metaverse: The Good, The Bad and The Ugly," *TechRxiv,* 2022.
[20] M. Buhr, T. Pfeiffer, D. Reiners, C. Cruz-Neira, and B. Jung, "Real-Time Aspects of VR Systems," in *Virtual and Augmented Reality (VR/AR)*: Springer, 2022, pp. 245-289.
[21] A. Puura, S. Silm, and A. Masso, "Identifying relationships between personal social networks and spatial mobility: A study using smartphone tracing and related surveys," *Social Networks,* vol. 68, pp. 306-317, 2022.
[22] C. W. Munyendo, Y. Acar, and A. J. Aviv, ""Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya," *Symposium on Security and Privacy (SP)*, Computer Society, pp. 1521-1521.
[23] C. Jain, "Virtual Fitting Rooms: A Review of Underlying Artificial Intelligence Technologies, Current Developments, and the Biometric Privacy Laws in the US, EU and India," *Current Developments, and the Biometric Privacy Laws in the US, EU and India,* 2022.
[24] U. Lee *et al.*, "Toward Data-Driven Digital Therapeutics Analytics: Literature Review and Research Directions," *arXiv preprint arXiv:2205.01851,* 2022.
[25] S. Hollensen, P. Kotler, and M. O. Opresnik, "Metaverse–the new marketing universe," *Journal of Business Strategy,* 2022.
[26] P. Kononow. "What is Personal Data in GDPR." https://dataedo.com/blog/what-is-personal-data-under-gdpr.
[27] "GDPR - User-Friendly Guide to General Data Protection Regulation." https://www.gdpreu.org/#special-category-data
[28] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open Journal of the Computer Society,* 2022.
[29] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "Metachain: A novel blockchain-based framework for metaverse applications," *arXiv preprint arXiv:2201.00759,* 2021.
[30] R. Zhao, Y. Zhang, Y. Zhu, R. Lan, and Z. Hua, "Metaverse: Security and Privacy Concerns," *arXiv preprint arXiv:2203.03854,* 2022.
[31] C. B. Fernandez and P. Hui, "Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse," *arXiv preprint arXiv:2204.01480,* 2022.
[32] V. Nair, G. M. Garrido, and D. Song, "Exploring the Unprecedented Privacy Risks of the Metaverse," *arXiv preprint arXiv:2207.13176,* 2022.
[33] R. Di Pietro and S. Cresci, "Metaverse: Security and Privacy Issues," *International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2021: IEEE, pp. 281-288.
[34] S. B. Far and A. I. Rad, "Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges," *Journal of Metaverse,* vol. 2, no. 1, pp. 8-16, 2022.
[35] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technology and Society Magazine,* vol. 37, no. 2, pp. 52-61, 2018.
[36] H. Murphy. "Facebook patents reveal how it intends to cash in on metaverse." https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647.
[37] "Metaverse Data Protection and Privacy: The Next Big-Tech Dilemma?" https://www.xrtoday.com/virtual-reality/metaverse-data-protection-and-privacy-the-next-big-tech-dilemma/.