Metaversalize

www.meta.reapress.com

Metaverse. Vol. 1, No. 4 (2024) 171–190.

Paper Type: Original Article

A Systematic Review of Metaverse Environment

Asif Zaman[1,*], Mushfiqur Rahman Abir[1], Tanjil Hasan Sakib[1], Asgor Hossain Reaj[1]

[1] Computer Science and Engineering, American International University, Bangladesh; zasif4805@gmail.com; mushfiqurrohomanabir@gmail.com; 98sakib@gmail.com; asgorreaj@gmail.com.

Citation:

Received: 15 June 2024 *Revised: 01 September 2024* *Accepted: 05 October 2024*	Zaman, A., Abir, M. R., Sakib, T. H., & Reaj, A. H. (2024). A systematic review of metaverse environment. *Metaversalize, 1*(4), 171-190.

Abstract

The rise of the metaverse, a blend of virtual and augmented realities, opens vast possibilities for social engagement, economic transactions, and digital innovation. However, establishing a reliable metaverse involves significant technical and ethical hurdles. From a technical perspective, creating the metaverse necessitates a robust infrastructure, including high-speed internet, advanced hardware, and scalable platforms capable of supporting many simultaneous users. Key challenges include ensuring interoperability among various systems and maintaining cybersecurity to protect user data and privacy. On the ethical front, the metaverse must tackle issues related to digital identity, inclusivity, and equitable access, striving to bridge digital divides and ensure the representation of diverse demographics. Furthermore, there is a need to develop measures to combat misinformation, harassment, and digital addiction, which requires robust governance frameworks. This paper delves into these complex challenges, advocating for a multi-stakeholder approach that brings together policymakers, technologists, and ethicists to establish comprehensive standards and regulations. By addressing both the technical and ethical aspects, the objective is to create a metaverse that is secure, inclusive, and advantageous for all users.

Keywords: Metaverse, Trust, Privacy, Security, Ethics.

1 | Introduction

We now inhabit a world that merges our natural surroundings with virtual spaces, creating a dynamic coexistence between the two worlds [1]. Education, communication, and daily activities increasingly integrate into this digital realm. The term "metaverse" is derived from "Meta," meaning beyond, and "Verse," signifying the universe. It represents a 3D virtual world where individuals can simultaneously exist in physical and digital spaces through avatars [2]. Often hailed as the next revolutionary step and the future of the internet, the metaverse concept isn't entirely new. Neil Stevenson first introduced it in his 1992 novel, Snow Crash [3].

Corresponding Author: zasif4805@gmail.com

https://doi.org/10.22105/metaverse.v1i1.17

The idea gained significant attention again with the film Ready Player One, which depicts a virtual world called "OASIS" where users can engage in various activities through customized avatars [4].

Today, the metaverse is a hot topic among researchers and investors, attracting substantial financial interest. For instance, metaverse Group, a real estate firm specializing in virtual properties, made headlines by purchasing digital land on the Decentraland platform for a staggering $2.43 million. This reflects the broader economic potential of the metaverse, with its revenue opportunities projected to increase from $500 billion to $800 billion between 2020 and 2024 [5]. In the gaming industry, platforms like Roblox, Fortnite, and Sandbox are thriving examples of the metaverse's rapid growth [6]. The concept gained even more mainstream attention following Mark Zuckerberg's announcement of Facebook's rebranding to Meta [7].

The surge in publications in recent years across various bibliographic databases using the keyword "metaverse" in their titles or abstracts, as depicted in *Fig. 1*, underscores this interest, showing Google trend's past 5 year's web search results on metaverse. A key aspect of the metaverse is its universal appeal—it transcends age groups and geographical boundaries, offering the potential to transform our world and add a new dimension to culture and everyday life. With this rapid expansion and enthusiasm, it is crucial to establish and uphold the trustworthiness of the metaverse and its applications to ensure user acceptance and trust [8].

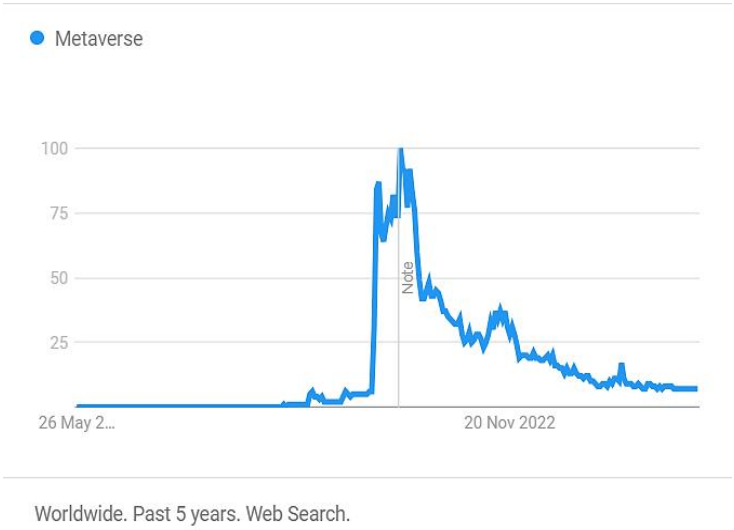

Fig. 1. Google trend's interest over time on metaverse in the last five years.

In today's digital landscape, users seek systems that provide a good user experience and efficiency and offer reliability without compromising privacy. Trustworthiness is essential to attract and retain user interest. For the metaverse, trustworthiness encompasses more than just ethical considerations; it includes various factors such as system fairness, robustness, data protection, system explainability, and operational transparency.

A comprehensive and informative study is needed to support investors and researchers in building a robust metaverse ecosystem. This study should cover the latest advancements, challenges, and strategies to enhance the trustworthiness of the metaverse, providing current, projected, and future insights. The present study delivers a detailed analysis and evaluation of the metaverse's current progress and obstacles, along with strategies to overcome these challenges and ensure the metaverse's reliability. Briefly, the main contributions of this paper are summarized as follows:

I. An introduction to metaverse, the number of articles published on metaverse over the year on different databases.

II. Discussion about the progression of metaverse over the years with its architecture, advancement, and opportunities.

III. Different types of challenges of metaverse with a taxonomy are divided into three sectors: technical dependencies, Artificial Intelligence (AI) techniques, and ethical challenges.

IV. Factors of trustworthiness of metaverse and how to make metaverse trustworthy with a taxonomy.

V. Future research opportunities for making the metaverse ecosystem more trustworthy.

The rest of the paper is structured as follows. Section 2 highlights the history, architecture, advancements, and opportunities of the metaverse. Section 3 addresses the challenges of the metaverse from different perspectives. Section 4 combines the concept of Trustworthy Artificial Intelligence (TAI) with the metaverse, highlighting the factors of trustworthiness and creating a trustworthy metaverse environment. Section 5 discusses future research opportunities, and Section 6 concludes the paper.

2 | Metaverse Environment

The metaverse, originating from the combination of "transcendence meta" and "universe," describes a networked virtual 3D environment where real and virtual worlds intersect, fostering fully immersive experiences and collaborative activities [9]. Initially focused on the structure of virtual worlds, the metaverse has evolved into a platform centered on social interactions and content sharing.

The concept of the metaverse has been in development since 1838, when Verhoeff first described the binocular vision [10]. The term "metaverse" was coined by Neil Stevenson in 1992, referring to a virtual duplicate of the real world. The idea gained wider public attention with the 1999 science fiction movie "The Matrix" [11]. The introduction of virtual currency was a significant milestone for the metaverse, with There Bucks, an online currency, debuting in 2003 [12]. This was followed by Roblox's creation of an online gaming platform in 2004, marking another step towards the metaverse [13].

The concept took on new dimensions with technological advancements like Google's Cardboard device and Google AR Glass in 2014 [14]. In 2015, the Ethereum Blockchain and Decentraland established a pioneering virtual environment, further cementing the metaverse's foundations [15]. The introduction of devices like Oculus, Pokémon Go, and Microsoft HoloLens in 2016 significantly enhanced the metaverse user experience.

In 2021, Facebook rebranded to Meta, signaling a significant commitment to metaverse development [7]. The metaverse continued to expand in 2022 with the Benetton group's retail project "Stepping into the metaverse" [16]. Apple's announcement of the "Apple Vision Pro" release date in 2023 promises to further revolutionize the metaverse experience, paving new pathways for its growth and development [17].

2.1 | Fundamental Technologies

The metaverse describes a collective virtual shared space where individuals can interact seamlessly and interconnectedly with each other and digital objects. Various technologies and dependencies are crucial to achieving such a complex virtual environment.

These technologies create a multifaceted architecture that forms the foundation of the metaverse and its diverse functionalities. The metaverse represents the convergence of various cutting-edge technologies, each creating a seamless, immersive, and interconnected virtual world. The metaverse's potential will likely expand as technology advances, leading to novel experiences and opportunities across numerous industries and aspects of our lives.

Web3.0, the next generation of the Internet, is a fundamental dependency for the metaverse. It facilitates decentralized applications and smart contracts that enable trustless interactions and secure transactions of digital assets within the virtual world [24].

Finally, Extended Reality (XR) technologies, encompassing Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), allow users to immerse themselves in the virtual environment, interact with digital objects, and experience a blended mix of the real and digital world within the metaverse [25].

AI enhances user experiences by personalizing content, creating lifelike avatars, providing real-time translations, optimizing content delivery, and generating dynamic environments based on user preferences and behavior [18], [19].

Blockchain technology ensures transparency, immutability, and security within the metaverse, enabling virtual economies, managing digital assets, and establishing ownership rights over virtual goods through Non-Fungible Tokens (NFTs) [20], [21].

Big Data technologies are essential for processing and analyzing the vast amounts of data generated by user interactions, virtual environments, and economic activities, improving user experiences and system performance [22].

The upcoming 6G wireless communication technology is pivotal for the metaverse. It will enable seamless real-time communication, reduced latency, and enhanced interactions between users and devices within the virtual environment [23].

2.2 | Innovations

The metaverse is a game-changing idea that is gaining traction quickly and offering businesses and investors alike great options. Offering a shared VR environment for user creation and interaction, it has enormous promise in various businesses. Prominent corporations are investing significantly in initiatives connected to the metaverse, intensifying the competition to profit from this new frontier. The metaverse offers a bright future for creative endeavors in everything from virtual real estate to gaming, education, and more.

Big businesses are aggressively embracing the metaverse's potential because they see it as the internet's "next chapter" and a huge opportunity for a number of different sectors. For example, in October 2021, Facebook, the largest social media platform globally, underwent a major transformation by changing its name to Meta, indicating its dedication to the metaverse [7]. The business disclosed intentions to devote a sizeable $10 billion to the metaverse project [26].

According to renowned research and advisory firm Gartner, one of the top five emerging trends and technologies for 2022 is the metaverse [27]. Due to increased awareness, there has been a significant increase in investment; global spending on VR/AR, the core technologies of the metaverse, is expected to increase from $12 billion in 2020 to $72.8 billion in 2024. As a result, sectors including Blockchain, gaming, retail, the arts, and healthcare are setting themselves up to be key players in this developing ecosystem. 3D AR advertising is expected to spread across social media platforms as user involvement in virtual places rises [28].

Companies from various industries are investing heavily in metaverses as they realize how useful they can be for leisure and business purposes. Metaverse-like elements are being incorporated into gaming platforms to allow for virtual concerts and other interactive events. People are even purchasing virtual real estate in the metaverse, demonstrating its rising popularity and proving that this technology is here to stay. But in October 2022, the well-known VR platform Decentraland suffered a blow when it revealed that monthly active users had dropped significantly from earlier months [29]. Some have concluded that the metaverse market is still not entirely stabilized due to this downturn. Notwithstanding these obstacles, the metaverse's general trajectory points to a future of sustained innovation and expansion, propelled by large investments and breakthroughs in a variety of technology fields.

2.3 | Opportunities

The metaverse represents a realm of boundless opportunities poised to revolutionize our lives. It seamlessly merges AR, VR, and the internet, unveiling endless possibilities from virtual shopping and entertainment to social networking and education. This section explores the remarkable potential of the metaverse, highlighting its capacity to reshape industries, foster creativity, and deepen human connections.

The metaverse offers a plethora of opportunities across various domains. Firstly, in terms of accessibility, it can promote inclusivity by providing accessible experiences for individuals with disabilities and bridging the digital divide. Secondly, it delivers unparalleled immersive experiences such as gaming, VR, and entertainment, crafting virtual worlds with high engagement, interactive storytelling, and realistic simulations [30]. Moreover, the metaverse facilitates social interaction through avatars, gamification, and social guidance, fostering well-

being and mental health support [31]. In education and training, XR technologies and gamification can revolutionize learning into an enjoyable and immersive experience [32], [33]. Healthcare benefits from real-time collaboration among scientists and professionals and virtual testing through Digital Twins (DTs) technology [34]. For architecture and design, virtual prototyping and collaborative design become feasible [35]. The metaverse also unlocks opportunities in the digital economy, with community-owned economies and social tokens offering incentives and connections for participants [36]. However, ensuring cybersecurity, privacy, and legal compliance remains critical, alongside considerations for environmental impact and sustainability benefits such as reducing carbon emissions and e-waste [37].

3 | Metaverse Environment Challenges

The metaverse represents a promising future where individuals can engage in immersive virtual environments. However, achieving this vision requires overcoming multiple challenges. We have divided these challenges into three categories, represented in *Fig. 2*.

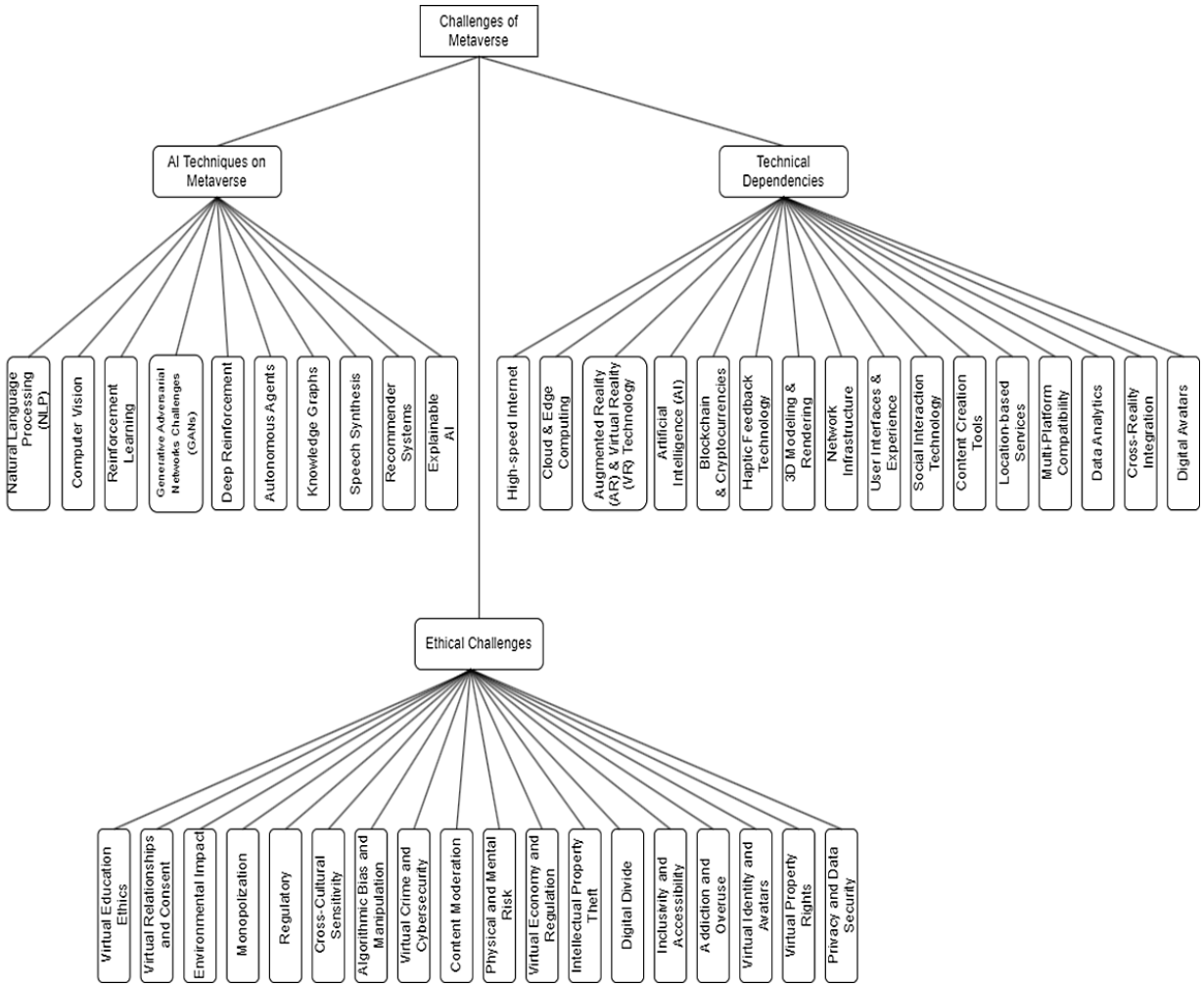

Fig. 2. Metaverse technical and ethical challenges.

Furthermore, the following tables offer a structured and standardized overview of the challenges the metaverse faces, providing a comprehensive understanding of the technical, AI-related, trust, and ethical obstacles that must be navigated to create a successful and sustainable metaverse.

3.1 | Technical Dependencies

As the metaverse grows, it relies on various technical dependencies to run smoothly and efficiently. These dependencies cover many technologies, from high-speed internet and cloud computing to AI and Blockchain.

These technical elements are key in enabling the features and experiences that define the metaverse. However, addressing the challenges associated with these dependencies is essential to ensuring a secure, accessible, and user-friendly metaverse environment. In this context, understanding and optimizing these technical dependencies is key to unlocking the full potential of the metaverse and creating a connected digital world for users worldwide.

Table 1 presents an overview of the challenges associated with the technical dependencies on the metaverse. The metaverse, a virtual shared space, relies on various technologies to function effectively. High-speed internet is crucial for seamless communication, collaboration, and gaming experiences, but global accessibility and infrastructure development pose significant challenges. Cloud and edge computing are essential for storage and processing power in virtual worlds, but data privacy and latency issues must be addressed. AR and VR technology enable immersive simulations and training, but motion sickness and content creation remain concerns.

AI provides Non-Player Characters (NPCs) and personalized experiences, yet ethical considerations and algorithm bias demand attention. Blockchain and cryptocurrencies facilitate virtual asset ownership but encounter scalability and energy consumption challenges. Haptic feedback technology enhances sensory experiences but requires complex integration and cost considerations. Other challenges include 3D modeling, network infrastructure, user interfaces, social interaction technology, content creation tools, location-based services, multi-platform compatibility, data analytics, cross-reality integration, and digital avatars, all of which need to be addressed for the metaverse's successful development and widespread adoption.

Table 1. Challenges of the technical dependencies on metaverse.

Dependencies	Applications	Fields	Challenges
High-speed Internet	Virtual meetings and conferences, real-time collaboration, online gaming	Communication, collaboration, entertainment	Global accessibility, infrastructure development, net neutrality
Cloud and edge computing	Storage, processing power, and scalability for virtual worlds and experiences	Infrastructure, content delivery	Data privacy and security, latency issues
AR and VR technology	Immersive simulations, training, virtual tourism remote	Training and education, tourism, entertainment	Motion sickness, hardware affordability, content creation
AI	NPCs for dynamic virtual environments, personalized experiences	Gaming, simulation	Ethical considerations, algorithm bias
Blockchain and cryptocurrencies	Virtual asset ownership, secure transactions, digital identities	Digital, finance, ownership	Scalability, energy consumption
Haptic feedback technology	Enhanced sensory experiences and touch interactions in virtual environments	Gaming, medical, design	Complex integration, cost, and compatibility
3D modeling and rendering	Creation of virtual objects, environments, and avatars	Design, gaming, entertainment	High-fidelity graphics, rendering, speed
Network infrastructure	Seamless cross-platform interactions, low-latency interactions	Technology, communication	Bandwidth limitations, synchronization issues
User interfaces and experience	Intuitive navigation and interaction in virtual worlds	Design, human computer interaction	Standardization, accessibility
Social interaction technology	Virtual social platforms, avatar interactions	Social media, human behavior	Ensuring privacy, preventing virtual harassment

Table 1. Continued.

Dependencies	Applications	Fields	Challenges
Content creation tools	Virtual content development, creative tools	Design, entertainment	User-friendly interfaces, content ownership
Location-based services	Geospatially tied experiences, virtual tourism	Tourism, navigation	Data privacy, accurate geolocation
Multi-platform compatibility	Cross-platform interactions, seamless experiences	Technology, communication	Standardization, device compatibility
Data analytics	User behavior analysis, virtual environment optimization	Analytics, virtual worlds	Data privacy, data accuracy
Cross-reality integration	Blending virtual and real-world experiences	MR, gaming	Real-time synchronization, user immersion
Digital avatars	Personalized virtual representations of users	Social media, identity	Avatar customization, realistic movements

3.2|AI Techniques Challenges

AI techniques play a key role in the world of metaverse. AI makes the metaverse possible through intelligent NPCs, voice assistants, realistic avatars, and personalized experiences. However, with the integration of AI come several unique challenges that need to be carefully addressed. Understanding and managing AI techniques on the metaverse is essential to responsibly and ethically harnessing AI's potential, helping to create a truly transformative and inclusive digital realm for users worldwide.

Table 2 outlines the challenges various AI techniques face in the metaverse context. Several AI techniques, such as Computer Vision, Natural Language Processing (NLP), Generative Adversarial Networks (GANs), Deep Reinforcement Learning, Autonomous Agents, Knowledge Graphs, Speech Synthesis, Recommender Systems, and Explainable AI, are discussed along with their respective applications and fields of use. For NLP, concerns center around privacy and language understanding for voice assistants and virtual characters in virtual assistants and gaming. In Computer Vision, issues arise with privacy, the uncanny valley, and ethical considerations for realistic avatars and object recognition [38] in VR/AR and social media. Reinforcement Learning poses challenges regarding training complexity and reward design for AI-controlled NPCs and adaptive gameplay in gaming and virtual worlds. GANs face realism, training data, and intellectual property obstacles when generating photorealistic environments and art creation in virtual environments and creativity.

Deep Reinforcement Learning encounters difficulties in NLP, Computer Vision, and Reinforcement Learning in training complexity, balancing, and generalization for intelligent NPCs and game design optimization in gaming and virtual worlds. Autonomous Agents must tackle behavior complexity and realism concerns to achieve realistic NPCs in gaming and virtual worlds. Knowledge Graphs must address data integration and domain-specific challenges for semantic web and contextual understanding in information retrieval. Speech Synthesis faces the challenge of naturalness and voice diversity when creating realistic voices for virtual characters in voice assistants and gaming. Recommender Systems confront privacy and the filter bubble while providing personalized content and experience in content recommendation. Lastly, Explainable AI requires interpretable models and user trust to understand AI decision-making processes, addressing concerns related to AI transparency and ethics [39]. These challenges collectively shape the development and application of AI in the metaverse.

Table 2. Challenges of the AI techniques on metaverse.

AI Techniques	Applications	Fields	Challenges
NLP	Voice assistants, virtual characters	Virtual assistants, gaming	Privacy concerns, language understanding
Computer vision	Realistic avatars, object recognition	VR/AR, social media	Privacy, uncanny valley, ethics
Reinforcement learning	AI-controlled NPCs, adaptive gameplay	Gaming, virtual worlds	Training complexity, reward design
GANs	Photorealistic environments, art creation	Virtual environments, creativity	Realism, training data, intellectual property
Deep reinforcement learning	Intelligent NPCs, game design optimization	Gaming, virtual worlds	Training complexity, balancing, generalization
Autonomous agents	Realistic NPCs	Gaming, virtual worlds	Behavior complexity, realism
Knowledge graphs	Semantic web, contextual understanding	Information retrieval	Data integration, domain-specific challenges
Speech synthesis	Realistic voice for virtual characters	Voice assistants, gaming	Naturalness, voice diversity
Recommender systems	Personalized content and experience	Content recommendation	Privacy, filter bubble
Explainable AI	Understanding AI decision-making processes	AI transparency, ethics	Interpretable models, user trust

3.3 | Ethical Challenges

The metaverse blurs the lines between the physical and digital realms, raising complex questions about privacy, data security, virtual property rights, and digital identity, among others. Additionally, concerns surrounding addiction and overuse, inclusivity and accessibility, as well as the digital divide, have garnered significant attention in ensuring equitable participation within this virtual landscape. *Table 3* outlines the importance of acknowledging and navigating these ethical challenges to ensure a trustworthy and beneficial metaverse ecosystem for all participants.

By addressing these dilemmas, stakeholders can foster a metaverse that promotes user well-being, privacy, inclusivity, and responsible technological advancements. As the metaverse evolves, ongoing discussions, collaboration, and ethical guidelines will be crucial in shaping its future development. The following discussion of some of the most important ethical challenges is given.

I. Privacy and data security: This challenge concerns protecting users' personal data and ensuring robust data security within VR platforms. This includes protecting sensitive information from unauthorized access and possible misuse. VR platforms are applications, and the relevant areas to address this challenge are technology and data management.

II. Virtual property rights: This challenge defines the ownership and rights associated with virtual assets and copyrights. This includes ensuring fair remuneration for creators and preventing unauthorized use or theft of virtual property. The applications include all kinds of virtual property and digital devices.

III. Virtual identities and avatars: This addresses issues related to virtual identities and avatars on social VR platforms. This challenge includes concerns about identity representation, online anonymity, and potential risks of identity deception. The applications include social VR platforms, and the domain of interest is social media and virtual identity.

Table 3. Ethical challenges of the metaverse.

Ethical Challenges	Applications	Fields
Privacy and data security	VR platforms	Technology, data management
Virtual property rights	Protection of virtual asset ownership and copyright	Gaming, digital assets
Virtual identity and avatars	Social VR platforms	Social media, virtual identity
Addiction and overuse	VR and AR entertainment	Psychology, healthcare
Inclusivity and accessibility	MR applications	Education, assistive technology
Digital divide	Metaverse in developing regions	Economics, global development
Intellectual property theft	3D modeling and assets, digital art and creations	Copyright law, creative arts
Virtual economy and regulation	Cryptocurrencies in the metaverse	Finance, governance
Physical and mental risk	VR sports, therapy, combat simulations	Health, safety, psychology
Content moderation	User-generated metaverse content	Community management, ethics
Virtual crime and cybersecurity	Metaverse marketplaces, virtual property, and asset	Cybersecurity, virtual law
Algorithmic bias and manipulation	AI-driven metaverse systems	AI, ethics
Cross-cultural sensitivity	Social and educational metaverse	Diversity and inclusion, cultural studies
Regulatory challenges	Metaverse governance bodies	Policy, legal studies
Monopolization	Metaverse infrastructure	Economics, technology
Environmental impact	Virtual worlds and climate change	Sustainability, environmental studies
Virtual relationships and consent	VR dating and intimacy apps	Ethics, human-computer interaction
Virtual education ethics	Online learning platforms	Education, pedagogy

IV. Addiction and overuse: This challenge focuses on the potential addictive behaviors and mental health consequences of the overuse of VR and AR entertainment devices. It also includes understanding and addressing the impact of immersive experiences on users' well-being. The applications include VR and AR entertainment, and the areas of interest are psychology and health.

V. Inclusivity and accessibility: This challenge is about ensuring that MR applications are accessible to all users, regardless of their abilities or backgrounds. Virtual experiences must be designed to be inclusive and adaptable for different users. The applications include MR applications, and the areas concerned are education and assistive technology.

VI. Digital divide: The digital divide addresses the inequalities in access to the meta-perspective in developing regions and its impact on global development and economy. This challenge relates to bridging the gap and ensuring equitable opportunities for participation in the metaspace. Applications include metaverse in developing regions, and the relevant fields are economics and global development.

VII. Intellectual property theft: This challenge relates to copyright and intellectual property concerns related to 3D modeling, virtual tools, digital art, and creations. It involves protecting the rights of creators and preventing unauthorized use or copying of digital works. The applications include 3D modeling and virtual tools, and the area covered is copyright and creative works.

VIII. Virtual economy and regulation: This addresses the use of cryptocurrencies in the metaverse and the development of a governance framework for virtual economies. This challenge involves addressing digital currencies' financial and regulatory aspects in virtual environments. The applications include cryptocurrencies in the metaverse, and the domains concerned are finance and governance.

IX. Physical and mental risks: Physical and mental risks are related to managing risks to the physical and mental well-being of users in VR sports, therapy, and combat simulations. This challenge involves ensuring safety protocols and psychological well-being in immersive experiences. Applications include VR sports, therapies, and combat simulations, and the domains concerned are health, safety, and psychology.

X. Content moderation: This challenge focuses on managing user-generated content in the metaverse and ensuring ethical community management. It involves implementing of policies to prevent harmful or offensive content. Applications contain user-generated metaverse content, and the relevant domains are community management and ethics.

XI. Virtual crime and cybersecurity: This addresses cybersecurity challenges in metaverse marketplaces, virtual property and assets, and the creation of virtual law. This challenge is to protect users and digital assets from cyber threats in virtual environments. The applications include metaverse marketplaces; the areas covered are cybersecurity and virtual law.

XII. Algorithmic bias and manipulation: This challenge deals with bias in AI-driven metaverse systems and the ethical implications of algorithmic decision-making. The applications include AI-driven metaverse systems, and the domain of interest is AI and ethics.

XIII. Cross-cultural sensitivity: Cross-cultural sensitivity promotes diversity and inclusion in the social and educational metaverse while being culturally sensitive. This challenge includes avoiding cultural biases and stereotypes in virtual experiences. Applications include the social and educational metaverse, and relevant areas include diversity and inclusion and cultural studies.

XIV. Regulatory challenges: Establishing governance bodies to address policy and legal issues related to meta-perspectives. This challenge includes developing regulatory frameworks to ensure responsible and accountable metaverse operations. Applications include metaverse governing bodies; the relevant fields are policy and legal studies.

XV. Monopolization: Examining the economic consequences of monopolization in the metaverse infrastructure. The challenge is to prevent disproportionate control over the operation of the metaverse by certain entities. The applications include metaverse infrastructure, and the relevant fields are economics and technology.

XVI. Environmental impact: Assessing the sustainability and environmental consequences of virtual worlds in the context of climate change. This challenge is to promote environmentally friendly practices within the metaverse. Applications include virtual worlds and climate change; the relevant domains are sustainability and environmental science.

XVII. Virtual relationships and consent: Addressing ethical considerations in VR dating and intimacy applications for human-computer interaction. This challenge is related to ensuring respectful and consensual interactions within virtual relationships. The applications include VR dating and intimacy applications, and the domain of interest is ethics and human-computer interaction.

XVIII. Ethics in virtual education: Ensuring ethical practices in online learning platforms and addressing pedagogical concerns. This challenge concerns the promotion of fair and effective virtual education methods. The applications include online learning platforms; the domain concerned is education and pedagogy.

The metaverse poses complex ethical challenges, including privacy, data security, inclusion, intellectual property, etc. While *Table 3* outlines some of the key concerns, it is vital to recognize that the evolution of this digital environment requires continued research and collaboration. Addressing these challenges will help to foster a responsible and user-centric metaverse and shape a thriving and inclusive virtual world for the future. Continued dialogue and vigilance are essential to navigate the dynamic ethical considerations of this evolving space.

4 | Trustworthy Artificial Intelligence (TAI) in the Metaverse

In recent years, the extensive adoption of AI technologies has revolutionized various industries, including healthcare, finance, transportation, and entertainment. While AI systems become more prevalent, there is a growing need for transparency and accountability in making decisions [40]. This has led to the emergence of Trustworthy Artificial Intelligence (TAI) as a crucial field of research. TAI aims to address these concerns by providing human-readable explanations for the predictions and actions of AI models. Both technical advancements and societal demands have driven the progress in TAI. On the technical side, researchers have made significant strides in developing methods that help understand complex AI models, which are often seen as black boxes. These methods enable extracting meaningful insights from AI systems, such as the importance of features, decision rules, or causal relationships. Furthermore, societal demands for transparency have played a role in advancing TAI research. As AI systems significantly impact critical domains like healthcare diagnosis, autonomous vehicles, and legal decision-making, ensuring fairness, accountability, and ethical use of AI is crucial. Transparent AI models allow stakeholders to comprehend the underlying reasoning behind the outcomes generated by AI, fostering trust, mitigating biases, and enabling effective collaboration between humans and AI.

4.1 | Factors of Trustworthiness in the Metaverse: Perspective on Machine Learning Models

In the information technology sector, continuous adaptation is crucial for outperforming competitors, and independent systems form the foundation for most IT firms. However, due to machine learning models' unique characteristics, traditional quality assurance and testing techniques may not be sufficient. This section discusses the challenges of ensuring trustworthiness in machine learning models and emphasizes the importance of transparency and openness in gaining market trust.

4.1.1 | Fixing machine learning models

Fixing machine learning models is more complex and less controllable compared to traditional software development. Often, ineffective model performance can be attributed to inappropriate hyperparameter values chosen during development, which may not suit the end users' requirements. Consequently, users of machine learning models must decide whether to utilize the existing model or invest in developing their own.

4.1.2 | Adaptability in machine learning models

Unlike conventional software, machine learning models' functionality is derived from data, making applying standard coding and debugging practices difficult. The learning process involves using algorithms to create accurate models capable of generalizing to unseen data. Since machine learning is based on estimation, achieving precise results is challenging, leading to the need for continuous iteration and improvement.

4.1.3 | Transparency in machine learning models

Trust in machine learning models developed by others hinges on increased visibility and openness. Model consumers should carefully consider the level of transparency a model offers before relying on it for critical applications. Transparency concerns in machine learning models encompass various unknowns, which must be addressed to establish trust [41].

Ensuring trustworthiness in machine learning models is crucial for their successful integration into the metaverse and other applications. The challenges of adaptability and bug fixes, combined with the need for transparency and openness, must be addressed to enhance model visibility and establish market trust in these powerful AI-driven systems [42].

4.1.4 | Trustworthy ai in the metaverse: the concept of transparency and pitfalls

Companies have increasingly promoted AI in the metaverse as a solution that can replace human intelligence and deliver superior results. However, this marketing narrative often obscures the reality that simple data analysis conducted by human analysts is still a crucial component of these AI solutions. Using metaphors and simplifications to present AI as a fully autonomous and self-operating system conceals the significant involvement of human labor in the development and functioning of AI technologies. Thus, there is a need for highlighting transparency.

4.1.5 | Lack of transparency and misleading representations

Many technology companies rely on abstract and overly simplified representations of AI products, omitting crucial details about the underlying technology and misrepresenting the essence of the product. This lack of transparency contributes to the opaqueness of machine learning algorithms, making it challenging for users to understand how these systems influence decision-making processes [43]. Convolutional storytelling in marketing and deceptive user interfaces further adds to the complexity of understanding AI systems.

4.1.6 | Trust issues of the metaverse

As AI becomes integral to the metaverse, ensuring trust and security in these virtual networks is paramount. Metaverse networks must incorporate constant awareness and visibility and robust security measures such as strong passwords, multi-factor authentication, advanced firewalls, and threat detection technologies [44]. Encryption must also be employed for data in transit and at rest to protect against potential attacks, such as phishing, malware URLs, and other online threats.

One critical aspect of trust in the metaverse is accurately identifying individuals and organizations. Blockchain-based identity verification technologies offer a promising solution, but their decentralized nature poses potential weaknesses, as illustrated by previous fraud incidents involving NFTs [41]. The deployment of biometric technologies, such as fingerprint or face recognition, should also be considered to bolster identity verification.

The trustworthiness of the metaverse requires transparent communication about the human labor involved in AI solutions and the underlying technology. Ensuring security in virtual networks demands constant awareness and robust cybersecurity measures.

Furthermore, identity verification technologies, whether blockchain-based or biometric, must be carefully implemented to foster a sense of trust and confidence in the metaverse.

4.1.7 | Building trusted metaverse

The metaverse is a topic that many people question whether it is a disturbing or soft trend. There are many unanswered questions, including what it will look like, how it will affect us, and how it will fit into our everyday lives. According to the metaverse notion, physical barriers will no longer hinder our ability to interact with people and businesses and consume information. By using cutting-edge digital tools, we are exposing ourselves to a world that will know no bounds. The privacy and cybersecurity issues with the metaverse are among the most important for many people. As we enter this new era of digital exploration, it is crucial to set up this virtual world of interaction with safe concepts, dependable principles, and privacy-based technology. We have much work ahead of us to lay out the fundamentals of how the actual world will interact with this virtual future.

Metaverse has countless positive impacts on people's life, society, and culture and will increase in the future. People are diving into metaverse and using it personally and professionally, including sectors like medicine,

education, marketing, gaming, etc. However, these systems also carry equally huge risks and can impact negatively [45]. As the web evolved, it faced challenges from bad actors and vulnerabilities. With the emergence of the metaverse we must reimagine definitions, rights, and rules. Legal frameworks and security considerations need to be addressed to ensure trust and prevent excessive regulation [46]. Safeguarding sensitive data and privacy protection are crucial in the metaverse, especially considering potential early adoption by young users. Data privacy and its impact on this new digital realm must be given attention. To make the metaverse system trustworthy, the given steps can be followed:

Step 1 (Fulfilling human rights). First, the metaverse system must respect and preserve all the fundamentals of human rights [47]. For example, providing someone with any facility should not destroy others' fundamental rights, and a proper monitoring system should respect everyone's fundamental human rights.

Step 2 (Monitoring team). There should be a proper system between the user and the virtual world so that the user can quickly solve any problem in the virtual world. The system should also track all users to catch unexpected circumstances quickly [47]. Additionally, it should monitor user activity and alert them if somebody is using the metaverse system too much by ignoring their real-world responsibilities.

Step 3 (Robustness and safety). Like all AI-driven systems, metaverse must also be robust in handling undesirable and unexpected situations to reduce security risks and gain user trust in system performance. Furthermore, metaverse should be resilient to any attack as it is also vulnerable to being attacked by adversaries [49]. If the system is attacked, it may work differently or produce unwanted results. To overcome this situation, different techniques must be used while developing the metaverse system.

There should also be a fallback option to reduce any chance of an accident, and the system must work so that it does not hurt the user. To solve the problem, the metaverse system must be developed accurately enough to make correct decisions and simultaneously have a variety of alternatives to overcome any undesirable scenario. This is decisive at times and in circumstances where human lives are perilous. Moreover, metaverse should be reliable, work in different conditions, and produce the same output when repeatedly performed under the same inputs.

Step 4 (Privacy and data protection). Providing security and protecting users' data is one of the most critical parts of the metaverse system. To use the system, the user might need to provide their personal information to the system. These data are essential for the system to provide the correct and desired output [50]. Hence, the metaverse system must permanently preserve the security of the data supplied by the user and the user's personal information. The system must not misuse it in any way, and there should be specific rules and regulations regarding accessing users' data [51]. However, the system must be trained to detect unwanted data and reject any malicious data to make the system more efficient. At the same time, using Blockchain technology can be the most effective solution for resolving security issues. Metaverse will require real-world rules to safeguard users against abuse, fraud, and loss if it is to remain a viable location to live and conduct business. Global regulation is hard to implement and requires time. However, metaverse creators can take proactive measures to develop their meta-code of behavior. Regulators and the designers of these virtual environments should start collaborating right now if the metaverse is to be genuinely sustainable.

The concern about voice and content going to external third-party SaaS providers is valid for enterprises considering adopting metaverse solutions. Many metaverse platforms rely on cloud-based hosting and third-party services for voice and content management, which can raise concerns about data privacy, security, and ownership. To address these concerns, metaverse providers can take several steps:

I. Provide clear data security and privacy policies: Metaverse providers should clearly articulate how they will handle user data, including voice and content, and measures to protect user privacy and security.

II. Offer on-premise or self-hosted options: Metaverse providers can offer on-premise or self-hosted options for enterprises particularly sensitive to data privacy and security, allowing organizations to retain complete control over their data.

III. Enable end-to-end encryption: Metaverse providers can implement end-to-end encryption for voice and content, ensuring that data is protected from interception and unauthorized access.

IV. Ensure data ownership: Metaverse providers should ensure that users retain ownership of their data and that clear policies are in place for how user data will be handled in the event of a service termination.

By taking these steps, metaverse providers can help alleviate the concerns of enterprises and make their solutions more attractive to organizations that are hesitant to adopt metaverse technologies due to data privacy and security concerns.

Step 5 (User friendly). The metaverse system also needs to be user-friendly so that anyone can easily use it, as some users might not have any technological knowledge. Therefore, all the processes in the metaverse system must also be simple and secure. For example, continuous authentication will be required when identifying a user. According to Frank Dickson, programmed vice-president for security and trust at research company IDC, "metaverse will need to be more than simply multifactor authentication since it is intended to be an immersive experience." Users will not want to pause, get out their phone, and enter a six-digit code if they are in the metaverse. Therefore, this authentication should be as frictionless and unnoticeable as it can be without compromising security. Additionally, if the metaverse system does not offer a user-friendly environment, it will be challenging to retain the attention of its current users and attract new ones. To prevent scenarios like these, the metaverse ecosystem should be as simple as possible and conceal any complexity from the consumers' point of view.

Step 6 (Transparency in metaverse). Whenever the metaverse system decides, there must always be a justification. It is vital to analyze a specific choice the AI system made in certain circumstances. To achieve this, the user should be able to inspect the system's surroundings. Moreover, if the system is transparent and visible to the user, it will be easier for them to trust metaverse. It is also necessary for the user to know how the system interacts with them and on which basis the system produces the output.

Step 7 (Fairness). The metaverse should be designed and implemented so that the system does not behave in a biased manner or provide any biased result. If the decision-making of metaverse is not fair, then a user might get the wrong information and miss leads in day-to-day life [52]. For example, while producing any output, the metaverse algorithm should not be biased in any particular factor and treat all the factors equally. Otherwise, there is a significant chance that users will face big trouble in their virtual world.

Step 8 (Social effect). Environmentally responsible design, development, and usage methods must be followed while creating a metaverse system. For instance, the metaverse energy must be monitored and kept within predetermined ranges. In terms of entertainment, employment, or social life, metaverse technologies can both improve and harm our social life [53]. The metaverse has physical and mental repercussions that harm our social lives. To mitigate this, the metaverse mechanisms must be regularly observed and monitored. It should also be remembered to abide by social norms and regulations and to keep sensitive social information private.

Step 9 (Monetizing and updating). The metaverse system should be appropriately monetized and updated regularly to stay current. Because technology is constantly evolving, it is crucial to monetize the system and maintain it updated to ensure that metaverse will act as expected in every phase of its life cycle. In addition, users' needs and interests vary over time. Therefore, adding new features and functionality to the system is crucial to keep things moving smoothly and reassure users that metaverse will be around for a long time.

Step 10 (Maintaining ethical perspective). For users to trust the entire metaverse process and use it in their everyday lives, metaverse must be ideal from both a technological, functional, and ethical standpoint [54]. Local governmental and international ethical standards and regulations should be integrated into metaverse's overall system and structures. If they do not adhere, metaverse risks losing users' credibility and acceptance.

Step 11 (Moderating content). By enabling new types of interactions and bringing conventional in-person experiences online, marketers can form stronger connections in the immersive metaverse. Although many promising possibilities exist, it creates new opportunities for harmful conduct. Given the high level of digital hazards, particularly for weaker groups, the metaverse environment may see an increase in safety worries. As individuals engage, agile content moderation will be essential. In a place without borders like the metaverse, businesses will have a lot more work to implement best practices because content management is usually driven top-down by regulators based on regional laws and norms. Laws and norms in this area have to be updated. Companies wishing to enter the metaverse should do so with a content moderation partner they can rely upon, as this is a rapidly evolving environment, and the pace will probably only get up [55].

Step 12 (Detecting fraud). Many platforms in this new metaverse ecosystem could let consumers buy digital assets. For instance, companies like Nike and Disney have previously developed NFTs that are unique virtual assets. Therefore, it is crucial to ensure that consumers buy such assets safely and maintain the security of their digital belongings in this new environment. As a result, customers will also need to make their payments online, which creates serious concerns about the security of online transactions. With its built-in security characteristics that forbid altering transaction records, Blockchain technology holds promise as a potential solution. Because of its resilience against cyberattacks, it is a strong contender for reducing fraud. However, companies will still be on the hook for having robust fraud detection protocols in place. Maintaining marketplace security requires combining human teams and AI-powered detection systems. Finding ways to incentivize better behaviors and reward positive interactions could play a more prominent role in gaining users' trust.

Step 13 (Overcoming cyber-syndrome). There is a significant possibility that people will have cybersickness as digital platforms and the metaverse are increasing daily. As a result, a user using metaverse might face new types of problems. The system should be created so that the user will be continuously informed about their usage time and mental and physical status through the system to prevent this scenario and give the user trust in the metaverse. When a user reaches a particular threshold, a system should be in place to prevent them from accessing metaverse. The system should not additionally put consumers in situations that endanger their health. Based on their preferences, age, and state of health, various user categories should have different workspaces.

Step 14 (General data protection regulation). Managing General Data Protection Regulation (GDPR) [56], compliances and regulations in the metaverse ecosystem will be complex. Metaverse platforms and applications will likely collect and process large amounts of personal data, including user behavior, preferences, and interactions. As such, they must comply with various data protection regulations, including GDPR, to ensure user data is collected, processed, and stored securely and transparently. Here are some ways that GDPR, compliances, and regulations can be managed in the metaverse ecosystem:

I. Implement privacy by design: Metaverse providers should implement privacy by design principles from the outset, ensuring that data protection considerations are embedded into every platform design and development aspect.

II. Provide transparency: Metaverse providers should be transparent about how they collect and use user data, providing clear and concise privacy notices that explain what data is collected, how it is used, and whom it is shared with.

III. Obtain user consent: Metaverse providers should obtain user consent before collecting and processing personal data and provide users with a clear and easy-to-understand mechanism for withdrawing consent.

IV. Protect user rights: Metaverse providers should ensure that users can exercise their data protection rights, including accessing, rectifying, and deleting their data.

V. Conduct regular audits: Metaverse providers should conduct regular audits to ensure that they comply with applicable data protection regulations and identify areas for improvement.

VI. Partner with trusted service providers: Metaverse providers should partner with trusted service providers with a strong track record in complying with data protection regulations.

Managing GDPR, compliances, and regulations in the metaverse ecosystem will require careful planning, implementation, and monitoring. Metaverse providers prioritizing data protection and privacy will likely build greater user trust, leading to greater adoption and success.

These are the several essential ways to make the metaverse trustworthy amidst various challenges. By focusing on aspects such as human rights, monitoring, robustness, data privacy, user-friendliness, transparency, fairness, social effects, monetization, content moderation, fraud detection, cyber-sickness prevention, and compliance with data protection regulations like GDPR, we can pave the way for a safe and reliable metaverse that users from diverse backgrounds and industries can embrace. These strategies, among others, contribute to building trust and credibility in this evolving digital landscape.

5 | Future Research Opportunities

Metaverse opens up new opportunities for interaction with online communities and is expected to drive business model innovation and the creation of new services. To build fair metaverse concepts in the future, we should focus on marketing concepts, business models, interaction with the user, ecological partnership, and technology readiness. The limitations of metaverse, which can be a reasonable research criterion in the future, are as follows.

5.1 | TAI for Smart Decision Making

The smart decision layer, acting as the "brain" of the metaverse-empowered Web 3.0, leverages AI for decision-making and service recommendation. AI models should be designed to build trust and transparency to be explainable, robust, fair, and aligned with ethical and societal values. Ensuring the AI model's precision and reliability, even in extreme situations not encountered during training, is essential to guaranteeing the trustworthiness of Web 3.0 services.

5.2 | Tackling the Uncanny Valley with Metahuman Representations

Metahumans, realistic digital human representations, hold great promise in enhancing the immersive experience. However, imperfect human-like visual representations that fall into the Uncanny Valley can evoke negative emotions in users. Striking a balance between realistic representation and avoiding the Uncanny Valley is critical. Advancements in AI technologies are expected to enable the generation of ultra-high-fidelity Metahumans in the future [57].

5.3 | Heterogeneous Viewing Devices and Computation-Intensive Rendering

Users interact with AI, Blockchain, and metaverse-based Web 3.0 through diverse devices such as VR/AR/MR headsets and smartphones. However, some devices lack the necessary computing power to execute computation-extensive rendering tasks for high-quality metaverse videos. On the other hand, ultra-low motion-to-photon latency is essential to prevent cyber-sickness when using VR/AR/MR headsets. Smart task offloading mechanisms need to be designed to migrate rendering tasks from viewing devices to edge servers or cloud centers to ensure smooth and low-latency experiences [58].

5.4 | Revolutionary Blockchain Consensus for Decentralized Web

User-generated data is stored in Blockchain to achieve a decentralized web and protect data ownership and authenticity. However, Blockchain technology faces scalability and resource-efficiency challenges, hindering its application in Web 3.0. Revolutionary Blockchain consensus mechanisms should be developed to speed up transaction processing while maintaining reliability. Sharding, a promising research direction, can help reduce communication, computation, and storage overhead by splitting transactions among smaller groups of nodes.

5.5 | Proactive Edge Caching for Reduced Latency

Proactive edge caching can be employed to address spatial and temporal coherence challenges in users' Fields of View (FoV) and among different users. This technique can help in reducing latency for metaverse video trans- mission and ensure a seamless and immersive user experience [59].

6 | Conclusion

The metaverse promises an immersive environment without limits and has broad development and application prospects. Metaverse is still taking shape, and brands from all industries are coming in front to play a role in designing it. This paper provided an in-depth idea about metaverse, its application, and why it is so important. We also discussed different challenges, especially the ethical challenges of the metaverse ecosystem. Finally, we discussed the characteristics of TAI and how to gain trust in metaverse. With the growing interest and usage of metaverse in the current world, which significantly impacts our lives, it is crucial to understand how to trust it. All the key factors in the VR space need to work together to achieve common standards and protocols for building virtual worlds for the metaverse to become fully trusted and developed. Regulatory bodies should also establish scrutiny and monitor how to make this metaverse concept fully trusted and a reality.

References

[1] Moneta, A. (2020). Architecture, heritage, and the metaverse. *Traditional dwellings and settlements review*, *32*(1), 37–49. https://www.jstor.org/stable/27074915

[2] Díaz, J. E. M., Saldaña, C. A. D., & Avila, C. A. R. (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

[3] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A survey on metaverse: Fundamentals, security, and privacy. *IEEE communications surveys and tutorials*, *25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

[4] Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021). *Metaverse for social good: A university campus prototype* [presentation]. Proceedings of the 29th ACM international conference on multimedia (pp. 153–161). https://doi.org/10.1145/3474085.3479238

[5] Park, S. M., & Kim, Y. G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. *IEEE access*, *10*, 4209–4251. https://doi.org/10.1109/ACCESS.2021.3140175

[6] Narin, N. G. (2021). A content analysis of the metaverse articles. *Journal of metaverse*, *1*(1), 17–24. https://dergipark.org.tr/en/pub/jmv/issue/67581/1051382

[7] Kraus, S., Kanbach, D. K., Krysta, P. M., Steinhoff, M. M., & Tomini, N. (2022). Facebook and the creation of the metaverse: Radical business model innovation or incremental transformation? *International journal of entrepreneurial behaviour and research*, *28*(9), 52–77. https://doi.org/10.1108/IJEBR-12-2021-0984

[8] Toreini, E., Aitken, M., Coopamootoo, K., Elliott, K., Zelaya, C. G., & van Moorsel, A. (2020). *The relationship between trust in AI and trustworthy machine learning technologies* [presentation]. FAT* 2020 - proceedings of the 2020 conference on fairness, accountability, and transparency (pp. 272–283). https://doi.org/10.1145/3351095.3372834

[9] Guo, Y., Yu, T., Wu, J., Wang, Y., Wan, S., Zheng, J., … & Dai, Q. (2022). Artificial intelligence for metaverse: A framework. *CAAI artificial intelligence research*, *1*(1), 54–67. https://doi.org/10.26599/air.2022.9150004

[10] Jones, R. K., & Lee, D. N. (1981). Why two eyes are better than one: the two views of binocular vision. *Journal of experimental psychology: Human perception and performance*, *7*(1), 30–40. https://doi.org/10.1037/0096-1523.7.1.30

[11] Tunca, S., Sezen, B., & Wilk, V. (2023). An exploratory content and sentiment analysis of the guardian metaverse articles using leximancer and natural language processing. *Journal of Big Data*, *10*(1), 82. https://doi.org/10.1186/s40537-023-00773-w

[12] Hemp, P. (2006). Avatar-based marketing. *Harvard business review*, *84*(6), 48–57. http://www.etchouse.com/mcma510/readings/hemp-2006.pdf

[13] Kou, Y., & Gui, X. (2023). *Harmful design in the metaverse and how to mitigate it: A case study of user-generated virtual worlds on roblox* [presentation]. Proceedings of the 2023 acm designing interactive systems conference (pp. 175–188). https://doi.org/10.1145/3563657.3595960

[14] Ponce, B. A., Menendez, M. E., Oladeji, L. O., Fryberger, C. T., & Dantuluri, P. K. (2014). Emerging technology in surgical education: combining real-time augmented reality and wearable computing devices. *Orthopedics*, *37*(11), 751–757. https://doi.org/10.3928/01477447-20141023-05

[15] El Faqir, Y., Arroyo, J., & Hassan, S. (2020). *An overview of decentralized autonomous organizations on the blockchain* [presentation]. Proceedings of the 16th international symposium on open collaboration (pp. 1–8). https://doi.org/10.1145/3412569.3412579

[16] Chrétien-Ichikawa, S. (2022). Shanghai fashion and post-1990s youth through the Phygital Lens. In *Creative industries and digital transformation in China* (pp. 117–146). Springer. https://doi.org/10.1007/978-981-19-3049-2_6

[17] Maeng, Y., Lee, C. C., & Yun, H. (2023). Understanding antecedents that affect customer evaluations of head-mounted display VR devices through text mining and deep neural network. *Journal of theoretical and applied electronic commerce research*, *18*(3), 1238–1256. https://doi.org/10.3390/jtaer18030063

[18] Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2023). Artificial intelligence for the metaverse: A survey. *Engineering applications of artificial intelligence*, *117*, 105581. https://doi.org/10.1016/j.engappai.2022.105581

[19] Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International cybersecurity law review*, *3*(2), 467–494. https://doi.org/10.1365/s43439-022-00056-9

[20] Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., & Zheng, Z. (2022). Fusing Blockchain and AI with metaverse: A survey. *IEEE open journal of the computer society*, *3*, 122–136. https://doi.org/10.1109/OJCS.2022.3188249

[21] Regner, F., Schweizer, A., & Urbach, N. (2019). *NFTs in practice-non-fungible tokens as core component of a Blockchain-based event ticketing application* [presentation]. 40th international conference on information systems, icis 2019 (pp. 1–17). https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1045/wi-1045.pdf

[22] Zhang, H., Lee, S., Lu, Y., Yu, X., & Lu, H. (2023). A survey on Big Data technologies and their applications to the metaverse: Past, current and future. *Mathematics*, *11*(1), 96. https://doi.org/10.3390/math11010096

[23] Tang, F., Chen, X., Zhao, M., & Kato, N. (2023). The roadmap of communication and networking in 6g for the metaverse. *IEEE wireless communications*, *30*(4), 72–81. https://doi.org/10.1109/MWC.019.2100721

[24] Kiong, L. V. (2022). *Web3 made easy: A comprehensive guide to Web3: everything you need to know about web3, Blockchain, DeFi, Metaverse, NFT and GameFi*. Liew Voon Kiong. https://l1nq.com/NCLkG

[25] Adams, D. (2022). Virtual retail in the metaverse: Customer behavior analytics, extended reality technologies, and immersive visualization systems. *Linguistic and philosophical investigations*, *21*(21), 73–88. https://doi.org/10.22381/lpi2120225.

[26] Kshetri, N. (2022). Web 3.0 and the metaverse shaping organizations' brand and product strategies. *IT professional*, *24*(02), 11–15. https://doi.org/10.1109/MITP.2022.3157206

[27] Wagner, R., & Cozmiuc, D. (2022). Extended reality in marketing—a multiple case study on internet of things platforms. *Information*, *13*(6), 278. https://doi.org/10.3390/info13060278

[28] McLean, G., & Wilson, A. (2019). Shopping in the digital world: Examining customer engagement through augmented reality mobile applications. *Computers in human behavior*, *101*, 210–224. https://doi.org/10.1016/j.chb.2019.07.002

[29] Drapkin, A. (2023). *Metaverse companies: Who's involved and who's investing in 2023*. https://tech.co/news/metaverse-companies-whos-involved-whos-investing

[30] Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the metaverse: A hybrid-narrative review based on the technology affordance perspective. *Journal of strategic information systems*, *31*(2), 101717. https://doi.org/10.1016/j.jsis.2022.101717

[31] Hennig-Thurau, T., Aliman, D. N., Herting, A. M., Cziehso, G. P., Linder, M., & Kübler, R. V. (2023). Social interactions in the metaverse: Framework, initial evidence, and research roadmap. *Journal of the academy of marketing science*, *51*(4), 889–913. https://doi.org/10.1007/s11747-022-00908-0

[32] Ong, T., Wilczewski, H., Paige, S. R., Soni, H., Welch, B. M., & Bunnell, B. E. (2021). Extended reality for enhanced telehealth during and beyond covid-19: Viewpoint. *JMIR serious games*, *9*(3), e26520. https://doi.org/10.2196/26520

[33] Khan, N., Muhammad, K., Hussain, T., Nasir, M., Munsif, M., Imran, A. S., & Sajjad, M. (2021). An adaptive game-based learning strategy for children road safety education and practice in virtual space. *Sensors*, *21*(11), 3661. https://doi.org/10.3390/s21113661

[34] Wiederhold, B. K., & Riva, G. (2022). Metaverse creates new opportunities in healthcare. *Annual review of cybertherapy and telemedicine*, *20*, 3–7. https://psycnet.apa.org/record/2023-49082-001

[35] Schumacher, P. (2022). The metaverse as opportunity for architecture and society: Design drivers, core competencies. *Architectural intelligence*, *1*(1), 11. https://doi.org/10.1007/s44223-022-00010-z

[36] Thomason, J. (2022). Metaverse, token economies, and non-communicable diseases. *Global health journal*, *6*(3), 164–167. https://doi.org/10.1016/j.glohj.2022.07.001

[37] Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). Blockchain integration in the era of industrial metaverse. *Applied sciences*, *13*(3), 1353. https://doi.org/10.3390/app13031353

[38] Hosain, T., Zaman, A., Abir, M. R., Akter, S., Mursalin, S., & Khan, S. S. (2024). Synchronizing object detection: Applications, advancements and existing challenges. *IEEE access*, *12*, 54129–54167. https://doi.org/10.1109/ACCESS.2024.3388889

[39] Hosain, M. T., Jim, J. R., Mridha, M. F., & Kabir, M. M. (2024). Explainable AI approaches in deep learning: Advancements, applications and challenges. *Computers and electrical engineering*, *117*, 109246. https://doi.org/10.1016/j.compeleceng.2024.109246

[40] Hosain, M. T., Anik, M. H., Rafi, S., Tabassum, R., Insia, K., & Siddiky, M. M. (2023). Path to gain functional transparency in artificial intelligence with meaningful explainability. *Journal of metaverse*, *3*(2), 166–180. https://doi.org/10.57019/jmv.1306685

[41] Hawblitzel, C., Howell, J., Lorch, J. R., Narayan, A., Parno, B., Zhang, D., & Zill, B. (2014). *Ironclad apps:{End-to-End} security via automated {Full-System} verification* [presentation]. 11th USENIX symposium on operating systems design and implementation (OSDI 14) (pp. 165–181). https://www.usenix.org/conference/osdi14

[42] Koh, N., Li, Y., Li, Y., Xia, L., Beringer, L., Honoré, W., … & Zdancewic, S. (2019). *From C to interaction trees: Specifying, verifying, and testing a networked server* [presentation]. Proceedings of the 8th ACM SIGPLAN international conference on certified programs and proofs (pp. 234–248). https://doi.org/10.1145/3293880.3294106

[43] Miron, M., Tolan, S., Gómez, E., & Castillo, C. (2021). Evaluating causes of algorithmic bias in juvenile criminal recidivism. *Artificial intelligence and law*, *29*(2), 111–147. https://doi.org/10.1007/s10506-020-09268-y

[44] Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pan, J., Protzenko, J., … & Zinzindohoué, J. K. (2017). *Implementing and proving the TLS 1.3 record layer* [presentation]. SP 2017-38th IEEE symposium on security and privacy (pp. 463–482). https://inria.hal.science/hal-01674096/

[45] Rassmann, K. A. (2022). *A goal, question, metric approach to coherent use integration within the devops lifecycle*. https://drum.lib.umd.edu/handle/1903/29022

[46] Jim, J. R., Hosain, M. T., Mridha, M. F., Kabir, M. M., & Shin, J. (2023). Towards trustworthy metaverse: Advancements and challenges. *IEEE access*, *11*, 118318–118347. https://doi.org/10.1109/ACCESS.2023.3326258

[47] Liddicoat, J., & Doria, A. (2011). Human rights and internet protocols : Comparing processes and principles. *Retrieved july*, *13*, 1–13. https://www.internetsociety.org/wp-content/uploads/2017/08/Human20Rights20and20Internet20Protocols-20Comparing20Processes20and20Principles.pdf

[48] Yellowlees, P. M., & Marks, S. (2007). Problematic internet use or internet addiction? *Computers in human behavior*, *23*(3), 1447–1453. https://doi.org/10.1016/j.chb.2005.05.004

[49] Chang, C. L., Hung, J. L., Tien, C. W., Tien, C. W., & Kuo, S. Y. (2020). *Evaluating robustness of ai models against adversarial attacks* [presentation]. Proceedings of the 1st ACM workshop on security and privacy on artificial intelligence (pp. 47–54). https://doi.org/10.1145/3385003.3410920

[50] Bessen, J. E., Impink, S. M., Reichensperger, L., & Seamans, R. (2020). GDPR and the importance of data to AI startups. *NYU stern school of business*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3576714

[51] Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia business law review*, *2019*(2), 494–620. https://heinonline.org/HOL/LandingPage?handle=hein.journals/colb2019&div=15&id=&page=

[52] Zhou, J., Chen, F., & Holzinger, A. (2022). Towards explainability for AI fairness. In *XxAI - beyond explainable AI* (Vol. 13200 LNAI, pp. 375–386). https://doi.org/ 10.1007/978-3-031-04083-2_18

[53] Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., … & Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information systems frontiers*, *25*(5), 2071–2114. https://doi.org/10.1007/s10796-023-10400-x

[54] Kshetri, N. (2022). Policy, ethical, social, and environmental considerations of Web3 and the metaverse. *IT professional*, *24*(3), 4–8. https://doi.org/10.1109/MITP.2022.3178509

[55] Langvardt, K. (2017). Regulating online content moderation. *Geo. LJ*, *106*, 1353. https://heinonline.org/HOL/LandingPage?handle=hein.journals/glj106&div=39&id=&page=

[56] Voigt, P., & dem Bussche, A. (2017). *The eu general data protection regulation (GDPR)*. Springer. https://doi.org/10.1007/978-3-319-57959-7

[57] Gorlini, C., Dixen, L., & Burelli, P. (2023). Investigating the uncanny valley phenomenon through the temporal dynamics of neural responses to virtual characters. *2023 IEEE conference on games (CoG)* (pp. 1–8). IEEE. https://doi.org/10.1109/CoG57401.2023.10333130

[58] Zhang, X., Min, G., Li, T., Ma, Z., Cao, X., & Wang, S. (2023). AI and Blockchain empowered metaverse for Web 3.0: Vision, architecture, and future directions. *IEEE communications magazine*, *61*(8), 60–66. https://doi.org/10.1109/MCOM.004.2200473

[59] Mahmoud, M., Rizou, S., Panayides, A. S., Kantartzis, N. V., Karagiannidis, G. K., Lazaridis, P. I., & Zaharis, Z. D. (2023). A survey on optimizing mobile delivery of 360° videos: Edge caching and multicasting. *IEEE access*, *11*, 68925–68942. https://doi.org/10.1109/ACCESS.2023.3292335