REVIEW ARTICLE

Futuristic Metaverse: Security and Counter Measures

Nidhi Ramolia[1], Pranav Piyushbhai Tank[1], R. N. Ravikumar[1], Babar Zeb[2], Manish Kumar[1,3] and Sushil Kumar Singh[1,*]

[1] Department of Computer Engineering, Marwadi University, Rajkot, India
[2] Department of Software Engineering, College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan
[3] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Republic of Korea

Abstract

This paper presents a comprehensive analysis of the security and privacy challenges in the Metaverse, introducing a novel framework for evaluating and addressing these emerging threats. Our research makes three key contributions: (1) a systematic classification of Metaverse-specific security vulnerabilities across interconnected virtual and physical environments, (2) a framework for assessing privacy risks in AR/VR-enabled social interactions, and (3) targeted solutions for securing blockchain-based digital assets and identity management in the Metaverse. Our analysis highlights how traditional cybersecurity approaches must evolve to address the unique challenges posed by the fusion of physical and virtual worlds, immersive 3D environments, and cross-platform interactions. We examine the technological foundations of the Metaverse—including augmented reality (AR), virtual reality (VR), blockchain, and 5G networks—and assess their security implications. Our findings identify critical gaps in current security protocols and propose novel countermeasures for protecting user privacy, securing digital transactions, and maintaining data integrity across virtual environments. This research provides a roadmap for future security implementations in the Metaverse and identifies key areas requiring further investigation.

Keywords: metaverse, security, virtual reality, metaverse security, applications, challenges.

1 Introduction

The Metaverse represents the next evolution of internet connectivity, creating immersive digital realms where individuals, locations, and objects coexist virtually. Unlike traditional internet interactions, the Metaverse enables direct user immersion and real-time interaction with digital identities. This immersive experience is enabled by multiple technologies, including virtual reality (VR), augmented reality (AR), artificial intelligence, and blockchain, creating a complex ecosystem that requires robust security measures. As this platform advances, it faces unique security challenges beyond traditional cybersecurity concerns. These include:

Academic Editor:
Jing Na

Submitted: 28 October 2024
Accepted: 27 November 2024
Published: 04 January 2025

Vol. 2, **No.** 1, 2025.
10.62762/TIS.2024.194631

***Corresponding author:**
Sushil Kumar Singh
sushilkumar.singh@marwadieducation.edu.in

Citation
Ramolia, N., Tank, P. P., Ravikumar, R. N., Zeb, B., Kumar, M., & Singh, S. K. (2025). Futuristic Metaverse: Security and Counter Measures. *ICCK Transactions on Intelligent Systematics*, 2(1), 49–65.

- Privacy risks from increased personal data exposure.
- Security vulnerabilities in cross-platform interactions.
- Authentication challenges in immersive environments.

Unlike simply being online without interaction, you can interact with other digital identities in the Metaverse. Cybersecurity challenges like phishing, account hacking, and malware are common to both the Internet and the Metaverse, highlighting similarities between the two environments [1]. As the use of digital currencies and NFTs continues to expand, they may become more attractive targets for hackers. The Metaverse denotes a digital realm that enables users to interact with digital content in a manner comparable to real-world experiences. Research on multi-layer networks suggests that the Metaverse represents an advanced evolution of the Internet, emphasizing enhanced social connectivity and exhibiting significant potential for creativity due to its decentralized architecture [2]. The Metaverse comprises interconnected 3D virtual realms primarily centered on social interaction. As this platform advances and expands, it's anticipated to gradually reveal more personal information about its users, not only to the platform itself but also to fellow users. In the Metaverse, you can engage in different types of interactions, such as video calls, voice chats, messaging, augmented reality (AR), virtual reality (VR), and mixed reality (XR). Figure 1 presents an overview of the Metaverse architecture. Artificial intelligence is the driving force behind the Metaverse's automation capabilities, providing unparalleled strength and depth to its functionalities. Exploring the metaverse will introduce fresh opportunities and challenges, encompassing social and economic matters that will directly manifest within its virtual realm.

Realising the metaverse requires substantial technical investment, particularly in edge-enabled infrastructures that support the seamless integration of physical and digital environments [3]. The development of a sustainable metaverse requires the collaboration of multiple technology domains. In the creation of immersive virtual environments, VR support is essential. The metaverse gives rise to new socioeconomic paradigms, including metaeconomics and metamanagement, which govern virtual enterprises and digital cities operating within these immersive environments [4]. Maximizing privacy in Metaverse and bringing real-world objects requires digital twins. For the metaverse to access more real-world information, it needs to be able to connect to sensors in smart devices. By using smart sensors and related technologies, we can improve how we collect and process data, ultimately making the connection between the physical world and virtual environments more reliable and diverse. Flexible AI-assisted frameworks have been proposed to support the development of diverse Metaverse applications, enabling rapid prototyping and human-guided content creation within virtual environments [5]. AI

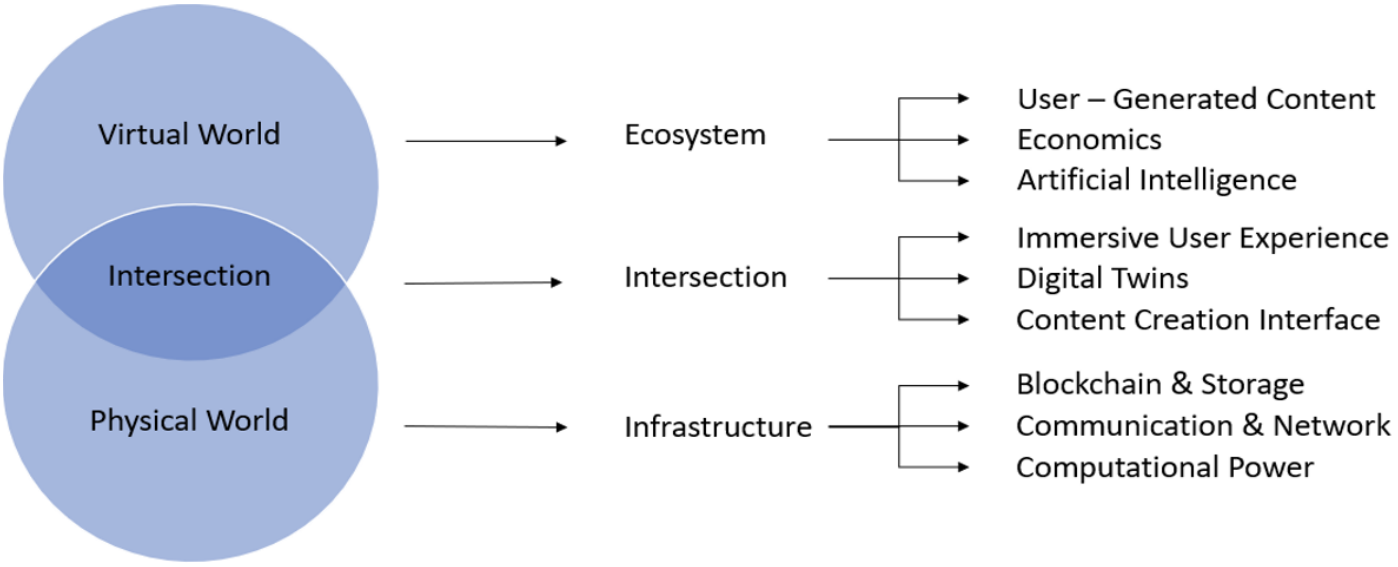

Figure 1. Metaverse architecture overview, illustrating the key components of the Metaverse ecosystem including virtual worlds, user interaction interfaces, and underlying infrastructure.

and blockchain technology integration can establish a metaverse ecosystem characterized by intelligence, transparency, and fairness. In general, traditional computer science methods hold significant promise for the future development of the metaverse. However, several critical challenges must be addressed to ensure the safe development and management of the metaverse. As we navigate this technological landscape, we encounter human-centric challenges such as interpreting movement and gaze, managing resources responsibly, ensuring privacy and security, and efficiently handling real-time information. These challenges reflect fundamental human concerns and values, underscoring the importance of establishing a secure and trustworthy digital environment. Addressing these issues is essential for the sustainable growth of the metaverse. At the same time, sectors such as culture, tourism, and news media can benefit significantly from disseminating content through an integrated metaverse platform, offering more immersive experiences and fostering a deeper understanding of human society as a whole [6].

The Metaverse has been conceptualised as a collection of interconnected 3D virtual worlds, with its architectural fragmentation and diversity of platforms representing both a design challenge and a long-standing characteristic of virtual environment ecosystems [7]. As the Metaverse expands into new application domains, security and privacy requirements must be systematically addressed across diverse deployment scenarios and user groups [8]. There has been extensive research carried out globally on the concept of the metaverse. In the bustling metaverse market, the competitive landscape of the Metaverse is underpinned by advances in AR and VR display technologies, which serve as the foundational interfaces through which users access and interact with virtual environments [9]. Every company leverages state-of-the-art technology and expansive markets to establish competitive edges within the metaverse. The Metaverse introduces a broad surface of security and privacy risks that extend well beyond those encountered in conventional internet environments, necessitating dedicated threat analysis and countermeasure design [10]. Major technology companies have begun investing substantially in metaverse infrastructure. For instance, Google has consolidated its AR and VR research under a unified organizational structure and is exploring immersive telepresence through projects such as Project Starline. These industry-level commitments signal that the metaverse is transitioning from a conceptual framework toward deployed systems, intensifying the urgency of addressing its security and privacy challenges before widespread adoption occurs.

The remainder of this paper is organized as follows. Section 2 reviews related work, providing an overview of existing approaches to Metaverse security and privacy challenges. Section 3 outlines the proposed security measures and countermeasures, detailing technical methodologies and practical solutions for safeguarding the Metaverse ecosystem. In Section 4, we introduce an evaluation framework to assess the effectiveness of these proposed measures, supported by experimental insights. Section 5 examines the convergence of advanced technologies in the Metaverse, including blockchain, AI, VR, and AR, and discusses key challenges and future research directions such as interoperability, energy-efficient protocols, and human-computer interaction enhancements. Finally, Section 6 concludes the paper by summarizing the main findings and highlighting the significance of the proposed contributions in advancing Metaverse security.

2 Related Work

Snow Crash, a novel by Neal Stephenson, introduced the concept of the Metaverse 30 years ago. This vision of an immersive, persistent virtual world has since inspired a generation of researchers and technology developers. Recent advancements in blockchain, VR/AR, AI, cloud computing, and IOT have brought attention to the Metaverse in the tech industry. The metaverse can reduce discrimination, eliminate individual differences, and promote socialization in human society. However, just like everything else, security and privacy concerns are associated with the metaverse. Here, the metaverse is viewed as an advanced form of virtual reality (VR), offering a far more immersive and expansive experience compared to existing VR technologies. This section systematically examines what could go wrong with security and privacy in the metaverse, drawing on existing literature and identified threat surfaces. We will also provide potential solutions to address these concerns.

2.1 Technological Aspects

The metaverse encompasses a wide range of technologies working together to create immersive and interconnected virtual experiences. While existing research has made significant strides in understanding

the Metaverse's technological foundations, several critical gaps remain in addressing its security challenges. Our analysis of the current literature reveals three key areas requiring further investigation.

Encryption: Encryption plays a crucial role in ensuring the safety of user interactions and data. Communication within virtual environments remains confidential when end-to-end encryption is employed [11]. Data is encrypted on the sender's device and decrypted solely on the recipient's end. This includes various means of communication, such as text messages, voice chats, and video calls to prevent eavesdropping attempts. Encryption secures virtual transactions, transfers digital assets, and prevents unauthorized manipulation or theft in the metaverse. The use of encryption techniques, including symmetric and asymmetric encryption, establishes a secure security framework. Key management ensures secure key generation, distribution, storage, and rotation. While encryption technologies offer important protections, the Metaverse also raises broader societal concerns—including dark patterns, addiction risks, and misuse of immersive environments—that demand attention alongside purely technical security measures [12]. Metaverse security constantly evolves to incorporate the latest cryptographic standards and algorithms, making it resilient against emerging threats.

Biometric Authentication and Identity Management: Verifying a user's identity involves using unique physiological or behavioral traits for biometric authentication [13]. Biometric markers provide secure and personalized authentication, reducing the risk of unauthorized access. Users can log in by scanning their facial features, adding an extra layer of security beyond passwords. Identity management is the process of creating, maintaining, and safeguarding user identities. It involves managing user information, such as user names and passwords, and ensuring that only authorized individuals have access to sensitive data and systems. Managing digital identities is an important task that involves assigning and overseeing avatars or virtual personas. Establishing a user's digital footprint- which includes their preferences, interactions, and digital assets- is central to identity management. Identity management systems safeguard authorized access to the metaverse, preventing misuse.

Decentralization: Decentralization is crucial in strengthening the security of the metaverse by distributing control and infrastructure across multiple nodes or servers. This model distributes the risk of failure and improves virtual environment resilience. Blockchain technology, which is often associated with decentralization, ensures tamper resistance and transparency in transactions, thereby fostering trust among users. Decentralization empowers users, allowing them greater control over their virtual identities and assets [14]. Without central authority, the metaverse is more resistant to censorship, creating an open and inclusive digital space. Additionally, the distributed processing architecture improves scalability, enabling it to handle a growing user base and increased transaction volume. Decentralization is essential for creating secure, resilient, and user-centric metaverse environments, although it poses challenges in ensuring practicality and seamless user experience.

Blockchain Technology: It is possible to use blockchain technology for decentralized and secure data storage in the metaverse. Blockchain's role as an economic infrastructure—providing verifiable, tamper-resistant records of transactions and ownership—extends naturally into metaverse environments where digital assets and interactions require equivalent guarantees [15]. Blockchain is essential for security in the metaverse, with its transparent and tamper-resistant ledger providing an immutable record of user interactions. Smart contracts, which are self-executing codes on the blockchain, offer an automated method of enforcing security measures. This ensures that transactions adhere to predefined rules without the need for intermediaries. Tokenization on the blockchain provides secure digital ownership verification. Decentralized identity management allows users to have control over their digital identities, reducing the risks of identity theft. Cryptographic consensus mechanisms, such as proof-of-work or proof-of-stake, help prevent tampering and fraud and ensure the metaverse's integrity. These mechanisms have practical deployment precedents beyond currency: in metaverse energy-trading applications, blockchain consensus has been shown to enable secure and sustainable peer-to-peer transactions without relying on centralized intermediaries [16]. Transactions in the metaverse are made transparent and auditable, promoting trust and preventing hidden manipulation by users [17]. Finally, the potential of blockchain in terms of interoperability makes it possible for users and assets to move seamlessly across various metaverse platforms, resulting in a

cohesive virtual experience. In general, the use of blockchain technology significantly improves the security standards in the metaverse by providing transparency, decentralization, and cryptographic integrity. Combining blockchain with biometric authentication further strengthens this foundation by binding verified user identities to cryptographic credentials, enabling cross-platform trust without centralised identity authorities [18].

AI-Powered Security Measures: AI can help secure the metaverse through behavioral analysis algorithms, identifying unusual patterns and AI-driven content moderation, and filtering out malicious content in real-time. Biometric authentication, such as facial or voice recognition, provides an additional layer of identity verification [19].

Threat detection algorithms continuously monitor for cyber threats and unauthorized access, responding swiftly to mitigate risks. AI-powered encryption technology improves the security of communication and data transfer. AI-driven virtual security guards monitor virtual spaces, while predictive analytics help to identify potential security risks. Smart contracts, which are also powered by AI, automatically enforce rules within the metaverse, ensuring secure and fair transactions. The key to establishing a robust metaverse security framework is to use a dynamic approach, combining these measures and adapting to evolving threats. Furthermore, the Metaverse could leverage blockchain technology to establish privacy protection frameworks that oversee user conduct and mitigate privacy breaches [20].

2.2 Seminal Contribution:

The metaverse has generated significant interest among researchers. Several survey papers have been published exploring different aspects of the metaverse. These papers delve into various important technologies that constitute and are reviewed within the Metaverse. Establishing authenticated and trusted spatial boundaries within the Metaverse is an emerging research challenge, with blockchain-based user-centric approaches offering a promising direction for securing virtual spaces and their associated identities [30]. Metaverses are becoming integral to our lives, bridging virtual experiences with the physical world. Mixed reality (MR) offers immersive training opportunities in fields like aircraft maintenance, particularly with digital twins of aircraft. This approach enables authentic experiences while facilitating physical distancing during pandemics. Additionally, modern machinery replicas in MR benefit aviation colleges, allowing easy manipulation, sharing, and updating for enhanced training [31]. Yang et al. [32] propose a secure authentication framework to guarantee the traceability of avatars in the Metaverse using blockchain; however, their work focuses primarily on identity verification scenarios and does not fully address the broader integration of AI-driven dynamic access control. This gap between theory and practice is particularly evident in security protocol design. Huang et al. [33] present a comprehensive survey of security and privacy issues in the Metaverse, systematically examining its architectural components, enabling technologies, and associated threat surfaces. Their work provides an in-depth taxonomy of security and privacy challenges across multiple layers, including identity management, data protection, and virtual asset security. However, although the survey offers a broad conceptual overview, it does not sufficiently integrate user interaction behaviors with dynamic risk assessment models, leaving unresolved how complex human–system interactions in immersive environments translate into evolving and compound security vulnerabilities.

While existing research has made significant strides in understanding the Metaverse's technological foundations, several critical gaps remain in addressing its security challenges. To contextualize our analysis within the current research landscape, Table 1 synthesizes key recent studies on Metaverse security, highlighting their methodological approaches, contributions, and identified limitations. This shows that more and more people believe that the metaverse, a virtual world, will be at the center of future advancements and bring lots of benefits [34].

3 Metaverse Security and Counter Measures:

The metaverse, a connected virtual universe, introduces distinct security challenges akin to real-world scenarios alongside unique digital environment-specific concerns. Here are fundamental security considerations and corresponding measures for the metaverse:

Data Privacy: Deploy end-to-end encryption to safeguard user data from unauthorized access during transmission. Employ data anonymization methods like tokenization or differential privacy to mitigate the risk of identifying individuals from stored data. Enforce stringent access controls, role-based permissions, and data encryption at rest to protect

Table 1. Summary of selected research on Metaverse security.

Ref.	Year	Technology	Method	Advantages	Disadvantages
Chen et al. [21]	2022	Metaverse Security & Privacy.	Systematic overview of Metaverse security and privacy threats.	Comprehensive identification of attack surfaces and privacy risks across Metaverse layers.	Increasingly sophisticated attacks in the Metaverse require more targeted defence mechanisms.
Cheng [22]	2023	Metaverse related technologies	Survey, Applications, Security, and Opportunities.	Overview of Metaverse-related technologies and applications.	Security risks of Metaverse development may be more prominent and complex.
Wu and Zhang [23]	2023	Metaverse related technologies.	Analysis of digital identity and privacy security in the Metaverse.	Addresses legal safeguards and regulatory frameworks for user rights protection.	Limited access to broadband internet and expensive VR headsets.
Kuru et al. [24]	2024	Urban Metaverse Cybersecurity.	Analysis of cyberthreats and countermeasures in urban metaverse deployments over wireless networks.	Systematic identification of urban-specific cyberattack vectors and proposed countermeasures for smart-city metaverse scenarios.	Countermeasures remain largely theoretical and require validation in real urban metaverse deployments.
Truong et al. [25]	2023	Federated learning & Blockchain.	MetaCIDS utilizes blockchain and online federated learning technology.	Proposed MetaCIDS, a collaborative intrusion detection framework for the metaverse.	Traditional security approaches have limitations in the large-scale distributed metaverse.
Chow et al. [26]	2022	Metaverse using cybersecurity.	Utilization of technologies such as VR and AR in the Metaverse.	Cybersecurity threats on Metaverse in relation to visualization technologies.	Visualization technologies in the Metaverse give rise to emerging cybersecurity threats.
Kabanda et al. [27]	2022	Metaverse & Cyber Security.	Pragmatism paradigm used.	Overview of Metaverse-related technologies and applications.	Security risks of Metaverse development may be more prominent and complex.
Qayyum et al. [28]	2024	AI-XR metaverse applications.	Analyze security, privacy, and trustworthiness associated with AI techniques.	First attempt to analyze challenges of using AI techniques in AI-XR metaverse applications.	Potential risks such as privacy breaches, security invasion, and unfair AI outcomes.
Adil et al. [29]	2024	5G/6G–enabled Metaverse Technologies.	VR, AR, robots, and digital twins.	Taxonomy and applications of Metaverse technology.	Security challenges in 5G and 6G-enabled Metaverse technology applications.

sensitive information. In 2022, Meta publicly disclosed the deployment of secure computing techniques to protect user data across its Horizon Worlds platform, offering an early industry example of how privacy-preserving methods can be operationalized in large-scale metaverse environments [35].

Identity Management: Implement strong authentication methods such as biometric verification, multi-factor authentication (MFA), or passwordless authentication to guarantee secure user access. Introduce identity verification procedures such as Know Your Customer (KYC) checks for transactions with elevated risk levels. Utilize session management strategies to identify and thwart session hijacking or unauthorized account access attempts. Platforms like Roblox have introduced MFA as part of their publicly documented user protection policies, representing an industry-level commitment to reducing unauthorized account access in large-scale virtual social environments [36].

Cyber Attacks: Edge intelligence architectures play a central role in Metaverse security by enabling low-latency threat detection and distributed enforcement of security policies closer to end users and devices [37]. Educate users on prevalent cyber-attack methods such as phishing emails, malware, and social engineering tactics. Conduct routine security awareness training sessions to foster a culture of good cybersecurity practices among metaverse users. Machine learning techniques have demonstrated significant potential in automating threat detection within Metaverse environments, enabling proactive identification of phishing attempts, account compromise, and other cyber threats at scale [38].

Virtual Currency Security: Enhance the security of virtual currency wallets by employing robust encryption, multi-signature authentication, and hardware-based security features. Monitor transactions closely for any signs of suspicious activity and integrate anti-money laundering (AML), and Know Your Transaction (KYT) protocols to identify and thwart fraudulent transactions. Regularly audit virtual currency platforms and smart contracts to pinpoint potential vulnerabilities and ensure continuous security reinforcement. In 2023, OpenSea adopted enhanced AML and KYT protocols,

Table 2. Security issues and solutions for different technologies using Metaverse.

Reference	Security issues	Solutions
Jaber [42]	Security and privacy risks related to data breaches and identity theft	The paper provides an overview of the metaverse world and its architecture.
Kürtünlüoğlu et al. [45]	The security of the authentication phase in virtual reality environments is vital.	The paper compares the security of information-based, biometric, and multi-model authentication methods in virtual reality environment.
Tariq et al. [46]	Deepfakes can be used for impersonation in gaming scenarios.	Deepfakes in the metaverse have serious security implications for gaming, online meetings, and virtual offices.
Metz and Gurău [47]	Limitations of the current version of the metaverse are discussed.	Handling risks like terrorism and illegal money transactions in the metaverse.
Kim et al. [48]	Limitations on avatar.	The suggested authentication system makes the avatar's identity remains reliable and can be traced back accurately.
Bale et al. [49]	Cybersecurity concerns and broader societal impacts of the Metaverse on human users.	Comprehensive examination of how metaverse technologies affect human well-being, safety, and security, identifying the need for holistic protection frameworks beyond purely technical countermeasures.
Patwe and Mane [50]	Centralized authentication mechanisms in the Metaverse have limitations and security threats.	The paper proposes a Blockchain-enabled architecture for decentralized authentication in the Metaverse.

improving fraud detection and ensuring compliance with financial regulations in its NFT marketplace [39].

Continuous Monitoring and Response: Utilize real-time monitoring tools to identify security threats and vulnerabilities within metaverse environments. Establish incident response procedures and escalation protocols to address security incidents promptly. Regularly conduct security assessments, penetration testing, and vulnerability scans to detect and address metaverse systems and infrastructure weaknesses. Continuous security assessment, including penetration testing and vulnerability scanning, is identified as a critical practice across the Metaverse ecosystem to ensure that emerging threats are proactively identified and mitigated [40].

3.1 Security Issues:

As we explore the security concerns of the metaverse, it becomes clear that privacy issues may arise due to the vast amount of personal information that users share. Unauthorized access to user data or a breach in the metaverse's infrastructure could lead to identity theft or misuse of sensitive information. It is, therefore, imperative that content moderation is implemented to combat the proliferation of harmful content, including hate speech, harassment, or illicit material. Such content can negatively affect the user experience and the community's well-being.

Cybersecurity threats are a major concern in the metaverse, with both individual users and virtual platform infrastructure targeted by phishing attempts and hacking incidents [41]. The potential for financial losses and service disruption is significant. Virtual assets, including in-game currencies, digital goods, and virtual real estate, are particularly vulnerable to theft and fraud and, therefore, require robust security measures to safeguard them. Identity theft is a complex problem within the metaverse. Users may encounter difficulties in authenticating their identity, and there is a risk of impersonation or fraudulent activities. Therefore, it is crucial to implement advanced authentication methods, such as biometrics or multi-factor authentication, to protect the identity of users [42]. Establishing a comprehensive and adaptable security framework as the metaverse expands is crucial. Technological innovation, user education, and collaboration between metaverse platforms are ongoing efforts that will be essential to address multifaceted security challenges effectively.

To synthesize the security concerns discussed across various technological dimensions, Table 2 summarizes representative issues identified in the literature alongside their proposed countermeasures. This highlights the fragmented yet evolving nature of current research in Metaverse security.

3.2 Existing Solutions:

For the Metaverse to function smoothly, the systems in place must be secure and dependable. Security threats are associated with the original Internet and the convergence of technologies in the Metaverse. Common security countermeasures are summarized below.

3.2.1 Data

The Metaverse holds a massive amount of data, making traditional data management methods insufficient for the task at hand. To address this challenge, decentralised architectures, such as blockchain-enabled authentication frameworks, offer a fresh approach to handling identity and access management within the Metaverse, reducing reliance on vulnerable centralised systems [50]. In the Metaverse, big data technology makes it possible to store, process, and analyze huge amounts of data, helping us make sense of all the information available. As a result, we can learn important things from the data, helping us make better decisions and understand trends [43, 44]. However, ensuring data security is vital in the Metaverse, as it strives to keep valuable information safe from being lost or stolen. Sensitive information requiring protection includes data related to users' biometrics and behaviors. Therefore, it's essential to find a way to safeguard sensitive business and personal information in the Metaverse.

First and foremost, it's essential to make sure that the servers and devices used by users are physically secure. Regardless of whether a user's data is stored on their own device, in a company's data center, or in a public cloud, managers need to ensure that the facility is kept safe and protected from any compromises or damage. Secondly, it's essential to have sensible access management and control in place.

We should stick to the idea of giving out the least amount of access needed across the Metaverse. For instance, when it comes to getting into databases and networks, permissions should only be granted for specific tasks and kept as minimal as possible [51]. This measure is put in place to protect data and functions from mistakes or intentional harm. Lastly, ensuring we have a trustworthy backup of all our essential data that is regularly checked is crucial for keeping it safe. These backups must be as secure as the main database and core system to ensure that only the right people can access them.

3.2.2 Network

Network security is of utmost importance when protecting customer data and information, ensuring reliable access and network performance, keeping shared data secure, and preventing cyber threats. Having a strong network security system in place can stop sensitive information from being exposed, which not only builds trust with users but also prevents further financial losses for companies. Ensuring our network systems run smoothly and giving lawful access to data is essential for giving users the best possible service. With all the different devices in the Metaverse, keeping our network secure comes with new challenges. Due to the resource constraints of many edge devices (e.g., AR/VR headsets, IoT sensors) in the Metaverse, embedding security at the hardware and firmware level is crucial. At the network and access level, implementing a zero-trust architecture is another essential security measure worth considering. Next-generation communication infrastructures, including 6G networks, are expected to provide the high-bandwidth, low-latency foundation necessary to support zero-trust security models and continuous authentication at scale within the Metaverse [52]. With so much data to handle in the Metaverse, adopting a zero-trust approach is the best way to reduce or eliminate the risk of sensitive information being stolen.

Cloud computing and cloud storage play vital roles as foundational technologies for the metaverse. As more activities migrate to the cloud, traditional network architectures must evolve to accommodate the shift from local to cloud-based access. In this context, innovations such as software-defined networking (SDN) and software-defined wide area networking (SD-WAN) are essential, as they enhance network flexibility while maintaining security across private, public, and hybrid cloud environments. These technologies can be viewed as additional layers of protection within modern network infrastructures, ensuring data security regardless of where it is stored or accessed. Integrating 6G connectivity with edge AI further amplifies these capabilities by enabling intelligent, low-latency enforcement of security policies at the network edge [53]. Therefore, cloud security remains a critical concern, playing an instrumental role in safeguarding the metaverse ecosystem.

3.2.3 Communication

In the metaverse, people are incredibly interactive and social, fostering frequent communication among users. To engage in activities such as sharing, cooperating, and building trust and understanding, communication is essential. While most users value privacy and are hesitant to share sensitive information with unauthorized parties, it is still crucial to protect communication. This means ensuring that only authorized communicators can access and understand the content while preventing unauthorized parties from intercepting or recovering the information.

3.2.4 Privacy

In the Metaverse, safeguarding privacy relies on encrypting and anonymizing user data, forming the cornerstone of protection. To uphold user privacy, the Metaverse needs to offer a user-friendly data management platform, empowering individuals to dictate what information they share. In protecting data privacy, being transparent about what information is being gathered is essential. It's about clearly identifying and understanding the data being collected. Given that data within the Metaverse may stem from diverse origins, it's crucial to have the capability to track where each piece of data comes from. This helps ensure clarity and accountability in understanding data sources. In XR experiences, like virtual reality, it gathers personal details such as biometric data, facial features, and info from the virtual world. Securing the transmission of such sensitive data requires dedicated communication protocols: native metaverse communication architectures that leverage blockchain for spectrum management offer a promising direction for ensuring confidentiality and integrity of biometric data streams [54]. Safeguarding this information is crucial for user privacy and security. So, a digital ID system that uses biometric data and is supported by blockchain technology emerges as the answer. Biometric data can serve as the basis for creating a unique set of keys through cryptography. These keys act like digital fingerprints, allowing individuals to prove their identity within the network and authorize transactions securely. By using key pairs for digital IDs, we can provide a stronger level of security, ensuring that individuals' identities are protected. Moreover, content created by users (UGC) will play a crucial role in shaping the Metaverse. Yet, UGC often includes sensitive personal information, posing significant privacy concerns. Furthermore, the Metaverse could leverage blockchain technology to establish privacy protection frameworks that oversee user conduct and mitigate privacy breaches. Applications of Metaverse are shown in Figure 2 and discuss what is the application of Metaverse in the current generation.

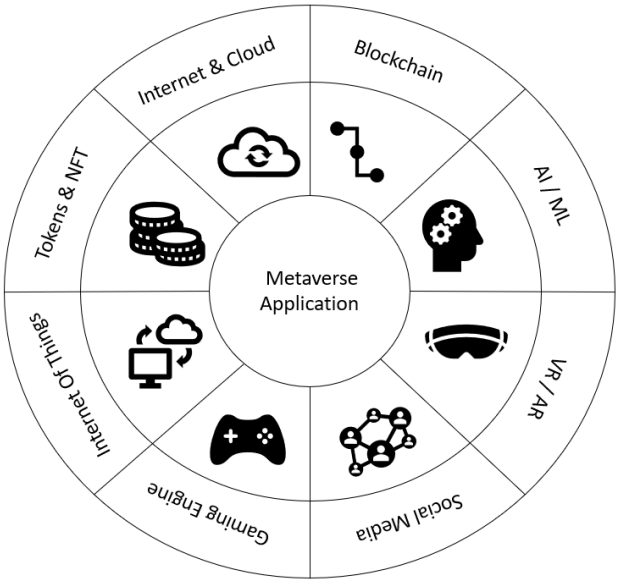

Figure 2. Applications of Metaverse.

3.2.5 Identity, Content, and Economic Security in the Metaverse

For the Metaverse to be a safe and stable environment, it's important to establish reasonable rules and measures. A significant aspect to consider is managing user identities. Users can possess various identities and easily transition between different virtual realms. It's important that a user's digital identity is persistent, unique, and cannot be copied, modified or deleted by anyone. The system should consistently implement measures to safeguard user identities, like using blockchain technology for identity protection, to deter unauthorized access and misuse of personal data. AI technology has the capability to assist with automatically verifying identities and analyzing user behavior. AI technology can assist in automatically verifying identities and analyzing user actions and behaviors. Virtual reality technologies and their integration with IoT infrastructures provide the enabling layer through which users generate, share, and interact with content in the Metaverse, forming the technical foundation of its emerging digital economy [55]. The Metaverse economy is more dynamic and open than traditional e-commerce, with blockchain technology and emerging industries playing a central role in driving economic growth. Decentralized autonomous organizations (DAOs) reduce the risks of centralized control [56], while proof-of-work consensus mechanisms enhance transaction security. Verified digital asset ownership is foundational to virtual economic stability: blockchain provides an immutable, auditable record of every transaction, enabling reliable tracking and protection of digital belongings across the Metaverse. Beyond economic transactions, the Metaverse also holds significant promise for immersive training and professional development, where the integrity and security of participant data are equally important [57]. Effectively addressing security within content and applications is therefore essential for ensuring the overall safety of the Metaverse ecosystem.

4 Proposed Evaluation Framework for Metaverse Security Measures

We propose a structured framework to evaluate the security measures discussed. This framework uses a combination of risk assessment, experimental validation, and benchmarking against existing solutions to ensure transparency and reproducibility.

Risk Assessment Methodology

We adopt a layered risk assessment model to evaluate potential vulnerabilities in the Metaverse, categorized into four layers:

Data Layer: Analyzing risks related to data privacy and encryption (e.g., risk of data breaches, unauthorized access).

Network Layer: Evaluating network protocols (e.g., use of IDS/IPS, zero-trust architecture) for risks of DDoS attacks or malware.

Transaction Layer: Scrutinizing blockchain-based solutions for digital asset protection, including wallet security and smart contract audits.

User Interaction Layer: Evaluating user behavior and awareness (e.g., susceptibility to phishing or social engineering attacks).

Each layer's risk is scored using a Likelihood x Impact model (on a scale of 1–5), providing a comprehensive risk profile for the Metaverse ecosystem.

Experimental Validation

To substantiate the effectiveness of the proposed security measures, we propose conducting controlled experiments and simulation-based studies. Examples include:

Simulation of Cyber Attacks: Implement a controlled phishing attack scenario within a virtual environment to measure the response rate and effectiveness of user education campaigns.

Performance Testing of Blockchain Protocols: Evaluate transaction latency, throughput, and resistance to tampering under varying loads and attack conditions.

Biometric System Validation: Test biometric authentication systems under real-world conditions to measure error rates (false positives/negatives) and resistance to spoofing attacks.

Benchmarking and Case Studies

We propose benchmarking the discussed solutions against existing real-world implementations to assess their effectiveness. Case studies include:

Meta Horizon Worlds Privacy Implementation: Analyze the effectiveness of Meta's privacy measures, such as end-to-end encryption and anonymization.

Epic Games' User Security Campaigns: Compare user engagement and outcomes of phishing prevention campaigns.

Roblox MFA Implementation: Benchmark user adoption rates and security improvement metrics post-implementation.

Validation Metrics

The evaluation framework employs the following key metrics:

Security Effectiveness: Reduction in successful attacks (e.g., phishing, identity theft).

Performance Overhead: Impact of security measures on system performance (e.g., latency, computational overhead).

User Adoption and Awareness: Metrics from user surveys and behavioral studies, measuring understanding and use of security tools.

Cost-Efficiency: Resources required to implement and maintain security measures.

Iterative Improvement

The framework emphasizes an iterative approach, where feedback from risk assessment, experiments, and benchmarking is used to refine and enhance the proposed security measures.

5 Convergence of Advanced Technology in Metaverse

In the metaverse, security is of utmost importance. Encryption and authentication protocols are meticulously implemented to safeguard user data and communications. Advanced cryptographic techniques, including end-to-end encryption, ensure that sensitive information remains confidential during transmission. Traditional network security measures, such as firewalls and intrusion detection systems, form a robust perimeter defense, actively monitoring and repelling any malicious activities within the virtual landscape.

Decentralized identity solutions, often built on blockchain technology, provide users with control

over their personal information and establish a tamper-resistant framework for identity verification. Smart contracts, inherent to many metaverse platforms, play a pivotal role in automating and securing transactions, mitigating the risks associated with fraudulent activities.

Artificial intelligence plays a crucial role in metaverse security by analyzing vast datasets and detecting anomalous patterns indicative of potential threats. Machine learning algorithms continuously evolve to adapt to emerging security challenges, offering a dynamic defense mechanism [58].

Biometric authentication methods, ranging from facial recognition to fingerprint scanning, add an extra layer of user verification, ensuring that access to virtual spaces remains highly secure. Virtual Private Networks (VPNs) play a vital role by encrypting communication channels, safeguarding the privacy of user interactions within the metaverse.

Regular security audits are conducted with diligence to identify and address vulnerabilities in the system. This proactive approach ensures that the metaverse remains resilient to evolving cyber threats. In tandem, community involvement is encouraged through effective moderation tools and reporting systems, allowing users to actively contribute to identifying and reporting suspicious activities or content.

As the metaverse continues to evolve, dedicated virtual security teams stand as the front line of defense, equipped to respond swiftly to emerging threats. Their role encompasses continuous research, staying abreast of the latest security developments, and implementing real-time measures to fortify the security infrastructure of the metaverse, creating a safe and trustworthy virtual environment for all participants.

5.1 Blockchain for Metaverse:

When contemplating the metaverse, one's imagination may be filled with an array of captivating experiences or entertaining games. However, it's crucial to acknowledge that the metaverse represents more than just a realm of fantasy; it encompasses a parallel world with an inevitable economic ecosystem closely intertwined with our own. Using blockchain technology will make data in the metaverse more flexible and adaptable. However, because blockchain requires copying data across the chain, it can slow down how quickly information moves. With the growing population in the metaverse, there's a corresponding need for an increased number of blocks, which in turn requires substantial computing resources. At the same time, integrating AI-based solutions into these next-generation network environments introduces its own security and privacy concerns, as AI models may themselves become targets of adversarial attacks or data poisoning [59]. Due to this, users will incur elevated transaction costs to validate shared transactions. Next-generation blockchain designs must therefore address scalability and computational efficiency as prerequisites for practical deployment within high-throughput metaverse environments.

5.2 AI for Metaverse:

The Metaverse is like a big network that connects everything together, including our physical world, through intermediaries. It's not something separate from reality but rather intertwined with it. Artificial intelligence has the capacity to bolster all technological aspects within the Metaverse. Given the vast volume of content generated within this digital realm, AI can facilitate extensive and ongoing content creation to sustain the Metaverse. Blockchain further complements AI in this context by providing tamper-resistant logging of content provenance and ownership, ensuring that AI-generated assets within the metaverse can be traced, verified, and securely transferred [60]. In the world of the Metaverse, AI is used for things like chatbots. By using artificial intelligence to understand speech, see things like humans do, and understand language, the Metaverse becomes easier and more useful for everyone. However, AI-enabled grouping and identity mechanisms in the Metaverse also introduce security vulnerabilities, as adversarial actors may exploit avatar systems and AI-driven interactions to conduct infiltration or social engineering attacks [61]. Furthermore, the Metaverse offers exciting opportunities for education and training. By incorporating artificial intelligence, people can immerse themselves in lifelike virtual settings for learning. They can also receive assistance from virtual teaching aides and participate in educational programs available within the Metaverse. The potential for collaboration between artificial intelligence and the Metaverse is vast, especially considering that the Metaverse is still in its early stages of development.

5.3 Virtual Reality (VR) for Metaverse:

Virtual reality offers entirely synthetic perspectives, immersing individuals in virtual environments

where they interact with various elements using different user interaction methods. It represents the extreme end of the Reality-Virtuality Continuum. Artificial intelligence amplifies VR's capabilities within the metaverse by enabling adaptive content generation, intelligent avatar behaviour, and real-time environmental personalisation, making the boundary between synthetic and perceived reality increasingly indistinct [62], requiring users to focus on virtual environments and fully disconnect from physical reality. In commercial virtual spaces, people can get creative and make things like virtual paintings using VR technology. They can experiment with different tools and features to change objects and express their artistic ideas. Multiple users can collaborate in real-time within these environments, which necessitates a collective perception of space, presence, and simultaneous interaction supported by communication methods and mechanisms for sharing information [63]. It's imperative that everyone in a virtual world, which is like a smaller part of the metaverse, sees the same things. This way, they can all interact with each other at the same time and in the same way. Imagine the ultimate metaverse experience where virtual and real-world interactions blend seamlessly, including using augmented and mixed reality together. Constructing the metaverse requires integrating simultaneous actions across various virtual shared spaces, involving interactions between objects, avatars, and their engagements. Synchronizing every operation within virtual environments accurately reflects dynamic states and events [64]. Yet, managing and organizing these changing situations on a large scale is a big challenge, especially when there are lots of people using the virtual world at the same time. They're all moving virtual things around instantly, and if there's even a tiny delay, it could make the experience less enjoyable for them.

5.4 Augmented Reality (AR) for Metaverse:

Augmented reality (AR) isn't just about virtual worlds - it's about making real-life experiences even better by adding digital elements. You can get virtual stuff sent to you through different senses, like hearing, seeing, smelling, and feeling, to make things more exciting and immersive. Early AR system frameworks focused mainly on visual enhancements, organizing and displaying digital overlays onto physical surroundings. Yet, these systems often forget about how users move around. They usually make people sit still and use controllers to interact with text and flat screens, which isn't very active or engaging. Considerable research efforts have been directed towards enhancing user interaction with digital entities in AR. It's essential to ensure that digital entities overlaid onto the user's physical surroundings, potentially originating from the metaverse, allow users to seamlessly integrate simultaneous actions, akin to those experienced in virtual reality (VR). Making it easy and natural for people to interact with digital things in augmented reality (AR) is a big challenge. It's like building a bridge between real people and the virtual world of the metaverse. Gesture-based ways of interacting, like the ones you see in movies like Minority Report, provide a really intuitive way for people to do things in AR. One notable freehand interaction technique, Voodoo Dolls [65], enables users to select and manipulate virtual content using pinch gestures with both hands. Another solution called HOMER works by using a virtual hand to point at and interact with AR objects. Essentially, when people use AR, they're still in the real world but can also do things with virtual stuff. Making this work well needs a lot of tech improvements in figuring out where things are in the real world and matching them up with their virtual versions accurately [68, 69], while securing the underlying network channels that carry AR data streams remains equally critical [67]. AR overlays also introduce threat vectors such as visual content injection, requiring threat-aware system design [66]. Securing the underlying communication channels that carry AR data streams is equally important, as vulnerabilities in next-generation networks can expose sensitive spatial and biometric information transmitted during immersive interactions [67].

5.5 Discussion and Future Scope

The Metaverse, an emerging and transformative concept, integrates a range of advanced technologies to create immersive virtual environments. Despite rapid progress, several challenges remain, presenting significant opportunities for future research and innovation.

One of the most significant challenges in the Metaverse is ensuring scalability and low latency in large-scale virtual environments. Real-time interactions demand substantial bandwidth, particularly for technologies like VR and AR. Current network infrastructures often struggle to support seamless user experiences at scale. To address this, future research could integrate edge computing with 5G/6G networks to reduce latency and enable efficient processing of data closer to the user [70, 71]. Additionally, the development

of adaptive load-balancing algorithms could help manage network traffic during peak usage, ensuring smooth performance in high-demand scenarios.

Another pressing issue is privacy and data security, as the Metaverse handles vast amounts of sensitive user data in interconnected ecosystems. Data breaches and identity theft pose serious risks to users. Future work can explore privacy-preserving machine learning (PPML) techniques that protect sensitive information during AI training processes. Furthermore, adopting blockchain-based decentralized identity (DID) systems would empower users to control their data securely while reducing reliance on centralized systems vulnerable to cyberattacks [72–75].

The lack of interoperability across platforms presents a barrier to seamless user experiences in the Metaverse. Currently, most ecosystems operate in silos, limiting the mobility of digital assets, identities, and interactions. Future research could focus on standardizing communication protocols and developing interoperable blockchain frameworks that facilitate asset transfers and user interactions across platforms. Such advancements would enable a unified Metaverse, fostering greater collaboration and innovation.

User safety and content moderation remain critical concerns in the Metaverse. Real-time detection and mitigation of harmful content, such as hate speech or harassment, are challenging due to the volume and diversity of interactions. To address this, future work could develop AI-driven content moderation systems leveraging natural language processing (NLP) and sentiment analysis to detect and filter inappropriate content. Integrating these systems with community-based governance mechanisms can further enhance trust and safety, ensuring a positive user experience.

The energy efficiency and sustainability of the Metaverse are growing concerns, particularly due to the computational demands of VR/AR rendering and blockchain operations. The carbon footprint of these technologies could hinder their long-term viability. Research into energy-efficient VR rendering algorithms and the adoption of green blockchain protocols, such as proof-of-stake (PoS) or proof-of-authority (PoA), can significantly reduce energy consumption and improve the sustainability of Metaverse ecosystems.

Lastly, improving human-computer interaction (HCI) within the Metaverse is vital for creating inclusive and intuitive user experiences. Current interfaces often lack accessibility for diverse user groups, including individuals with disabilities. Future research should focus on developing gesture-based interaction systems and brain-computer interfaces (BCIs) that provide more natural and immersive ways for users to engage with virtual environments. Such advancements would ensure that the Metaverse is technologically advanced and universally accessible.

6 Conclusion

This article thoroughly examines the Metaverse, an emerging technology that has garnered significant attention in recent times. Although there have been studies on the Metaverse, they've mostly focused on narrow topics like technology and security, missing a broader understanding of what the Metaverse is all about and how it could be used. This paper dives deep into the basics, the tech, the uses, the security worries, and possible fixes for the Metaverse. It's a topic that hasn't been looked at in detail as far as we know. This paper thoroughly examines the main ideas, tech, uses, security issues, and how we can fix them in the Metaverse, shining a light on a topic that hasn't been explored fully as far as we know. It talks about how the Metaverse is set up technically and how people are using it now, focusing on the security problems we're facing and what we can do about them. Furthermore, the paper outlines the obstacles and future pathways for the Metaverse, considering its vast potential and the ongoing exploration rooted in related technologies over the past couple of years.

Data Availability Statement

Not applicable.

Funding

This work was supported by the Research Seed Grant from Marwadi University, Rajkot, Gujarat, India, under Grant MU/R&D/22- 23/MRP/FT13.

Conflicts of Interest

Sushil Kumar Singh served as an Associate Editor of the *ICCK Transactions on Intelligent Systematics* at the time of manuscript submission. To ensure the integrity of the peer-review process, Sushil Kumar Singh had no involvement in the editorial review, peer review, or decision-making process for this manuscript. The

manuscript was handled independently by another editor in accordance with the journal's editorial policies. The remaining authors declare that they have no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Sun, J., Gan, W., Chao, H. C., & Yu, P. S. (2022). Metaverse: Survey, applications, security, and opportunities. *arXiv preprint arXiv:2210.07990*. [CrossRef]

[2] Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2023). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. *IEEE Communications Surveys & Tutorials*. [CrossRef]

[3] Xu, M., Ng, W. C., Lim, W. Y. B., Kang, J., Xiong, Z., Niyato, D., ... & Miao, C. (2022). A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *IEEE Communications Surveys & Tutorials, 25*(1), 656-700. [CrossRef]

[4] Wang, F. Y., Qin, R., Wang, X., & Hu, B. (2022). Metasocieties in metaverse: Metaeconomics and metamanagement for metaenterprises and metacities. *IEEE Transactions on Computational Social Systems*, 9(1), 2-7. [CrossRef]

[5] Zhu, H. (2022). MetaAID: A Flexible Framework for Developing Metaverse Applications via AI Technology and Human Editing. *arXiv preprint arXiv:2204.01614*.

[6] Rehm, S. V., Goel, L., & Crespi, M. (2015). The metaverse as mediator between technology, trends, and the digital transformation of society and business. *Journal For Virtual Worlds Research*, 8(2). [CrossRef]

[7] Dionisio, J. D. N., Iii, W. G. B., & Gilbert, R. (2013). 3D virtual worlds and the metaverse: Current status and future possibilities. *ACM computing surveys (CSUR)*, 45(3), 1-38. [CrossRef]

[8] Kang, G., Koo, J., & Kim, Y. G. (2023). Security and privacy requirements for the metaverse: A metaverse applications perspective. *IEEE Communications Magazine*, 62(1), 148-154. [CrossRef]

[9] Zhan, T., Yin, K., Xiong, J., He, Z., & Wu, S. T. (2020). Augmented reality and virtual reality displays: perspectives and challenges. *Iscience*, 23(8). [CrossRef]

[10] Di Pietro, R., & Cresci, S. (2021, December). Metaverse: Security and privacy issues. In *2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA)* (pp. 281-288). IEEE. [CrossRef]

[11] Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., ... & Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet of Things Journal, 10*(16), 14671-14688. [CrossRef]

[12] 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. [CrossRef]

[13] Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & human digital twin: Digital identity, biometrics, and privacy in the future virtual worlds. *Multimodal Technologies and Interaction, 8*(6), 48. [CrossRef]

[14] Gupta, A., Gupta, R., Gohil, K., Tanwar, S., & Garg, D. (2024). Blockchain-based decentralized oracle network framework for identity management in metaverse environment. *Security and Privacy, 7*(6), e414. [CrossRef]

[15] Berg, C., Davidson, S., & Potts, J. (2019). Blockchain technology as economic infrastructure: Revisiting the electronic markets hypothesis. *Frontiers in Blockchain*, 2, 493418. [CrossRef]

[16] Abou El Houda, Z., & Brik, B. (2023). Next-power: Next-generation framework for secure and sustainable energy trading in the metaverse. *Ad Hoc Networks*, 149, 103243. [CrossRef]

[17] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 25(1), 319-352. [CrossRef]

[18] Delgado-Mohatar, O., Fierrez, J., Tolosana, R., & Vera-Rodriguez, R. (2020). Blockchain and biometrics: A first look into opportunities and challenges. In *Blockchain and Applications: International Congress* (pp. 169-177). Springer International Publishing. [CrossRef]

[19] Kumar, P., Kumar, R., Aloqaily, M., & Islam, A. N. (2023). Explainable AI and blockchain for metaverse: A security, and privacy perspective. *IEEE Consumer Electronics Magazine*. [CrossRef]

[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. [CrossRef]

[21] Chen, Z., Wu, J., Gan, W., & Qi, Z. (2022, December). Metaverse security and privacy: An overview. In *2022 IEEE International Conference on Big Data (Big Data)* (pp. 2950-2959). IEEE. [CrossRef]

[22] Cheng, S. (2023). Metaverse Security. In *Metaverse: Concept, Content and Context* (pp. 145-163). Cham: Springer Nature Switzerland. [CrossRef]

[23] Wu, H., & Zhang, W. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. *Security and Safety*, 2, 2023011. [CrossRef]

[24] Kuru, K., & Kuru, K. (2024, November). Urban metaverse cyberthreats and countermeasures against these threats. In *2024 6th International Conference on Blockchain Computing and Applications (BCCA)* (pp. 228-235). IEEE. [CrossRef]

[25] Truong, V. T., & Le, L. B. (2023). MetaCIDS: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning. *IEEE Open Journal of the Computer Society*. [CrossRef]

[26] Chow, Y. W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and cybersecurity in the metaverse: A survey. *Journal of Imaging*, 9(1), 11. [CrossRef]

[27] Kabanda, G., Chipfumbu, C. T., & Chingoriwo, T. (2022). A Cybersecurity Model for a Roblox-based Metaverse Architecture Framework. *British Journal of Multidisciplinary and Advanced Studies*, 3(2), 105-141. [CrossRef]

[28] Qayyum, A., Butt, M. A., Ali, H., Usman, M., Halabi, O., Al-Fuqaha, A., ... & Qadir, J. (2024). Secure and trustworthy artificial intelligence-extended reality (AI-XR) for metaverses. *ACM Computing Surveys*, 56(7), 1-38. [CrossRef]

[29] Adil, M., Song, H., Khan, M. K., Farouk, A., & Jin, Z. (2024). 5G/6G-enabled metaverse technologies: Taxonomy, applications, and open security challenges with future research directions. *Journal of Network and Computer Applications*, 103828. [CrossRef]

[30] Seo, J., Ko, H., & Park, S. (2024). Space authentication in the metaverse: A blockchain-based user-centric approach. *IEEE Access, 12*, 18703-18713. [CrossRef]

[31] Siyaev, A., & Jo, G. S. (2021). Towards aircraft maintenance metaverse using speech interactions with virtual objects in mixed reality. *Sensors*, 21(6), 2066. [CrossRef]

[32] Yang, K., Zhang, Z., Youliang, T., & Ma, J. (2023). A secure authentication framework to guarantee the traceability of avatars in metaverse. *IEEE Transactions on Information Forensics and Security*, 18, 3817-3832. [CrossRef]

[33] Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics, 6*(2), 234-247.[CrossRef]

[34] Park, S. M., & Kim, Y. G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. *IEEE access*, 10, 4209-4251. [CrossRef]

[35] Meta. (2022, June 28). *June 2022 | Meta*. Retrieved from https://about.fb.com/news/2022/06/

[36] *Roblox Terms of Use*. (2024). roblox.com. Retrieved from https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use

[37] Xu, Y., Feng, D., Zhao, M., Sun, Y., & Xia, X. G. (2023). Edge intelligence empowered metaverse: architecture, technologies, and open issues. *IEEE Network, 37*(6), 92-100. [CrossRef]

[38] Otoum, Y., Gottimukkala, N., Kumar, N., & Nayak, A. (2024). Machine learning in metaverse security: Current solutions and future challenges. *ACM Computing Surveys, 56*(8), 1-36. [CrossRef]

[39] Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial crimes in web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. *IEEE Open Journal of the Computer Society*, 4, 37-49. [CrossRef]

[40] Sami, H., Hammoud, A., Arafeh, M., Wazzeh, M., Arisdakessian, S., Chahoud, M., ... & Guizani, M. (2024). The metaverse: Survey, trends, novel pipeline ecosystem & future directions. *IEEE Communications Surveys & Tutorials*. [CrossRef]

[41] Bhardwaj, A., & Kaushik, K. (2023). Metaverse or Metaworst with Cybersecurity Attacks. *IT Professional*, 25(3), 54-60. [CrossRef]

[42] Jaber, T. A. (2022). Security Risks of the Metaverse World. *Int. J. Interact. Mob. Technol.*, 16(13), 4-14.[CrossRef]

[43] Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based metaverse: A survey. *Applied Sciences*, 12(24), 12993. [CrossRef]

[44] Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2023). Metaverse: Security and privacy concerns. *Journal of metaverse, 3*(2), 93-99. [CrossRef]

[45] Kürtünlüoğlu, P., Akdik, B., & Karaarslan, E. (2022). Security of virtual reality authentication methods in metaverse: An overview. *arXiv preprint arXiv:2209.06447*. [CrossRef]

[46] Tariq, S., Abuadbba, A., & Moore, K. (2023, July). Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices. In *Proceedings of the 2nd Workshop on Security Implications of Deepfakes and Cheapfakes* (pp. 16-19). [CrossRef]

[47] Metz, D., & Gurău, M. M. (2017). Emerging and Disruptive Technologies: The Metaverse. Implications on Global Security. *Land Forces Academy Review*, 27(4), 411-422. [CrossRef]

[48] Kim, M., Oh, J., Son, S., Park, Y., Kim, J., & Park, Y. (2023). Secure and privacy-preserving authentication scheme using decentralized identifier in metaverse environment. *Electronics, 12*(19), 4073. [CrossRef]

[49] Bale, A. S., Ghorpade, N., Hashim, M. F., Vaishnav, J., & Almaspoor, Z. (2022). A comprehensive study on metaverse and its impacts on humans. *Advances in Human-Computer Interaction, 2022*(1), 3247060. [CrossRef]

[50] Patwe, S., & Mane, S. (2023, April). Blockchain enabled architecture for secure authentication in the metaverse environment. In *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)* (pp. 1-8). IEEE. [CrossRef]

[51] Ooi, B. C., Chen, G., Shou, M. Z., Tan, K. L., Tung, A.,

Xiao, X., ... & Zhang, M. (2023, April). The metaverse data deluge: What can we do about it?. In *2023 IEEE 39th International Conference on Data Engineering (ICDE)* (pp. 3675-3687). IEEE. [CrossRef]

[52] Tang, F., Chen, X., Zhao, M., & Kato, N. (2022). The Roadmap of Communication and Networking in 6G for the Metaverse. *IEEE Wireless Communications*, 30(4), 72-81. [CrossRef]

[53] Chang, L., Zhang, Z., Li, P., Xi, S., Guo, W., Shen, Y., ... & Wu, Y. (2022). 6G-enabled edge AI for metaverse: Challenges, methods, and future research directions. *Journal of communications and information networks*, *7*(2), 107-121. [CrossRef]

[54] Xu, H., Li, Z., Li, Z., Zhang, X., Sun, Y., & Zhang, L. (2022, May). Metaverse native communication: A blockchain and spectrum prospective. In *2022 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 7-12). IEEE. [CrossRef]

[55] Hu, M., Luo, X., Chen, J., Lee, Y. C., Zhou, Y., & Wu, D. (2021). Virtual reality: A survey of enabling technologies and its applications in IoT. *Journal of Network and Computer Applications*, 178, 102970. [CrossRef]

[56] Lee, L. H., Braud, T., Zhou, P. Y., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2024). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *Foundations and trends® in human-computer interaction*, 18(2–3), 100-337. [CrossRef]

[57] Upadhyay, A. K., & Khandelwal, K. (2022). Metaverse: the future of immersive training. *Strategic HR Review*, 21(3), 83-86. [CrossRef]

[58] Fu, Y., Li, C., Yu, F. R., Luan, T. H., Zhao, P., & Liu, S. (2022). A survey of blockchain and intelligent networking for the metaverse. *IEEE Internet of Things Journal*, *10*(4), 3587-3610. [CrossRef]

[59] Kuzlu, M., Catak, F. O., Zhao, Y., Sarp, S., & Catak, E. (2023). Security and privacy concerns in next-generation networks using artificial intelligence-based solutions: A potential use case. In *Wireless Networks: Cyber Security Threats and Countermeasures* (pp. 205-226). Cham: Springer International Publishing. [CrossRef]

[60] Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... & Liyanage, M. (2022). Blockchain for the metaverse: A review. *arXiv preprint arXiv:2203.09738*. [CrossRef]

[61] Park, W. H., Siddiqui, I. F., & Qureshi, N. M. F. (2022). AI-Enabled Grouping Bridgehead to Secure Penetration Topics of Metaverse. *Computers, Materials & Continua*, 73(3).

[62] 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. [CrossRef]

[63] Mahmood, T., Fulmer, W., Mungoli, N., Huang, J., & Lu, A. (2019, October). Improving information sharing and collaborative analysis for remote geospatial visualization using mixed reality. In *2019 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)* (pp. 236-247). IEEE. [CrossRef]

[64] Liu, S., Zou, H., Zhao, X., Wang, C., & Fan, Y. (2023). Preface: Security and Safety in the "Metaverse". *Security and Safety*, 2, E2023014. [CrossRef]

[65] Pierce, J. S., Stearns, B. C., & Pausch, R. (1999, April). Voodoo dolls: seamless interaction at multiple scales in virtual environments. In *Proceedings of the 1999 symposium on Interactive 3D graphics* (pp. 141-145). [CrossRef]

[66] Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, 128, 103127. [CrossRef]

[67] Salahdine, F., Han, T., & Zhang, N. (2023). Security in 5G and beyond recent advances and future challenges. *Security and Privacy*, 6(1), e271. [CrossRef]

[68] Swan, J. E., Singh, G., & Ellis, S. R. (2015). Matching and reaching depth judgments with real and augmented reality targets. *IEEE transactions on visualization and computer graphics*, *21*(11), 1289-1298. [CrossRef]

[69] Swan, J. E., Livingston, M. A., Smallman, H. S., Brown, D., Baillot, Y., Gabbard, J. L., & Hix, D. (2006, March). A perceptual matching technique for depth judgments in optical, see-through augmented reality. In *IEEE Virtual Reality Conference (VR 2006)* (pp. 19-26). IEEE. [CrossRef]

[70] 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. [CrossRef]

[71] Wu, X., Yang, Y., Bilal, M., Qi, L., & Xu, X. (2023). 6G-enabled anomaly detection for metaverse healthcare analytics in Internet of Things. IEEE Journal of Biomedical and Health Informatics. [CrossRef]

[72] Mebrahtom, D., Hadish, S., Sbhatu, A., Aloqaily, M., & Guizani, M. (2023, September). Trust but verify-blockchain-empowered decentralized authentication schema on the metaverse: A self-sovereign identity approach. In *2023 international conference on intelligent metaverse technologies & applications (imeta)* (pp. 1-8). IEEE. [CrossRef]

[73] Moudoud, H., & Cherkaoui, S. (2023, June). Federated learning meets blockchain to secure the metaverse. In *2023 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 339-344). IEEE. [CrossRef]

[74] Chaudhari, A., Mali, Y. K., Kulkarni, A., Jain, D., Sharma, L., Mahajan, K., ... & Bhogle, A. (2024, April). Cyber security challenges in social meta-verse and mitigation techniques. In *2024 MIT Art, Design and Technology School of Computing International Conference*

(*MITADTSoCiCon*) (pp. 1-7). IEEE. [CrossRef]

[75] Kürtünlüoğlu, P., Akdik, B., Duygu, R., & Karaarslan, E. (2023, October). Towards more secure virtual reality authentication for the metaverse: a decentralized method proposal. In *2023 16th International Conference on Information Security and Cryptology* (*ISCTürkiye*) (pp. 1-6). IEEE. [CrossRef]

Nidhi Ramolia is currently pursuing M.Tech. in the Department of Computer Engineering at Marwadi University, Rajkot, Gujarat, India, under the supervision of Dr. Sushil Kumar Singh. She is interested in IoT, Blockchain, and Metaverse.

Pranavbhai Piyushbhai Tank is an Assistant Professor in the Department of Computer Engineering at Marwadi University, Rajkot, Gujarat, India. He is pursuing a Ph.D. under the supervision of Dr. Sushil Kumar Singh from the same university. His interest in Blockchain, and Cloud Computing.

Ravikumar RN is working as an Assistant Professor in the Department of Computer Engineering at Marwadi University. He completed his Bachelor of Engineering in CSE from Anna University in 2010 and his Master of Engineering in CSE from VMRF University in 2013. Currently, he is pursuing a PhD from Amity University, Rajasthan, India. His research interests include Recommendation Systems, AI, ML, DL, and Computer Vision. With 11 years of teaching experience in different cross-cultural areas (India, Maldives, Dubai), he serves as a Project Coordinator, heavily involved in implementing Project-Based Learning and ensuring Teaching-Learning Methodologies. He is also the Lead and Co-founder of the Research Activities Club, promoting quality research activities among young graduates.

Babar Zeb holds a Bachelor's degree in Computer Science from the Institute of Management Sciences in Peshawar and a Master's degree in Software Engineering from the College of Electrical and Mechanical Engineering at NUST, Islamabad. With a strong passion for artificial intelligence and machine learning, he focuses on innovative solutions that leverage cutting-edge technology to address real-world challenges.

Manish Kumar received his B.Tech. degree in Applied Electronics and Instrumentation Engi- neering from Biju Patnaik University of Tech- nology, Rourkela, India, in 2010, followed by an M.Tech. degree in Biomedical Engineering from Manipal University, Udupi, India, in 2013. He earned his Ph.D. in Electrical and Electronics En- gineering from the Birla Institute of Technology, Ranchi, India. From 2022 to 2024, he served as a Visiting Assistant Professor in the Department of Computer Science and Engineering at Seoul National University of Science and Technology, Seoul, South Korea. Currently, he is an Associate Professor in the Department of Computer Engi- neering at Marwadi University, Rajkot, Gujarat, India. Dr. Kumar's research focuses on developing AI-based cybersecurity solutions, with a particular interest in creating robust countermeasures against cyberattacks in the healthcare sector. He has au- thored over 50 research articles, edited a book on IoT, and holds a patent related to AI applications.

Sushil Kumar Singh is an Associate Professor in the Department of Computer Engineering at Marwadi University, Rajkot, India. He received Ph.D. degree from Seoul National University of Science and Technology, Seoul, South Korea. He received M.Tech. Degree in Computer Science and Engineering from Uttarakhand Technical University, Dehradun, India. He also received an M.E. degree in Information Technology from Karnataka State University, Mysore, India. He has also been the lab leader of the UCS Lab at the Department of Computer Science Engineering, Seoul National University of Science and Technology, Seoul, South Korea. He has received the Best Lab Leadership Award from UCS Lab for 2019-2021. He is selected in Top 2% Scientist for the (2022-2023, 2023-2024) year as per the list compiled by Stanford University and published by Elsevier. He has more than 13 years of experience teaching in the field of computer science. He has published Five Books: Computer C Programming, Cyber Security, Big Data Analytics, Mobile Computing, and Secure and Intelligent IoT-Enabled Smart Cities. He has also published many high-quality papers (Q1, Top 10% JCR Rank) in international journals and conferences. He has already delivered international lectures in many countries. His research interests include Blockchain, Artificial Intelligence, Big Data, Internet of Things, Smart City Security, and Cyber-Physical Systems. He is an Associate/ Guest Editor in the Human-centric Computation and Information Sciences (HCIS) Journal, IEEE Journal of Biomedical and Health Informatics (IEEE JBHI) Journal, IGI Global Publication, and Wiley Scrivener Publication. He is a reviewer of the IEEE Wireless Communication Magazine, IEEE SYSTEMS, IEEE Internet of Things, FGCS, TETT, EXSY, JISA, Computer Network, MDPI, CIE, HCIS, JIPS, Computing (COMP), Multimedia Tools & Applications, and SCIS Journal. He also organizes the Research Activities Club, which promotes quality research activities among young researchers at Marwadi University, Rajkot, Gujarat, India.