Security Risks of the Metaverse World

https://doi.org/10.3991/ijim.v16i13.33187

Tanya Abdulsattar Jaber(✉)
Institute of Applied Arts, Middle Technical University, Baghdad, Iraq
tanya.galxy@mtu.edu.iq

Abstract—An interesting paradigm is a metaverse which represents the next generation of using the internet to improve human lives and provide a new way to communicate by building a system that let the user represented by their avatar to work, socialize and play virtually by integrating multiple technologies such as blockchain, artificial intelligence as well as virtual and augmented reality. However, this may preserve many problems related to the security and privacy of the system user starting from data breaches to identity theft, in this paper an overview of the metaverse world and the architecture that connects the virtual to the real world and discuss the main security and privacy risks within the Metaverse world.

Keywords—metaverse, Meta, security of metaverse, the privacy of metaverse, metaverse issues

1 Introduction

In recent months, the metaverse has become a prominent topic of debate on many tech news outlets. There's no way anyone could have been unaware of the metaverse's recent surge in popularity. Even though the metaverse has been present since 1992, many of you may believe it is a new phase [1]. The metaverse ensures a digital environment with a shared, open, and durable connecting communities, manufactured goods, digital solutions, content creators, user entertainment, workplaces, e-commerce, and a variety of other human real-world elements [2]. However, privacy and security of metaverse concerns are an important part of the metaverse's dynamics. While many businesses are pondering the possibilities of the metaverse, it is sensible to consider the possibilities [3]. The term "the metaverse" can be very vague and complex. It is not referred to specific technology itself but rather points to how we interact with the technology. Broadly speaking, the technologies companies use include virtual reality and augmented reality. In the more idealistic visions of the metaverse, it's interoperable, allowing you to take virtual items like clothes or cars from one platform to another. While some advocates claim new technologies like NFTs can enable portable digital assets, this simply isn't true [4]. The metaverse is a virtual-reality world depicted as a planet-encircling market where virtual real estate can be bought and sold. The term was coined by Neal Stephenson in his 1992 novel Snow Crash to describe a virtual world in wide use in his imagined future [5].

The term was coined by Neal Stephenson in his 1992 novel Snow Crash to describe a virtual world in wide use in his imagined future [5]. In the broadest terms, it's a virtual

space that is graphically rich and owns some level of verisimilitude. It's a virtual place where people can shop, play, work, and do socialize, and interact—in short, just like humans in real life people can act in the metaverse and do things [6]. The three main elements of metaverse include [7]:

- Virtual reality interface
- digital ownership,
- avatars

Virtual reality has come a long way from the '90s, when Stephenson wrote Snow Crash, to the present day, when headsets of decent quality exist. There are a few factors that have made it a reality, including the development of the blockchain and NFTs, which enable virtual items and real estate to be exchanged through the metaverse [8].

It should be noted that in many games and virtual spaces, including Second Life, everybody can have and own virtual items and even trade them not necessarily using blockchain technology but using a license agreement [9]. Regardless, proponents of the metaverse are enthralled by NFTs' uniqueness and alleged portability. The pandemic of covid-19, which has radically changed humans' lifestyles around the world, is also a significant factor in the metaverse trend [10]. With millions of people spending so much time in virtual meetings (Zoom meetings for example) for work, and with personal use to communicate aiming to enter more exciting and colorful environments without leaving homes, it is normal to have technology companies try to make some profits from this circumstance [11].

2 The architecture of metaverse

The world of Metaverse with hyper spatiotemporal, 3Dimmersive virtual shared space and self-sustaining developed by combining virtual space (physically persistent) that is augmented digitally the physical reality. Precisely, the metaverse is a world simulated made up of avatars mainly controlled by users, digital objects, virtual surroundings, as well as other elements generated by computers in which humans avatar can communicate, collaborate, and socialize with one another using any smart device. The metaverse is built by combining the ternary physical, the ternary mental, and the ternary spiritual [12]. There are two worlds: human and digital. Figure 1 depicts the metaverse's overall design, taking into account its inherent tenacity. The relationships between the metaverse's components, the worlds (physical and digital), and information flow within the metaverse are detailed in the following sections [13].

1) Human society: Humans are considered to be the center of the metaverse [14]. The human world is made up of human users, their interior psychologies, and their social relationships. Metaverse users can control and engage their digital avatars using smart (physically wearable) technologies (e.g., virtual reality/augmented reality helmets) for working, playing, connecting, and socializing, with surrounding entities in the metaverse or with other avatars [15].

2) Physical infrastructures: The real world (physical world) provides the metaverse with supporting infrastructures (such as sensing/control, communication, computation, and storage infrastructures) that enable multisensory data processing, transmission, caching, and perception, besides the physical control, allowing interactions between

the two worlds (digital and human) efficiently. The pervasiveness of smart objects, actuators, and sensors, in particular, make up the infrastructure of control/sensing that allows for all-surrounding and multimodal data perception from the human body and environment, as well as high-precision device control. The communication infrastructure consists of several hetero networks wired or wireless (e.g., satellite communications, cellular communications, and unmanned aerial vehicle (UAV) communications,), providing networking connections. Furthermore, the storage infrastructure and cost computation, which is provided usually by cloud service providers (cloud edge end computing) [16], provides significant computation and storage capacities. A virtual environment, for example, runs at a 30 fps (frame per second) a minimum [17], imposing massive processing loads and latency limits.

3) Interconnected virtual worlds: reference to many standards such as (IEEE 2888 and ISO/IEC23005) [18], [19], building a digital world by providing a series of virtual worlds that is interconnected as well as distributed usually called sub-metaverse, every single one of them can provide virtual services/goods (e.g., online museum, social dating, online concert, and gaming) and virtual environments (e.g., virtual cities and game scenes) to digital & physical users that represented digitally in the metaverse world using avatars. (Avatar's characters on the internet). In the metaverse, avatars are computer representations of real users (existing human users). Inside many programs provide metaverse, a single user can build different avatars for himself, which can include human shapes, animals, imagined creatures, and so on. Virtual reality settings. Virtual environments in the metaverse are mimicked real or fictional surroundings (made up of 3D digital objects and their properties). In addition, virtual settings in the metaverse can have a different spatial and temporal dim (e.g., representing future imagined worlds or re-represent the ancient times) [19].

4) Metaverse engine: Using blockchain, artificial intelligence, interactivity, and digital twin technologies, the metaverse engine [20] generates, maintains, and updates the virtual world using inputs of real large data from the actual world. Specifically, Users in real locations can operate their avatars (digitally avatars) in the world of metaverse using their bodies & senses using XR & HCI (particularly brain-computer interface (BCI)) techniques for a variety of communal activities and collective such as dating, virtual goods trade, and vehicle racing. Within the Metaverse, the economy (virtual economy) can be developed as a natural outgrowth of avatars' activities of digital creation. To enrich the metaverse ecology, AI algorithms execute individualized content/avatar creation, metaverse rendering (large-scale), and provisioning of intelligent service. Furthermore, the knowledge gained by AI-based big data analytics. [20].

5) In-world information flow: Using technologies such as block chain, artificial intelligence (A.I.) interactivity, and a digital twin which represents the metaverse engine [21] generate maintain and updates the virtual world using large inputs from the actual world (as input data). Specifically, Users in real locations can operate their digital avatars in the metaverse via their senses and bodies using XR and HCI (particularly brain-computer interface (BCI)) techniques for a variety of communal activities and collective such as dating, virtual goods trade, and vehicle racing. Within the Metaverse, the economy (virtual economy) can be developed as a natural outgrowth of avatars' activities of digital creation. To enrich the metaverse ecology, AI algorithms execute large-scale metaverse rendering and individualized avatar/content creation large-scale metaverse rendering, and intelligent service provision. Furthermore, the knowledge gained by AI-based big data analytics [22].

6) Information flow across worlds: internet of things (IoT), Subjective consciousness, and the Internet are the main media of the realms of metaverse worlds, Humans see objective data originally comes from the physical world, and translate these data into a piece of knowledge and AI interactions through subjective consciousness, and utilizing that knowledge and intelligence to make some changes to the objective reality within the scene. [23] Users can also use HCI technology to interact with physical items and use XR technology to experience virtual AR (e.g., holographic telepresence). The real world of humans, as well as digital worlds, are linked by the Internet and mix each other, which is the world's largest known computer network that serves one purpose. Users can create, share, and acquire knowledge by interacting with the metaverse world through devices that consider smart (smart devices) such as wearable devices, smartphones, and special purposes helmets (virtual reality helmets). By leveraging interconnected smart devices for digitalization, the infrastructure of the internet of things connects the digital and physical worlds, allowing information to flow freely [24].

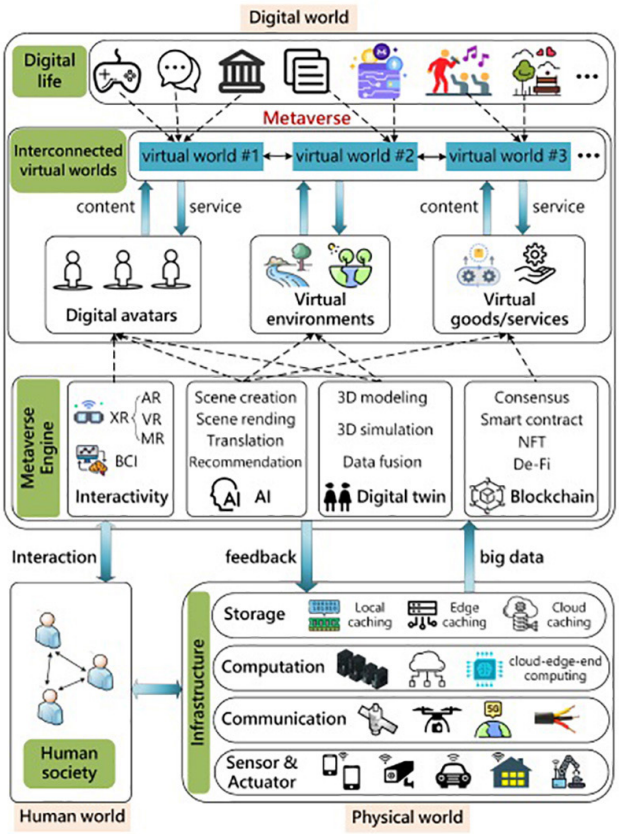

Fig. 1. Metaverse architecture with the integration of digital worlds, the human and physical worlds

3 Literal surveys

The metaverse has sparked a lot of interest in the scientific community. Recently multiple surveys articles from various elements of the technology of metaverse up till now. In [25], for example, define 4 qualities of feasible 3Dimensional metaverse or virtual worlds, including scalability, realism, interoperability, and ubiquity, and exploring current virtual world technological advances. Authors in [26] look at 8 key technologies that make up the virtual world (metaverse), besides 6 elements (user-centric) that influence it. Within [27] authors investigate the main role of artificial intelligence techniques within the metaverse's evolution and foundation. The potential impact of artificial intelligence integrated with blockchain technology for existing and future metaverse buildings is investigated in [28]. In [29], the authors survey the state of development of metaverse. In [30], they described the three components of metaverse (hardware, software, and content), as well as illustrative applications, user interaction, and implementation. From perspectives of communication, networking, computing, and blockchain, authors in [20] give a deep survey on the metaverse that is edge-enabled. In [31], they looks at the social and legal implications of potential problems related to privacy in the game of user Second Life (online). Unlike previous surveys on the general metaverse [25], [2], [26], [32], [30], artificial intelligence-enabled metaverse [28], [27] metaverse (edge-enabled) [20], or potential in service provisioning in social virtual reality/augmented reality games [32], goods and services retailing [33], under and post-graduate education [34] [42] [43], social goods [35], and computational arts [36] table one refer to the previous surveys and briefly explain technologies used. Table 1 shows the main characteristics of each paper.

Table 1. Metaverse survey and state of art papers

Year	Reference	Contribution
2008	[31]	Discuss the risk of privacy problems for gaming life from a legal and social perspective
2009	[33]	Retailing applications within the metaverse
2013	[25]	Discuss the metaverse world's main features and possible/existing improvements in the virtual and augmented technologies
2018	[32]	Discuss the countermeasures and issues related to privacy on the metaverse games
2020	[34]	Education applications within the metaverse
2021	[35]	Social goods applications within the metaverse
2021	[1]	Technologies for the building the metaverse applications
2021	[37]	Compatibilities of metaverse developments for virtual reality and social metaverse
2021	[36]	Digital arts applications within the metaverse
2022	[28]	Interference of blockchain and artificial intelligence in the world of the metaverse technology
2022	[27]	Implement a discussion of the main effect of artificial intelligence on the metaverse technology
2022	30	Implement a discussion of the H.W and S.W and content implication in the world of the metaverse
2022	20	Metaverse communication, network, and computations

4 Security risks of the metaverse world

When Meta have been born (Facebook changed its name to Meta), it sparked an explosion of interest in the metaverse. While a complete operating metaverse may come soon within a few next years, the world's work on accepting the new technology by preparing its creation which is already underway. The world is much closer to immersive encounters within metaverse virtual settings than anyone could have imagined. The popularity of virtual reality headsets has exploded in last recent years. Estimates show up an estimate that by 2024, the total number of virtual reality headset units sold will have surpassed 34 million [38]. On the other hand, improvements in the blockchain and cryptocurrency area, such as the improved blockchain networks as well as the scalability of the blockchain networks, provide a plethora of prospects for metaverse expansion. Amid all the changes in the metaverse, metaverse security issues are becoming increasingly important in determining the metaverse's future roadmap [39–44].

Metaverse can be employed in many applications such as medical image treatments, visual cryptography [45], deep fake (e.g. GAN algorithm) [46], and pandemic counter (such as covid-19) [47], and enhancing the data communication [48].

4.1 Privacy and security risks in the metaverse

The metaverse, since it is a new technology, it gets its main share of setbacks and concerns about global metaverse privacy and security. The metaverse promises to present a whole new era of technological and social encounters which are unrivaled in terms of impressiveness and interoperability. However, using these tools isn't a quiet safe situation, there is a downside to immersive and interoperability experiences [38]. The technology that enables metaverse platforms to come with its own set of hazards. AR and VR, which provide the metaverse's interface, are the two most prominent technologies driving the metaverse. On the other side, the metaverse may be affected by the security and privacy problems raised by these technologies [39]. After analyzing the metaverse current systems many metaverse security vulnerabilities are the most famous and affect metaverse technology.

4.2 Security risks of augmented reality

Augmented Reality, or AR, is one of the metaverse's basic foundations, and new AR breakthroughs are unquestionably intriguing. New AR breakthroughs may be able to give new instruments and methods for data collection. Simultaneously, augmented reality opens up a slew of new possibilities for changing links between the virtual and physical worlds. However, Augmented Reality (AR) is to blame for a slew of major metaverse security issues, particularly when it comes to user privacy. The following points will help security experts to consider the security vulnerabilities that may exist in the metaverse as a result of augmented reality [40]. And artificial intelligence in network [41]

- If an AR gadget is hacked how this should affect the user's privacy.
- How will AR companies utilize and protect the information gathered from users.

- Where do firms keep augmented reality data, and what encryption mechanisms do they use.
- Do augment reality corporations share augmented reality data with 3d parties, and if so, for what reason and how do they use this data.

All the concerns highlight metaverse blockchain security vulnerabilities including credential theft, social engineering, and denial of service (DOS). Here's a quick run-down of the most significant privacy concerns within metaverse as a result of Augmented Reality technology.

Social engineering attacks. Anyone might use appropriate papers to confirm their identification in the real world. Users in the metaverse, on the other hand, must employ digital avatars to verify voice, video records, and face features. AR and VR gadgets allow people to engage with each other and the metaverse. Using social engineering tactics or identity theft strategies, hackers can persuade users to give personal information.

Credential theft. It is considered the most difficult metaverse difficulty that the user might face currently is detecting theft. In the metaverse world, any other user with access ability to private network credentials might simply take the legal user identity. Wearable devices rather than bringing technology and helping us improve our lives could be used by criminals or hackers to breach the credentials of network users'. In reality, a big worry of merchants deploying shopping applications based on virtual reality and augmented reality technology is hacking. Theft of credentials of network users might jeopardize users' personal information and financial data saved in their accounts (metaverse user accounts).

Security risks of VR. Not only augmented reality (AR) technology is the only one to blame for metaverse security vulnerabilities. Virtual Reality (VR) technology also shares the blame for a slew of noteworthy privacy concerns in the world of the metaverse. The reason why virtual reality (VR) is such a susceptible target within the metaverse is many privacy problems arise from data gathered by Virtual Reality (VR) technology, such as retina scans, using biometric data in face geometry, fingerprints, and voice prints.

Identity theft, the loss of human connection, and Ransomware are the notable privacy threats linked with the metaverse world as a result of virtual reality (VR) technology.

Identity theft. The metaverse's virtual reality technology makes it a vulnerable target for hackers and criminals for identity theft. Many deep learning techniques such as deep fake and deep dream algorithms may readily assist in the manipulation of user's verification sound and pictures reaching the point where they appear as natural user data. Consider the case where hackers have gotten access to a virtual reality headset's data such as motion-tracking. By using the hacked motion-tracking data from VR headsets, the hackers could now simply create digital copies. Hackers can then utilize digital replicas in conjunction with another person's virtual reality experience to conduct an attack that is known as a social engineering attack.

Ransomware. Ransomware according to many researchers considers the next serious threat that reflects the use of virtual reality (VR) in the metaverse. Hackers might, for example, embedded features in virtual reality platforms that mainly aims to trick the platform users into disclosing their secret personal information shared within the platform. Hackers may utilize vulnerabilities of the virtual reality within the

metaverse for specific attacks such as ransomware attacks, much like they can with AR social engineering attacks. Users' metaverse experiences might be readily compromised if hostile agents get access to virtual reality (VR) equipment that is used by users for accessing the world of the metaverse.

Reduced perception of physical space. Losing the natural connection to the real world is one of the biggest challenging entries between metaverse existing issues beyond the boundaries of security and privacy. The immersive and extremely engaging metaverse experiences made possible by VR technology are a major reason for the metaverse's success. VR, on the other hand, isolates a person far from his actual world for a certain amount of time. Metaverse Users engrossed within virtual reality encounters have no audio-visual link to the outside world. As a result, security problems in the metaverse as a result of VR also extend to physical security concerns in the user's environment. And for avoiding any possible physical security difficulties within the metaverse, users should constantly be mindful of their surroundings.

Radicalization and polarization. The last metaverse blockchain possible security vulnerabilities would refer to the metaverse's potential for radicalization and polarization. The privacy and security threats within the world of metaverse that have been explored so far are linked to technological shortcomings that enable the metaverse. The security threats of radicalization and polarization within the world of the metaverse, on the other hand, are derived from the fundamental premise of a shared reality. Without a doubt, the metaverse world is a vast platform for combining various apps, people, services, and assets. It can serve as the main access point for all resources is critical to its success. The metaverse, on the other hand, proposes presence and cohabitation in a shared, permanent virtual realm. Fusion of the drastically distinct as well as perhaps conflicting user groups can raise serious security risks in the metaverse. Many MMORPG gaming settings, for example, have documented incidents of low-skilled players and cyber-bullying of females. All persons have their characteristics and behave completely differently in the actual world. As a result, it's quite conceivable that they'd exhibit the same characteristics in the metaverse's virtual environments. Some users may be able to take advantage of how another user acts in the metaverse. As a result of extreme conduct and polarization in the metaverse world, security and privacy problems from harassment to trolling the metaverse arise.

5 Conclusion

The hidden side of the metaverse is shown in this examination of many metaverse security vulnerabilities. Many of us have thought that the metaverse is inherently safe from security and privacy threats because of blockchain. On the other hand, the metaverse isn't only about building apps based on blockchain technology. Augmented reality and virtual reality technologies in the metaverse world can result in a host of security and privacy vulnerabilities, such as social engineering attacks, ransomware attacks, network credential theft, and identity theft. Hackers may be able to hijack the identity of a user within the metaverse world by exploiting weaknesses in AR and VR devices. Furthermore, the lack of a visual-audio connection to the physical world (real world) makes the metaverse a physical security risk. Most significantly, polarization and radicalization in the metaverse are huge security and privacy issue. Find out more.

6 References

[1] Lee, Lik-Hang, 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).

[2] Ning, Huansheng, et al. "A survey on metaverse: The state-of-the-art, technologies, applications, and challenges." arXiv preprint arXiv:2111.09673 (2021).

[3] Di Pietro, Roberto, and Stefano Cresci. "Metaverse: security and privacy issues." 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2021. https://doi.org/10.1109/TPSISA52974.2021.00032

[4] Duan, Hanahan, et al. "Metaverse for social good: A university campus prototype." Proceedings of the 29th ACM International Conference on Multimedia. 2021. https://doi.org/10.1145/3474085.3479238

[5] Dincelli, Ersin, and Alper Yayla. "Immersive virtual reality in the age of the metaverse: A hybrid-narrative review based on the technology affordance perspective." The Journal of Strategic Information Systems 31.2 (2022): 101717. https://doi.org/10.1016/j.jsis.2022.101717

[6] Han, Dai-In Danny, Yoy Bergs, and Natasha Moorhouse. "Virtual reality consumer experience escapes: Preparing for the metaverse." Virtual Reality (2022): 1–16. https://doi.org/10.1007/s10055-022-00641-7

[7] Wang, Fei-Yue, et al. "Metasocieties in metaverse: Metaeconomics and meta management for meta enterprise and megacities." IEEE Transactions on Computational Social Systems 9.1 (2022): 2–7. https://doi.org/10.1109/TCSS.2022.3145165

[8] Xi, Nannan, et al. "The challenges of entering the metaverse: An experiment on the effect of extended reality on workload." Information Systems Frontiers (2022): 1–22. https://doi.org/10.1007/s10796-022-10244-x

[9] Fernandez, Carlos Bermejo, and Pan Hui. "Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse." arXiv preprint arXiv:2204.01480 (2022).

[10] Szczukiewicz, Konrad. "NFT metaverse startups and a possibility of fundraising through token issuance." Zeszyty Naukowe UPH seria Administracja i Zarządzanie 57.130 (2021). https://doi.org/10.34739/zn.2021.57.04

[11] Zaki, M., Rana and Hala Bahjat Abdul Wahab. "4G network security algorithms: Overview." International Journal of Interactive Mobile Technologies 15.16 (2021). https://doi.org/10.3991/ijim.v15i16.24175

[12] Tang, Sheng Kai, and June-Hao Hou. "Designing a framework for metaverse architecture." (2022).

[13] Park, Je-Ho. "Wrapping based open metaverse platform architecture." Journal of the Semiconductor & Display Technology 21.1 (2022): 1–4.

[14] L. Heller and L. Goodman, "What do avatars want now? Posthuman embodiment and the technological sublime," in International Conference on Virtual System Multimedia (VSMM), 2016, pp. 1–4. https://doi.org/10.1109/VSMM.2016.7863165

[15] C. S. Genay, A. Lecuyer, and M. Hachet, "Being an avatar "for real": A survey on virtual embodiment in augmented reality," IEEE Transactions on Visualization and Computer Graphics, 2021. https://doi.org/10.1109/TVCG.2021.3099290

[16] C. Kai, H. Zhou, Y. Yi, and W. Huang, "Collaborative cloud-edge-end task offloading in mobile-edge computing networks with limited communication capability," IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 2, pp. 624–634, 2021. https://doi.org/10.1109/TCCN.2020.3018159

[17] S. Kumar, J. Chhugani, C. Kim, D. Kim, A. Nguyen, P. Dubey, C. Biennial, and Y. Kim, "Second life and the new generation of virtual worlds," Computer, vol. 41, no. 9, pp. 46–53, 2008. https://doi.org/10.1109/MC.2008.398

[18] ISO/IEC 23005 (MPEG-V) standards. Accessed: Sep. 20, 2021. [Online]. Available: https://mpeg.chiariglione.org/standards/mpeg-v
[19] IEEE 2888 standards. Accessed: Dec. 20, 2021. [Online]. Available: https://sagroups.ieee.org/2888/
[20] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," arXiv preprint arXiv:2203.05471, 2022.
[21] Daelimhelim, Sahraoui, et al. "Edge-enabled metaverse: The convergence of metaverse and mobile edge computing." arXiv preprint arXiv:2205.02764 (2022). https://doi.org/10.36227/techrxiv.19606954.v1
[22] Thompson, John S., et al. "Editorial a decade of green radio and the path to "Net Zero": A united kingdom perspective." IEEE Transactions on Green Communications and Networking 6.2 (2022): 657–664. https://doi.org/10.1109/TGCN.2022.3172596
[23] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning-based trust computational model for IoT services," IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 39–52, 2019. https://doi.org/10.1109/TSUSC.2018.2839623
[24] Jaber, Tanya Abdulsattar, and Mohammed AbdulRidha Hussein. "Study on known models of NB-IoT applications in Iraqi environments." IOP Conference Series: Materials Science and Engineering. vol. 518. no. 5. IOP Publishing, 2019. https://doi.org/10.1088/1757-899X/518/5/052013
[25] J. D. N. Dionisio, W. G. B. III, and R. Gilbert, "3D virtual worlds and the metaverse: Current status and future possibilities," ACM Computing Surveys (CSUR), vol. 45, no. 3, pp. 1–38, 2013. https://doi.org/10.1145/2480741.2480751
[26] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," arXiv preprint arXiv:2110.05352, 2021.
[27] T. Huynh-The, Q.-V. Pham, X.-Q. Pham, T. T. Nguyen, Z. Han, and D.-S. Kim, "Artificial intelligence for the metaverse: A survey," arXiv preprint arXiv:2202.10336, 2022.
[28] Yang, Y. Zhao, H. Huang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," arXiv preprint arXiv:2201.03201, 2022.
[29] Kumar, J. Chhugani, C. Kim, D. Kim, A. Nguyen, P. Dubey, C. Biennial, and Y. Kim, "Second life and the new generation of virtual worlds," Computer, vol. 41, no. 9, pp. 46–53, 2008. https://doi.org/10.1109/MC.2008.398
[30] M. Park and Y.-G. Kim, "A metaverse: Taxonomy, components, applications, and open challenges," IEEE Access, vol. 10, pp. 4209–4251, 2022. https://doi.org/10.1109/ACCESS.2021.3140175
[31] Leenes, "Privacy in the metaverse: Regulating a complex social construct in a virtual world," The Future of Identity in the Information Society, pp. 95–112, 2008. https://doi.org/10.1007/978-0-387-79026-8_7
[32] 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. https://doi.org/10.1109/MTS.2018.2826060
[33] M. Bourlakis, S. Papagiannidis, and F. Li, "Retail spatial evolution: Paving the way from traditional to metaverse retailing," Electronic Commerce Research, vol. 9, no. 1–2, pp. 135–148, Jun 2009. https://doi.org/10.1007/s10660-009-9030-8
[34] J. Díaz, C. Andres, D. Saldana, C. Alberto, and R. Avila, "Virtual world as a resource for hybrid education," International Journal of Emerging Technologies in Learning (iJET), vol. 15, no. 15, pp. 94–109, 2020. https://doi.org/10.3991/ijet.v15i22.14393
[35] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in ACM International Conference on Multimedia (MM), Oct. 2021, pp. 153–161. https://doi.org/10.1145/3474085.3479238

[36] L. Lee, Z. Lin, R. Hu, Z. Gong, A. Kumar, T. Li, S. Li, and P. Hui, "When creators meet the metaverse: A survey on computational arts," CoRR, vol. abs/2111.13486, 2021.
[37] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, "A survey on metaverse: The state-of-the-art, technologies, applications, and challenges," arXiv preprint arXiv:2111.09673, 2021.
[38] Su, Zhou, et al. "A survey on metaverse: fundamentals, security, and privacy." (2022).
[39] Zhang, Rui, Rui Xue, and Ling Liu. "Security and privacy on the blockchain." *ACM Computing Surveys (CSUR)* 52.3 (2019): 1–34. https://doi.org/10.1145/3316481
[40] Roesner, Franziska, Tadayoshi Kohno, and David Molnar. "Security and privacy for augmented reality systems." *Communications of the ACM* 57.4 (2014): 88–96. https://doi.org/10.1145/2580723.2580730
[41] Jaber, Tanya Abdulsattar. "Artificial intelligence in computer networks." *Periodicals of Engineering and Natural Sciences* 10.1 (2022): 309–322. https://doi.org/10.21533/pen.v10i1.2616
[42] Marini, Arita, et al. "Mobile augmented reality learning media with metaverse to improve student learning outcomes in science class." International Journal of Interactive Mobile Technologies 16.7 (2022). https://doi.org/10.3991/ijim.v16i07.25727
[43] Herawati, Septy Nur, et al. "Android-based interactive media to raise student learning outcomes in social science." International Journal of Interactive Mobile Technologies 16.7 (2022). https://doi.org/10.3991/ijim.v16i07.25739
[44] N. Alseelawi, H. T. Hazim, and H. T. Salim ALRikabi, "A novel method of multimodal medical image fusion based on hybrid approach of NSCT and DTCWT," International Journal of Online Biomedical Engineering, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011
[45] I. A. Aljazaery, and A. H. M. Alaidi, "Encryption of color image based on DNA strand and exponential factor," International Journal of Online Biomedical Engineering, vol. 18, no. 3, pp. 101–113, 2022. https://doi.org/10.3991/ijoe.v18i03.28021
[46] S. H. Abbood, M. S. Rahim, and A. M. Alaidi, "DR-LL Gan: Diabetic retinopathy lesions synthesis using generative adversarial network," International Journal of Online and Biomedical Engineering, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28005
[47] A. F. Al-zubidi, N. F. AL-Bakri, R. K. Hasoun, and S. H. Hashim, "Mobile application to detect Covid-19 pandemic by using classification techniques: Proposed system," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24195
[48] H. T. ALRikabi and H. T. Hazim, "Enhanced data security of communication system using combined encryption and steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24557

7 Author

Tanya Abdulsattar Jaber received the BSc and MSc degrees in Computer Sciences in 2013 and 2016, respectively from the University of Technology. In 2016 she worked at the Institute of Applied Arts, Middle Technical University, Baghdad, Iraq, and worked as an assistant lecturer in 2016. She published six articles on the security of information, the internet of things, and AI in computer networks her research interests are general security, Encryption algorithms, cloud computing, and AI. (Institute of Applied Arts, Middle Technical University, Baghdad, Iraq).

Article submitted 2022-04-17. Resubmitted 2022-05-14. Final acceptance 2022-05-14. Final version published as submitted by the authors.