International Journal of Security and Privacy in Pervasive Computing
Volume 15 • Issue 1

A Descriptive Study on Metaverse:
Cybersecurity Risks, Controls, and Regulatory Framework

Glorin Sebastian, Georgia Institute of Technology, USA*
https://orcid.org/0000-0003-2543-9127

ABSTRACT

Maximalist, interconnected set of experiences straight out of sci-fi, based on 3D virtual environment through personal computing, and augmented reality headsets—a world known as the Metaverse—this is the futuristic vision of internet that technology giants are investing in. There has been some research on data privacy risks in the metaverse; however, detailed research on the cybersecurity risks of virtual reality platforms like metaverse have not been performed. This research paper addresses this gap of understanding the various possible cybersecurity risks on metaverse platforms. This study tries to understand the risks associated with metaverse by describing the technologies supporting metaverse platform and understanding the inherent cybersecurity threats in each of these technologies. Further, the paper proposes a cybersecurity risk governance regulatory framework to mitigate these risks.

KEYWORDS

Augmented Reality, Cybersecurity, Metaverse, Mixed Reality, Privacy, Virtual Reality

INTRODUCTION

The famous global news website quartz defines metaverse as an immersive next-generation version of the internet, rendered by virtual or augmented reality technology (Nover, S., 2021.). Internet has evolved over the years, having transitioned from internet on desktop to web and now on mobile phones. Information transfer has also evolved from text to sharing photos to watching video content, with Web 1.0 - read only, Web 2.0 focused on person-to-person connection, Web 3.0 will be decentralized and focused on user interaction and will limit and control users' content (Nath, K., Dhar, S. and Basishtha, S., 2014). The next frontier in internet evolution is the metaverse, where you feel virtually present. While virtual reality has been classified for a while now, as one of the emerging technology trends used for gaming and virtual experiences, it differs from metaverse, since metaverse will be more immersive, embodied internet where you are in the experience, be it getting together with family, play, work or at shopping. The recent entry of some of the biggest technology firms into metaverse has

DOI: 10.4018/IJSPPC.315591 *Corresponding Author

sparked the debate among the tech world and the general public on the relevance, risks, and benefits of such online platforms, after the moderately successful earlier attempts to create such platforms eg: Second life (Heath, Dan & Chip., 2011).

18 years after the first release of Second life in 2003, technology firms are reinvesting in virtual reality platforms. What has changed since then? It can be argued that technology has made great progress, especially average internet speed has increased from 64 Kbps to over 1 Gbps with the 5G networks (Vora, L.J., 2015.). There have been significant advances in supporting technologies such as 5G/6G networks, artificial intelligence, IoT, graphics and robotics. Also about 60% of the world's population now have access to internet (Johnson, Joseph, 2021). All these advances have made it much more conducive for the emergence of such virtual platforms, which is promised to be much more realistic and present than earlier. Research is still ongoing to better some of the components of metaverse for eg: VR supporting infrastructure including hardware such as VR headsets that have sensors to allow avatars to mimic real-world movements, which would make the VR experience much more lifelike. The metaverse would feature a marketplace for goods both physical and virtual items owned by avatars and implemented as NFT's (non-fungible tokens). Metaverse would have other multitude of applications which is described in section 1.3.

The venture capitalist Matthew Ball, whose writing on the metaverse has influenced Mark Zuckerberg, describes in his article on the metaverse that "future solutions are often understood and, in a sense, agreed upon well in advance of the technical capacity to produce them. Still, it's often impossible to predict how they'll fall into place, which features matter more or less, what sort of governance models or competitive dynamics will drive them, or what new experiences will be produced" (Ball, M.,2020). As Matthew described, there are still many issues relating to metaverse which needs to be discussed and one of them is the security and privacy risk as well as perceived risks to this platform and a control governance model to mitigate these risks. These are researched and discussed in the following sections.

Basic Concepts of Metaverse

In order to understand the technology risks associated with Metaverse and to formulate a technology governance model, it is first important to gain familiarity with the main concepts of Metaverse. These eight concepts listed below essentially summarize the metaverse experience and also helps with perceiving the technology risks associated with the underlying technologies:

1. **Avatar:** Living 3D representations of the users and user expressions. One can have different avatars for work, gaming and for hanging out. Modular Codec Avatars (MCA) generates hyper-realistic faces driven by the cameras in the VR headset. MCA extends traditional Codec Avatars (CA) by replacing the holistic models with a learned modular representation (Chu, Hang, et al.). Technology companies are bettering perceptual science to ensure the avatars feel real and present. Also it needs to be ensured that avatars are inclusive with diverse set of skin and physical features, to achieve this, companies are working with human and civil rights groups for avatar design.
2. **Presence:** Meta CEO described the metaverse as an "embodied Internet" that, unlike the Internet of today, gives one a "feeling of presence." Realistic presence is the key to feeling connected in the metaverse. The research teams at these technology companies are working to improve the environmental understanding, content placement and persistence, voice, and hand interactions to better this sense of presence. Presence platform is a broad range of machine perception and AI capabilities that empower developers to build mixed reality experiences on VR headsets. This would also apply to Mixed reality examples such as doing a workout in your living room.
3. **Home space:** Home space is the default environment in metaverse when the user puts on their VR headset. Users would be able to invite others to join the home space for hangouts and virtual parties as their virtual avatars.

4. **Teleportation:** Teleportation is a type of mobility process which allows the user to virtually move around in a VR environment. With teleportation in the VR, the user using the controller points at and moves to a location they'd like, after initiating the teleportation action. this causes them to be instantly transitioned to the desired location via rapid animation (Teleportation Demo, Google).
5. **Interoperability:** Interoperability would be inbuilt into metaverse. Since there would be multiple metaverses, interoperability allows users to use their avatars and assets across applications, games as well as across different metaverses. There would be platforms such as Omniverse, that connects these 3D worlds into a shared virtual universe (Brian Caulfield, 2021) and it is significant that interoperability is maintained across these platforms to not disrupt user experience.
6. **Virtual Goods:** Virtual goods are the virtual representation of real products. Examples of virtual goods could include paintings which can be sold as NFT's (Non fungible tokens) within the virtual world. Taco Bell sold tens of thousands of dollars of NFT Taco Art - iconic and original artwork inspired by their tacos at the price of their menu items (Chohan, R, and Jeannette P, 2021).
7. **Natural Interfaces:** Natural interfaces refer to virtual interfaces instead of keyboards and screens, the interaction will be more natural, using gestures, and having the sense of presence. In Virtual reality, most screens would be holograms i.e. For example instead of a computer screen virtual reality hardware would be enabled via holograms. Real-time 3D holography would enhance systems from VR to 3D printing. This would immerse VR viewers into more realistic scenery, while eliminating eye strain and other side effects of long-term VR use (Ackerman Daniel, MIT).
8. **Privacy and Safety:** Technology firms plan to have Privacy and open standards inbuilt into Metaverse. Metaverse needs to be compliant by default to major Privacy directives such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act) (Cavoukian, A., 2009). In their research, The Social Metaverse: Battle for Privacy, Ben Falchuk, Shoshana Loeb, and Ralph Neff describe that in Metaverse data privacy includes 3 types of information (Falchuk, B., Loeb, S. and Neff, R., 2018):
    a. **Privacy of personal information:** Any information that reveals something about physical, medical, physiological, economic, cultural, or social status. In case of Metaverse, the Avatars would be closely modelled after the user, hence would have massive amounts of Biometric information about the user including details such as iris scans etc. for authentication.
    b. **Privacy of behavior:** The Avatars would store details on information about user habits, activities, choices, etc. For example from the history of music events attended, or types of games played and history of purchases, the data about the user behavior can easily be determined.
    c. **Privacy of communications:** This includes, data and metadata relating to personal communications such as communication between friends and family during virtual events.

Technologies Enabling Metaverse

Figure 1 lists the technologies supporting the Metaverse ecosystem. It is significant to understand each of these technologies and their vulnerabilities to scope out the attack vectors and the cybersecurity and data privacy risks associated with the metaverse ecosystem:

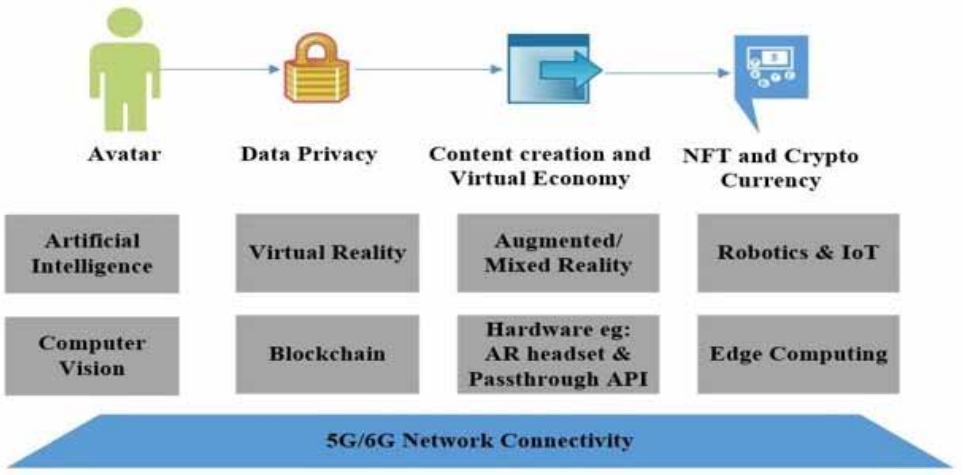
1. **Artificial Intelligence:** Artificial Intelligence (AI) includes building smart machines which can take perform tasks based on inbuilt algorithms. AI is being utilized in the metaverse across diverse areas such as content analysis, self-supervised speech processing, robotic interactions, computer vision and whole-body pose estimation. AI also helps plot facial expressions, emotions, and physical features to make the avatar more realistic and dynamic. The AI engine can analyze 2D user images or 3D scans to come up with a highly realistic simulated rendition.

2. **Virtual Reality:** Virtual reality (VR) is the use of computer graphics systems in combination with various display and interface devices to provide the effect of immersion in the interactive 3D computer-generated environment (Fairfield, J., 2021The best recognizable component of Virtual reality is the head-mounted display (HMD), that have inside out tracking (built-in sensors) that uses cameras outside of the headset, to keep track of its position orientation. Some of the main players in the virtual reality space include Oculus Quest, and HTC Vive. The HMD hardware providers work with VR publishers and developers eg: Gaming companies such as Vertigo Games, which is a VR publisher and developer to create virtual user experiences.
3. **Augmented reality and Mixed reality:** Mixed reality (MR) refers to the inclusion of virtual computer graphics objects into real world, or alternatively the inclusion of real-world components into a virtual environment. The former is referred to as augmented reality, while the latter is augmented virtuality (Pan, Z., Cheok, A.D., Yang, H., Zhu, J. and Shi, J., 2006). Azuma has described the characteristics that are fundamental to an augmented reality interface: it combines the real and the virtual. Also, it is interactive in real time. Finally, it is registered in a three-dimensional view (Azuma, Ronald T, 1997). Most metaverse providers depend on content creators to create Augmented reality effects. For example: For Meta, Spark AR Go allows to build more Augmented reality effects, that will enable creators to take their creations and project it as holograms and Augmented reality. It is to be noted that the tech companies are working on further technologies such as Spatial Anchors and Scene Understanding Capabilities that will make these mixed-reality experiences even more seamless in the future. A great example of augmented reality is linking AR to physical locations, such as guided tours or scavenger hunts.
4. **Passthrough API:** Passthrough API was released by Facebook's VR wing Oculus that allows developers to build and test applications that enable merging real and augmented reality content using AR headsets and smart glasses. These interoperable APIs are crucial to ensure users are able to use avatars and digital assets across metaverses. These API's also help enable teleportation across these virtual environments. Technology firms are working to improve these APIs to upgrade to resolution colored mixed reality passthrough API. It combines an array of sensors with reconstruction algorithms, to represent physical world in a headset with sense of depth and perspective (Youtube, connect 2021).
5. **AR/VR and mixed reality hardware:** Hardware devices including head-mounted VR displays (HMD), with built-in sensors to capture input from user is an integral part of Virtual reality and is the physical connection between the end user and the virtual world. While considerable progress has been made in this technology, research is ongoing to continuously better the system interfaces in a natural manner (usitc.gov,2012), and also to increase the number of inputs that the device accepts and transfers. Progressive research is also happening to improve haptic gloves in order to create realistic sense of touch in the metaverse to feel texture and pressure when you touch virtual objects. This would allow users to teleport into a virtual destination and enjoy the company of friends in a virtual setting.
6. **Blockchain, NFTs and Crypto:** Blockchain is a digitally distributed, decentralized, public ledger, in which data is stored in blocks, instead of structured tables (Nofer, M., Gomber, P., Hinz, O. and Schiereck, D., 2017). The generated data is stored into blocks, which is further linked onto previous blocks, chained in a chronological order. Users (called nodes) store blockchain data locally and synchronize them with other blockchain data stored on peer devices with a consensus model. In the case of an error in one of the nodes, the other nodes can be referenced to correct this error. Decentralization and security are two of the traits of blockchain (Berg, C., Davidson, S. and Potts, J., 2019.)(Cai, W., Wang, Z., Ernst, J.B., Hong, Z., Feng, C. and Leung, V.C., 2018). Non-Fungible Token (NFT) is a type of cryptocurrency (Fairfield, J., 2021.) derived by the smart contracts of Ethereum. NFT is unique and cannot be exchanged like-for-like (equivalently, non-fungible), making it suitable for identifying something or someone in a unique way. Using NFTs on smart contracts (in Ethereum (Shirole, M., Darisi, M. and Bhirud, S., 2020)), a creator can

easily prove the existence and ownership of digital assets in the form of videos, arts, event tickets, etc. Furthermore, the creator also earns royalties each time of a successful trade on any NFT market or by peer-to-peer exchanging (Wang, Q., Li, R., Wang, Q. and Chen, S., 2021.). With Augmented reality, more items from physical world can be brought into metaverse and setup as Non fungible tokens, thus both NFT's and Cryptocurrencies would have huge applications and are expected to be the medium of exchange of value in the metaverse.

7. **Computer vision:** "Computer vision is a field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos, and other visual inputs" (ibm.com,2022). It trains computes to understand the visual world. It further enables localization and mapping, scene understanding and image processing (Lee, L.H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C. and Hui, P., 2021.). Sub-domains of computer vision include scene reconstruction, object detection, event detection, etc. and would be one of the main technology enablers of the metaverse ecosystem.
8. **Edge Computing:** Edge computing refers to the enabling technologies that allow computation to be performed at edge of the network, mainly on downstream data in cloud services and upstream data for IoT services. Here "edge" is defined as "any computing and network resource along the path between data sources and cloud data centers" (Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L., 2016.). For example, a micro data center and a cloudlet (Satyanarayanan, M., Bahl, P., Caceres, R. and Davies, N., 2009.) is the edge between a mobile device and cloud. The argument of edge computing is that computing should happen near data sources. Some of the benefits of Edge computing over cloud computing include, reduced response time from 900 to 169 ms (Yi, S., Hao, Z., Qin, Z. and Li, Q., 2015) and reduced energy consumption by 30-40%. Instead of hosting personal data on leased cloud storage, edge computing allows this to be stored on personal devices, hence also reducing the exposure to data leaks, and improving the cyber posture.
9. **Robotics & IoT:** According to Statista (Lionel, S, 2021), by 2025, the total IoT connected devices worldwide will reach 30.9 billion, compared to existing 13.8 billion connected devices in 2021. Metaverse would allow blending IoT and AR/VR/MR technologies thereby enabling multi-modal interaction systems to achieve compelling user experiences (Kim, J.C., Laine, T.H. and Åhlund, C., 2021.). Also these virtual environments are channels for communication between robots and virtual environments, due to their feature of visualizing contents (Chacko, S.M. and Kapila, V., 2019). For metaverse to be most effective, the data from different technologies powered by IoT and 5G network connectivity, should work together seamlessly.

Figure 1. Metaverse ecosystem and supporting technologies



Applications of Metaverse

1. **VR Simulation Training Medicine/Other Sectors:** Metaverse and Virtual Reality can be used for simulation training in multiple sectors including Medicine and Surgery. Figure 2 represents application of VR in medical technology, with medical professionals performing surgery using Virtual reality applications. For example, Using AR medical technology, Johns Hopkins neurosurgeons performed the institution's first-ever AR surgeries on living patients in June. During the initial procedure, physicians placed six screws in a patient's spine during a spinal fusion. The team donned headsets made by Augmedics, equipped with a see-through eye display that projects images of a patient's internal anatomy, such as bones and other tissue, based on CT scans (John Hopkins, 2021).
2. **Gaming:** Gaming is one biggest application of metaverse. Virtual, extended, and mixed reality, players can play head-to-head against others around the world on games such as chess and tennis. Major platforms like Epic are starting to build out the metaverse with gaming applications using the VR and AR ecosystem. Some of the gaming studios live service games that launch updates and new downloadable content regularly making sure gaming can build active communities.
3. **Smart Cities:** Metaverse is going to have a lot of adoption in smart cities. Smart cities are constantly learning as they work with sensors from the Internet of Things (IoT), video cameras, social media, and other information sources to gather information about the needs of their citizens. Cites have started adoption of metaverse for their governance. For example, Seoul's metaverse plan aims to be completed by 2026 and could roll out in phases starting next year (Lee, Michelle Ye Hee.,2021). It would first be available on smartphones. Eventually, augmented reality tools, such as goggles and controllers, may be used, officials said. the city will open its metaverse i20 center, which will serve as a virtual city where the residents meet with local officials (in their avatar forms) to request services or file complaints.
4. **Metaverse Economy:** With the Metaverse being built out, there is expected to be a parallel virtual economy that would be fueled by the content creators and influencers. The exchange of value would be using Blockchain technologies such as Crypto Currency and NFT's (Non fungible tokens). Several companies have already entered Metaverse to do business virtually. Eg: Nike has several patents related to selling products in the metaverse, recently created Nikeland in conjunction with Roblox.
5. **Other Applications:** Metaverse is expected to have many more applications eventually. One example Metaverse Enables users to train with virtual trainers. Applications such as Supernatural, FIT-XR and Player 22 already have guided bodyweight exercise, and VR hardware companies are in process of developing fitness accessories that would make it more comfortable for workouts.

LITERATURE REVIEW

To understand the comprehensive landscape of existing studies related to the cybersecurity and privacy risks in metaverse, a review of the relevant literature was conducted. In the first attempt, the search keywords used included "metaverse", "cybersecurity", "privacy risks" in the title, the abstract, or the body of the articles. The focus was mainly on primary sources known for high-quality studies on virtual environments. Even though there were quite a few studies on metaverse, including applications of Virtual Reality, Augmented and Mixed reality to industry, the ones studying the cybersecurity and privacy risks were very few and are listed below. The earlier studies did not in detail research on all the cybersecurity risks to the Metaverse platform and the technologies supporting it nor suggest mitigation controls that could be implemented by both the metaverse platform provider and the end users. Refer to Table 1 for details of the literature review.

Figure 2. VR application in medical surgery

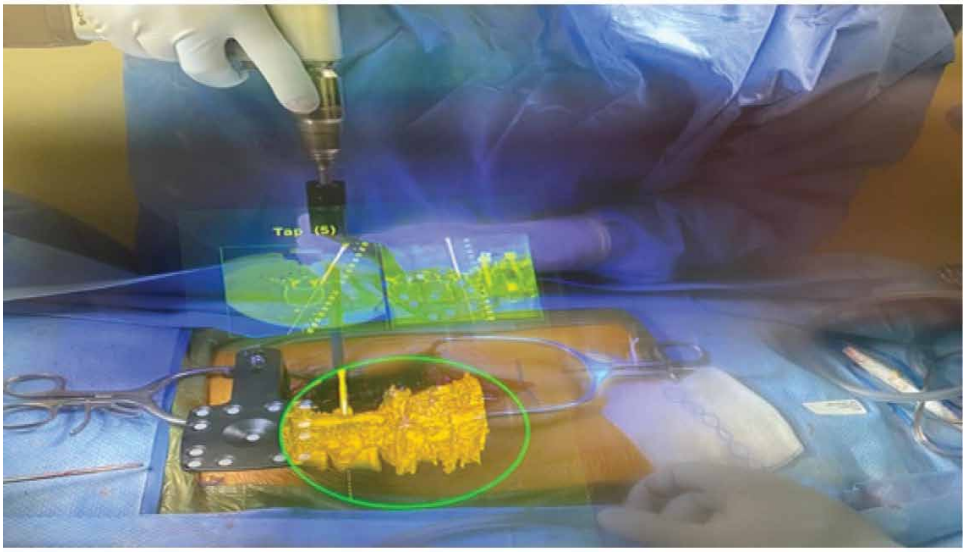


Table 1. The literature review for privacy and security risks for Metaverse

Topic	Authors	Discussion
Privacy in the Metaverse. In IFIP on the Future of Identity in the Information Society, pages 95–112. Springer, 2007 (Leenes, R., 2007).	Ronald Leenes	Study based on Second life, shows users behave similarly in Metaverse as in real life.study suggests users to have multiple avatars to confuse attackers in the metaverse
"The social metaverse: Battle for privacy," IEEE Technology and Society Magazine, vol. 37, no. 2, pp.52–61, 2018.	Falchuk, S. Loeb, and R. Neff	Also mainly talks about criminal harassment, social engineering attacks and suggests a few approaches such as using multiple avatars or request private copy of section of metaverse or using a disguise avatar.
Metaverse: Security and Privacy Issues IEEE TPS, December 12-15, 2021	Roberto Di Pietro,Stefano Cresci	Apart from the suggestions in earlier research, this paper suggests on controls over algorithmic fairness and authentication in the metaverse
All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda, 2021	Lik-Hang Lee, Tristan Braud, PengyuanZhou, et al.	The paper while providing a comprehensive view on Metaverse, also touches on the approach to protect users from continuous monitoring, and protecting biometric and digital twin data
A survey on metaverse: Fundamentals, security, and privacy. arXiv preprint arXiv:2203.02662.	Wang, Yet. Al (2022).	Details the fundamentals, security, and privacy concerns of metaverse
Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse. arXiv preprint arXiv:2204.01480.	Fernandez, C. B., & Hui, P. (2022).	focuses on 3 major pillars to guide development of the metaverse: privacy, governance, and ethical design. Further talks about modular governance as well as ethical considerations
Regulating the Metaverse, a Blueprint for the Future. In International Conference on Extended Reality (pp. 263-272). Springer, Cham.	Rosenberg, L. B. (2022).	This research outlines the dangers of the metaverse along with proposals for sensible regulation.
A Study on Metaverse Awareness, Cyber Risks, and Steps for Increased Adoption. International Journal of Security and Privacy in Pervasive Computing (IJSPPC), 14(1), 1-11.	Sebastian, G. (2022).	This study tries to understand public awareness, perception, and concerns about metaverse adoption from a cybersecurity and IT risk perspective.
Privacy Concerns and Measures in Metaverse: A Review. In 2022 15th International Conference on Information Security and Cryptography (pp. 80-85). IEEE.	Canbay, Y., Utku, A., & Canbay, P. (2022, October).	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.

DISCUSSION ON CYBER RISKS IN THE METAVERSE

A 2022 article by Forbes Technology Council (Weijde, R. ter.,2022) mentions there are many areas of the Metaverse where further clarity is needed, the main among them being Crime - How do you "police" the metaverse? Other areas of ambiguity mentioned include ownership of materials and work ethics. While these fine aspects of crime, law, and ethics are being sorted out and defined within this fairly new horizon of virtual reality, the best way forward for companies aiming for higher adoption of metaverse would be to proactively anticipate cybersecurity risks and adopt efficient controls. Section 1.2 explained in detail the technologies that support the metaverse. This section further describes the technology risks associated with metaverse, and companies planning on increased adoption of metaverse should anticipate these risks and proactively adopt mitigation controls. Table 2 lists the mitigation controls for each of the cyber risks listed below. Further, Figure 3 shows how the cyber risks in each of the technology supporting the metaverse ecosystem is being effectively mitigated:

1. **Data Privacy:** Data privacy is the most important cybersecurity risk in the metaverse. Privacy concerns with the user information that is being collected stored and the purposes for which it is utilized. It is to be noted that the information collected for virtual reality would also include biometric data which is sensitive. This biometric information if leaked, could be used for forging avatars with disastrous consequences. Based on the geography of the end users, the data privacy directives such as GDPR and CCPA would apply to the user data collected. Privacy needs to be inbuilt into the Metaverse. Using privacy frameworks such as privacy by design would be the best way to accomplish this (Cavoukian, A., 2009). The main concerns would be around what data is being harvested, how long and where is it stored and what is it used for. Targeted advertising based on collected data would be sensitive and anti-trust would also be an issue in metaverse to lookout for.
2. **Access Risk:** Access controls would be crucial in the metaverse, be it authenticating into the user avatar or authenticating users into a private chat or games room. access controls could be risk-based access controls, role based, discretionary or other access control types, based on the requirements of the user. These controls need to be effective to ensure the users are able to decide whom they will communicate and interact with or if they'd want to block someone from accessing the applications.
3. **Security of NFT (Non fungible tokens) and Blockchain:** The exchange of value in the Metaverse is expected to be completed using cryptocurrencies and NFT (Non fungible tokens) both of which as applications of Blockchain technology. There have been a number of examples of Blockchain smart contract platform vulnerabilities which have been exploited by malicious actors. Due to the distributed nature of blockchain, once the contract is deployed, the code is not modifiable, As a result, if there is any vulnerability in the deployed contract, especially the smart contracts that manage a lot of Ethereum tokens, it can lead to very serious consequences. Some of the examples of breaches by utilizing the code vulnerability include in 2016 the "DAO" incident became the most well-known security breach. With the development of a smart contract audit, some traditional vulnerability analysis methods such as symbolic execution, fuzzing test, and taint analysis are gradually being introduced into the audit of smart contracts (Dawson, M., Burrell, D.N., Rahim, E. and Brewster, S., 2010.). Some of the controls suggested to mitigate the vulnerabilities include correctly verifying the identity of the caller via methods such as signature verification.
4. **Code vulnerabilities in the Metaverse/Application platform:** Code vulnerabilities in the Virtual Reality platform is one of the major cyber risks associated with Metaverse. This could be the Metaverse platform itself or the applications running within Metaverse for example Blockchain based crypto currencies or gaming applications. Some of the controls that need to be in place to prevent code and platform-based vulnerabilities include practicing secure coding techniques including using secure coding standards such as SEI-CERT, MISRA and C11 Annex

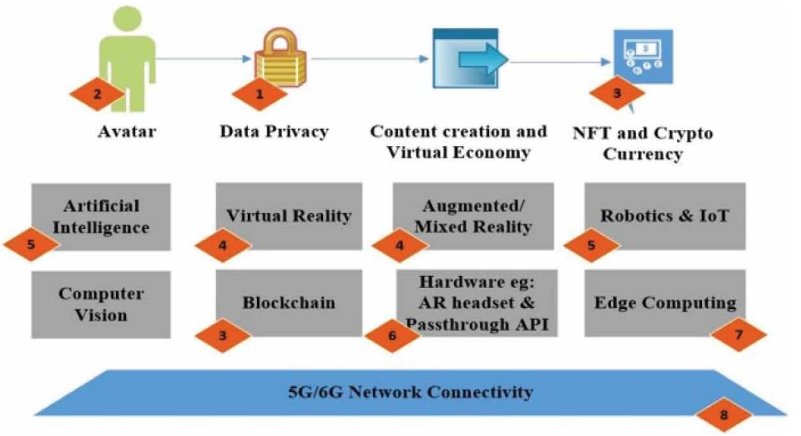
J (for C or C++ programming languages) and OWASP and BSI standards for Java, Python, and other programming languages. Regular code review by Team leads and Internal Audit teams and integrating secure software development techniques into SDLC cycle is also important to find and mitigate any code vulnerabilities (Dawson, M., Burrell, D.N., Rahim, E. and Brewster, S., 2010.). Automatic code quality tools such as Static Application Security Testing (SAST) (Ebert, C. and Weyrich, M., 2019.) can be used to automate and improve code quality. Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST) are very helpful to uncover code vulnerabilities as well. Another key step to prevent bad actors from using any known code vulnerabilities is applying timely vendor patches and effective change management controls.

5. **Algorithmic fairness:** With increased adoption of Artificial intelligence, algorithms increasing role in making substantive decisions in modern society, ranging from insurance and credit decisions to resume screening, however the algorithmic decisions are often opaque with not a lot of explanation for the decisions taken. In this case, it is mandatory to ensure the platforms and applications relying on algorithmic decision making are making use of fair algorithms and do not discriminate based on user features such as race, gender etc. Understanding the algorithmic decision factors and then measuring the impact of each influencing input factors such as race or gender on the final decision of the system (Datta, A., Sen, S. and Zick, Y., 2016).
6. **API/Sensor Security:** Gartner predicted that by 2022, API abuses will move from an infrequent to most frequent attack vector resulting in data breaches for enterprise web applications (Gartner,2021). APIs expose application logic and sensitive data such as Personally Identifiable Information (PII) and because of this have increasingly become a target for attackers. Without secure APIs, rapid innovation would be impossible. Hence It is important to review and define the vulnerable APIs. Companies need to do risk assessment of APIs, fix vulnerabilities, detect abuses and respond automatically. Authenticated APIs are generally considered safe; however the companies need to control access using private APIs which are invite only. API Security is a huge risk in Metaverse given the huge number of interfaces and APIs including neural interfaces and brain computer interfaces that would interact with AR devices as well as passthrough API which increases the interoperability. Example of an API in Metaverse is EMG (Electromyography) input on the muscles on the wrist with contextualized AI.
7. **Cloud Data Security/Data Center Security:** Cloud Data Security is critical in Metaverse since the virtual data would be stored in cloud, some of the main controls in Cloud include Data encryption, key management, Security risk assessment, Authentication and authorization, media protection, Contingency planning, privacy, legal and compliance, Data center operations, incident response, awareness, and training (Hendre, A. and Joshi, K.P., 2015). Data Center Security is significant as well, ensuring the physical safety of Data Center along with technical controls such as incident management and timely audits are essential. For Edge Computing – specifically data privacy/security, utilize tools to protect data privacy and security at the edge of the network, but tools are still missing to handle diverse data attributes for edge computing (Nofer, M., Gomber, P., Hinz, O. and Schiereck, D., 2017).
8. **Network Security:** The fifth generation (5G) and the sixth generation (6G) are the communication network foundations of the Metaverse. 5G has the advantages of high speed, low delay, ubiquitous network, low power consumption and interconnection of all things, while 6G will break the limitations of time and virtual reality, providing the network foundation for the Metaverse. In the 5G and 6G network environment, quantum communication already ensures communication security in the Metaverse (Chowdhury, M.Z., Shahjalal, M., Ahmed, S. and Jang, Y.M., 2020). Further, quantum communication improves overall security due to the superposition properties of qubits. However, there needs to be technical controls like CDN (Content delivery network) for DDoS Protection, WAF (Web application firewall) for Known Threat Protection Bot Mitigation, API Gateway for authentication and authorization at the Network layer.

Table 2. Cyber and IT risks for Metaverse and mitigation controls

IT/Cyber Risks	Mitigating Controls
1. Data Privacy issues	Based on the privacy directives, the users should be given the opportunity to decide on that data that would be shared. Companies need to ensure disclosure on the user data collected, where it is stored and what it is used for. Also adopting controls for purpose, data and storage limitation as well as confidentiality and integrity is necessary.
2.Access Risk	Effective Access controls need to be in place for authenticating users into their avatars or into a private chat or games room.
3.Blockchain based NFT, Crypto currency Vulnerabilities	Vulnerability analysis methods such as symbolic execution, fuzzing test, and taint analysis are gradually being introduced into the audit of smart contracts. Other suggested controls to mitigate the vulnerabilities include correctly verifying the identity of the caller via methods such as signature verification.
4.Platform/Application code vulnerabilities	Following coding best practices such as SEI-CERT, MISRA, C11 Annex J, OWASP, regular code reviews and testing using tools such as SAST/DAST/IAST (Static/Dynamic/ Interactive Application Security Testing)
5.Algorithmic fairness	As part of Security audits, understand the algorithmic decision factors and then measure the impact of each influencing input factors on the final decision of the system to ensure there is no discrimination.
6.API/Sensor security	The objective is to control access using private APIs which are invite only. Companies need to do risk assessment of APIs, fix vulnerabilities, detect abuses and respond automatically. Authenticated API's are assumed safe.
7.Data Center/Cloud Security	Controls in Cloud include Data encryption, key management, Security risk assessment, Authentication and authorization, media protection, Contingency planning, privacy, legal and compliance, Data center operations, incident response, awareness, and training (Datta, A., Sen, S. and Zick, Y., 2016). Utilize tools to protect data privacy and security at the edge of the network, but tools are still missing to handle diverse data attributes for edge computing (Nofer, M., Gomber, P., Hinz, O. and Schiereck, D., 2017.).
8.Network Security	Technical controls like CDN for DDoS Protection, WAF for Known Threat Protection, Bot Mitigation, API Gateway for authentication and authorization at the Network layer

Figure 3. Metaverse ecosystem and supporting technologies with Cyber/IT risk indicators



CONCLUSION

Virtual, augmented, and mixed reality worlds like metaverse represent a great opportunity and a big leap ahead (if not a quantum leap) for technology, one that is capable of advancing and transforming many fields like medicine, education. Metaverse adoption is expected to increase in the coming months and years as more and more companies get interested in adoption of virtual, augmented, and mixed reality technologies. While virtual worlds like second life had relatively low adoption of less than 1 million users, Metaverse is expected to do better with advanced technology support including increased adoption of high-speed internet (5G,6G), artificial Intelligence and robotics as well as higher

investment in research by technology giants such as Facebook and Microsoft and its increased use not just in gaming but in fields such as medicine, education, and other real-life applications. While it may take a few years or decades to fully develop metaverse platforms, the time is ripe for working towards making it a reality.

During the Connect 2021 video (Youtube, connect 2021), it was mentioned that one of the concerns of the tech community is that the speed with which the new technologies emerged left the policy makers and regulators playing catch up, another important hurdle that most technology firms have faced scrutiny is based on cybersecurity and privacy risks. Forbes Tech Council article (Weijde, R. ter.,2022), describes the areas of ambiguity for metaverse are specifically around policing crime and work ethics.

Hence, it is important that, in order to ensure these risks, especially cybersecurity and privacy risks do not hamper the progress of Virtual reality technology, companies proactively anticipate IT and cyber risks and adopt preventive mitigation controls. Our research addresses these concerns by reviewing the cybersecurity risks in the supporting technologies in detail and suggests mitigation controls for these risks. Further, our research provides an IT Cyber risk governance framework template, which companies can leverage as a starting point and periodically assess and customize based on their specific risk exposure, thus, greatly assisting organizations trying to enter and build their own metaverse platforms.

FUTURE RESEARCH

This research was meant to provide a high-level understanding of the IT risks associated with the technologies supporting Metaverse, and controls that would mitigate the risks, thereby proposing an IT risk governance model for Metaverse. As Metaverse matures, further risks could be identified, and the proposed IT risk governance model can be further expanded. A risk ranking approach can also be followed while prioritizing the implementation of mitigation controls based on specific organizations. Further, while the proposed IT governance framework is generic and not specific to any industry, in the future industry-specific IT governance frameworks can be proposed based on industry specific IT risks.

STATEMENTS AND DECLARATIONS

The author did not receive support from any organization for the submitted work. The author certifies that he had no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. All methods were carried out in accordance with relevant guidelines and regulations.

COMPLIANCE WITH ETHICAL STANDARDS

The author certifies that he has no other potential conflicts of interest. The research did not involve human participants.

REFERENCES

Ackerman, D. (2021). *Using Artificial Intelligence to Generate 3D Holograms in Real-Time.* MIT News. https://news.mit.edu/2021/3d-holograms-vr-0310

API Security. (n.d.). *Protect Your Apis from Attacks and Data Breaches*. Gartner. https://www.gartner.com/ en/webinars/4002323/api-security-protect-your-apis-from-attacks-and-data-breaches

Azuma, R. T. (1997). A survey of augmented reality. *Presence*, *6*(4), 355–385. doi:10.1162/pres.1997.6.4.355

Ball, M. (2020). *The Metaverse: What It Is, Where to Find It, and Who Will Build It*. https://www.matthewball.vc/all/themetaverse

Berg, C., Davidson, S., & Potts, J. (2019). Blockchain technology as economic infrastructure: Revisiting the electronic markets hypothesis. *Frontiers in Blockchain*, *2*, 22. doi:10.3389/fbloc.2019.00022

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized applications: The blockchain-empowered software system. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 53019–53033. doi:10.1109/ACCESS.2018.2870644

Canbay, Y., Utku, A., & Canbay, P. (2022, October). Privacy Concerns and Measures in Metaverse: A Review. In *15th International Conference on Information Security and Cryptography* (pp. 80-85). IEEE. doi:10.1109/ISCTURKEY56345.2022.9931866

Caulfield, B. (2021). *What Is the Metaverse?* The Official NVIDIA Blog. https://blogs.nvidia.com/blog/2021/08/10/what-is-the-metaverse/

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.

Chacko, S. M., & Kapila, V. 2019, October. Augmented reality as a medium for human-robot collaborative tasks. In *2019 28th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)* (pp. 1-8). IEEE. doi:10.1109/RO-MAN46459.2019.8956466

Chohan, R., & Paschen, J. (2021). What marketers need to know about non-fungible tokens (NFTs). *Business Horizons*.

Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open Journal of the Communications Society*, *1*, 957–975. doi:10.1109/OJCOMS.2020.3010270

Chu, H. (2020). Expressive telepresence via modular codec avatars. In *European Conference on Computer Vision*. Springer.

Datta, A., Sen, S., & Zick, Y. (2016, May). Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems. In *2016 IEEE symposium on security and privacy (SP)* (pp. 598-617). IEEE.

Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Integrating software assurance into the software development life cycle (SDLC). *Journal of Information Systems Technology and Planning*, *3*(6), 49–53.

Ebert, C., & Weyrich, M. (2019). Validation of autonomous systems. *IEEE Software*, *36*(5), 15–23. doi:10.1109/MS.2019.2921037

Fairfield, J. (2021). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal*.

Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine*, *37*(2), 52–61. doi:10.1109/MTS.2018.2826060

Fernandez, C. B., & Hui, P. (2022). *Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse.* 10.1109/ICDCSW56584.2022.00058

He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart contract vulnerability analysis and security audit. *IEEE Network*, *34*(5), 276–282. doi:10.1109/MNET.001.1900656

Heath, D., & Chip. (2011, Nov. 8). Why Second Life Failed: How the 'Milkshake Test' Helps Predict Which Ultrahyped Technology Will Succeed, and Which Won't. *Slate Magazine*.

Hendre, A., & Joshi, K. P. (2015, June). A semantic approach to cloud security and compliance. In *2015 IEEE 8th International Conference on Cloud Computing* (pp. 1081-1084). IEEE. doi:10.1109/CLOUD.2015.157

Hopkins, J. (2021). *Johns Hopkins Performs Its First Augmented Reality Surgeries in Patients*. https://www.hopkinsmedicine.org/ news/articles/johns-hopkins-performs-its-first-augmented-reality-surgeries-in-patients

Johnson, J. (2021). *Internet Users in the World 2021*. Statista. https://www.statista.com/ statistics/617136/digital-population-worldwide/

Kim, J. C., Laine, T. H., & Åhlund, C. (2021). Multimodal interaction systems based on internet of things and augmented reality: A systematic literature review. *Applied Sciences (Basel, Switzerland)*, *11*(4), 1738. doi:10.3390/app11041738

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., & Hui, P. (2021). *All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda*. arXiv preprint arXiv:2110.05352.

Lee, M. Y. H. (2021). Seoul Wants to Build a Metaverse. A Virtual New Year's Eve Ceremony Will Kick It off. *The Washington Post*. https://www.washingtonpost.com/world/asia_pacific/ metaverse-seoul-virtual/2021/11/27/03928120-4248-11ec-9404-50a28a88b9cd_story.html

Leenes, R. (2007, August). Privacy in the Metaverse. In *IFIP International Summer School on the Future of Identity in the Information Society* (pp. 95–112). Springer.

L.J. (2015). Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G. *International Journal of Modern Trends in Engineering and Research, 2*(10), 281-290.

Nath, K., Dhar, S., & Basishtha, S. (2014, February). Web 1.0 to Web 3.0-Evolution of the Web and its various challenges. In *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)* (pp. 86-89). IEEE. doi:10.1109/ICROIT.2014.6798297

Newton, C. (2021). *Mark Zuckerberg is betting Facebook's future on the metaverse*. The Verge.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. doi:10.1007/s12599-017-0467-3

Nover, S. (2021). *The Vocabulary You Need for the Metaverse*. Quartz. https://qz.com/2089665 /everything-you-need-to-know-to-understand-the-metaverse/

Pan, Z., Cheok, A. D., Yang, H., Zhu, J., & Shi, J. (2006). Virtual reality and mixed reality for virtual learning environments. *Computers & Graphics*, *30*(1), 20–28. doi:10.1016/j.cag.2005.10.004

Rosenberg, L. B. (2022). Regulating the Metaverse, a Blueprint for the Future. In *International Conference on Extended Reality* (pp. 263-272). Springer. doi:10.1007/978-3-031-15546-8_23

Satyanarayanan, M., Bahl, P., Caceres, R., & Davies, N. (2009). The case for vm-based cloudlets in mobile computing. *IEEE Pervasive Computing*, *8*(4), 14–23. doi:10.1109/MPRV.2009.82

Sebastian, G. (2022). A Study on Metaverse Awareness, Cyber Risks, and Steps for Increased Adoption. *International Journal of Security and Privacy in Pervasive Computing*, *14*(1), 1–11. doi:10.4018/IJSPPC.308785

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637–646. doi:10.1109/JIOT.2016.2579198

Shirole, M., Darisi, M., & Bhirud, S. (2020). Cryptocurrency token: An overview. *IC-BCT*, *2019*, 133–140.

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017, November). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 Internet Measurement Conference* (pp. 432-444). Academic Press.

Teleportation Demo. (n.d.). Google VR. https://developers.google.com /vr/elements/ teleportation

ter Weijde, R. (2022, March 3). *Understanding The Metaverse*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2022/03/03/understanding-the-metaverse/

The Metaverse and How We'll Build It Together Connect. (2021). YouTube. https://www.youtube.com/watch?v=Uvufun6xer8

U.S.I.T.C. (2012). *Certain Video Game Systems and Wireless Controller and Components Thereof*. USITC, 337-770, No. 446916-36.

Vailshery. (2021). *Internet of things (iot) and non-iot active device connections worldwide from 2010 to 2025*. Academic Press.

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). *Non-fungible token (NFT): Overview, evaluation, opportunities, and challenges.* https://www.ibm.com/topics/computer-vision

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015, November). Fog computing: Platform and applications. *Third IEEE workshop on hot topics in web systems and technologies (HotWeb)*, 73-78.