Scientiarum: A Multidisciplinary Journal
Volume 1, Issue 2, April 2025, pp. 12–17
DOI: 10.54646/SAPARS.2025.08

REVIEW

Privacy issues in metaverse

Bharath Kalyan*, **Pavanish Reddy, Roshini and Sayeesha**

University of Memphis, Memphis, United States

***Correspondence:**
Bharath Kalyan,
born2win1987@yahoo.com

Received: 31 March 2025; **Accepted:** 10 April 2025; **Published:** 19 April 2025

Objective: The term, "Metaverse" has gained attention from academicians and the corporate companies recently. Metaverse is the term used to denote the virtual-reality environment through which the users' interaction takes place. The attention on this topic has increased especially after the announcement given by the major tech giants on their new investments in the field of augmented reality (AR), virtual reality (VR), blockchain technology, latest 5G network and many more.

Methods: Even though these technologies are growing faster, the companies and the target audience are prone to many privacy issues. Though there are minimal number of articles published, there are not many studies available regarding this. We will explain the traits of Metaverse in detail and will offer a framework on blockchain technology to arrest the privacy issues.

Results: We are making enough research on the security issues and will provide our results from the point of view of resolving malicious attacks, privacy issues, decentralized systems, issue with real-world communication and many more. We will also summarize the problems with regards to the security needs.

Conclusion: This research paper is to give you an insight on the privacy issues related to the use of metaverse. This is also to provide an idea on the projects that are happening and their related issues in addition to the recent technologies and the solutions that can improve the security. In this paper, we also propose an idea for the usage of blockchain technology for improving the trustworthiness and the security of using Metaverse.

Keywords: Metaverse, augmented reality (AR), virtual reality (VR), blockchain technology, Privacy Isuses

Introduction

The Metaverse which refers as the concept which encompasses both physical world and the digital realm, that usually aims to virtualize and to able to digitize reality. It brings together with the wide range of technologies with the goal that is used to map and even surpass the real world. Metaverse which relies on numerous technologies that to address with the security risks associated with its development and it can be complex and prominent. Metaverse has the better advantages, and it can be applied to the various upcoming technologies. In this survey metaverse related technologies used to highlight potential security and privacy concerns. Additionally, metaverse which has still myth that are not solved yet about its potential. Overall, this kind of survey which provides a comprehensive review of security and the challenges in privacy posed by key technologies in the Metaverse applications. This research survey provides more way about its security and the potential content for its development. It aims is to offer the valuable insight and research for the development of this particularly in the terms of security and privacy concerns.

Facebook announced its decision to change its name to Meta to Epic games, Metaverse technologies made huge investment around billion dollar and made an announcement in public saying that it would remain its existence for the same in the upcoming years. J.P.Morgan said that "*metaverse is a seamless convergence of our physical and digital lives, creating a unified, virtual community where we can work, play, relax, transact and socialize*". And there is no any specific definition for Metaverse it can be defined as something new, which requires development in future in internet.

The conception behind the Metaverse includes using of virtual reality (VR), augmented reality (AR) and avatars. This helps to bring in great significance in network and the key important aspect is creation of a significant aspect of the metaverse will involve the emergence of multiple virtual worlds, specifically designed to enhance digital social interactions. By incorporating a three-dimensional aspect to the web, these virtual worlds aim to provide a more authentic and realistic experience for users. One key feature that has been proposed for the metaverse is interoperability. As with any new and cutting-edge technology, careful consideration and implementation will be crucial. Innovation technological development shall raise a complex and legal topic in disputes such as NFT-related, legal disputes, predominantly which involves trademark rights and licensing considerations for NFT owners and creators, in addition to the range of licenses which are used by creators. The questions relating to Intellectual property rights shall arise and are closely connected, this can be discussed with an example to evaluate the identity of the creators in metaverse are subjected to be more difficult as compared to the results from a decentralized collaborative process which is in turn performed by the unmasked or untraceable person behind the avatars.

It is said that digital identity and location are subjected to increase more in volume so digital security is at most important for the owners as well as the users who are dealing with the digital identity information.

In addition to these issues, privacy may well top the list since privacy data of person in this become valuable which means it is voluminous than it already is because technologies will become increasingly integrated into the multifaceted aspects of users' lives. Businesses which operate in a metaverse increasingly generate revenue streams by advertising their products to users. For example, metaverse shops may directly communicate with metaverse users aiming to promote their products or services and, in doing so, collect personal information. Furthermore, privacy will likely be a major concern as the metaverse continues to expand. With technology becoming more ingrained in our daily lives, the amount of valuable personal data within the metaverse will only increase. As businesses in the metaverse rely on advertising to generate revenue, they may directly target users to promote their products or services, resulting in the collection of personal information.

Metaverse in digital healthcare and its challenges

The metaverse which represents the simulated environment that used to combine the digital, physical, and human with the goal of strong sense of mutual presence among the individuals. In the area of healthcare, the metaverse which has the potential to revolutionize the e-health services by offering the immersive experiences and seamless integration of data collection, analysis, and treatment.

In the metaverse health care system, patients can used to receive virtual treatment from nurse, and it is like face to face like experience. The patients' symptoms and vital signs, which are used to collect the data by usage of wearable devices then it is processed and analysed using the Machine Learning and AI models. From these learning-based models that is to inform the treatment decisions.

For better understanding, when the user is provided with the metaverse online health services uses the advancement of biometric feature so that the data consists of and together with the recognitions of audio and video recording that might be insure and can be leaked by hackers and it can be stored in private networks. The client who is fake can also try to use the fake picture and interact with patients that are used to obtain the patient confidential information.

The Specialist or Physicians tries to utilize the information or seek feedback from the existing models that provides the treatments. Metaverse which serves as the service reflects as the wholesome incorporate the network with the health services using Metaverse.

The information has the two main sources which is to be noted: The first one is the data collected from the original world are exploited for it in the VR. The second one is the source of information which is generated the output of the virtual worlds that include the data generated by the assets, of Machine learning diagnostic models and has the person picture and information of their medical history.

For the safeguarding with the privacy and the data flows in the secure level with the exchange with the different kinds of the layers that are identified with the attack surface with the great importance that ensures the high band transmitting with trusted performances for this medical services.

Comparing to old electronic health care system metaverse called as the services which provide medical services which offer certain advantages:

- Enhanced Access: Metaverse breaks down barriers and allows individuals in remote areas to access remote consultations that used to provide monitoring from the doctor. For this level of integration and accessibility which cannot be efficiently achieved through the old services.
- Immersive Experience: It provides the patients with interactive experience. People can use the healthcare services in the way which are not possible with existing services. VR based training can be utilized that enhances the skills of health professionals.
- Real time collaboration: The metaverse enables among the health professionals, regardless of their geographical locations. Surgeons can used to engage with the methodology and communicate with specialists from world. This multidisciplinary digital care management which it is not feasible in the old existing medical services.

The metaverse as a health service which is still evolving with the full potential and definition that are to be realized. To achieve immense experience, with its infrastructure relies on technologies such as 6G wireless networking, AI/Machine learning, blockchain, and digital twins. The integration of these technologies that introduces new privacy and security threats that it needs to be addressed.

To create the experiences of healthcare that this infrastructure which needs to be integrated and access to monitor and manage with the sensitive aspects of People. It is usually achieved with the advancement of utilization with cutting-edge technologies like the future sixth generation of WIFI infrastructure, ML/AI with the advancement of blockchain and digital twins.

The recent technologies in the metaverse health care services it is much needed to acknowledge to identify the weakness and it can be used to inherited with the corresponding services. The new additional threats which may arise in the metaverse technology, and it is not exists in the old existing cyber security and in the real world.

The security challenges in the metaverse include:

- Data Fusion: In the metaverse collects the information and processes with huge number of different kinds of the private data from all around. Safeguarding the security and privacy of such granular sensitive information is crucial.
- Networking Nodes: The metaverse which consists of immense heterogeneous networking with the diverse hardware and communication interface implementations. The Security solution will be conventional, and it face challenges in securing beyond the generations of communication networks, requires the sensitive information and it has the less securable concepts.
- Data collection: The level of measurements in this are existing old which can be consistent and can be portable can run through any platforms. These technologies in the metaverse which used to track user's actions, interactions, facial expressions, vocal pitch etc. These mechanisms with the strong regulations is needed to protect the data privacy of user.

Overall, the metaverse-as- a- health services which has potential to revolutionize healthcare by providing the immersive experience and with enabling the real time collaboration with advanced technologies. Additionally, addressing privacy and security challenges is crucial to be secured with more scalable manner in the medical care systems.

Data collection

In terms of these concepts some authors propose with the usage of block chain technology with the enhanced and existing Artificial Intelligence which usually enhance data security and trust in the healthcare services within in this technology. These papers are lack with the comprehensive view of secure purpose that exists between the number of different sections among the network of metaverse. This author suggests us with the usage of block chain technology that ensures the safeguard and the secrecy of these concepts but with the little result delays that are associated with block chain ML models that can slow the prosper of these apps making it impractical for usage.

While the systematic literature review explores with needed mechanisms of block chain-based technology for medical care management in this application to operable without any delays and considers about the designs of this application. Many existing concepts which lack with the comprehensive view of privacy and vulnerabilities prevails across the different kinds of the layers and the section of the Metaverse networking and many papers neglecting the challenges of requirements for the use cases like medical service. The review which also fails to satisfy the risks which are not addressed. Consequently, metaverse does not offer insights into the barriers and the required facilities for these cases like healthcare. Similarly, other research articles which focus on the communication, data privacy and security that neglects the comprehensive views on privacy and security. It always safeguards the learning models, and it may cause the inference the delay that will hinder the growth of metaverse application and makes it impractical as the generic solutions.

For example, research they do not specify the address of the risks which arises from the ML/AI algorithms and that are mandatory which takes care of the metaverse inventions. Certain authors may consider these communication and networking security of this technologies with the advancement as the use case the digital healthcare services which is more important in the terms of the privacy and secure that are not addressed. To emphasize the concepts between the others of this paper which can be usually compared to the current paper and can have the discussions:

- Comprehensive Perspective: It focuses on specific aspects of metaverse such as networks, digital twins or block chains, this article which takes the holistic approach that to consider the digital way of medical services as the significant use case and it offers certain guideline for secure and ensures the privacy concerns with the different layers of these platforms which exists between the accessing and public aspects.
- Security and Privacy of View of holistic approach: Many Papers considers that this concept can be used more than one with secure which meeting the Privacy from the different areas. Each section begins with examples and the use cases that are related to metaverse healthcare, which highlights the barriers and its inference which are already discussed.

- Novel Solutions and perspectives: In addition to covering well-established solutions, this paper also explores with the new innovations and less-gathered mechanisms that have been given promise in WIFI technology in the upcoming periods. These novel solutions which can be applied to healthcare metaverse services as well. The concepts such as artificial intelligence learning and physical privacy, machine learning, rules in communication which can enhance the security and privacy in the metaverse (1).

Will metaverse affects the data privacy?

The privacy rules shall be applicable to the users of metaverse. The question arises every time is that is the real identity of the virtual avatar is traceable? And will it affect and reveal the identity of individual? Metaverse works by giving access to create their own avatars which are pseudonymous. There are two reasons behind the avatar's in-metaverse actions, which in turn reduces the intensity of any protection pseudonymization. First reason shall be In the world of the metaverse, an avatar takes on a unique sub-identity that sets it apart from others. However, this sub-identity may inadvertently reveal data regarding the real-life identity it represents via behaviour's or data. This can result in a mix of benefits and potential anonymity risks. For example, an avatar's uniqueness may need to be verified for access in a meeting room that is virtual, highlighting the personal nature of this information. This raises the question of whether the avatar can be considered a separate entity with its own privacy rights, or if it simply serves as a pseudonymous version of its creator. If avatars do have privacy rights, the next consideration is whether they themselves or their "owners" hold these rights in the virtual world.

Which rules shall apply for privacy?

The risk of improper use of something or victimization of personal data are high and the data scams and breach of data which can be ported from one metaverse to another. High chances of exploitation of personal data so it is necessary to display privacy rules. Users and operators shall enter into agreement which shall in turn supervise the data transfers and certain security standards and shall take up the responsibility of compliances for such as data breach. Moreover, the metaverse often involves virtual promotion. There is a growing need for stringent and clear privacy values to safeguard the consumers' rights utilizing the metaverse. Additionally, the metaverse serves as a convergence point for various privacy regulations due to its global accessibility and diverse offerings. Many such cases which involves multiple privacy regimes for every individual and every data this can be well explained with an example The European data protection has a union which monitors the behavior the EU citizens and the business which offers goods and services in terms of EU even though the business presence is not present in Europe (article 3 sec. 2 GDPR). The companies present in Europe shall use the metaverse wielded under US company shall follow GDPR rights as well.

For a case point, the consumer protection act in California shall apply to all the residents in the country CA as defined in the Section 17014 of Title 18 of California Code of Regulations. These regulations define who is a consumer and how he is protected. No specific provisions which opts in or opts out for coverage, Under section 1798.192 Claims that effort to relinquish CCPA privileges are dead against the public policy and states them "void and unenforceable."

The given is to ensure the success which is not guaranteed this type of languages which is included in terms of service. The forum selection which includes the disputes with the resolution clauses that can be able to provide some kind of certainty that regards to any legal disputes, and it will be resolved, and the person will be responsible for solving these. The other kinds of Clauses may provide proper guidance on which laws apply to the interpretation of the Metaverse Terms of Service.

If the regulator initiates an investigation, these kinds of approaches which may not be so effective. In additional such clauses which may not be universally enforced which means that the litigation that could still occurs in the multiple jurisdictions. So, it is crucial for the companies that to comprehend with the privacy rules that applies to the data and parties.

The rights of data subject which enforces in Metaverse:

- **Addressee for enforcing the data subject rights:**

The query that arises as that to against the individuals who can exercise their rights regardless of the protection rules of the data are applicable. It is not the clear kind in metaverse, as operators who typically acts as controllers, which may reluctant that to disclose the identity of the voluntarily that to comply with the data subject the requests. It used to hide the mail aliases or other kind of proxy sites. This challenge which can be intensified if the person privacy that have been violated by the other user, an advertiser, and so on.

- **The Data Subject Rights:**

The different kinds of the rights and the obligations can apply and depend on the privacy regime in effect. An individual who consumes the services or purchases the Specified NFTs in metaverse, their personal kind of data are stored and collected the access is done.

This article is based on the mutual understanding and working principles data privacy and the technological development in a metaverse that compile a set of ordinary and sensitive data. These updated features of technology run under an international virtual store of metaverse, operated by US. They persuade law and order by handling sensitive data confidentially in the company. In the current virtual world, they run these technological aspects with a legal requirement, which competes the modern privacy law with noticeable disclosures for a collection of data. Many other global teams were maintaining their privacy based on the factor that would differentiate between an ordinary data and the sensitive data. The miserable in holding a data privacy would gradually end up in complexity of potential laws to pursuits. The privacy law includes all variation in noticing their needs and distinguishes the other data types to determine their variable accessing the rights. The disclosure of should end up in clearing the details of requirement and they should be understandable. This will be difficult when it is lengthy. The disclosure determines the volume of data which explains its new type and these shows the user who read the disclosure. The profiling data are certain beneficial feature which operates a metaverse. The metaverse helps in tracking the user and monitor their activity. GDPR is used with respect to the US-based privacy law. The processing of GDPR does not make decision based on processing and profiling the legal measure of an individual. Taking up decision may not be accepted with explicit duty of data privacy. The profiling process of a data must get concerned with subject regarding all explicit measures. Data privacy is maintained in a standard line of design and analyze the defaults with the impact. When there is an introduction of newer technology, the parties which capture privacy would fall in legal pits. They need to procure the virtual interphase from the reality and stabilize the personal data as sensitive data in an online platform. The blocking system would terminate the personal data with another server user when connected with internet. The people who create an adverse network in newer technology should maintain one's privacy policy in data, security in sensitive information and work with limited access under government law.

In a virtual environment, they can monitor and check the user's actions, communication, and actions. They might have valid reasons to do so, such as to keep an eye on inappropriate behavior and material. To ensure that users are aware of and have authority over the handling of their personal information in a metaverse, what notification and consent techniques should the creator keep in place? These are all concerns that need to be addressed into consideration and rectified immediately. b) GDPR article 25 following the guidelines of protecting information by layout and default, as outlined in GDPR article 25 and ISO 27701, indicates that by default, user's personal information will only be processed so far as it is necessary to accomplish the objectives of the service they are utilizing. This means requesting these sorts of questions and actively developing features to protect user's rights to confidentiality. In particular, authorities must build up the necessary technical and organizational protections from the beginning to protect the privacy of data subjects and apply privacy principles as specified in GDPR article 25. Due to this, the person who created the metaverse must have policies in place to make sure that only the required amount of data is obtained and processed to fulfill the objectives of the data processing operation, as well as the information is properly protected, for instance through advanced encryption, particularly by using blockchain technology. 8 c) From the US perspective, data privacy by design while current regulations in the US include requirements for risk assessments. During their enforcement decisions, enforcers like regulatory authorities are probably going to take into account when a company's SDLC, comprises privacy by design. Any business that ignores privacy by design faces the risk of encountering legal action and regulatory attachment. 6. Security and privacy expectations in the metaverse a) confidentiality protection is more than just data security. In addition, there could be risks from incidents of harassment and other violations of privacy. 9. We also need to deal with conflicts between the metaverse and the rules of the real world. 10. Do a reasonable expectation of privacy and TOS co-extend? Even though fraud remains a possibility with VR, 11) Having so many additional metaverses being established, there will be an increased chance of online fraud will rise significantly. Because of this reason, flaws in new technologies like blockchain and metaverse will be targeted by cybercriminals in the future. They may find alternative ways for identity theft, creation, and "deepfakes". Protecting people from these new identity exploitations techniques will be a challenge for metaverse designers. In the metaverse, probably there is a need for visible or invisible virtual security guards - and virtual cops.

When we are sending personal information from one metaverse to another metaverse the risks may occur particularly by connecting with the data privacy. In this metaverse it allows risks for both the personal information as well as the purchased item agreement details. It was a very important note of metaverse because the directors or managers are conscious of the related privacy risks. For developing the metaverse some of the directors are worried about their financial activities which are against the law.

Under Article 20 sec the data adjustability and have ability to exchange data, in which the data subjects have a right to collect personal information. The worried people will be organized and used repeatedly with the help of the format that is readable by machines and have a right to distribute information to controller. Having adjustability and the ability to exchange or use data will be mostly required for the metaverse workers because that helps them collect information in the metaverse. It should help the users to change from the platforms, which leads to loss of value between the directors as to able to exchange data that can destroy the processed data value.

One of the major risks I found in this situation is adjustability therefore, a large quantity of information is sent in the metaverse. Recognizing the responsible parties will be vital to resolving who are accountable for data privacy, how the data breach circumstances are rejected, and what happens as a result of such circumstances. The data controllers and data processors duties are to differ from one power to another.

The market may view a data controller as to implement some appropriate measures to the privacy risk. In the conclusion, therefore the metaverse incorporates a similarity of the practical world to the actual world, where the importance of data security is accepting novel measurements and elevating new questions. In the metaverse, the privacy of information is worth noting to deal. In the metaverse, the customers may see an increase in cyber issues that are reciprocal to the increase in vulnerability. Since, this is not only a doubtful argument that can protest the development of metaverse. Here, blockchain technology is a new concept in which there will be naval ideas for the people who are losing money through agreements based on blockchain ecosystems. This will be applied to the metaverse because the risks must be suspended for the blockchain customers to take advantage of that new technology.

The Rise of metaverse, Facebook's Official name change to Meta in October 2021, that has brought about the new era of social networks and three-dimensional virtual worlds. Its main aim to provide user with immersive and personalized experiences by leveraging various technologies. To ensure the security for the Person' digital content and data within the metaverse that remains the crucial concern. Blockchain technology which emerges as promising solution due to its decentralized nature, immutability, and transparency. To gain with the comprehensive understanding of blockchain's role in the metaverse a thorough survey on its application that has been conducted.

The invention of the Meta since it is called as Facebook which it has the new trends in the networking and with the advancement of the virtual worlds usually called as metaverse. It usually aims to provide the user with the personalized experience with the cutting-edge technologies. The Security concerns with the user's digital information and the data within the metaverse is the crucial concern. Block chain technology which offers the promising solution, which is decentralized, and it is transparent in nature. For gaining the understanding of blockchain's role in the meta, survey which ensures the application that has been conducted (2).

The concept of metaverse which undergone with the significant evolution that strives to create dynamic and interactive environments that used to cater the various virtual experience and with the user interactions. This evolution which has given rise to metaverse platforms which utilizes the blockchain technology and non-fungible tokens which is to establish the ownership with the elements, and it enhances with the features and the information.

This paper which are intricate and diverse the nature of the information withing the platforms, and used to highlights the unique dynamics and the characteristics. This article which introduces with an innovate and the metaverse analysis tool that are developed by authors that with the harness in the machine learning techniques and used to collect and analysing the wide range of the information which includes the transaction of block chain, platform independent specific metadata and the social media trends. The outcomes of this approach which are presented through the compelling with the use case scenario which focuses on the digital parcels in trading that are called as metaverse real estate. This case which serves as the effective tool tries to demonstrate and results with the showcases of the immense potential of using machine learning to gain valuable insights into the metaverse ecosystem (3).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Letafati M, Otoum S. On the privacy and security for e-health services in the metaverse: an overview. *Ad Hoc Net.* (2023) 150(1):103262. doi: 10.1016/j.adhoc.2023.103262
2. Huynh-The, et al. Blockchain for the metaverse: a review. *Future Gener Comput Syst.* (2023) 143. doi: 10.1016/j.future.2023.02.008
3. Casale-Brunet S, Mattavelli M, Chiariglione L. Exploring blockchain-based metaverses: data collection and valuation of virtual lands using machine learning techniques. *Dig Bus.* (2023) 3(2). doi: 10.1016/j.digbus.2023.100068

Further Reading

4. Amiet N. Blockchain vulnerabilities in practice. *Digit Threats Res Pract.* (2021) 2(2):1–7. doi: 10.1145/3407230
5. Artzt M, Weingarden G. Metaverse and privacy. *Int In-House Counsel J.* (2022) 15(59):7763–70.
6. Chance C. *The Metaverse: What Are the Legal Implications?.* Clifford Chance (2022). Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-thelegal-implications.pdf
7. Goodwin. *Metaverse in China.* Goodwin (2022). Available at: https://www.goodwinlaw.com/publications/2022/05/05_11-metaverse-in-china
8. Morgan JP. *Opportunities in the Metaverse.* J. P. Morgan (2022). Available at: https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-themetaverse.pdf?mc_cid=0b22b34707&mc_eid=55476ebd9d
9. Richter T. *Handbook of Blockchain Law 222/223.* For Blockchain Technology (2020).
10. van der Laan J. *Dealing with Internet Mediated Securities Fraud.* (2008). doi: 10.2139/ssrn.4261431
11. Vatsa V. Dcoding identity in the metaverse. *The Decrypting Story.* (2022). Available at: https://yourstory.com/the-decrypting-story/decoding-identity-metaverse.
12. Chen Z, Wu J, Gan W, Qi Z. Metaverse security and privacy: an overview. *IEEE International Conference on Big Data (Big Data)* (2022).