Received 21 March 2024; revised 21 April 2024; accepted 25 April 2024. Date of publication 6 May 2024; date of current version 10 September 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3397044

User Safety and Security in the Metaverse: A Critical Review

SAURABH SHARMA[1,2], JAITEG SINGH[1], ANKUR GUPTA[2], FARMAN ALI[3], FAHEEM KHAN[4], AND DAEHAN KWAK[5] (Senior Member, IEEE)

[1]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, India

[2] Department is Computer Science and Engineering, Model Institute of Engineering and Technology, Jammu 181122, India

[3]Department of Applied AI, School of Convergence, Sungkyunkwan University, Seoul 03063, South Korea

[4]Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea

[5]Department of Computer Science and Technology, Kean University, Union, NJ 07083, USA

CORRESPONDING AUTHORS: J. SINGH, F. ALI, AND F. KHAN (e-mail: jaiteg.singh@chitkara.edu.in; farman0977@skku.edu; faheem@gachon.ac.kr)

(Saurabh Sharma and Daehan Kwak contributed equally to this work.)

(Special Issue on Challenges and Opportunities in Metaverse-Based Communication and Networking)

ABSTRACT The Metaverse envisions a future where immersive online interactions become the norm. However, this vision can only be safely realized if user safety and privacy are prioritized. This review critically evaluates existing user safety and security measures within the Metaverse. We have highlighted the limited ability of existing solutions to protect against harassment, identity theft, and the misuse of personal data collected in this environment. This research comprehensively analyzes user safety and security dimensions within virtual worlds and presents a taxonomy to classify the unique threats and vulnerabilities Metaverse users may encounter. This review reveals critical gaps, including the lack of comprehensive security frameworks and balanced privacy-preserving models in virtual immersive environments. In response, we propose a novel Metaverse Security Architecture designed with Zero-Trust principles. This architecture prioritizes user control over data, identity, and experiences. It also emphasizes proactive security measures to mitigate diverse potential harms in virtual worlds. Our research highlights the critical importance of such robust, user-centric frameworks in enabling a Metaverse that is immersive, safe, and secure for all its participants.

INDEX TERMS Data breaches and impersonation, identity theft, metaverse, privacy, user security, user safety, user privacy, virtual worlds, zero-trust architecture.

I. INTRODUCTION

THE CONCEPT of the Metaverse offers an exciting glimpse into the future of the Internet. It permits people to engage in immersive virtual environments where they can connect, socialize, collaborate, and have fun in creative and unique ways. However, issues such as user safety, privacy, and security can arise in these virtual worlds. Ball defines the Metaverse as a “massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments” [1]. The term ‘massively scaled’ refers to the massive reach and connectivity of virtual worlds. These virtual worlds are not restricted to individual virtual spaces. Instead, users can visit different virtual worlds within a unified network. It is the top priority to ensure user engagement and experiences in virtual environments.

As users spend a lot of time in these digital environments, a huge volume of private data might be created and shared. This data contains information such as names and locations of users. Apart from this, sensitive information such as biometric data, behavior patterns, and even emotional responses are collected by advanced sensors [2]. This information becomes an easy target for malicious actors. Problems such as identity theft, financial fraud, or social exploitation can arise due to this [3].

Moreover, the immersive nature of the Metaverse can worsen the dangerous impact of issues such as harassment, abuse, and cyberbullying. The Metaverse provides a degree of anonymity to its users, which can reduce perceived social constraints and encourage harmful behaviors. It amplifies the psychological impact on victims despite the absence of direct physical harm [4]. Additionally, the decentralized structure of many Metaverse platforms complicates the task of content moderation and law enforcement for users who have suffered harm in these spaces. Since user adoption is critical to the success of the Metaverse, ensuring that users feel safe and secure within it is of paramount importance. It is also important to safeguard assets and personal information [5]. Metaverse users may face threats such as viruses and cyber-attacks [6]. Instances of virtual property theft and fraud involving assets are further complicating the landscape. The absence of defined regulations for governing the Metaverse is raising issues regarding user security and legal frameworks [7].

Considering these challenges, user safety and security are non-negotiable foundations upon which any successful and sustainable Metaverse is built [8]. Users may rightfully question their safety and privacy if robust safety and security measures are not in place, which may limit the mainstream adoption of these exciting technologies [9]. Therefore, a critical analysis of the existing user privacy and security issues is needed.

This review article aims to bridge this knowledge gap. A taxonomy of risks and threats faced within virtual worlds is presented, offering insight into the various ways users' safety can be compromised. The effectiveness of existing user security solutions is also critically evaluated. Areas have been pinpointed where more robust and effective measures are urgently needed. In response to the existing critical gaps, we propose a novel Metaverse Security Architecture designed with Zero-Trust principles, which emphasizes user-centric control [10]. This paper aims to inspire researchers and professionals to actively discover creative solutions to the Metaverse's emerging security challenges. The subsequent sections will elaborate on these contributions in detail.

A. CONTRIBUTION

The main goal of this article is to focus on the security and safety aspects concerning individual users in the Metaverse. Towards this end, a detailed literature review has been carried out, the state-of-the-art examined, and initial thoughts on the creation of a robust security framework for the Metaverse are articulated. Thus, the main contributions of this paper are:

1) A taxonomy of security issues related to individual users in the Metaverse is presented.
2) Existing work in the domain is consolidated, and open issues concerning the security of individual users are presented.
3) A Metaverse security framework based on Zero-Trust Architecture (ZTA) principles is proposed to address user safety and security within the Metaverse.

B. STRUCTURE OF THE PAPER

The remainder of the paper is organized as shown in Figure 1: Section II discusses the motivation underlying the need for research in user security and privacy, describing real-world scenarios that highlight the existing threats. Section III tackles security issues related to individual users in the Metaverse, where the taxonomy for user security and privacy is presented and discussed. Section IV highlights existing research contributions on user security and privacy issues in the Metaverse. Open challenges in securing users in immersive virtual worlds are thoroughly discussed. In Section V, a novel Metaverse security architecture based on zero-trust principles is outlined. Finally, Section VI concludes the paper and suggests future directions for research in this important domain.

C. RESEARCH METHODOLOGY

We conducted this review following the PRISMA guidelines [11] by performing a thorough search to select research articles from various electronic databases, including Web of Science, Scopus, IEEE Xplore, and the ACM Digital Library. This study includes articles published between 2012 and 2023, all of which are available through openly accessible Web indexes that list the full content or metadata of academic writings [12]. The articles were selected using the query: ((Metaverse) AND (security OR privacy OR safety OR threat) AND (user safety OR user security OR cyberbullying OR harassment)). The systematic selection of the research studies is detailed in Figure 2.

II. BACKGROUND & MOTIVATION

The emergence of the Metaverse introduces security challenges that cannot be neglected. It is vital to address these challenges to create a robust environment for users, ensuring the Metaverse's long-term success and widespread acceptance. The prevalence of attacks on users in the early iterations of the Metaverse has highlighted the need for providing foolproof guarantees of user safety. These issues are highlighted through several case studies below:

A. CASE STUDIES

The frequency of security issues in virtual worlds is not yet fully understood. There is increasing evidence indicating that these environments can indeed compromise user safety and overall welfare [8]. Recent studies, discussed in news articles about online gaming harassment, shed light on an increasing pattern of online harassment and abuse in virtual worlds. This shows the urgent need for implementing user-centric security protocols in these virtual realms [13]. This section provides insights into real-world security challenges faced by users, conducting a comprehensive analysis based

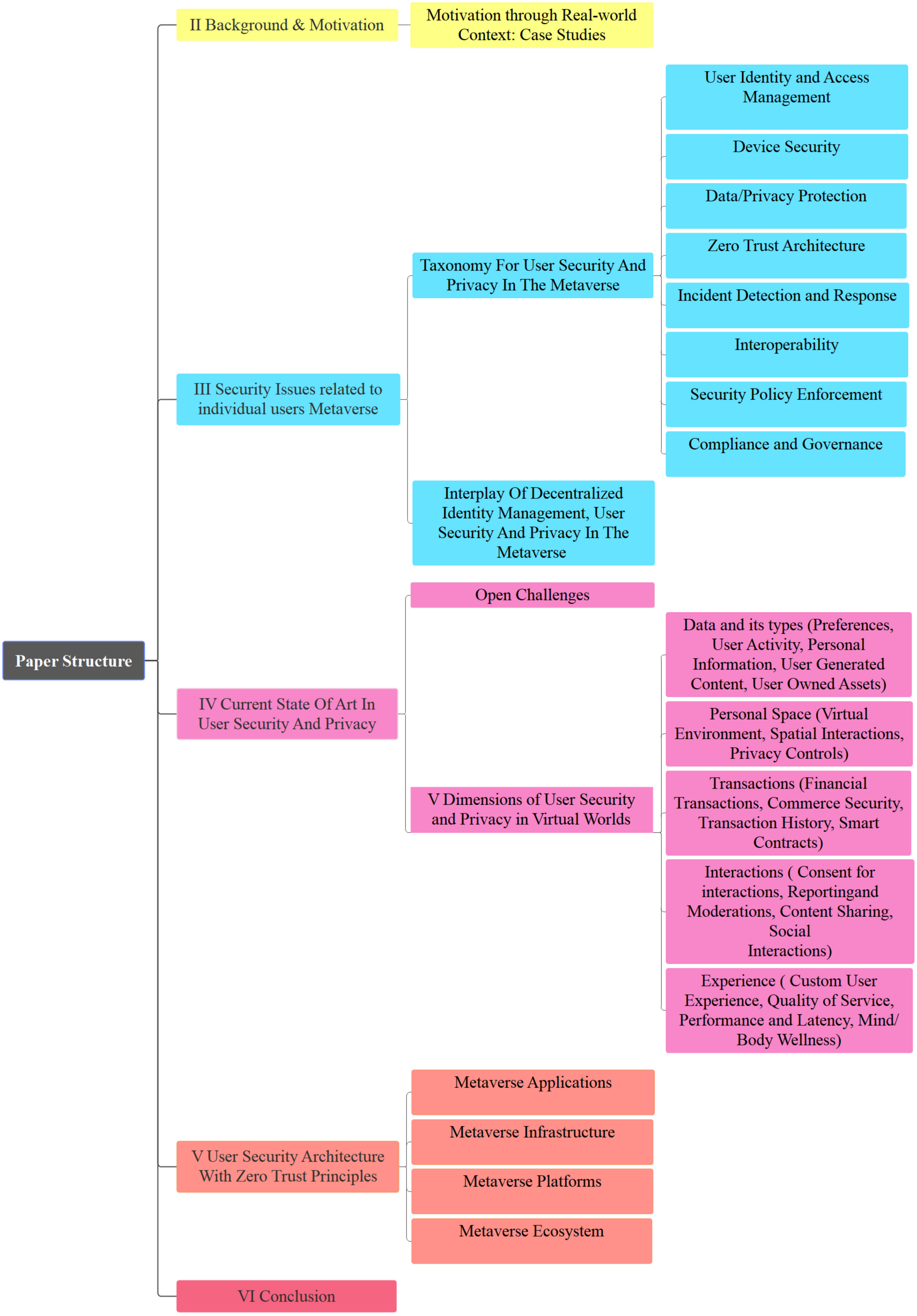
Paper Structure
II Background & Motivation
Motivation through Real-world Context: Case Studies
III Security Issues related to individual users Metaverse
Taxonomy For User Security And Privacy In The Metaverse
User Identity and Access Management
Device Security
Data/Privacy Protection
Zero Trust Architecture
Incident Detection and Response
Interoperability
Security Policy Enforcement
Compliance and Governance
Interplay Of Decentralized Identity Management, User Security And Privacy In The Metaverse
IV Current State Of Art In User Security And Privacy
Open Challenges
V Dimensions of User Security and Privacy in Virtual Worlds
Data and its types (Preferences, User Activity, Personal Information, User Generated Content, User Owned Assets)
Personal Space (Virtual Environment, Spatial Interactions, Privacy Controls)
Transactions (Financial Transactions, Commerce Security, Transaction History, Smart Contracts)
Interactions (Consent for interactions, Reportingand Moderations, Content Sharing, Social Interactions)
Experience (Custom User Experience, Quality of Service, Performance and Latency, Mind/ Body Wellness)
V User Security Architecture With Zero Trust Principles
Metaverse Applications
Metaverse Infrastructure
Metaverse Platforms
Metaverse Ecosystem
VI Conclusion

FIGURE 1. Structure of the paper.

on the numerous instances outlined in the articles [14], [15]. Details of these incidents are presented in Table 1. The highlighted incidents emphasize the importance of establishing a virtual environment that is secure, respectful, and inclusive for all users. Tracking incidents in virtual reality can be challenging and often goes unreported due to the nature of real-time interactions. The absence of efficient reporting mechanisms delays the timely resolution of incidents,

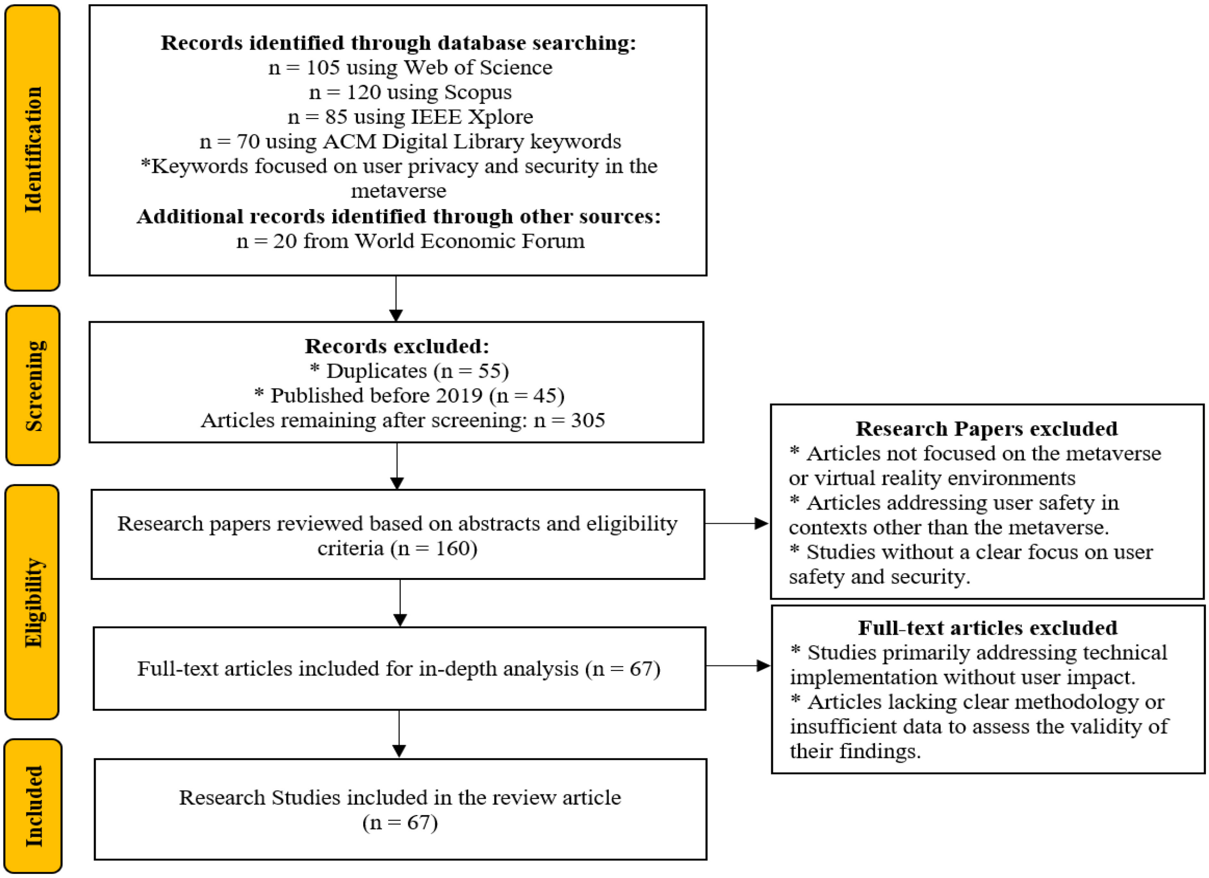
Identification
Records identified through database searching:
n = 105 using Web of Science
n = 120 using Scopus
n = 85 using IEEE Xplore
n = 70 using ACM Digital Library keywords
*Keywords focused on user privacy and security in the metaverse
Additional records identified through other sources:
n = 20 from World Economic Forum
Screening
Records excluded:
* Duplicates (n = 55)
* Published before 2019 (n = 45)
Articles remaining after screening: n = 305
Eligibility
Research papers reviewed based on abstracts and eligibility criteria (n = 160)
Research Papers excluded
* Articles not focused on the metaverse or virtual reality environments
* Articles addressing user safety in contexts other than the metaverse.
* Studies without a clear focus on user safety and security.
Full-text articles included for in-depth analysis (n = 67)
Full-text articles excluded
* Studies primarily addressing technical implementation without user impact.
* Articles lacking clear methodology or insufficient data to assess the validity of their findings.
Included
Research Studies included in the review article (n = 67)

FIGURE 2. Systematic selection of research studies for user safety and security analysis in the Metaverse.

thereby allowing the unchecked continuation of toxic behavior.

The case studies analyzed in [13] and [14] reveal a troubling pattern of harassment, toxic behavior, and a lack of accountability within virtual environments. Incidents of virtual groping and sexually suggestive gestures, alongside offenders dismissing their responsibilities, are profoundly disturbing. These incidents highlight the urgent need for clearly defined norms of conduct and a greater emphasis on user safety and privacy. The widespread occurrence of abuse and threats within VRChat, especially those targeting minors, further depicts the severe risks posed by inadequate moderation and insufficient protective measures. The necessity for strong content filtering and age-specific protection is demonstrated by incidents involving minors being exposed to explicit content. In such incidents, improving the reporting mechanisms and enforcing stringent content regulation should be pursued as means of fostering safety, responsibility, fairness, and inclusiveness in the virtual environment.

Users can buy virtual goods in the virtual worlds which are increasingly becoming prime targets for cybercrime. Scammers use phishing attacks to mimic real Metaverse platforms and trick users into giving up their login details, resulting in the theft of property and cryptocurrency. There was a reported incident involving a nurse and a fitness trainer who spent their assets on platforms such as The Sandbox and Decentraland [15]. Unfortunately, they were tricked by phishing links and, upon entering their information on these fraudulent websites, lost access to their digital wallets and saw their virtual investments vanish. This situation highlights the dangers of phishing in the Metaverse. The unfamiliarity of this environment makes it harder for users to spot malicious behavior. Moreover, the existing setup of the Metaverse complicates efforts to regain stolen assets, leaving victims exposed to risk.

The threat of sexual exploitation and sexual abuse of children, both offline and online, is a serious challenge for global society. Online grooming activities on social media and online gaming platforms have seen a steep increase, as well as the production of self-generated material displaying younger children. The Metaverse, a concept of the Internet where the physical and digital worlds blend together, has caught the attention of individuals who engage in the exploitation of children. This has led to an increase in victimization. The development of technologies such as virtual reality (VR) and augmented reality (AR) has brought the Metaverse closer to reality, posing a potential risk of online child sexual exploitation and abuse adopting similar technologies. More research and actions are necessary to prevent and address the issue of exploitation and abuse of children within the realm of emerging technologies [16].

TABLE 1. Analyzing incidents from case studies.

Incident	Description	Impact
Virtual harassment: Groping and explicit gestures	In a virtual lobby, the avatar of one player engaged in explicit gestures and groped the avatar of another player [13].	Causes psychological distress and undermines respect and safety within the virtual environment.
Lack of accountability	During a confrontation in the game, the offender evaded responsibility by citing the virtual nature of the situation [14].	Perpetuates toxic behavior, hinders the creation of a respectful and inclusive community.
Toxic behavior in VRChat	Within the virtual reality game VRChat, there was a prevalent occurrence of violations of the terms of service and instances of abuse [14].	Challenges the maintenance of a safe and respectful environment for all users.
Sexual and violent threats targeting minors in VRChat	Avatars utilized by users in the VRChat game were found to be engaging in inappropriate behavior, specifically making sexual and violent threats, some of which involved minors [14].	Highlights the urgent need for age verification and robust measures to protect children.
Exposure of a minor to explicit content in VRChat	The user engaged in the act of displaying explicit content to a minor within the VRChat game [14].	Emphasizes the necessity of strong content moderation and age-appropriate safeguards.
Metaverse phishing scams	Cybercriminals create phishing websites that imitate legitimate Metaverse platforms, often appearing in search results [15].	Results in the theft of virtual land, cryptocurrency, and other digital assets.
Kasha Desrosiers' investment loss	A nurse invested in The Sandbox and SuperWorld. Clicking on a phishing link resulted in theft from her MetaMask wallet [15].	The loss of $16,000 undermines trust in the Metaverse economy and highlights financial vulnerability.
Tracy Carlinsky's investment loss	A fitness instructor invests in The Sandbox. Clicks on phishing links resulted in a loss of assets shortly after purchase [15].	Loss of $20,000 in virtual land demonstrates the speed and severity with which Metaverse investors can be targeted.

In a report by Pluto VR and The Extended Mind, it was found that 36% male users and 49% female users have faced instances of sexual harassment while engaging in virtual reality (VR) environments. This issue of misconduct within VR is not recent but has been an ongoing concern since VR technologies became commercially available. The immersive quality of VR, which can engage the senses, intensifies the impact of these assaults on victims. The anonymity and ability of users to deny responsibility in the realm may embolden some male users to express hostility towards women. Determining the boundaries of these offenses is complex as they blur the distinction between "real" assault and harassment. Typically, developers only implement measures post-incident rather than proactively creating secure virtual spaces [17].

The interconnected nature of the Metaverse highlights numerous security breaches that can affect users both emotionally (by causing distress) and financially (through theft of assets). Thus, addressing these emerging challenges is crucial. The following sections will explore these security issues and highlight the collaborative efforts required to protect users within the Metaverse. Figure 3 explains the various types of security issues that exist in present virtual environments.

III. SECURITY ISSUES RELATED TO INDIVIDUAL USERS IN THE METAVERSE

The Metaverse faces numerous user safety and security challenges, including identity theft, data privacy concerns, the spread of malware and viruses, theft of virtual property, lack of regulation, instances of cyberbullying, and the presence of inappropriate content, as illustrated in Figure 3. Each of these issues poses distinct risks to users and to the integrity of the virtual space.

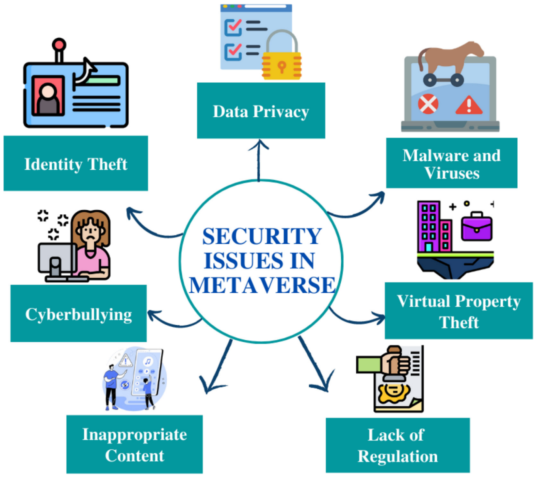

FIGURE 3. Security issues related to individual users.

1) USER'S IDENTITY THEFT

In the Metaverse, digital identities are crucial for interaction and access, making identity theft a significant threat. Hackers can exploit the anonymity and lack of centralized regulation by impersonating users and stealing usernames, passwords,

TABLE 2. Data privacy factors in the metaverse.

Factor	Description & Importance	Challenges
User consent	Users control what data is collected, how it is used, and who can access it. Essential for privacy and trust [23].	Ensuring choices are clear and settings are easy to find.
Data encryption	Protects data in transit and storage using strong encryption. Prevents unauthorized access even in case of a breach [24].	Managing encryption keys; the potential impact on performance.
Anonymization	Options for using pseudonyms and limiting personal details allow users to participate without revealing their identities [25].	Balancing privacy with the requirements of some experiences.
User control	Users can edit, delete, and restrict access to their data. User-friendly interfaces are key for accessibility [26].	Ensuring clear controls while preventing accidental exposure.
Transparency	Clear policies and explanations about how data is used [24] promote trust and enable informed user choices.	Avoiding overly complex language while providing details.
Compliance	Following relevant data privacy laws. A privacy-by-design approach prioritizes protection from the start [27].	Complexity of regulations, especially across borders.
Minimization	Collects only the minimum data needed for the service [28]. Reduces privacy risks and promotes ethical data use.	Defining 'minimum' can change and needs to be updated regularly.

and other sensitive data, ultimately compromising their digital assets and virtual presence [18]. This form of cybercrime introduces several unique challenges in the Metaverse:

1) Challenges in verifying user identities.
2) Risk of impersonation and spoofing.
3) Lack of comprehensive legal frameworks and enforcement mechanisms [19].

Verifying a person's true identity within a purely virtual realm poses unique challenges compared to the real world, where physical forms of identification exist. This makes it easier for malicious entities to operate under false identities. The Metaverse often encourages a degree of anonymity [5], disconnecting real-world identities from digital avatars. This makes traditional Know Your Customer (KYC) processes (used in banking and other sectors) difficult to implement [20]. Moreover, while biometric identification (facial recognition, fingerprints, etc.) could offer a solution, it faces threats from deepfakes and other spoofing technologies. Finding the right balance between user privacy and verification is crucial, as strict identity verification could clash with the desire for some user anonymity [21].

Impersonating others for the sake of manipulative relationships or to gain trust and extract information is a common social engineering tactic online. This technique has also extended to virtual worlds. Here, deepfakes and AI-generated videos and audio can convincingly mimic real people, making it harder for users to identify fraudulent profiles or content. In cases where verification becomes standard on some virtual platforms but not others, attackers could target those with weaker systems. Attackers can use those 'verified' fake profiles to gain trust elsewhere [22].

2) USER'S DATA PRIVACY

The evolution of avatars, social connections, and immersive encounters in the Metaverse necessitates the collection of extensive user data, which may include potentially sensitive information such as biometric traces, location data, and behavioral patterns. Failure to handle this data with care could expose users to significant privacy threats. Such data exposure could potentially lead to privacy risks such as targeted marketing, unauthorized profiling, and even the threat of extortion. It is essential to prioritize addressing these privacy concerns in order to protect data confidentiality in this evolving environment, as outlined in the accompanying Table 2.

3) MALWARE AND VIRUSES

Malware and viruses can damage virtual spaces and steal sensitive information. These malicious entities can spread easily within the Metaverse and negatively impact user experiences in these virtual worlds. Malicious files, links, phishing scams, and other social engineering strategies are common methods for gaining access to the Metaverse [22]. Attackers can steal NFTs (Non-Fungible Tokens) or in-game items, which can represent real-world money or hold sentimental value. They can also manipulate virtual currencies and disrupt economies within the Metaverse [29].

4) VIRTUAL PROPERTY THEFT

In the Metaverse, digital avatars possess virtual currency and other digital assets. These assets also have real value, making them targets for cyber attackers since they can be exchanged, purchased, and sold. Thus, to safeguard against the theft of these digital possessions in the Metaverse, it is vital to consider the following:

Authentication: Enforcing robust authentication measures is essential to stop virtual property theft. Platforms must require users to use passwords and multi-factor authentication to prevent unauthorized access to their accounts [30].

Secure Transactions: To prevent the theft of assets, it is crucial to ensure that networks are secure. Platforms must prioritize the security and encryption of all connections and enable users to verify these connections as part of their requirements [31].

User Education: Educating users is necessary in preventing virtual property theft. Platforms should offer training and support to empower users in recognizing risks such as phishing schemes and social manipulation tactics [32], [33], [34].

Digital Asset Management: Proper management of assets is essential for ensuring their security. Platforms should equip users with tools for backing up, storing, and accessing their assets to ensure management and protection [35], [36].

5) CYBERBULLYING IN THE METAVERSE

Cyberbullying is a serious problem that can result in both psychological and physical harm. It refers to the use of technology to harass or embarrass someone [37]. In Metaverse bullying situations, the impact can become even more transformative than in traditional online bullying [20]. People can experience a stronger sense of presence and potential real-world harassment situations in which they might find themselves physically unsafe.

Here are some examples of how cyberbullying happens in the virtual world:

1) Verbal Abuse: Derogatory comments, threats, and hateful language may come through voice chat or typed messages [38].
2) Immersive Harassment: Avatars may intimidate individuals by stalking or surrounding them with harmful virtual objects. Users' deepfake videos in compromising positions may be created [39].
3) Exclusion and Social Isolation: Groups can form to exclude others and then create a hostile virtual environment [40].
4) Identity Theft and Impersonation: This involves malicious acts such as stealing identities or impersonating others [41].

In the Metaverse, the ease of creating multiple avatars allows bullies to harass others anonymously and evade detection. The Metaverse's sensory capabilities can be utilized to target victims in new ways. This involves bombarding users with virtual objects, loud noises, or creating disturbing virtual scenarios. If the Metaverse connects with actual user data then bullies could use this information to target individuals in a more personalized manner. It is relatively easy to gather data on a user's location, appearance, or interests to carry out a more powerful attack [38].

6) EXPOSURE TO INAPPROPRIATE CONTENT

The Metaverse's vast and expanding virtual landscape offers freedom that comes with the risk of encountering inappropriate content. Specific concerns are as follows:

1) Virtual worlds feature content from numerous creators, making it difficult to enforce content guidelines [42].
2) The immersive nature of the Metaverse can amplify the emotional effects of inappropriate content, particularly affecting younger users in virtual physical settings [43].
3) Effective age verification methods are often absent in virtual worlds, increasing exposure risks for minors [44].
4) Some creators may be motivated to produce or share inappropriate content to attract attention and generate revenue, negatively impacting the community [45].

TABLE 3. Regulation types and their impact.

Regulation Type	Impact
Increased risks	Increased likelihood of security threats and privacy violations.
Security threats	Exposure to cyber-attacks, scams, and frauds.
Privacy violations	Unwanted sharing of personal data, loss of privacy.
Unfair competition	Inequitable business practices, lack of a level playing field.
Monopolies	Dominance of a single entity or platform, reduced competition.
Discrimination	Bias against certain groups or individuals.
Inconsistent standards	Lack of uniformity in technical and operational standards.
Interoperability issues	Difficulty in connecting and exchanging data between different platforms.
Fragmentation	Division and isolation of communities and markets.

7) LACK OF REGULATION

The accelerating growth of the Metaverse has triggered many issues regarding the lack of regulation in virtual worlds. Currently, there is no clear regulatory framework in place, which may lead to the dissemination of unethical content, cyberbullying, and other inappropriate behaviors. These issues can have lasting effects on children's mental health [46] and may leave individuals emotionally and physically harmed, with the responsible person remaining unaccountable [47]. The Metaverse without regulation could lead to a place that would have an immense number of negative impacts on users at psychological levels. It can also raise ethical issues in virtual worlds. This can be illustrated with the example in which the user participates in actions that would certainly violate copyright laws, intellectual property rights, and various legal matters. Table 3 presents the impact of different regulation types in virtual worlds.

The section on types of user security issues in the Metaverse has addressed emerging concerns regarding user safety in virtual worlds. Among the types discussed, user identity theft and decentralized identity management have particularly gained significant attention within the research community.

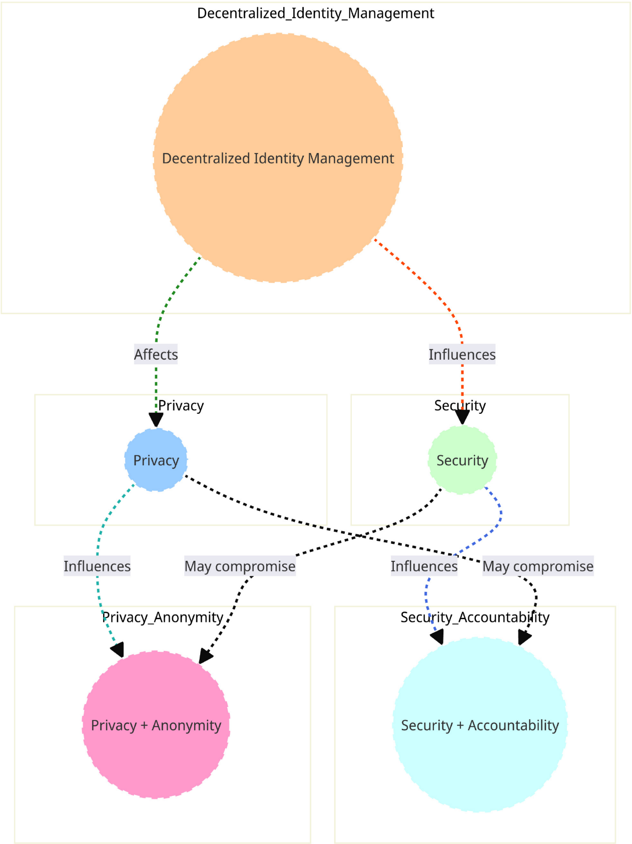

FIGURE 4. Interplay of Decentralized Identity Management (DIDM), user security and privacy.

A. INTERPLAY OF DIDM, USER SECURITY AND PRIVACY IN THE METAVERSE

Figure 4 explains the relationships and interplay between different components in a Decentralized Identity Management (DIDM) system. The key concepts in decentralized identity management are Security, Privacy, Accountability, and Anonymity. These concepts are closely interrelated and have a significant influence on each other.

The DIDM module represents the management of identities in a decentralized manner. It ensures a secure and private exchange of information within a virtual environment. We require security measures to protect the integrity, confidentiality, and availability of data and resources in virtual worlds. The privacy aspect involves protecting users' personal information and address how user data is collected, used, and shared in the Metaverse.

The security and accountability module combines security measures with accountability mechanisms, such as audit trails or logging. With this module, Metaverse users can be held responsible for their actions. This module represents the need to balance security measures with appropriate levels of accountability, ensuring responsible management of identities. This concept is influenced by the Security aspect.

The privacy and anonymity module augments the privacy measures while simultaneously providing anonymity as a user interacts with other entities and objects. It highlights the importance of preserving user anonymity alongside privacy protections.

Security measures impact the aspects of privacy and anonymity. These privacy measures can also compromise Security and Accountability. We can clearly observe the trade-offs when users try to prioritize one aspect (security or privacy) over the other.

Figure 4 showcases the challenges involved in ascertaining identities and holding users accountable when using third-party identity and avatar management systems. If user privacy is prioritized, then accountability declines; conversely, if accountability is prioritized, then user privacy is impacted. Users seek freedom and prefer that the platform does not snoop on their activities within the Metaverse. Hence, building a privacy-preserving system that reins in violations of platform usage and conduct is non-trivial.

B. TAXONOMY FOR USER SECURITY AND PRIVACY IN THE METAVERSE

Figure 5 presents a comprehensive taxonomy for the key aspects of user security and privacy within the Metaverse. This taxonomy combines critical elements of user privacy and also integrates the principles of Zero Trust Architecture (ZTA). It sets up a system to safeguard the user's interactions within virtual environments. Within these realms, it is essential to have methods for confirming the identities of users through biometrics and multi-factor authentication (MFA). It is key to ensure that only approved individuals can enter [18]. Role-based authorization models help us to fine-tune access control. If we want to protect devices from threats, then endpoint security measures must be incorporated, which include antivirus and anti-malware solutions [25]. It is also important to patch security vulnerabilities. In order to ensure the trustworthiness of devices, we can conduct continuous assessments. Health checking and compliance status are also done repeatedly [47], [48].

Data security is enhanced when employing end-to-end encryption mechanisms for information, whether it is stored or in transit. Precautions are taken to prevent access and data breaches [49] and it is advisable to classify data based on its sensitivity level in order to implement context-based access controls [50]. Data loss prevention (DLP) tools are also utilized to classify and safeguard data [51].

Securing the Metaverse network involves dividing it into segments to boost security. Various methods like setting up firewall solutions and intrusion detection are used for this purpose [52]. These tools help us to monitor and control network traffic well by identifying any unauthorized access attempts.

Security protocols such as access control lists (ACLs) and firewalls will help in imposing security guidelines. Policy enforcement points (PEPs) are also significant to safeguard these policies. This framework requires threat detection and incident response capabilities [53]. The use of machine learning and artificial intelligence (AI) techniques can further enhance real-time threat detection capabilities.

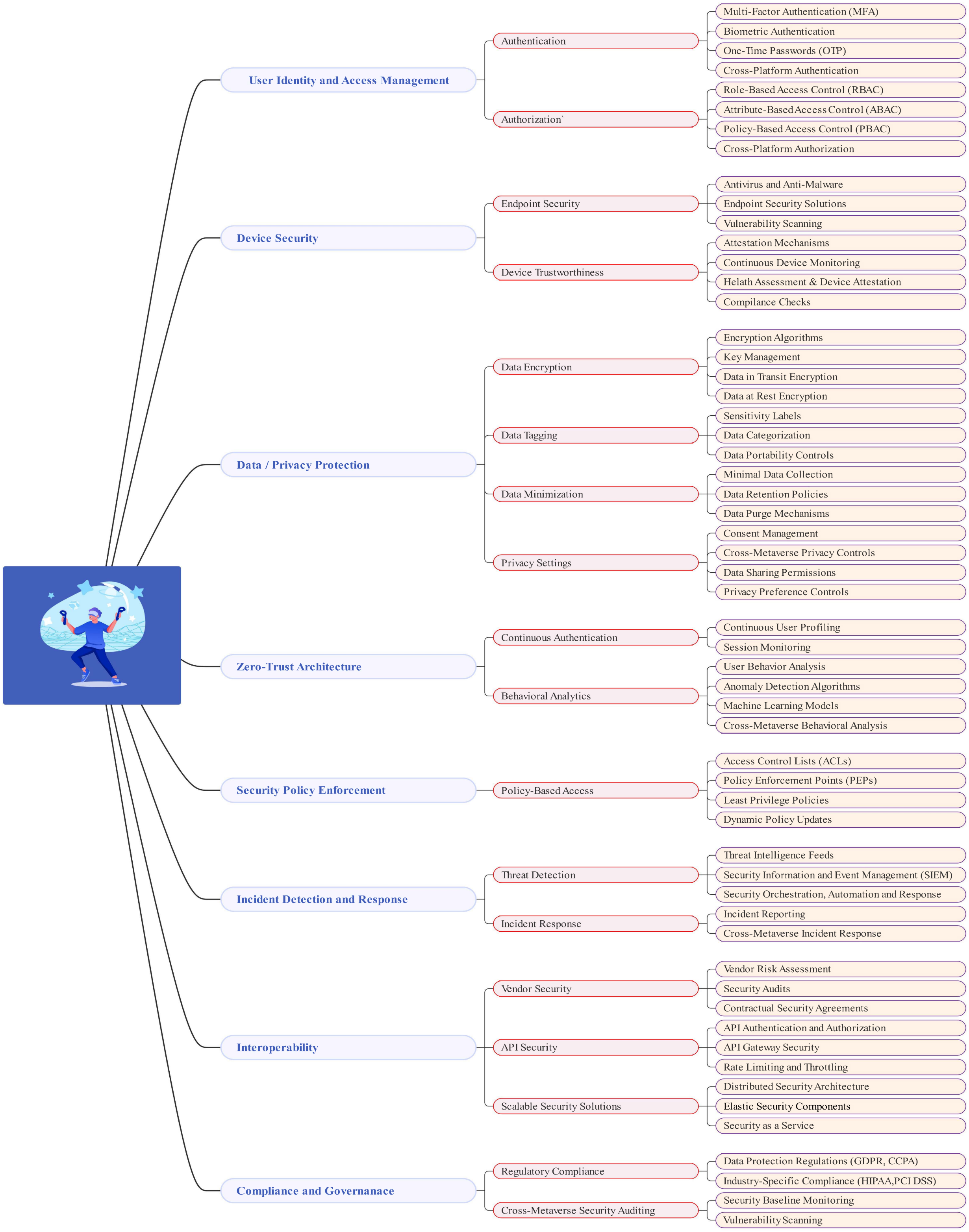
User Identity and Access Management
Authentication
Multi-Factor Authentication (MFA)
Biometric Authentication
One-Time Passwords (OTP)
Cross-Platform Authentication
Authorization`
Role-Based Access Control (RBAC)
Attribute-Based Access Control (ABAC)
Policy-Based Access Control (PBAC)
Cross-Platform Authorization
Device Security
Endpoint Security
Antivirus and Anti-Malware
Endpoint Security Solutions
Vulnerability Scanning
Device Trustworthiness
Attestation Mechanisms
Continuous Device Monitoring
Helath Assessment & Device Attestation
Compilance Checks
Data / Privacy Protection
Data Encryption
Encryption Algorithms
Key Management
Data in Transit Encryption
Data at Rest Encryption
Data Tagging
Sensitivity Labels
Data Categorization
Data Portability Controls
Data Minimization
Minimal Data Collection
Data Retention Policies
Data Purge Mechanisms
Privacy Settings
Consent Management
Cross-Metaverse Privacy Controls
Data Sharing Permissions
Privacy Preference Controls
Zero-Trust Architecture
Continuous Authentication
Continuous User Profiling
Session Monitoring
Behavioral Analytics
User Behavior Analysis
Anomaly Detection Algorithms
Machine Learning Models
Cross-Metaverse Behavioral Analysis
Security Policy Enforcement
Policy-Based Access
Access Control Lists (ACLs)
Policy Enforcement Points (PEPs)
Least Privilege Policies
Dynamic Policy Updates
Incident Detection and Response
Threat Detection
Threat Intelligence Feeds
Security Information and Event Management (SIEM)
Security Orchestration, Automation and Response
Incident Response
Incident Reporting
Cross-Metaverse Incident Response
Interoperability
Vendor Security
Vendor Risk Assessment
Security Audits
Contractual Security Agreements
API Security
API Authentication and Authorization
API Gateway Security
Rate Limiting and Throttling
Scalable Security Solutions
Distributed Security Architecture
Elastic Security Components
Security as a Service
Compliance and Governanace
Regulatory Compliance
Data Protection Regulations (GDPR, CCPA)
Industry-Specific Compliance (HIPAA,PCI DSS)
Cross-Metaverse Security Auditing
Security Baseline Monitoring
Vulnerability Scanning

FIGURE 5. Taxonomy for user privacy and security in the metaverse.

Security orchestration, automation and response (SOAR) systems aids in automating incident responses [54] by coordinating actions and automating workflows.

Interoperability between virtual worlds can be achieved using application programming interfaces (APIs) and authentication protocols [23]. In this taxonomy, secure integration depends on rate-limiting practices and API security measures. Further compliance with data protection regulations such as GDPR (General Data Protection Regulation) and industry-specific standards such as HIPAA (Healthcare Insurance Portability and Accountability Act) and PCI DSS (Payment Card Industry Data Security Standard) is maintained through regular security audits and vulnerability scanning [55].

IV. CURRENT STATE OF ART IN USER SECURITY AND PRIVACY

The Metaverse incorporates everything from virtual reality to augmented reality and immersive Internet experiences [56]. It has become the subject of interest for many professionals, thinkers, and researchers from various fields. Through their efforts, they have highlighted various challenges related to user safety and security in virtual worlds.

The compiled literature review outlined in the subsequent section discusses various articles published from 2020 to 2024 on user safety and security issues in virtual worlds. Researchers have examined various technological advancements in the Metaverse [57] and scrutinized emerging concerns regarding user security [49]. Significant attention has also been given to user authentication, the detection and mitigation of Distributed Denial of Service (DDoS) attacks [41], user identity management, digital trust frameworks, identification processes, accessibility considerations, and the types of immersive interactions within the social Virtual Reality (VR) landscape [31].

One key area of investigation has been the exploration of distributed Metaverse architectures, where researchers have focused on designing systems that can operate seamlessly across distributed networks [51]. Moreover, the integration of emerging technologies, such as blockchain into the Metaverse ecosystem, is a subject of keen interest that offers potential solutions to enhance user security and privacy protocols [25], [58].

A cross-chain transaction model for digital content and asset interaction in the Metaverse has been implemented [59]. It enhances security through cryptographic methods and employs a notary mechanism based on HTLC. However, these security measures still need to be further enhanced for cost-effectiveness. The design and analysis of the TCID framework, developed in collaboration with the Dutch government, satisfies seven functional requirements [60]. It ensures desirable properties of control, credibility, and network-level anonymity for users' identity data.

Many researchers have also assessed the effectiveness and meaningfulness of the prevalent "Notice and Consent" approach, especially in the emerging virtual world [61]. They have explored and proposed enhancements to the traditional "Notice and Consent" approach and suggested alternative frameworks to traditional "Terms and conditions" that aligned with evolving regulatory environments [62].

The Metaverse is constantly evolving due to advancements in technology and shifts in user behavior. This research aims to understand the challenges within the Metaverse, improving our capabilities and paving the way for a more secure digital future [12], [54]. The interdisciplinary nature of these studies acknowledges that addressing the complexities of this realm requires a multifaceted approach.

Table 4 provides a comprehensive overview of research contributions concerning user security and privacy in the Metaverse. It summarizes the authors, years of publication, methodologies employed, research objectives, limitations addressed, and potential future directions within this domain. User safety concerns in various fields have been analyzed in this research contribution table.

A. DIMENSIONS OF USER SECURITY AND PRIVACY IN VIRTUAL WORLDS

In the growing world of the Metaverse, user security and privacy have become focal points. Within these aspects, 'Data' stands as an element covering components essential for protecting user data and creating a safe virtual space [41]. Figure 6 depicts the 5 major dimensions of user security and privacy in virtual worlds. These dimensions are types of data, personal space, transaction types, types of user interactions, and user experience. These dimensions have an impact on all entities involved in virtual worlds.

The personal space dimension explores privacy controls, spatial interactions, and types of virtual environments. The transaction dimension is very crucial, as it deals with all types of financial and commerce-based activities in virtual worlds. User preference, custom user experiences, and consent for interactions also play significant roles in implementing the best security policies for the Metaverse.

User Preferences, Activities, and Personal Information: User preferences play a role in shaping the Metaverse. They involve a variety of options and settings that enhance the user's experience. These preferences include tasks such as choosing avatars, selecting virtual environment themes, and managing communication preferences. Safeguarding user preferences is vital for upholding privacy. It ensures that individuals retain authority over their identities and interactions. Privacy controls empower users to specify who can view their preferences, allowing for personalized experiences while safeguarding choices from scrutiny [39]. User engagement within the Metaverse involves a range of activities such as browsing, interacting with objects, and taking part in events. As users engage in these activities, they generate data known as 'user activity data.' Safeguarding this data is crucial for maintaining privacy and ensuring security. By employing encryption techniques to protect this data, Metaverse platforms can assure users that their actions within the realm remain confidential and well-protected against unauthorized access [5]. User profile information includes names, ages, genders, locations, and other identifiable specifics. In the virtual world, people often exchange data to personalize their personas. However, it is crucial to prioritize safeguarding this data. Strong encryption techniques help keep user information private and out of

TABLE 4. Research contributions on user security and privacy.

Paper	Year	Methodology	Objectives	Limitations	Future Scope
H. Hadan [43]	2024	Survey of 464 XR users and 18 scenarios assessing user awareness, concerns, and coping strategies related to XR data	Understand user perceptions of privacy in XR environments, identify factors influencing these perceptions (data type, sensitivity, etc.), explore user awareness of XR data collection capabilities, and examine user strategies for protecting their privacy in XR	User awareness shows limited understanding of XR data collection, potentially impacting reported strategies. The study focused on user perceptions, not exploring developers' practices, and there is potential for self-reporting bias in survey responses.	Develop educational materials to raise user awareness of XR data privacy, design user-friendly privacy control interfaces for XR environments, investigate and promote transparent data collection practices within the XR industry.
D. Kumarapeli [45]	2024	VR user studies with data collection on user behavior across sessions and activities, employ machine learning to analyze user identification accuracy under normal and obfuscated behavior conditions, and investigate the impact of physical user characteristics on identification.	Assess privacy risks of VR behavioral identification (machine learning), evaluate user identification accuracy across VR sessions (83% same activity, 80% different activity), analyze the effectiveness of user behavior alteration (78% accuracy), and investigate the influence of physical characteristics on identification.	Limited user study participant pool, controlled VR environment may not reflect real-world usage patterns, and focuses on technical identification accuracy, neglecting user privacy perception.	Develop privacy-preserving VR authentication methods, explore alternative VR user identification techniques, and investigate user attitudes towards VR data collection and privacy concerns.
C. Warin [63]	2024	Review XR privacy threats and existing solutions, prototype user privacy panel, and cross-platform privacy API, user studies for usability and effectiveness.	Increase user awareness of XR privacy risks, empower users to control XR features with a privacy panel, develop cross-platform API for privacy-preserving XR data, evaluate solution's usability and privacy protection effectiveness.	Prototype stage - needs user testing and refinement, focuses on user control and may not address all threats, relies on user studies, real-world use might differ.	Refine privacy panel based on user feedback, integrate API with XR development platforms, explore advanced XR data privacy techniques, and analyze long-term impact on user behavior and XR privacy.
S. Tariq [38]	2023	Literature review on deepfakes, Metaverse security, and CIA triad	Analyze deepfake impersonation in Metaverse (gaming, meetings, offices), discuss security impacts on CIA triad and explore darkverse, digital cloning, and Metaverse privacy/regulation challenges.	New technology, evolving security, limited use case focus, and scarce real-world Metaverse data.	Develop deepfake detection/mitigation framework, explore AI for combating deepfakes, analyze legal/ethical implications of regulation, and investigate social/psychological impacts on user behavior.
B. Gupta [5]	2023	The research uses a Digital Twin framework with semantic technologies and simulation environments, employing support vector machine learning for DDoS attack identification and detection in IoT networks.	Leverage Digital Twin for effective Metaverse entity management and achieve 93.25 percent accuracy in DDoS attack identification and mitigation.	The study primarily focuses on DDoS attack detection and is yet to be tested with a broader range of real-world datasets to ascertain its robustness across various scenarios.	The framework provides a promising base for integrating advanced machine learning techniques into the Metaverse and suggests further exploration in diverse datasets and cybersecurity applications.

(Continued)

reach for unauthorized individuals [72]. Moreover, it is important to incorporate consent tools that enable users to manage how their details are shared with others.

User-Generated Content: In the Metaverse, users can freely showcase their creativity through crafting avatars, virtual objects, and environments. This user-generated content (UGC) contributes to enriching the realm [73]. To safeguard UGC, it is crucial to set up data management guidelines [6]. These guidelines include organizing content based on its sensitivity and enforcing access restrictions. Moreover, establishing ownership rights enables users to retain authority over their creations [18].

TABLE 4. **(Continued.) Research contributions on user security and privacy.**

Y. Huang [41]	2023	Introduction of four key Metaverse characteristics, surveying Metaverse progress, applications, and investigating security, privacy issues, and future concerns.	Provide an overview of Metaverse characteristics, progress, security and privacy concerns, and societal implications.	Challenges include defining the Metaverse, limited scope tied to current progress, unpredictability of security and privacy issues, and a lack of comprehensive real-world data for long-term societal impact assessment.	Advance Metaverse standardization, security, and societal understanding through continuous updates, in-depth studies, and long-term monitoring.
R. Cheng [39]	2023	Focuses on immersive interaction in social VR as a precursor to the Metaverse.	Develop a research agenda for zero-trust user authentication in social VR.	Acknowledges challenges such as attacks on user authentication and impersonation.	Investigate biometrics for continuous VR user authentication, explore federated learning for privacy, enhance multimodal data accuracy, and aim for adaptable VR authentication for improved usability.
G. Kang [27]	2023	Analysis of existing Metaverse studies and international standards	Propose security and privacy requirements for secure Metaverse applications	Lack of Metaverse-specific security and privacy studies	Implement and validate proposed security and privacy requirements.
C. Chetan [18]	2023	Comprehensive analysis of technology advancements and security concerns in Metaverse authentication, identification, accessibility, and potential for businesses.	Identify limitations of traditional security methods and propose effective alternatives, including enhanced authentication using hashing, encryption, and biometric data.	Insufficient focus on security and privacy, vulnerable traditional methods, challenges in data handling, and identity theft risks.	Enhance security and privacy measures through advanced methods, robust data handling, user authentication mechanisms, and encryption advancements.
Y. Wang [57]	2023	The distributed Metaverse exhibits a revolutionary architectural design, characterized by the presence of three interconnected worlds, which facilitate various forms of interactions.	This study aims to examine the innovative distributed Metaverse architecture and gain a comprehensive understanding of its fundamental properties, particularly in relation to ternary-world interactions.	Challenges in scalability and interoperability due to the intrinsic characteristics of the Metaverse, such as immersive realism, hyper-spatiotemporality, sustainability, and heterogeneity.	Explore and develop tailored security and privacy countermeasures for the Metaverse, focusing on addressing challenges and enhancing protection against privacy invasions and security breaches.
National Security Agency [64]	2023	Prioritizes enhancing ICAM to counter cyberattacks, especially those involving compromised credentials, and integrates it into a comprehensive Zero Trust framework.	Provide recommendations for enhancing ICAM capabilities to mitigate cyberattacks and emphasize aligning with a mature ZT framework integrating controls across seven pillars.	Implementations require careful planning and face challenges aligning with Zero Trust designs, especially regarding constant re-authentication in certain scenarios.	Advance and strengthen FICAM roadmap for mature Zero Trust implementation, enhancing tools and processes for threat resistance and promoting robust Identity, Credential, and Access Management.
M. Xu [61]	2023	Trustless architecture using blockchain and OTCE technique based on trust evaluation.	Optimize resource integration and allocation through hardware and software consolidation, ensuring strong security in the Metaverse.	Requires extensive testing for real-world applicability.	Integrate AI for dynamic trust evaluation, and refine models for more efficient and accurate assessments.

(Continued)

User-Owned Assets: In the Metaverse, users own assets such as Non-Fungible Tokens (NFTs) and digital tokens, which hold real-world value and need protection measures in place [6]. Advanced cryptographic techniques are used to secure wallets and transactions to ensure the safety of user-owned assets. The use of technology in the Metaverse allows for ownership records that enable users to monitor and authenticate their assets effectively [7], [61], [74]. By focusing on user preferences, activities, personal information, user-generated content, and asset ownership, Metaverse

TABLE 4. (Continued.) Research contributions on user security and privacy.

C. Li [60]	2023	Analyzing Metaverse potential, collaborating with Accenture and World Economic Forum, and defining a building initiative.	Emphasize the impact, opportunities, social implications, and ensure economic and social progress in the Metaverse.	Limited exploration of potential risks and narrow focus on social aspects, primarily emphasizing Metaverse value creation.	Further research is needed to balance positive and negative outcomes, conduct longitudinal studies on challenges and their mitigation strategies. Additionally, a dedicated governance track focusing on privacy and safety should be implemented, gathering insights from a global, multi-stakeholder working group.
T. Huynh-The [65]	2023	Survey on blockchain technology in the Metaverse.	Introduce blockchain and its Metaverse applications, emphasizing reasons for adoption.	Limited to specific blockchain aspects in the Metaverse: data handling, interoperability, and privacy.	Explore broader blockchain applications within the Metaverse, address challenges through enhanced integration of blockchain technologies, investigate blockchain's impact on emerging technologies, and propose holistic approaches for Metaverse development.
Y. Ren [66]	2023	Introduce HCNCT, a cross-chain transaction model for digital content and asset interaction in the Metaverse.	Enhance security through cryptographic methods, and employ a notary mechanism based on HTLC.	Additional costs due to notary group inclusion.	Optimize the notary mechanism for cost-effectiveness, further enhancing security measures.
H. Wang [67]	2023	Multi-Identifier Management and Resolution	Design and implement MIS for Metaverse, ensure registration, resolution, and inter-translation functions.	Limited testing scenarios.	Explore integration with emerging blockchain technologies.
C. Li [68]	2023	Addressing various aspects of the Metaverse: impact analysis, human-centered design, data privacy, user engagement, child protection, literacy promotion, and global cooperation.	Promote understanding, prioritize safety, ensure trust, design user-friendly interactions, protect vulnerable groups, empower through education, and foster collaboration for the Metaverse.	Addressing privacy and safety challenges, integrating realities, ensuring data privacy, overcoming onboarding barriers, implementing child safety measures, enhancing educational efforts, and fostering collaboration are essential in the Metaverse.	Promote safety, privacy, inclusivity, child protection, literacy, and global cooperation in the Metaverse.
P. Cin [69]	2022	The research primarily employed an interdisciplinary approach, drawing expertise from privacy, cybersecurity, technology ethics, law, and other relevant fields. Over 60 experts and leaders in the digital trust community contributed their insights.	Digital trust safeguards stakeholder interests and aligns with societal expectations. A ”trust framework” assists technology leaders in setting objectives and values for security, accountability, inclusivity, ethics, and responsible usage.	The report primarily focused on immediate stakeholders in technology, potentially limiting a comprehensive exploration of digital trust. While outlining shared goals and values, it might not cover all nuances and perspectives on digital trust comprehensively.	Future exploration should encompass the involvement and obligations of stakeholders beyond immediate technology development, contributing to a more comprehensive implementation of digital trust.

(Continued)

platforms create an environment where individuals have control over their data, ensuring an experience for all users [41]. In this realm, individuals often find peace and opportunities for self-expression within their personalized ‘Personal Space’ tailored to meet their individual needs and preferences.

TABLE 4. (Continued.) Research contributions on user security and privacy.

B. Rawal [23]	2022	Broad evaluation of Metaverse, key elements and features, in-depth survey of Metaverse security and privacy.	Analyze Metaverse security and privacy threats, introduce Split-Metaverse architecture, highlight critical challenges in security defenses, and highlight critical challenges in privacy preservation.	High-performance client terminals and long response times, addressed issues with the Split-Metaverse architecture.	Implement an interoperable Split-protocol for improved resiliency and availability, enhance Metaverse security defenses and privacy preservation, design security and privacy countermeasures for the Metaverse, and enhance computing and communication technologies for evolved Metaverse worlds.
Z. Chen [52]	2022	Survey and analysis of Metaverse technologies, integration of existing tech for real-world mapping, analysis of current security solutions, explore unresolved Metaverse questions.	Identify security and privacy concerns, highlight regulatory needs, emphasize technological advancement.	Focus on known technologies; miss emerging risks, potential decline in user experience due to excessive regulation, governance challenges due to decentralization, balancing regulation and user experience.	Develop security measures for emerging Metaverse technologies, establish a legal framework for the Metaverse, strive for a responsible and secure Metaverse.
R. Pietro [49]	2021	Exploring the principles of the Metaverse and examining how different technological advancements can be integrated.	Providing insights into the potential opportunities and challenges posed by the Metaverse across different domains.	Acknowledging the probable threats to security and privacy and the complication of addressing them effectively.	Emphasizing the need for a multidisciplinary approach to navigate the Metaverse and uncover its full potential.
Q. Stokkink [70]	2021	Design and analysis of TCID, developed in collaboration with the Dutch government, satisfying seven functional requirements.	Ensure desirable properties of control, credibility, and network-level anonymity for users' identity data.	Latency incurred by network-level anonymization is relatively higher compared to identity data disclosure protocols but remains practical.	Broaden research focus beyond cryptographic data disclosure protocols to address performance and security concerns at the networking layer of SSI systems; enhance network-level privacy while maintaining acceptable latency; explore scalability and adoption of passport-grade SSI solutions.
A. Flanagan [71]	2020	Analysis of the digital landscape and privacy regulations, evaluation of the ‘Notice and Consent’ approach's effectiveness.	Assess the effectiveness and meaningfulness of the prevalent ”Notice and Consent” approach, especially in an increasingly digital world.	Limited understanding of data shared by users, inherent challenges in evaluating the effectiveness of the traditional ”Notice and Consent” approach, and potential biases in data analysis and interpretation.	Explore and propose enhancements to the traditional ‘Notice and Consent’ approach, research and propose alternative frameworks to traditional ”terms and conditions,” and align with evolving regulatory environments.

Virtual Environment: The core of personal space lies within the world itself, a realm where individuals shape their personas. This aspect encompasses elements such as avatars, which represent users in the Metaverse, serving as their alter egos [27]. Beyond appearances, avatars often embody user preferences, personal style, and unique abilities. Within these abodes, users find solace and privacy. These spaces can be personalized with decorations, furniture, and interactive features to allow users to express themselves fully. In the Metaverse, users have the freedom to create, possess, and interact with objects that reflect their tastes and preferences—from art collections to functional items [21].

Privacy Controls: Privacy controls act as safeguards for personal space, giving users the authority to decide who can enter their domain and what activities they are allowed to engage in [41]. Regarding access privileges, users can specify who is permitted to enter their residences or areas, varying from completely public to invitation-only. In

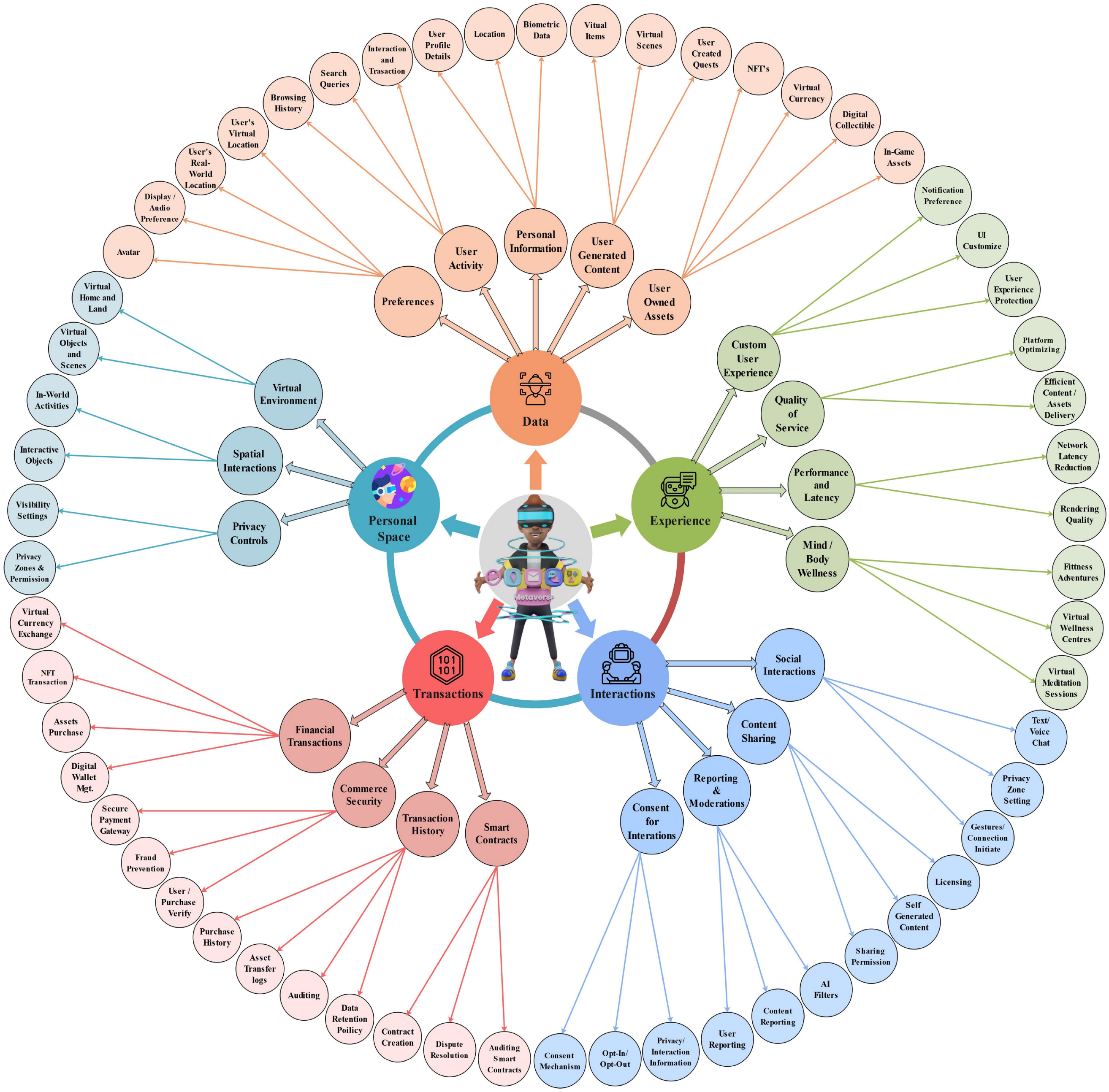

FIGURE 6. Dimensions of user security and privacy in virtual worlds.

terms of interaction limitations, users have the flexibility to define what actions others are allowed or restricted from performing within their designated space [23]. For instance, they can restrict object manipulation or impose constraints on activities. Additionally, privacy controls encompass user-generated content as well, allowing users the freedom to select individuals who can view, comment on, or interact with their works [75].

Spatial Privacy: Spatial privacy concerns emerge in the Metaverse as a result of proximity and location-dependent interactions among users [52]. Users may choose to conceal or limit their virtual whereabouts to a specific group of individuals. Utilizing spatial privacy settings can be beneficial in addressing this matter, enabling users to establish limits on how close others can come within their personal space. This holds particular significance in virtual social gatherings and activities, where proximity control is a coveted attribute [68].

Spatial Interactions: Personal Space encompasses more than just stationary settings. The topic concerns how people engage with their virtual environment and objects [6]. Users can interact with digital entities, manipulate their positions, make alterations to them, and even create new ones. Privacy settings can dictate which individuals have the authority to manipulate these objects [7]. Spatial interactions often include gestures or movements such as virtual handshakes, embraces, or nods [73].

The 'Transactions' dimension significantly influences the user experience [27]. This dimension includes a range of digital interactions, from financial transactions to smart contracts [19].

Financial Transactions: Individuals engage in buying and selling monetary tokens such as NFTs and virtual belongings in the transactional world of the Metaverse. To secure these transactions from fraud and theft, robust security measures are implemented [73]. Maintaining security involves crucial steps such as validating the identity of users participating in transactions. Moreover, encryption is used to protect data during the transmission process [42].

Commerce Security: Achieving commerce security in the Metaverse is challenging [27]. Users engage in transactions involving goods and services similar to those in the real world. To protect users' financial credentials, secure payment gateways are essential [5]. Additionally, monitoring transactions helps in the detection and prevention of fraud. Transaction verification processes check the authenticity of transactions by verifying the identities of the involved parties [73].

Transaction History: Every time a transaction occurs in the Metaverse whether it involves money or virtual items a record is generated to track that exchange. This record plays a role, in upholding transparency and security by monitoring transactions and asset movements. Managing and documenting these transaction histories is key to providing users with information about their actions. Establishing audit trails for transactions is crucial, for ensuring responsibility and traceability [73].

Smart Contracts: Smart contracts establish a model in which decentralized applications can operate in Metaverse ecosystems and across blockchains [76]. Smart contract conditions might include a wide range of characteristics. These capabilities enable greater interactivity and use-case situations within the Metaverse architecture [19]. Within this dynamic environment, ensuring user security and privacy during interactions is paramount [27].

Social Interactions: Social interactions are the heart of Metaverse. Users are busy in conversations, making friends, and building communities [22]. Maintaining privacy in interactions is essential. It's important to make sure that conversations, whether they're, through text or voice are safeguarded against listening and unauthorized intrusion. Managing friend requests securely and allowing users to control who can connect with them is also important in virtual worlds. Inclusive tools for social gestures such as hugs, handshakes, and high-fives should be used while respecting personal boundaries [77].

Content Sharing: Creating and sharing content plays an important role in the Metaverse [60]. Privacy concerns in this area pay attention to giving users the ability to determine who can view and edit their shared content by allowing them control over their creations. Implementing systems, for reporting and managing content as well as upholding a secure environment is also a key aspect to consider [50].

Reporting and Moderation: Users often encounter inappropriate content and unwanted behavior in virtual worlds. Thus, reporting and moderation mechanisms must be integrated. This will allow users to report violations and ensure prompt responses to their concerns in these environments [41]. The use of artificial intelligence for content moderation can efficiently identify and address rule violations, making this aspect crucial from the user's perspective [68].

Consent for Interactions: User consent is most significant in upholding privacy and security throughout interactions in the Metaverse. This involves implementing transparent and user-friendly procedures that allow users to grant or revoke consent during interactions and data exchanges. Users should be informed about the types of data collected under different consent options, how this data will be used [50], and be able to easily change their consent preferences as life situations and comfort levels evolve. Preferred communication channels should also be shareable with other users, who should have the choice of interaction types, such as voice chat, text, or in-world proximity. The experience component contains a range of factors that contribute to a secure, enjoyable, and personalized journey in the Metaverse [54].

User Experience Customization: In the Metaverse, users have the power to personalize their avatars, surroundings, and interfaces to match their tastes and identity. One aspect of customization involves tracking user behavior and actions to provide tailored content and recommendations [57]. The second aspect involves employing AI-driven algorithms to predict user preferences and enhance their Metaverse adventure [54].

Quality of Service: Ensuring optimal performance of Metaverse systems is crucial, necessitating the reduction of lag and latency to achieve seamless and efficient operations [14]. Protecting user actions, such as transactions or interactions, against potential risks and vulnerabilities is of utmost importance [39].

Performance and Latency: Performance and latency are key factors that influence a user's experience in the Metaverse [28]. Recommending or providing hardware specifications that enhance the Metaverse experience, such as VR headsets or high-performance GPUs, is critical [2], [78]. Minimizing the time delay between user actions and their consequences within the Metaverse is another vital aspect, creating a more immersive atmosphere [28].

B. THE ROLE OF THE METAVERSE STANDARDS FORUM

The Metaverse has presented unique challenges for user security due to its interoperable nature. It has the potential for fragmented identity management across various platforms. The Metaverse Standards Forum (MSF) is working to address these challenges [40] and create a secure future for Metaverse users:

1) The MSF has emphasized the importance of open standards to build secure virtual environments. Fragmented standards will lead to security vulnerabilities and they will hinder the user experience. The forum has brought together industry leaders to collaborate on interoperable security solutions [79].
2) The MSF has a dedicated working group on Privacy, Cybersecurity & Identity (PCI). This group focuses on user authentication, data privacy, and ownership across the Metaverse. Their efforts are centered on building user-centric security solutions [80].
3) The MSF is working on projects such as 3D Asset Interoperability, demonstrating their focus on developing practical solutions. The MSF is actively addressing technical challenges related to security in the Metaverse [81].
4) The MSF has also collaborated with organizations such as X Reality Safety Intelligence (XRSI), a leader in promoting privacy, safety, and security in immersive technologies [82].

The future of the MSF involves the creation and evolution of standards across areas relevant to security, such as identity management, and fostering user-centric security solutions. The forum has also stressed the significance of decentralized identity (DID) and blockchain as potential solutions for secure identity management in the Metaverse [83].

However, the MSF has yet to address issues concerning users' control over their own privacy and security, or the roles and responsibilities of Metaverse platforms in ensuring minimum viable security guarantees. Additionally, the role of national governments and their growing impatience with social media platforms, which demand greater accountability and comprehensive tracking of user activities, is not currently factored into the active considerations of the MSF and the research community.

C. OPEN CHALLENGES

After reviewing the existing research contributions, significant challenges remain in ensuring user security and privacy within the Metaverse. Here are some key areas requiring further exploration:

1) There is a lack of a comprehensive security framework that provides security guarantees and safe navigational experiences for individual users in the Metaverse.
2) Balanced privacy-preserving frameworks are scarce; users either operate in a completely anonymous fashion within the Metaverse, or the platform fully knows the real identity of the users and their activities.
3) Cross-platform solutions that address user identity and data protection challenges in the Metaverse are also limited.

These research gaps need urgent attention to ensure a secure and safe experience for all Metaverse users.

V. METAVERSE USER SECURITY ARCHITECTURE WITH ZERO TRUST PRINCIPLES

The security structure of the Metaverse consists of several levels, including Metaverse Users, Metaverse Applications, Metaverse Infrastructure, Metaverse Platforms, and Metaverse Ecosystem. These tiers are built upon the principles of Zero Trust, as illustrated in Figure 7.

Metaverse Users: This layer promotes strong authentication mechanisms and is dedicated to addressing issues such as identity management, credentials, and access management. User identities will be confirmed for those who interact with the Metaverse. In this layer, multi-factor authentication (MFA), biometric verification, and one-time passwords (OTP) are utilized as methods to enhance identity verification [41]. Once a user's identity is confirmed, this layer supervises the implementation of granular access controls within the Metaverse.

Implementation of Zero Trust means adhering to the principle of least privilege in this layer. Metaverse users will be assigned the minimum privileges needed to perform their intended tasks. Consequently, fine-grained access controls based on user roles, attributes, and context will be implemented. This approach helps reduce the attack surface within the Metaverse. The authorization component in this layer will enforce Policy Enforcement Points (PEP) [18], ensuring that resources and data are accessed strictly according to assigned user roles.

User behavior is continuously monitored in this layer with the help of advanced analytics. These analytics help establish baselines of normal activity. Any minimal deviations, such as changes in location or interaction patterns, will trigger flags [49]. Proactive measures against account takeovers, malicious actors posing as legitimate users, and other evolving threats will be initiated. User access privileges will be temporarily restricted in such events [19].

Metaverse Applications: This layer emphasizes secure application development, device health, and real-time network monitoring to protect the applications powering Metaverse experiences [3]. Applications are developed according to secure coding principles aimed at mitigating vulnerabilities such as injection attacks. Measures include strict input validation, regular vulnerability assessments, and penetration testing. Devices accessing the virtual worlds undergo regular health checks to verify system integrity, update security patches, and ensure the absence of known malware. Devices showing compromised postures will be isolated immediately to prevent risks to the ecosystem. Additionally, network traffic is continuously analyzed using AI-powered tools, enabling the detection of anomalies, potential malware communication patterns, or unauthorized data movements. Swift incident responses triggered by these tools are crucial to minimize the impact of breaches [76].

Metaverse Infrastructure: This layer secures the core infrastructure with a focus on network segmentation, secure configurations, and automated remediation in case of compromise. Following the Zero Trust principle, the

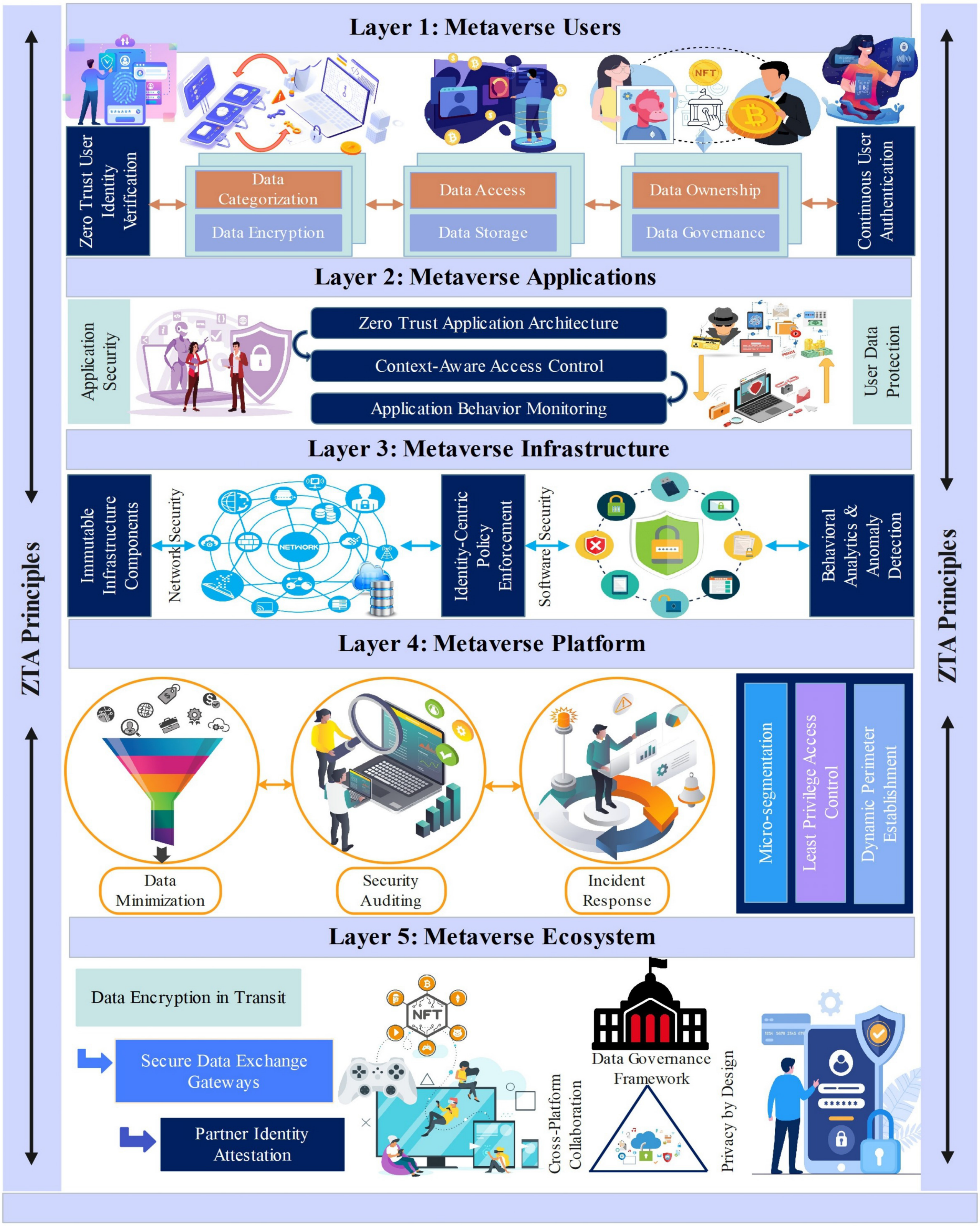
Layer 1: Metaverse Users
Zero Trust User Identity Verification
Data Categorization
Data Encryption
Data Access
Data Storage
NFT
Data Ownership
Data Governance
Continuous User Authentication
Layer 2: Metaverse Applications
Application Security
Zero Trust Application Architecture
Context-Aware Access Control
Application Behavior Monitoring
User Data Protection
Layer 3: Metaverse Infrastructure
Immutable Infrastructure Components
Network Security
NETWORK
Identity-Centric Policy Enforcement
Software Security
Behavioral Analytics & Anomaly Detection
Layer 4: Metaverse Platform
Data Minimization
Security Auditing
Incident Response
Micro-segmentation
Least Privilege Access Control
Dynamic Perimeter Establishment
Layer 5: Metaverse Ecosystem
Data Encryption in Transit
Secure Data Exchange Gateways
Partner Identity Attestation
NFT
Cross-Platform Collaboration
Data Governance Framework
Privacy by Design
ZTA Principles
ZTA Principles

FIGURE 7. Metaverse security architecture with Zero Trust principles.

Metaverse network will be segmented into smaller, isolated zones [39]. This segmentation prevents the lateral movement of attackers in case of a breach and reduces potential damage. Configuration baselines will be imposed to ensure that systems are securely hardened. Updates and patches will be applied carefully to minimize vulnerability windows for attackers. In the event of a compromise, automatic processes will kick in, involving the isolation of affected devices, targeted patching, or segmenting portions of the network. Human intervention is minimized, making breach control swift and efficient.

Metaverse Platforms: This layer enhances security for Metaverse platforms through network traffic analysis and the implementation of the principle of least privilege and micro-segmentation [2]. Network traffic is first analyzed for malicious patterns and anomalies, including attempts to exploit vulnerabilities or unauthorized activities. Access rights within Metaverse platforms are strictly controlled, adhering to the principle of least privilege to limit the damage potentially caused by compromised credentials or lateral movements. Fine-grained network segmentation within individual platforms prevents attackers from moving freely or scanning for other targets, making large-scale compromises much harder to execute [15].

Metaverse Ecosystem: The ecosystem layer ensures robust data protection, regulatory compliance, automation, and orchestration across all other layers of this architecture [58]. It secures sensitive information, both at rest and in transit, using strong encryption algorithms. Privacy-preserving techniques such as differential privacy or homomorphic encryption are employed to enable computations on data without exposing the raw data [3]. Data classification and tagging practices aid in complying with data privacy regulations such as GDPR or CCPA (California Consumer Privacy Act). Automated policy enforcement ensures that compliance is maintained without hindering innovation. Security workflows from threat detection to response are automated [50], centralizing security information for timely alerting with necessary context for prompt decision-making. User behavior analytics detect anomalies, and threat intelligence feeds protect the ecosystem from known and emerging threats [58].

The Metaverse Security Architecture proposed, incorporating the principles of Zero Trust, offers a forward-looking strategy for safeguarding the expanding Metaverse. This architectural framework, rooted in Zero Trust principles, aims to establish a privacy-centric environment that is future-ready. By adopting this approach to security, we can effectively shield users and their data and ensure the integrity of the ever-growing and evolving virtual realm.

VI. CONCLUSION

The Metaverse offers many exciting opportunities for its users, but ensuring robust safety and security measures is crucial to protect all stakeholders. Current security methods in virtual worlds are insufficient, leaving users at risk of harassment, identity theft, and misuse of their data. Drawing from real-life examples and highlighting the importance of user interactions in virtual environments, this article highlights the pressing need for enhanced user security and privacy.

This paper proposes an early Zero-Trust User Security Architecture to address some of these challenges surrounding user security. It grants users clear control over their data, identity, and interactions. This architecture integrates strong authentication mechanisms, including multi-factor authentication and biometrics, in response to emerging privacy concerns. Building a safe Metaverse is an ongoing task that requires the collaborative efforts of all parties in the ecosystem.

Future studies should focus on the effective implementation of user security models, ranging from platform-guaranteed security to user-controlled security provisions. Such solutions must ensure user privacy, provided the users do not engage in malicious activities.

REFERENCES

[1] M. Ball, *The Metaverse: And How It Will Revolutionize Everything*. New York, NY, USA: W.W. Norton Company, 2022.

[2] C. Warin and D. Reinhardt, "Vision: Usable privacy for XR in the era of the metaverse," in *Proc. Eur. Symp. Usable Security*, 2022, pp. 111–116. [Online]. Available: https://doi.org/10.1145/3549015.3554212

[3] G. Thakur, P. Kumar, C.-M. Chen, A. V. Vasilakos, Anchna, and S. Prajapat, "A robust privacy-preserving ECC-based three-factor authentication scheme for metaverse environment," *Comput. Commun.*, vol. 211, pp. 271–285, Nov. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366423003304

[4] S. G. Ali et al., "A systematic review: Virtual-reality-based techniques for human exercises and health improvement," *Front. Public Health*, vol. 11, Mar. 2023, Art. no. 1143947.

[5] B. B. Gupta et al., "DDoS attack detection through digital twin technique in metaverse," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, 2023, pp. 1–5.

[6] M. Weinberger and D. Gross, "A metaverse maturity model," *Global J. Comput. Sci. Technol.*, vol. 22, no. 2, p. 39, 2023.

[7] A. Giacobino, D. Grierson, H. P. Singh, P. McHale, and S. Maggs, "Cosmos cash: Public permissionless approach towards SSI and use cases," in *Proc. IEEE Int. Conf. Blockchain*, Espoo, Finland, 2022, pp. 462–467.

[8] A. Umar, "Metaverse for public welfare and the united nations sustainable development goals," in *Proc. Int. Conf. Cloud Comput., Big Data Internet Things (3CBIT)*, Wuhan, China, 2022, pp. 160–165.

[9] R. A. Nugroho, S. G. Prakoso, K. N. Hidayati, A. D. Rahmawati, A. T. Kartinawanty, and S. A. Santoso, "Challenges of the metaverse adoption for the health of the elderly: Case in Surakarta," in *Proc. IEEE Int. Conf. Comput. Sci. Inf. Technol. (ICOSNIKOM)*, 2022, pp. 1–6.

[10] J. Seo, H. Ko, and S. Park, "Space authentication in the metaverse: A blockchain-based user-centric approach," *IEEE Access*, vol. 12, pp. 18703–18713, 2024.

[11] A. D. Samala et al., "Metaverse technologies in education: A systematic literature review using PRISMA," *Int. J. Emerg. Technol. Learn.*, vol. 18, pp. 231–252, Mar. 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:257420933

[12] M. U. A. Babu and P. Mohan, "Impact of the metaverse on the digital future: People's perspective," in *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, Coimbatore, India, 2022, pp. 1576–1581.

[13] "USTC." 2022. [Online]. Available: http://staff.ustc.edu.cn/~pyzhou/papers/metaversearxiv.pdf

[14] S. Frenkel and K. Browning. "The metaverse's dark side: Here come harassment and assaults." 2021. [Online]. Available: https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

[15] P. T. EamonJavers, S. Zamost, and M. Maharishi, "Cybercriminals target metaverse investors with phishing scams." 2022. [Online]. Available: https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html

[16] K. Staciwa, "The metaverse, online sexual exploitation and sexual abuse of children—A new challenge for today's global society?" *Kwartalnik Prawo Nowych Technologii*, vol. 4, no. 4, pp. 45–49, 2022.

[17] "Virtual reality promised us a new world. instead, it's become a breeding ground for harassment." Elle. 2023. [Online]. Available: https://www.elle.com/culture/career-politics/a43520248/sexual-harassment-metaverse-virtual-reality-2023/

[18] C. N. Chetan, D. H. Ashit, and S. Joseph, "An approach to solve the identification and authentication challenges in metaverse," in *Proc. Somaiya Int. Conf. Technol. Inf. Manage. (SICTIM)*, Mumbai, India, 2023, pp. 69–72.

[19] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain," *IEEE Access*, vol. 10, pp. 98944–98958, 2022.

[20] Ï. Aygün, B. Kaya, and M. Kaya, "Detection of customer opinions with deep learning method for metaverse collaborating brands," in *Proc. Int. Conf. Data Anal. Bus. Ind. (ICDABI)*, Sakhir, Bahrain, 2022, pp. 603–607.

[21] A. Vernaza, V. I. Armuelles, and I. Ruiz, "Towards an open and interoperable virtual learning environment using metaverse at the university of Panama," in *Proc. Technol. Appl. Electron. Teach. (TAEE)*, Jun. 2012, pp. 320–325.

[22] "Deanonymizing mobility traces: Using social networks as a side ⋯." 2012. [Online]. Available: https://www.cs.umd.edu/~mwh/papers/GraphInfoFlow.CCS2012.pdf

[23] B. S. Rawal, A. Mentges, and S. Ahmad, "The rise of metaverse and interoperability with split-protocol," in *Proc. IEEE 23rd Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, San Diego, CA, USA, 2022, pp. 192–199.

[24] A. Tlili et al., "Is metaverse in education a blessing or a curse: A combined content and bibliometric analysis," *Smart Learn. Environ.*, vol. 9, p. 24, Jul. 2022. [Online]. Available: https://slejournal.springeropen.com/articles/10.1186/s40561-022-00205-x

[25] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "MetaChain: A novel blockchain-based framework for metaverse applications," in *Proc. IEEE 95th Veh. Technol. Conf. (VTC-Spring)*, Helsinki, Finland, 2022, pp. 1–5.

[26] B. C. Cheong, "Avatars in the metaverse: Potential legal issues and remedies," *Int. Cybersecurity Law Rev.*, vol. 3, pp. 467–494, Jun. 2022. [Online]. Available: https://link.springer.com/article/10.1365/s43439-022-00056-9

[27] G. Kang, J. Koo, and Y.-G. Kim, "Security and privacy requirements for the metaverse: A metaverse applications perspective," *IEEE Commun. Mag.*, vol. 62, no. 1, pp. 148–154, Jan. 2024.

[28] S.-M. Park and Y.-G. Kim, "A metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 10, pp. 4209–4251, 2022.

[29] M. Dąbrowski and P. Pacyna, "Blockchain-based identity discovery between heterogenous identity management systems," in *Proc. 6th Int. Conf. Cryptogr., Security Privacy (CSP)*, Tianjin, China, 2022, pp. 131–137.

[30] L.-H. Lee, "The digital big bang in the metaverse era," in *Proc. IEEE Int. Symp. Mixed Augmented Real. Adjunct (ISMAR-Adjunct)*, Singapore, 2022, p. 55.

[31] J. Lee, I. Yeo, and H. Lee, "Metaverse current status and prospects: Focusing on metaverse field cases," in *Proc. IEEE/ACIS 7th Int. Conf. Big Data, Cloud Comput., Data Sci. (BCD)*, Danang, Vietnam, 2022, pp. 332–336.

[32] J. Zhong and Y. Zheng, "Empowering future education: Learning in the edu-metaverse," in *Proc. Int. Symp. Educ. Technol. (ISET)*, Hong Kong, 2022, pp. 292–295.

[33] K. Kim, E. Yang, and J. Ryu, "Work-in-progress—The effect of students' perceptions on intention to use metaverse learning environment in higher education," in *Proc. 8th Int. Conf. Immersive Learn. Res. Netw. (iLRN)*, Vienna, Austria, 2022, pp. 1–3.

[34] H. Lin, S. Wan, W. Gan, J. Chen, and H.-C. Chao, "Metaverse in education: Vision, opportunities, and challenges," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Osaka, Japan, 2022, pp. 2857–2866.

[35] J. Y. Kim and J. M. Oh, "Opportunities and challenges of metaverse for automotive and mobility industries," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju Island, Republic of Korea, 2022, pp. 113–117.

[36] L. Zonaphan, K. Northus, J. Wijaya, S. Achmad, and R. Sutoyo, "Metaverse as a future of education: A systematic review," in *Proc. 8th Int. HCI UX Conf. Indonesia (CHIuXiD)*, Bali, Indonesia, 2022, pp. 77–81.

[37] J. Knox, "The metaverse, or the serious business of tech frontiers," *Postdigit. Sci. Educ.*, vol. 4, pp. 207–215, Mar. 2022.

[38] S. Tariq, A. Abuadbba, and K. Moore, "Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices," in *Proc. 2nd Workshop Security Implicat. Deepfakes Cheapfakes*, 2023, pp. 16–19. [Online]. Available: https://doi.org/10.1145/3595353.3595880

[39] R. Cheng, S. Chen, and B. Han, "Towards zero-trust security for the metaverse," *IEEE Commun. Mag.*, vol. 62, no. 2, pp. 156–162, Feb. 2024.

[40] C. Chen et al., "Privacy computing meets metaverse: Necessity, taxonomy and challenges," *Ad Hoc Netw.*, vol. 158, May 2024, Art. no. 103457. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870524000684

[41] Y. Huang, Y. J. Li, and Z. Cai, "Security and privacy in metaverse: A comprehensive survey," *Big Data Min. Anal.*, vol. 6, no. 2, pp. 234–247, Jun. 2023.

[42] "Digital identity guidelines—Enrollment and identity proofing," Natl. Inst. Stand. Technol., Gaithersburg, MD, USA, document SP 800-63A. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[43] H. Hadan, D. Wang, L. Nacke, and L. Zhang-Kennedy, "Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies," in *Proc. CHI*, May 2024, pp. 1–24.

[44] J. D. N. Dionisio, W. G. Burns III, and R. Gilbert, "3D virtual worlds and the metaverse: Current status and future possibilities," *ACM Comput. Surveys*, vol. 45, no. 3, p. 34, Jul. 2013.

[45] D. Kumarapeli, S. Jung, and R. W. Lindeman, "Privacy threats of behaviour identity detection in VR," *Front. Virtual Real.*, vol. 5, pp. 861–862, Jan. 2024. [Online]. Available: https://www.frontiersin.org/articles/10.3389/frvir.2024.1197547

[46] K. Lippert, M. N. R. Khan, M. M. Rabbi, A. Dutta, and R. Cloutier, "A framework of metaverse for systems engineering," in *Proc. IEEE Int. Conf. Signal Process., Inf., Commun. Syst. (SPICSCON)*, Dhaka, Bangladesh, 2021, pp. 50–54.

[47] M. Damar, "Metaverse shape of your life for future: A bibliometric snapshot," *J. Metaverse*, vol. 1, no. 1, pp. 1–8, 2021. [Online]. Available: https://dergipark.org.tr/en/pub/jmv/issue/67581/1051371

[48] G. Bansal, K. Rajgopal, V. Chamola, Z. Xiong, and D. Niyato, "Healthcare in metaverse: A survey on current metaverse applications in healthcare," *IEEE Access*, vol. 10, pp. 119914–119946, 2022.

[49] R. D. Pietro and S. Cresci, "Metaverse: Security and privacy issues," in *Proc. 3rd IEEE Int. Conf. Trust, Privacy Security Intell. Syst. Appl. (TPS-ISA)*, Atlanta, GA, USA, 2021, pp. 281–288.

[50] N. Naik and P. Jenkins, "Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity," in *Proc. 7th Int. Conf. Behav. Social Comput. (BESC)*, Bournemouth, U.K., 2020, pp. 1–6.

[51] T. Ünal and A. Tarhan, "Transformation of education with the metaverse awareness and metaverse generation," *Int. J. Acad. Res. Educ.*, vol. 8, no. 1, pp. 64–73, 2022.

[52] Z. Chen, J. Wu, W. Gan, and Z. Qi, "Metaverse security and privacy: An overview," in *Proc. IEEE Int. Conf. Big Data*, 2022, pp. 2950–2959.

[53] H. Kim, J. Park, S. Yang, J. Yun, M. Kang, and D. Park, "Edge-cloud cooperative image processing by partially streaming ROI data for metaverse applications," in *Proc. IEEE Int. Conf. Consum. Electron.-Asia (ICCE-Asia)*, Yeosu, Republic of Korea, 2022, pp. 1–3.

[54] J. Kaneriya and H. Patel, "A comparative survey on blockchain based self sovereign identity system," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Thoothukudi, India, 2020, pp. 1150–1155.

[55] T. Chen, H. Zhou, H. Yang, and S. Liu, "A review of research on metaverse defining taxonomy and adaptive architecture," in *Proc. 5th Int. Conf. Pattern Recognit. Artif. Intell. (PRAI)*, Chengdu, China, 2022, pp. 960–965.

[56] T. Langlotz, C. Degendorfer, A. Mulloni, G. Schall, G. Reitmayr, and D. Schmalstieg, "Robust detection and tracking of annotations for outdoor augmented reality browsing," *Comput. Graph.*, vol. 35, pp. 831–840, Aug. 2011.

[57] Y. Wang et al., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 319–352, 1st Quart., 2023.

[58] M. Wang, H. Yu, Z. Bell, and X. Chu, "Constructing an edu-metaverse ecosystem: A new and innovative framework," *IEEE Trans. Learn. Technol.*, vol. 15, no. 6, pp. 685–696, Dec. 2022.

[59] "Use case spotlight: The government of British Columbia uses the Sovrin network to take strides towards a fully digital economy." Mar. 2019. [Online]. Available: https://sovrin.org/use-case-spotlight-the-government-of-british-columbia-uses-the-sovrin-network-to-take-strides-towards-a-fully-digital-economy/

[60] C. Li and K. White, "Social implications of the metaverse: In collaboration with Accenture," presented at World Economic Forum, Jul. 2023.

[61] M. Xu, Y. Guo, Q. Hu, Z. Xiong, D. Yu, and X. Cheng, "A trustless architecture of blockchain-enabled metaverse," *High-Confidence Comput.*, vol. 3, no. 1, 2023, Art. no. 100088. [Online]. Available: https://doi.org/10.1016/j.hcc.2022.100088

[62] A. Almarzouqi, A. Aburayya, and S. A. Salloum, "Prediction of user's intention to use metaverse system in medical education: A hybrid SEM-ML learning approach," *IEEE Access*, vol. 10, pp. 43421–43434, 2022.

[63] C. Warin, D. Seeger, S. Shams, and D. Reinhardt, "PrivXR: A cross-platform privacy-preserving API and privacy panel for extended reality," in *Proc. 22nd Int. Conf. Pervasive Comput. Commun. Workshops Affiliated Events (PerCom Work Prog.)*, 2024.

[64] *Cybersecurity Information Sheet*, Nat. Security Agency, Fort Meade, MD, USA, Apr. 2023.

[65] T. Huynh-The et al., "Blockchain for the metaverse: A review," *Future Gener. Comput. Syst.*, vol. 143, pp. 401–419, Jun. 2023. [Online]. Available: https://doi.org/10.1016/j.future.2023.02.008

[66] Y. Ren, Z. Lv, N. N. Xiong, and J. Wang, "HCNCT: A cross-chain interaction scheme for the blockchain-based metaverse," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 20, no. 7, p. 188, 2023. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3594542

[67] H. Wang et al., "MIS: A multi-identifier management and resolution system in the metaverse," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 20, no. 7, p. 191, 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3597641

[68] C. Li and K. White, "Metaverse privacy and safety: In collaboration with Accenture," presented at World Economic Forum, Jul. 2023.

[69] P. D. Cin, S. Joyce, J. Jurgens, and A. Tuteja, "Earning digital trust: Decision-making for trustworthy technologies: In collaboration with Accenture, KPMG and PwC," presented at World Economic Forum, Nov. 2022.

[70] Q. Stokkink, G. Ishmaev, D. Epema, and J. Pouwelse, "A truly self-sovereign identity system," in *Proc. IEEE 46th Conf. Local Comput. Netw. (LCN)*, Edmonton, AB, Canada, 2021, pp. 1–8.

[71] A. J. Flanagan, J. King, and S. Warren, "Redesigning data privacy: Reimagining notice consent for human technology interaction," presented at World Economic Forum, Jul. 2020.

[72] M. Karthigha, C. Padmavathy, and V. S. Akshaya, "Blockchain based healthcare data management," in *Proc. Int. Conf. Autom., Comput. Renewable Syst. (ICACRS)*, Pudukkottai, India, 2022, pp. 392–396.

[73] V. Hyseni. "Challenges and solutions: Cybersecurity in the metaverse." PECB. 2023. [Online]. Available: https://pecb.com/article/challenges-and-solutions-cybersecurity-in-the-metaverse

[74] S. Rajput, A. Singh, S. Khurana, T. Bansal, and S. Shreshtha, "Blockchain technology and cryptocurrencies," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Dubai, UAE, 2019, pp. 909–912.

[75] S. C. Sethuraman, A. Mitra, G. Galada, A. Ghosh, and S. Anitha, "Metakey: A novel and seamless passwordless multifactor authentication for metaverse," in *Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES)*, Warangal, India, 2022, pp. 662–664.

[76] E. Dutkiewicz and D. Nguyen, "Keynote speaker 2: Enabling metaverse with secure and smart network resource slicing," in *Proc. 9th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Ho Chi Minh City, Vietnam, 2022, pp. 33–34.

[77] G. Zhang, J. Wu, G. Jeon, Y. Chen, Y. Wang, and M. Tan, "Towards understanding metaverse engagement via social patterns and reward mechanism: A case study of nova empire," *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 5, pp. 2165–2176, Oct. 2023.

[78] M. Qu, Y. Sun, and Y. Feng, "Digital media and VR art creation for metaverse," in *Proc. 2nd Asia Conf. Inf. Eng. (ACIE)*, Haikou, China, 2022, pp. 48–51.

[79] R. Morrison. "How will digital identity work in the metaverse?" 2022. [Online]. Available: https://techmonitor.ai/focus/how-will-digital-identity-work-in-the-metaverse

[80] "Shaping the future: The road to an open, user-centric metaverse." 2023. [Online]. Available: https://metaversestandardsforum.org/

[81] "Epic games teams up with autodesk to accelerate real-time immersive design capabilities across industries." 2024. [Online]. Available: https://www.epicgames.com/site/en-US/news/epic-games-teams-up-with-autodesk-to-accelerate-real-time-immersive-design-capabilities-across-industries

[82] "XRSI's ongoing collaboration with metaverse standards forum reinforces focus on privacy, cybersecurity identity." XRSI. 2023. [Online]. Available: https://xrsi.org/xrsis-ongoing-collaboration-with-metaverse-standards-forum-reinforces-focus-on-privacy-cybersecurity-identity

[83] S. Mishra, H. Arora, G. Parakh, and J. Khandelwal, "Contribution of blockchain in development of metaverse," in *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, Coimbatore, India, 2022, pp. 845–850.