A Review of Cyber Gray Areas in Common Metaverse Use Cases

Ethan Nesel

School of Engineering & Technology

University of Washington-Tacoma

Tacoma, USA

nesele@uw.edu

Dr. Yan Bai

School of Engineering & Technology

University of Washington-Tacoma

Tacoma, USA

yanb@uw.edu

*Abstract*—As almost every sector experiences a digital shift, many researchers and industry leaders alike are exploring ways they can utilize metaverse functionality for their respective areas of interest and operation. However, cybersecurity appears to be often left out of the conversation in favor of discussing functionality and features. In this paper, we provide an overview of the term metaverse as it is currently understood while also briefly examining its origins. Next, we conduct a literature review to examine some of the most promising industries in which the metaverse will be utilized. This review importantly offers a look into the pressing cybersecurity gray areas of metaverse technologies within specific use cases. The information is summarized in table format and the conclusion section highlights key points.

Keywords—Metaverse, Virtual Reality(VR), Augmented Reality(AR), Extended Reality(XR), Cybersecurity, Cyber Threats, Healthcare, Education, Gaming

# Introduction

In recent years society has become largely obsessed with making virtual experiences more tangible, and more immersive. Tech industry leaders and start-ups alike are fighting to bring better quality AR and VR experiences to customers. Adding haptic feedback, enhancing viewing quality, and introducing more functionality are all high priorities. For the companies that bring innovation, the profits are certain to be massive. Pop culture further highlights this obsession. From motion pictures like Ready Player One, Enders Game, and The Matrix, to S&P 500 company Facebook completely rebranding to Meta, the evidence is everywhere. We are witnessing the adoption of modern metaverses.

The term “metaverse” originates from Neal Stephenson’s 1992 science-fiction novel Snow Crash and is used to describe a fictional virtual world [1]. The metaverse consists of a monochrome planet with an unending looped road and purchasable plots of land [21]. Over time the term has changed and evolved in meaning, and researchers have not formally agreed upon a strict definition. However, according to a published review of the literature in 2022, there is a trend of five main technologies used to describe the metaverse. The term metaverse today is attributed the most to AR/VR, avatar-based and Second Life systems, learning management systems, social media, simulation, and artificial intelligence(AI) [2]. Additionally, the metaverse is described as a place that fosters collaboration, enables learning through advanced computing, and immerses users in a way that is not dissimilar from our reality [2,3]. Therefore the literature indicates metaverses can differ in their technological implementation but tend to maintain similar characteristics in what they enable.

To explain the sudden popularity boom and rush towards metaverse adoption, the COVID-19 pandemic and enabling technologies such as 5G and 6G are letting more organizations and researchers experiment with the concept of metaverses and different implementations [4].

Current and emerging metaverses are characterized as infants compared to what science fiction depicts. As with any technology in its early stages, cybersecurity is a huge concern and the wide array of technologies that are used to implement different takes on the metaverse means more vulnerabilities [5].

# Literature Review

## Healthcare

The literature is saturated with articles describing simple to complex implementations of metaverses within healthcare. In [6], the typical metaverse in healthcare is characterized by immersive AR/VR and the concept of a digital twin. The digital twin is a user's avatar which is represented by medically relevant data sources such as sensors, medical records, risk factors, and observations. In [7], it is proposed that a digital twin of the same definition could meet with a virtual 3D doctor, but it would be the collected data being truly examined rather than the physical form. Researchers describe the utility and security benefits of blockchain in storing patient data along with how AI can aid in diagnosis within [8]. In [9], a review of metaverses related to healthcare highlights the importance of 3D imaging and real-time playback within VR/AR/XR for metaverse doctor visits. High quality-of-service is essential for gaining support for metaverse-supported healthcare along with conducting accurate data collecting. Further support for blockchain and the development of NFTs to store personal healthcare records is discussed in [10].

The current healthcare landscape suffers from a wide range of cybersecurity threats that impact confidentiality, integrity, and accessibility. Ransomware, insider threats, denial of service, data breaches, and social engineering are all major threats that plague the healthcare sector [11]. Healthcare metaverses favor utilizing wearable devices, AR/VR technologies, and blockchain, along with additional supporting technologies, but this will only add to the number of vectors that hackers may attempt to usurp. In [12], healthcare cybersecurity is described using a two-branch approach in defining attacks. Attacks either disrupt the operation of devices or disrupt the integrity of information. In order to stop attacks from both branches, general cybersecurity practices are not enough. A comprehensive plan must be developed for utilizing technologies.

AR and VR are important to the healthcare metaverse model, but they pose a wide array of cybersecurity risks. Many of these risks are already a part of the general threats to the healthcare space and likely have mitigation strategies. However, some must be addressed for the metaverse. Firstly, AR suffers from serious privacy concerns due to the amount of data collected and the storage of the data. VR has the same issue but tends to collect different types of data such as eye tracking and hand movement [13]. In [14], the same issues of data collection and privacy are addressed regarding collected personally identifiable information (PII). Additionally, manipulation and social engineering through relatively new-to-market systems pose a serious issue for consumers. In [15], authentication and identity along with social issues are discussed as major cybersecurity issues associated with a metaverse with similar characteristics to healthcare metaverses. Ensuring patients are accurate and doctors are speaking to the right people is crucial. Furthermore, as the healthcare metaverse is in its infancy there are no standards for proper socialization. The question arises if someone acts inappropriately or questionably what measures would hold them accountable?

Wearable sensors primarily carry privacy and secrecy along with functionality cybersecurity concerns. Due to being often placed into environments where hackers may be lurking, wearable sensors may be subject to attack frequently. Keeping the device itself along with the link it uses to communicate safely is vital [16]. According to [17], wearable devices lack strong security as they rely on wireless networks and are often comprised of simple architecture. They claim that the industry will not likely be the first to address this issue, but researchers will help fill in the gap.

According to [18], blockchain has the potential to eliminate malicious activity and cyber threats altogether. Furthermore, blockchain can be used for a wide range of use cases, especially in fields like healthcare. However, blockchain technology is still not fully understood, and just like protocols, it may suffer due to undiscovered flaws [19]. Implementation of such technology into healthcare or other vital sectors may be disastrous when not enough study has been done yet. In [20], the security of blockchain itself is less of an issue and cautious optimism regarding blockchain implementation is advised. Maintaining privacy and keeping blockchain systems online, access control systems, and lack of service level agreements are all concerning factors.

## Education

The usage of metaverses for academics and especially for delivering immersive higher education is a popular topic within the research community. An educational metaverse may primarily utilize AR/VR and real-life elements to provide a mixed-reality(MR) experience which may be more effective than trying to teach specific situational concepts in the typical classroom setting [22, 23]. In [24], XR is described as the primary technology of the metaverse and will be extremely useful in teaching healthcare professionals. XR combines VR, AR, and MR to put individuals in a world similar to true reality. XR lessons are suggested to be far superior due to the fact that it improves upon the current practice of disseminating information. In [25], education is described to be one of the most important use cases of metaverse technology. The authors suggest an educational metaverse framework that consists of wearable reality devices and supporting technologies including communication & networks, computing technologies, analytical technologies, modeling and rendering technologies, interaction technologies, and authentication technologies, that facilitate lessons in the metaverse. In [26], it is believed that the educational metaverse that utilizes virtual and augmented reality will allow for never-before-seen immersive teaching.

Educational institutions are frequently targets of cyber-attacks due to their elevated status along with their control of PII and unpublished or proprietary material [27]. FireEye a leader in cybersecurity reports that universities are prime targets for APTs to conduct various forms of espionage, for cybercriminals to profiteer, and for hacktivists to spread their agendas [28]. The reality devices used to describe educational metaverses and any assisting technologies present new cybersecurity threat vectors.

According to [26], the most concerning cyber threats to educational metaverse implementation and sustainability include DDoS, spoofing, and ransomware attacks. With lots of infrastructure needed to support VR/AR and the programs they run, ransomware and DDoS attacks, which are more prevalent than ever, could halt lessons. Spoofing consequently, may allow criminals to deep fake or mask themselves and make it easier to groom or take advantage of children. In [29, 30], the authors elaborate and discuss the concept of so-called overlay attacks in which hackers obstruct VR content with their own. Removing content in an overlay attack can be particularly challenging. Not only could it be used to implement ransomware-style attacks, but it could also be used to show troublesome content to minors. This threat is made even more worrisome by the conclusions of [31], in which the authors suggest VR-formed memories are particularly durable.

Outside of hackers and creeps, having multiple students in a metaverse poses its own threats. VR is an additional environment for bullying and harassment to occur [31]. As [26] highlights, there are few established norms or policies commonly utilized in the virtual world. The question of who polices or monitors is left up for debate. Furthermore, [32] concludes that while users of VR technology will typically reflect much of their real selves into their avatar and decision-making process, some departures do occur. If in an unmonitored environment, it is possible that students will reflect this behavior and treat others worse than they would in just a typical monitored classroom setting.

## Video Games

Gamers wanting more immersion and realistic experiences mean the metaverse is undoubtedly part of the future of gaming. This is supported by the fact that gaming and tech firms have already invested billions into metaverse research and development [35]. According to [33], metaverse gaming is characterized by aspects such as play to earn, social environments, the flexibility of environment and controls, portable assets, and a mixed reality experience. Furthermore, the metaverse for gaming utilizes primarily the technologies of AR/VR, blockchain, the Internet of Things, and 3D reconstruction. In [34], the authors suggest video games already mirror the types of environments and interactions found in a metaverse, however, a haptic suit and headset paired with virtual currencies and portable assets will be the true difference. In [36], the authors highlight AR, VR, and MR as general key metaverse technologies. Combining these technologies with massively multiplayer online game worlds will create metaverse gaming. However, it is also pointed out that the metaverse should allow for total interconnectivity between platforms and worlds and this has yet to be fully developed.

As video games become more popular, cybercriminals are leveraging the situation to launch an increased amount of cyberattacks, these attacks are often low-level attacks such as phishing [37]. However, cyber threats such as hacking via trojans, and viruses, along with various methods of item fraud are also both major concerns for gaming [38]. DDoSing is additionally a prolific aspect of gaming both for gamers and game providers whether it be for revenge/publicity or other motives [39]. The commonality appears to be the most favored attacks are uncomplicated and focus on either affecting user availability or gaining items of value such as virtual items or PII. PII is super valuable and typically video game accounts are linked to names, addresses, financial information, and more making them valuable likely targets [40].

Considering the general motives of hacking in gaming, protecting the technologies utilized in metaverse games from the same style of attacks or those with similar motives is essential.  VR is a huge source for the potential of PII leakage including information such as eye and body movement that hackers have not before had access to [30]. Hackers who can manage to directly access systems or the database storing information will have access to a treasure trove of PII. The authors of [29] point out that the platforms VR systems run on may serve as an attack point that allows for every compatible device to be infiltrated.

Another proposed element of metaverse gaming, blockchain, enables virtual game currencies and personal items known as NFTs. However, blockchain currencies, NFTs, wallets, and exchanges are points of attack for hackers [41]. Furthermore, blockchain presents individuals with the opportunity to commit illegal acts such as laundering money and financing terrorism [42].  Video game developer Valve Software in 2019 acknowledged in-game items were a popular method for money laundering, specifically items in their game Counter Strike were utilized to perform the illegal activity [43]. This activity was happening between accounts that had some information tied to them. Cryptocurrencies and NFTs, the suggested metaverse gaming currency, are typically extremely hard to prove owned by specific individuals.

According to [44] the modern Internet of Things is threatened by eight primary threat types consisting of network failure, direct cyber-attacks, APTs, malicious action, disaster, natural phenomenon, and system failure. Trying to pinpoint specific threats within these is unrealistic without additional context considering the Internet of Things definition. Internet of Things refers to the collective network of devices and technology that enable communication between devices and the cloud along with the devices themselves [45]. Therefore each specific device model must be analyzed in a comprehensive fashion and the threats will need to be identified for metaverse usage of that IoT device.

Finally, hackers may attempt to wreak havoc on the 3D-reconstructed environment video games utilize for players to explore. 3D reconstruction is similar to 3D map technology or virtual properties where you navigate a virtual environment [46]. Outside of preventing users from accessing the world through Denial of Service attacks, a Chaperone attack may be utilized to interfere with the 3D world and user experience. The Chaperone attack manipulates the virtual environment to change boundaries and may lead to VR users becoming injured or damaging equipment [30]. In one study, researchers were able to directly gain access to the files of a virtual game’s room set up giving them the possibility to perform malicious activities [29].

# Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| Use Cases | Technologies | Typical Mitigation Techniques to Oppose Cyberattacks on Such Technologies | Open Challenges Presented by Literature |
| Healthcare | Digital Twin,  AR/VR/XR,  Blockchain,  3D Imaging,  Real-time-playback,  Wearable Devices, | Robust access control,  Encrypting digital twin environment,  Strong authentication,  Patching,  End-to-end encryption ,  Robust security policies,  Antivirus | Protecting PII associated with VR systems,  Blockchain is not entirely understood and is presenting new threats constantly,  Wearable devices must be protected in all environments |
| Education | AR/VR/MR/XR,  Communication & Networks,  Computing Technologies,  Analytical Technologies,  Modeling and Rendering,  Interaction Technologies,  Authentication Technologies | Strict access control,  Encrypting sensitive data,  Strict authentication policies,  Patching and updating,  Antivirus | Overlay attack poses a danger to children,  Support infrastructure needed to enable classroom metaverse will be a massive undertaking to protect |
| Gaming | AR/VR,  Haptic Suit,  Blockchain,  IoT,  3D Reconstruction | Home network firewalls,  VPN,  Patching,  Strong authentication,  Encryption,  Antivirus | VR devices are still relatively new and security is constantly challenged,  Virtual items enable fraud and money laundering,  Chaperone attack serious risk to gamers |

# Conclusion

Overall this paper has summarized the technologies believed to be part of the current and future metaverse for the use cases of healthcare, education, and gaming. Some of the most relevant grey areas that pose cyber concerns were addressed. Relevancy was based on current attack styles, motives, and the technology itself. It should be acknowledged many additional cyber concerns are associated with the highlighted technologies. The information presented was then summarized in table format. Future work may look into mitigating these specific threats or forming a framework for a specific use case.

##### References

1. Márquez Díaz, J. E., Camilo Andrés Domínguez Saldaña, & Rodríguez Ávila, C. A. (2020). Virtual World as a Resource for Hybrid Education. International Journal of Emerging Technologies in Learning, 15(15), 94–109. https://doi.org/10.3991/ijet.v15i15.13025
2. Ng, D. T. K. (2022). What is the metaverse? Definitions, technologies and the community of inquiry. Australasian Journal of Educational Technology, 38(4), 190–205. https://doi.org/10.14742/ajet.7945
3. Moro, C. (2023). Utilizing the metaverse in anatomy and physiology. Anatomical Sciences Education. https://doi.org/10.1002/ase.2244
4. Bansal, G., Rajgopal, K., Chamola, V., Xiong, Z., & Niyato, D. (2022). Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare. IEEE Access, 10, 119914–119946. https://doi.org/10.1109/ACCESS.2022.3219845
5. Chow, Y.-W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and Cybersecurity in the Metaverse: A Survey. Journal of Imaging, 9(1), 11–. https://doi.org/10.3390/jimaging9010011
6. Song, Y.-T., & Qin, J. (2022). Metaverse and Personal Healthcare. Procedia Computer Science, 210, 189–197. https://doi.org/10.1016/j.procs.2022.10.136
7. Krishnan Ganapathy. (2022). Metaverse and healthcare: A clinician’s perspective. Apollo Medicine, 19(4), 256–261. https://doi.org/10.4103/am.am\_103\_22
8. Ali, S., Abdullah, Armand, T. P. T., Athar, A., Hussain, A., Ali, M., Yaseen, M., Joo, M.-I., & Kim, H.-C. (2023). Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. Sensors (Basel, Switzerland), 23(2), 565–. https://doi.org/10.3390/s23020565
9. Carey, B. (2022). Simulation and Virtualization Technologies, Artificial Intelligence Diagnostic Tools, and Metaverse Healthcare Systems in 3D Immersive Environments. American Journal of Medical Research (New York, N.Y.), 9(2), 9–24. https://doi.org/10.22381/ajmr9220221.
10. Dogum, R., & Uribe, D. (2023). NFTs and Metaverse in Healthcare: What’s the Big Opportunity? Blockchain in Healthcare Today, 6(1). https://doi.org/10.30953/bhty.v6.266
11. PATEL, R. (2022). CYBERSECURITY RISKS IN THE HEALTHCARE INDUSTRY. Indian Journal of Scientific Research, 12(2), 45–. https://doi.org/10.32606/IJSR.V12.I2.00007
12. Coronado, A. J., & Wong, T. L. (2014). Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. Biomedical Instrumentation & Technology, Suppl.Horizons, 48, 26-30. https://www.proquest.com/scholarly-journals/healthcare-cybersecurity-risk-management-keys/docview/1530406049/se-2
13. Kaspersky. (2021, June 11). What are the security and privacy risks of VR and Ar. usa.kaspersky.com. Retrieved March 24, 2023, from https://usa.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr
14. Chow, Y.-W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and Cybersecurity in the Metaverse: A Survey. Journal of Imaging, 9(1), 11. MDPI AG. http://dx.doi.org/10.3390/jimaging9010011
15. Virtual reality security. IEEE Digital Reality. (2022). Retrieved from https://digitalreality.ieee.org/publications/virtual-reality-security
16. Jiang, Q., Qian, Y., Ma, J., Ma, X., Cheng, Q., & Wei, F. (2019). User centric three‐factor authentication protocol for cloud‐assisted wearable devices. International Journal of Communication Systems, 32(6), e3900–n/a. https://doi.org/10.1002/dac.3900
17. Jiang, H., Chen, X., Zhang, S., Zhang, X., Kong, W., & Zhang, T. (2015). Software for Wearable Devices: Challenges and Opportunities. https://doi.org/10.48550/arxiv.1504.00747
18. Cybersecurity world is full of threats, only Blockchain can come to the rescue. (2022, June 23). Cyber Security Monitor Worldwide (Amman, Jordan). Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&docref=news/18AD069AEC5E2B68.
19. Threat Intelligence Cybersecurity Expert Shares Stance on Blockchains Risks and Future. (2019, February 8). Cyber Security Monitor Worldwide (Amman, Jordan). Available from NewsBank: Access World News – Historical and Current: https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&docref=news/17176397D852AB58.
20. Paranjape, K., Parker, M., Houlding, D., & Car, J. (2019). Implementation Considerations for Blockchain in Healthcare Institutions. Blockchain in Healthcare Today, 2. https://doi.org/10.30953/bhty.v2.114
21. STEPHENSON, N. E. A. L. (2022). Snow crash. DEL REY.
22. De Gagne, J. C., Randall, P. S., Rushton, S., Park, H. K., Cho, E., Yamane, S. S., & Jung, D. (2022). The Use of Metaverse in Nursing Education: An Umbrella Review. Nurse Educator, Publish Ahead of Print. https://doi.org/10.1097/NNE.0000000000001327
23. Han, S., & Noh, Y. (2021). Analyzing Higher Education Instructors’ perception on Metaverse-based Education. Journal of Digital Contents Society, 22(11), 1793–1806. https://doi.org/10.9728/dcs.2021.22.11.1793
24. Dr. N. Kala. (2022). Revolutionizing Medical Education with Metaverse. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 26–32. https://doi.org/10.32628/CSEIT22844
25. Zhang, X., Chen, Y., Hu, L., & Wang, Y. (2022). The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics. Frontiers in Psychology, 13, 1016300–1016300. https://doi.org/10.3389/fpsyg.2022.1016300
26. Contreras, G. S., González, A. H., Fernández, M. I. S., Cepa, C. B. M., & Escobar, J. C. Z. (2022). The Importance of the Application of the Metaverse in Education. Modern Applied Science, 16(3), 34–. https://doi.org/10.5539/mas.v16n3p34
27. Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 39–. https://doi.org/10.3390/fi13020039
28. Cyber threats to the education industry - fireeye. (n.d.). Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-education.pdf
29. Casey, P., Baggili, I., & Yarramreddy, A. (2021). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing, 18(2), 550–562. https://doi.org/10.1109/TDSC.2019.2907942
30. Giaretta, A. (2022). Security and Privacy in Virtual Reality -- A Literature Survey. https://doi.org/10.48550/arxiv.2205.00208
31. Aliman, N.-M., & Kester, L. (2020). Malicious Design in AIVR, Falsehood and Cybersecurity-oriented Immersive Defenses. 2020 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), 130–137. https://doi.org/10.1109/AIVR50618.2020.00031
32. Messinger, P. R., Ge, X., Stroulia, E., Lyons, K., Smirnov, K., & Bone, M. (1970). On the Relationship between My Avatar and Myself. Journal of Virtual Worlds Research, 1(2). https://doi.org/10.4101/jvwr.v1i2.352
33. Applications of metaverse in virtual gaming. Appinventiv. (2023, February 17). Retrieved from https://appinventiv.com/blog/metaverse-gaming/
34. <https://web-p-ebscohost-com.offcampus.lib.washington.edu/ehost/pdfviewer/pdfviewer?vid=0&sid=e3d3f0d8-1542-4717-9143-a044b73b3a13%40redis>
35. Gross, A. (2022). Epic Games secures $2bn from Sony and Lego to build gaming metaverse. FT.com.
36. Nevelsteen, K. J. L. (2018). Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the Metaverse. Computer Animation and Virtual Worlds, 29(1). https://doi.org/10.1002/cav.1752
37. Cyber threats: Gamers are the new target during Covid-19. (2020). Financial Express.
38. Zhao, C. (2018). Cyber security issues in online games. AIP Conference Proceedings, 1955(1). https://doi.org/10.1063/1.5033679
39. Prolexic Reveals the Tainted World of Multiplayer Video Games and Denial of Service Attacks: Gaming communities provide fertile ground for DrDoS attacks against financial services, fellow players. (2013). PR Newswire.
40. Increased online gaming poses cyber-security risks for homes, businesses. (2021). Legal Monitor Worldwide.
41. 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. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 66, 102542–. https://doi.org/10.1016/j.ijinfomgt.2022.102542
42. Bjelajac, Ž., & Bajac, M. (2022). Blockchain technology and money laundering. Pravo, Teorija i Praksa, 39(2), 21–38. https://doi.org/10.5937/ptp2202021B
43. BBC. (2019, November 1). Valve shuts down money laundering via CS:Go Game. BBC News. Retrieved from https://www.bbc.com/news/technology-50262447
44. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. Applied Sciences, 11(10), 4580–. https://doi.org/10.3390/app11104580
45. What Is IoT (Internet of Things)? Amazon. (n.d.). Retrieved from https://aws.amazon.com/what-is/iot/#:~:text=The%20term%20IoT%2C%20or%20Internet,as%20between%20the%20devices%20themselves
46. Stouffer, C. (2022, August 8). Metaverse gaming: An overview + cybersecurity guide. Norton. Retrieved from https://us.norton.com/blog/kids-safety/metaverse-gaming