Mesopotamian journal of Cybersecurity
Vol. 5, No.2, **pp**. 770–803
DOIhttps://doi.org/10.58496/MJCS/2025/045; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Review Article

A Systematic Review of Metaverse Cybersecurity: Frameworks, Challenges, and Strategic Approaches in a Quantum-Driven Era

Hasan Ali Al-Tameemi [1,], Ghadeer Ghazi Shayea [1,], Mishall Al-Zubaidie [2,], Yahya Layth Khaleel [3,*], Mustafa Abdulfattah Habeeb [3,], Noor Al-Huda K. Hussein [4,], Raad Z. Homod [6], Mohammad Aljanabi [1,7], O.S. Albahri [8, 9,], A.H. Alamoodi [10,11,], Maad M. Mijwil[12, 13], Mohammed A. Fadhel [14,], Iman Mohamad Sharaf [15,], Mohanad G. Yaseen [7,], Ahmed Hussein Ali [7], U. S. Mahmoud[16], Saleh M. Mohammed [1, *] A.S. Albahri [1, 5,]

1 Technical Engineering College, Imam Ja'afar Al-Sadiq University (IJSU), Baghdad, Iraq
2 Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq
3 Department of Computer Science, College of Computer Science and Mathematics, Tikrit University, Iraq
4 Computer Technology Engineering Department, Technical College, Imam Ja'afar Al-Sadiq University (IJSU), Baghdad, Iraq
5 University of Information Technology and Communications (UOITC), Baghdad, Iraq
6 Department of Oil and Gas Engineering, Basra University for Oil and Gas, Iraq
7 Department of Computer, College of Education, AL-Iraqia University, Baghdad, Iraq
8 Computer Techniques Engineering Department, Mazaya University College, Nasiriyah, Iraq
9 Australian Technical and Management College, Melbourne, Australia
10 Applied Science Research Center, Applied Science Private University, Amman, Jordan
11 MEU Research Unit, Middle East University, Amman, Jordan
12 College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq
13 Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq
14 College of Computer Science and Information Technology, University of Sumer, Thi Qar, Iraq
15 Department of Basic Sciences, Higher Technological Institute, Tenth of Ramadan City, Egypt
16 College of Medical Informatics, University of Information Technology and Communications (UOITC), Baghdad, Iraq

ARTICLEINFO

Article History

Received: 9 May 2025
Revised: 15 Jun 2025
Accepted: 7 Jul 2025
Published: 24 Jul 2025

Keywords

Cybersecurity
Metaverse
AI-driven Security
Blockchain
Privacy Protection
Threat Detection
Intrusion Detection

ABSTRACT

This study aims to perform a detailed systematic review that investigates and synthesizes the available literature on the challenges and strategies in cybersecurity in the Metaverse. The methodology employed was to ensure a comprehensive literary analysis of the study methods, employing databases such as ScienceDirect (SD), Scopus, IEEE Xplore (IEEE), and Web of Science (WoS). The search was conducted by employing a query that would yield articles published until September 2024, resulting in a total of 325 papers. After vigorous screening, deduplication, and application of the inclusion and exclusion criteria, 34 studies were identified for quantitative synthesis. These papers were divided into three classes: cybersecurity, AI-based security and IoT applications, and Metaverse and virtual realities. This article provides a systematic and comprehensive overview of previous studies that highlighted four fundamental challenges of cybersecurity in the Metaverse and discussed three recommendations for future improvement. A systematic science mapping analysis was conducted to synthesize the results regarding key trust issues related to security in the Metaverse. In addition, the study investigated a wide spectrum of practical applications of cybersecurity within Metaverse environments, encompassing authentication approaches, intrusion detection systems, privacy preservation frameworks, AI-based threat identification, and blockchain-enabled security proposals. Furthermore, this review explores how quantum technologies can be integrated into Metaverse cybersecurity frameworks to address advanced threat models and enhance resilience. The study also highlighted developments in cybersecurity for the Metaverse while pinpointing existing gaps, emerging threats, and directions for future research that would inform frameworks for improved security. The insights provided bear great significance for researchers, practitioners, and policy actors engaged with the Metaverse cybersecurity and applications of artificial intelligence (AI).

**Corresponding author. Email: yahya@tu.edu.iq*

1. INTRODUCTION

In today's interconnected world, cybersecurity has become a cornerstone of digital infrastructure, crucial for protecting sensitive information, financial assets, and the integrity of systems [1], [2]. With the proliferation of internet-connected devices and services, cybersecurity encompasses a wide range of practices, technologies, and policies aimed at safeguarding networks, data, and systems from unauthorized access, damage, and cyberattacks [3], [4]. The growing reliance on digital platforms—ranging from financial services to healthcare and government operations—has made cybersecurity a top priority for both the public and private sectors [5]. From small businesses to multinational corporations, every entity faces the looming threat of cyber-attacks, which have grown in sophistication and scale over the years [6], [7].

Cybersecurity threats, including malware, ransomware, phishing, and advanced persistent threats (APTs), pose significant risks, leading to financial losses, data breaches, reputational damage, and even national security concerns [8], [9]. As technology advances, so do the tactics of attackers, who require organizations to continually update and strengthen their security frameworks [10], [11]. The rise of new technologies such as cloud computing, AI, and the Internet of Things (IoT) has expanded the attack surface, giving cybercriminals more opportunities to exploit vulnerabilities [12], [13]. One of the most significant developments in this technological landscape is the Metaverse—a virtual, interconnected universe where users interact in real time with each other and with digital environments [14], [15]. In this immersive space, the lines between physical and digital worlds blur, enabling activities ranging from social interactions to gaming, work, and commerce [16], [17]. Powered by augmented reality (AR), virtual reality (VR), blockchain, and AI, the Metaverse is set to transform how we communicate and experience digital life while also introducing new cybersecurity challenges as the digital and physical realms become more intertwined [18], [19].

With platforms such as Facebook (now Meta), Microsoft, and others spearing the development of Metaverse ecosystems, the vision of the virtual world is becoming more tangible [20]. In this digital universe, users can not only socialize but also engage in economic activities, purchase virtual goods, attend virtual events, and even own property [21], [22]. The Metaverse also holds the potential to revolutionize industries such as education, healthcare, and real estate by enabling virtual collaboration and interaction in ways previously unimagined [23].

However, as the Metaverse grows, it introduces new challenges and questions, particularly concerning issues of privacy, data security, and user safety [24], [25]. The Metaverse is expected to collect vast amounts of personal data, including biometric and behavioral information, raising concerns about how these data will be managed and protected [26]. Additionally, the virtual nature of the Metaverse opens the door to new forms of cybercrime, identity theft, and digital fraud, necessitating the development of robust cybersecurity frameworks [27]. As the Metaverse continues to take shape, understanding its implications—both opportunities and risks—will be critical in shaping a safe, inclusive, and secure virtual future.

With the rise of the Metaverse, the scope of cybersecurity challenges has further intensified. In these immersive virtual environments, the integration of AR, VR, and digital assets introduces unique security risks that require innovative solutions [28], [29]. Cybersecurity in the Metaverse goes beyond traditional concerns, encompassing privacy issues, identity verification, data integrity, and digital property protection [29], [30]. As our digital presence expands, the need for comprehensive, adaptive, and forward-thinking cybersecurity strategies becomes even more critical to protect both individuals and organizations from the evolving landscape of cyber threats [31].

This paper embarks on an in-depth analysis of the cybersecurity challenges posed by the metaverse, exploring the intersection of virtual worlds and cybersecurity frameworks. The key focus is on examining the nature of these new threats and identifying strategies to address them, ensuring the metaverse's security as its technological potential continues to grow. Through an extensive review of relevant research, this paper aims to provide a comprehensive understanding of how cybersecurity must evolve to meet the demands of this dynamic virtual landscape.

The key contributions of this research are outlined as follows:

1- Systematic Review of Cybersecurity in the Metaverse. The study conducts an organized analysis of the literature by identifying the emerging cybersecurity threats accompanying newly proposed mechanisms of fighting against them, as well as the insistence on AI, blockchain, and cryptographic methods contributing to security in a metaverse environment.

2- Taxonomy and Classification of Security Strategies: The literature has been categorized into three major classes: (i) Cybersecurity in Metaverse, (ii) AI-influenced security and IoT applications, and (iii) metaverse and virtual realities. This classification provides a systematic understanding of existing research and applications.

3- Challenge Identification and Gaps in Research: This paper identifies key security challenges, including data privacy risks, authentication complexities, vulnerabilities to AI-based attacks, and regulatory concerns. Research gaps related to counteracting such issues must be identified, along with possible future improvements to security.

4- Recommendations for Future Research and Development: On the basis of the findings, the study culminates in concrete recommendations aimed at building a robust and more viable cybersecurity framework. This study provides notable recommendations for AI-influenced threat detection, privacy-preserving architectures, and scalable identity management solutions.

The rest of this paper is structured as follows: Section 2 provides an overview of cybersecurity in terms of its metaverse and emerging threats, i.e., security concerns. Section 3 presents the importance of this study. Section 4 outlines the methodology used to conduct this systematic literature review, including the data collection, selection criteria, and analysis methods. Section 5 provides a taxonomy and classification of cybersecurity applications in Metaverse, highlighting the key security mechanisms and frameworks. Section 6 presents the literature discussion, considering the motivations, challenges, recommendations, and limitations, while Section 7 discusses the salient challenges, constraints, and open issues sampled in the literature, drawing special attention to research gaps that indeed require correction by recommendations and suggesting some potential avenues to advance security strategies. Finally, Section 8 presents perspectives on the Metaverse, while Section 9 presents a summary of the key findings and their implications for researchers, practitioners, and policymakers.

2. CYBERSECURITY AND METAVERSE: AN OVERVIEW

Currently, cybersecurity is a major cause for concern, not only for individuals but also for organizations, governments, and corporations [32]. This is due to the increasing number of electronic devices, the constant expansion of digital infrastructure, and the increasing sophistication of cyber threats [3].

Cybersecurity refers to the use of measures and practices needed to protect one's computer systems, networks, and data from unauthorized intrusion, disruption, or exploitation [33]. Cybersecurity is a broad area, as it includes various forms of threats, such as malware, phishing, denial of service attacks, and data breaches. With the existence of complex cyber networks, it is easy to conduct malicious operations globally, making it extremely difficult to secure cyberspace [34], [35]. The ever-growing interconnectedness between cyber and physical systems, as well as the overwhelming magnitude of cyber networks, also increases the complexity of securing cyberspace and reduces the options available to mitigate consequences and vulnerabilities [34].

The cybersecurity landscape is always changing, with threats and vulnerabilities appearing at a remarkable speed. Scholars have reported on the existence of advanced cyberattacks and noted that the uses of AI and machine learning make it easier for adversaries to carry out operations [36].

It is evident that roving cyber military groups or individual engineers employs multifaceted tactics against all these changes; therefore, the government, academia, and industry must work in a coordinated manner [37]. Protecting and regulating one's own business activities requires the careful formulation and issuance of a strategy that outlines clear actions to be taken in case of a cyber breach for both the public sector and private companies [34].

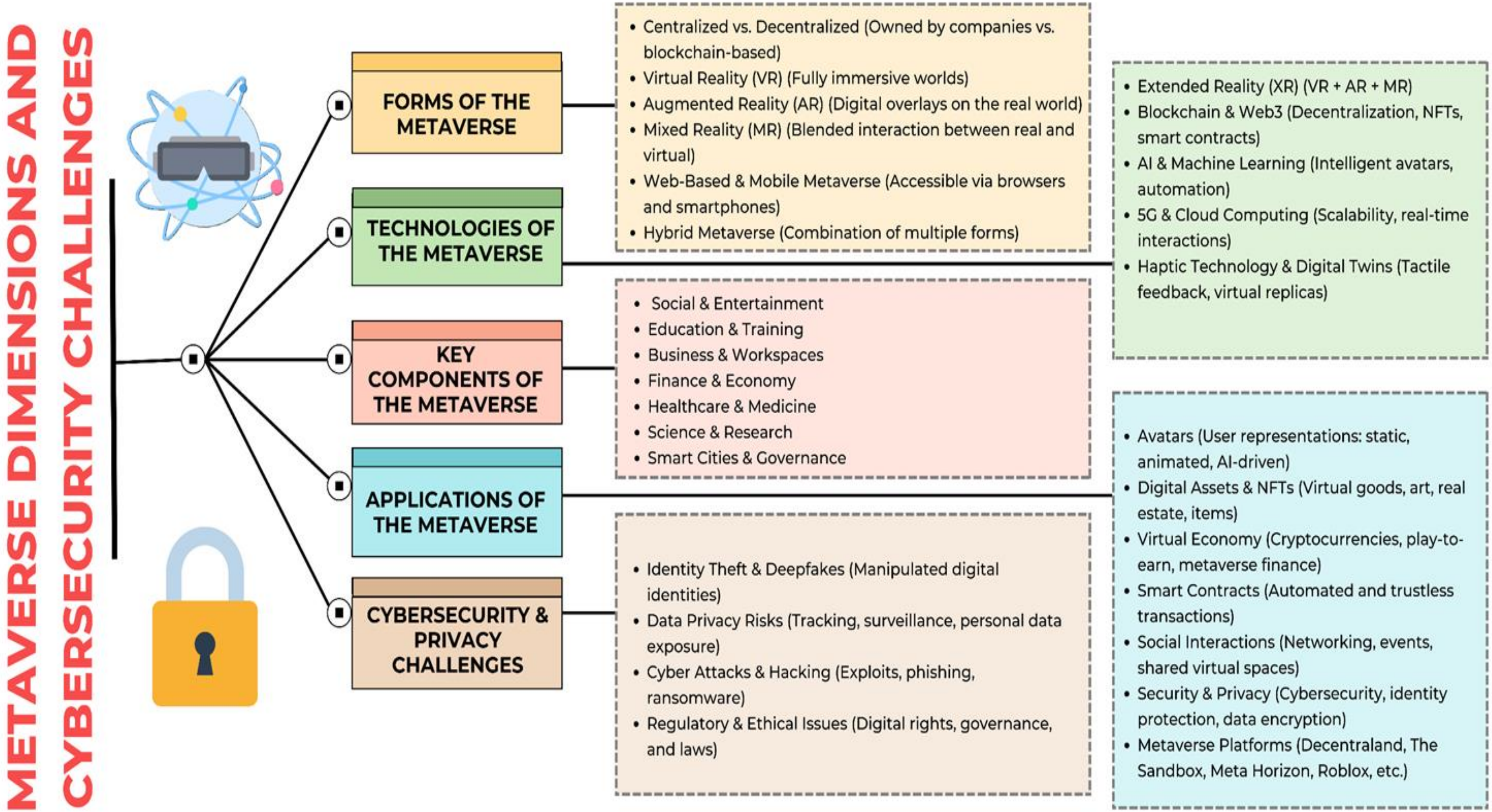
In addition, the preservation of cyber assets requires a thorough comprehension of cyber security principles on how to operate in a dynamically emerging hostile environment [38]. Cybersecurity education should be continuous; to mitigate these risks, both groups and individuals need to prioritize the best practices of cybersecurity [34], [36], [37].

On the other hand, as the world is increasingly leaning toward the concept of complex digital worlds, there has been a rise in phenomena known as metaverse, which has changed how cybersecurity is viewed together [39]. The metaverse is a fusion of the virtual, augmented, and extended physical worlds, which is very complicated and interlinked. This means that the ecosystem needs a proper security infrastructure to be in place to protect users and their data at all costs [40].

Metaverse is a broad and far-reaching framework composed of different technologies, such as AR/MR/VR/XR, digital twins, 5G/6G, IoT, and AI [41]. Ever since the COVID-19 pandemic, people have become increasingly familiar with remote work, which has impacted the development and acceptance of the metaverse [41]. The metaverse is completely novel, enabling and capable of carrying out social and work-related tasks; however, these innovations bring forth issues of security and privacy that were previously unknown [28].

The emergence of the digital ecosystem has made it very easy for new privacy and security threats to arise, especially in the context of the metaverse, which is one of its greatest challenges [28], [42]. Even though the shift between different media types and the requirement to analyse large volumes of data poses some privacy challenges to users, the major challenge lies in scalability and interoperability. In addition, boundaries between real and virtual environments blur [43].

Figure 1 outlines the metaverse structure, which combines different methods with essential technologies and fundamental elements that operate in the entertainment, educational, business, and medical domains. In addition, cybersecurity and privacy challenges in the metaverse present the main difficulties to users. Therefore, the metaverse progresses with its potential realized through the merger of security elements that need immediate attention until its full development.



METAVERSE DIMENSIONS AND CYBERSECURITY CHALLENGES
FORMS OF THE METAVERSE
TECHNOLOGIES OF THE METAVERSE
KEY COMPONENTS OF THE METAVERSE
APPLICATIONS OF THE METAVERSE
CYBERSECURITY & PRIVACY CHALLENGES

- Centralized vs. Decentralized (Owned by companies vs. blockchain-based)
- Virtual Reality (VR) (Fully immersive worlds)
- Augmented Reality (AR) (Digital overlays on the real world)
- Mixed Reality (MR) (Blended interaction between real and virtual)
- Web-Based & Mobile Metaverse (Accessible via browsers and smartphones)
- Hybrid Metaverse (Combination of multiple forms)

- Extended Reality (XR) (VR + AR + MR)
- Blockchain & Web3 (Decentralization, NFTs, smart contracts)
- AI & Machine Learning (Intelligent avatars, automation)
- 5G & Cloud Computing (Scalability, real-time interactions)
- Haptic Technology & Digital Twins (Tactile feedback, virtual replicas)

- Social & Entertainment
- Education & Training
- Business & Workspaces
- Finance & Economy
- Healthcare & Medicine
- Science & Research
- Smart Cities & Governance

- Avatars (User representations: static, animated, AI-driven)
- Digital Assets & NFTs (Virtual goods, art, real estate, items)
- Virtual Economy (Cryptocurrencies, play-to-earn, metaverse finance)
- Smart Contracts (Automated and trustless transactions)
- Social Interactions (Networking, events, shared virtual spaces)
- Security & Privacy (Cybersecurity, identity protection, data encryption)
- Metaverse Platforms (Decentraland, The Sandbox, Meta Horizon, Roblox, etc.)

- Identity Theft & Deepfakes (Manipulated digital identities)
- Data Privacy Risks (Tracking, surveillance, personal data exposure)
- Cyber Attacks & Hacking (Exploits, phishing, ransomware)
- Regulatory & Ethical Issues (Digital rights, governance, and laws)

Fig. 1: Overview of the Metaverse and its Relation to Cybersecurity

3. IMPORTANCE OF THIS SYSTEMATIC REVIEW OVER EXISTING REVIEWS

This section highlights the gaps that this review addresses over previous updated reviews, as this systematic review explores the study of the metaverse and cybersecurity from several aspects not addressed in previous studies.

Gabriel Kabanda et al. [44] reviewed a cybersecurity model for an architecture framework for the Roblox-based Metaverse that can be used for internationalization, the educational value chain, and the provision of online and e-learning courses. The study employs the interpretivist paradigm, which is distinguished by balanced axiology, a naturalist methodology, a relativistic ontology, and a subjectivist epistemology. A thorough review of the literature on AR, VR, and the metaverse was performed. They classified definitions of the metaverse into four categories—environment, interface, interaction, and social value—by outlining each facet of the metaverse. However, this review is focused solely on reviewing the cybersecurity model for the Roblox-based Metaverse. A survey of AI-based Metaverse cybersecurity and a discussion of pertinent security issues were given by Mitra Pooyandeh et al. [45]. On the basis of these findings, the problem of user identification—for which biometric techniques are most frequently employed—plays a significant part in the works that are presented. Although biometric data are seen to be the safest approach, because of their uniqueness, they can also be abused. With the aid of algorithms, an artificial intelligence-based cyber-situation management system needs to be able to examine data of any size. Nonetheless, their review was not systematic of the research included in the study.

Parichat Jaipong et al. [46] presented a narrative synthesis of cybersecurity and the Metaverse. A brief study of the literature and data from research publications on EBSCO, Google Scholar, Scopus, Web of Science, and ScienceDirect was conducted to investigate cybersecurity and the metaverse in the digital age. The inclusion criteria were peer-reviewed, English-language publications that provided a clear definition of cybersecurity and the Metaverse in the digital age. However, their mini-review has not extensively addressed security issues in the Metaverse. A review of cybersecurity simulations on the Metaverse using ontological and network science methodologies was presented by Tam N. Nguyen et al. [47]. In a package known as Cybonto, a novel ontology, they formally described 108 psychological constructs and thousands of linked routes on the basis of 20 tried-and-true psychology theories. The Cybonto psychology constructs were then ranked by their influence via 20 network science centrality techniques. The problem with this study is that the authors did not specify the databases in the research classification. Additionally, the number of reviewed studies was small compared with the number of studies included in our study.

Ibrar Yaqoob et al. [48] noted that using the Metaverse for smart cities might spur innovation and result in significant advancements. Along with the main advantages of implementing this technology and the prospects it offers for smart city applications, they discuss the main enabling technologies for the Metaverse. To demonstrate the usefulness of metaverse technology in a variety of industries, they provided case studies and active initiatives. Additionally, they list and discuss important research issues that are preventing the metaverse from reaching its full potential at the moment. However, although researchers have investigated metaverse applications in smart cities in terms of enabling technologies, opportunities, and challenges, they have not given much priority to studying cybersecurity with the Metaverse, which is an important issue in the current era. To look into the cybersecurity risks that the metaverse faces in connection with visualization technologies, Yang-Wai Chow et al. [49] presented a survey. Researchers have also discussed current research and future directions in the creation of defenses against these dangers. However, this research focuses only on the security of visualization technologies in the metaverse and neglects other aspects of technologies.

Mostafa Al-Emran et al. [50] provided an overview of cybersecurity behavior in the Metaverse and highlighted a range of potential prospects. They also discussed the current and prospective challenges and suggested large-scale research agendas that can be examined in future research. The research agendas encompass extensive subject areas, such as the security of the Metaverse, influential factors, human behavior in the Metaverse, virtual identity and access management, privacy, legal, and ethical issues, and cybersecurity education and awareness. However, the researchers did not address an important technology such as blockchain, which could support cybersecurity and the Metaverse. By reviewing a theoretical model that incorporates elements from technological threat avoidance theory and takes into account variables such as privacy concerns, perceived risks, and response costs, Mostafa Al-Emran et al. [51] sought to examine cybersecurity behavior barriers with the Metaverse approach. 395 Metaverse users provided the data, which were then evaluated via fuzzy-set qualitative comparative analysis and partial least squares-structural equation modelling. Their results demonstrated that while perceived risks have a negligible detrimental effect on cybersecurity behavior, perceived threats, privacy concerns, and response costs have a large negative impact. However, the researchers did not address AI-influenced security and IoT applications, making their review not comprehensive.

Mousa Al-kfairy et al. [52] concentrated on user perceptions and emphasized the importance of interoperability, social influence, and usability in this nascent digital metaverse environment. Through the integration of many scholarly viewpoints, this investigation underscores Metaverse's noteworthy influence across multiple industries, highlighting its capacity to transform digital interaction paradigms. The report also highlights interoperability as a critical issue and calls for the development of standardized protocols and technologies to enable smooth interactions across various metaverse systems. To improve user engagement, it promotes the use of inclusive, ergonomic designs. It discusses the moral and social issues raised by the Metaverse, such as worries about online harassment, intrusive advertising, and privacy violations. However, this review does not address authentication complexities, vulnerabilities to AI-based attacks, and regulatory concerns. To investigate the evolving cybersecurity landscape within these intersecting domains, Petar Radanliev [53] adopted a methodical review that blends a thorough literature analysis with targeted case study investigations. The focus is specifically on the Metaverse, examining its cybersecurity situation as of right now, possible advancements in the future, and the significant contributions of cloud, blockchain, and artificial intelligence technology. Their study evaluated several cybersecurity frameworks and standards to ascertain how well they manage the dangers connected to these cutting-edge technologies. Particular attention is given to the Metaverse's quickly changing digital economy, exploring how blockchain and artificial intelligence (AI) can improve its cybersecurity framework while recognizing the challenges posed by cloud computing. However, their review did not provide any recommendations for supporting cybersecurity in the Metaverse, and there is no clear indication of gaps in the included research.

4. METHODOLOGY

This systematic literature review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines, ensuring a rigorous and transparent approach [54]. The research employed a structured methodology where data collection was conducted prior to data analysis. To ensure a comprehensive overview of the relevant literature, a diverse range of bibliographic databases, including scientific and social science journals from various disciplines, were consulted. Specifically, the review utilized four prominent digital databases: ScienceDirect, Scopus, IEEE Xplore, and Web of Science. These databases were selected because of their extensive coverage of scientific and technological research, providing a robust foundation for identifying relevant studies and extracting valuable insights [55], [56].

4.1 Search Strategy

All scientific publications from inception until September 2024 composed the search strategy. The Boolean search incorporated the keywords ("cybersecurity" and "metaversion") via the AND logical operator (Fig. 2 illustrates the search query). The researchers chose their keywords methodically to obtain an effective retrieval of suitable literature.

4.2. Inclusion and Exclusion Criteria

The research paper examined two selection criteria:

- The research depended on articles written in English, which appeared in respected academic journals or conference proceedings.
- The papers analysed Cybersecurity exclusively for the Metaverse or vice versa.

The following set of exclusion criteria was used for paper selection:

- Research papers written in languages other than English.
- The research analysis excluded scientific papers that did not link cybersecurity with the metaverse or the metaverse with cybersecurity.

4.3. Study Selection

A systematic process determines how duplicate papers are removed prior to identification. Special attention was given to reviewing titles and abstracts from selected studies through Mendeley software, which resulted in the dismissal of many nonrelevant papers and achieved a focus on relevant literature. The evaluation process then moved to a focused review of all the articles where researchers applied the predetermined selection standards from Section 4.2. The selection process became more refined through the exclusion of articles that failed to fulfil the established criteria in this evaluation step. Figure 2 shows the steps for article filtering, which led to the selection of the final studies.

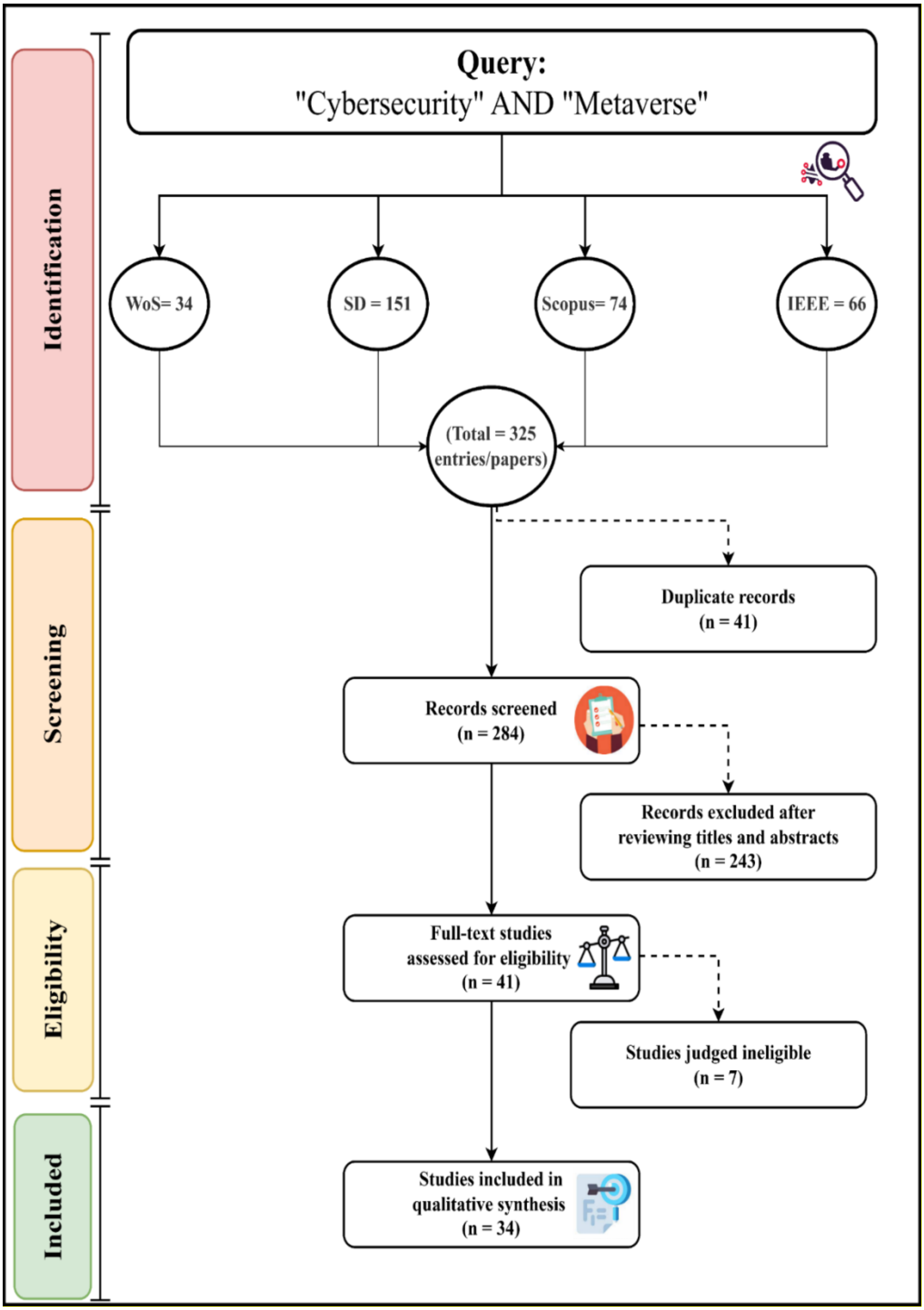

Identification
Screening
Eligibility
Included
Query:
"Cybersecurity" AND "Metaverse"
WoS= 34
SD = 151
Scopus= 74
IEEE = 66
(Total = 325 entries/papers)
Duplicate records (n = 41)
Records screened (n = 284)
Records excluded after reviewing titles and abstracts (n = 243)
Full-text studies assessed for eligibility (n = 41)
Studies judged ineligible (n = 7)
Studies included in qualitative synthesis (n = 34)

Fig. 2: SLR protocol.

The research followed systematic procedures to locate articles that fulfilled specified entry standards. An extensive database search produced 325 records, among which SD accounted for 151 papers, Scopus provided 74 papers, and IEEE delivered 66 papers, along with WoS, which supplied 34 papers. The analysis process started by reducing 41 duplicate records that left a total of 284 unique papers in the refined dataset. First, researchers reviewed titles and then abstracts and then discarded

243 studies that did not meet the research requirements. For the 41 articles remaining after full-text examination, researchers excluded 7 studies that did not match additional inclusion standards. The authors included thirty-four studies that met their requirements in their analysis of the final compilation.

5. CYBERSECURITY AND METAVERSE APPLICATIONS: TAXONOMY

The analysis process for the 34 selected articles required the establishment of three main subject groups to evaluate their details systematically according to suitable study criteria. The research findings form essential categories that researchers have divided into subgroups for better presentation organization (illustrated in Fig. 3). The research evaluation focused on analysing studies that used "cybersecurity" AND "metaverse" keywords to provide an extensive examination of the current state of technology in this field.

The examined articles presented three fundamental subcategories: “Cybersecurity”, “AI-Driven Security and IoT Applications”, and “Metaverse and Virtual Realities”. These categories contain two subcategories, which are explained further in the following list:

1. **Cybersecurity:** This category included 12 of 34 contributions (35.3%).
2. **AI-Driven Security and IoT Applications**: This category included 10 of 34 contributions (29.4%).
3**. Metaverse and Virtual Realities:** This category included 12 of 34 contributions (35.3%).

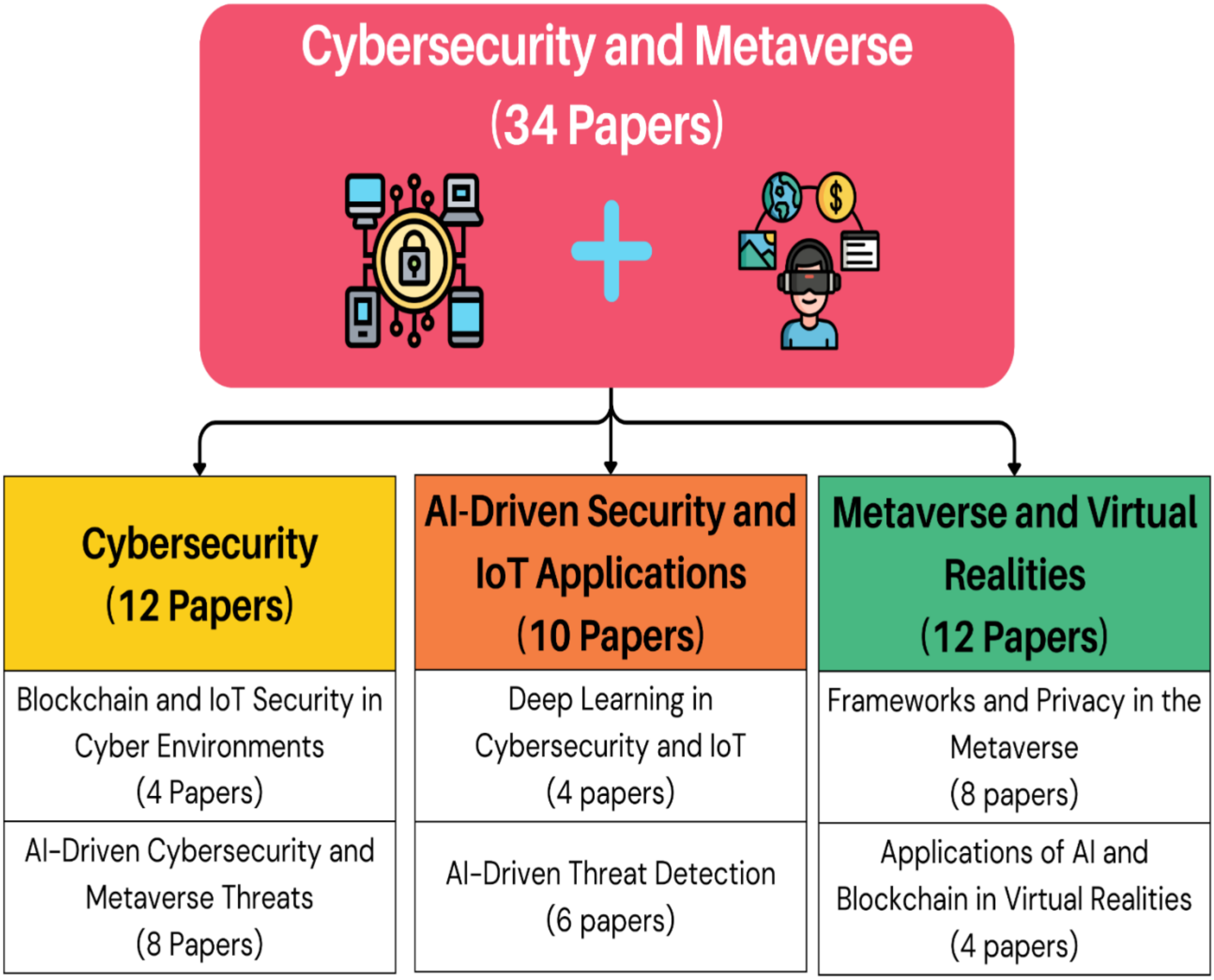

Cybersecurity and Metaverse
(34 Papers)
Cybersecurity
(12 Papers)
Blockchain and IoT Security in Cyber Environments
(4 Papers)
AI-Driven Cybersecurity and Metaverse Threats
(8 Papers)
AI-Driven Security and IoT Applications
(10 Papers)
Deep Learning in Cybersecurity and IoT
(4 papers)
AI-Driven Threat Detection
(6 papers)
Metaverse and Virtual Realities
(12 Papers)
Frameworks and Privacy in the Metaverse
(8 papers)
Applications of AI and Blockchain in Virtual Realities
(4 papers)

Fig. 3: Taxonomy of Cybersecurity and Metaverse Applications

5.1 Cybersecurity

This subsection discusses cybersecurity in terms of blockchain and metaverse threats.

5.1.1 Blockchain and IoT Security in Cyber Environments

While recent approaches such as a cyber range framework have simultaneously defined certain hardware 6G applications in information technology (IT) and operational technology (OT) to meet the requirements for security and privacy [57], the integration of digital twin models with artificial intelligence techniques to improve user experience has also been studied to strengthen defenses against cyber-attacks. First, inadequate practical investigations to prove that the proposed security model will be effective and multiply complexity, which will be introduced by some of the latest technologies, such as artificial intelligence, may prevent the adoption of commercial implementations. To ensure privacy and seamless interaction between users, the leveraging of blockchain technology in the metaverse has been proposed [58]. While it is an exciting prospect, integration with a blockchain has introduced scalability issues that could impact UX and system performance as a whole. Furthermore, trust in blockchain can be a double-edged sword, as dependence on it might create implementation challenges that needs to be addressed before widespread adoption in the metaverse.

For the security of metaverse applications, solid methods exist for app detection and classification. It has subsequently classified metaverse applications into three main categories—network infrastructures, real-time conversational applications, and nonreal-time applications—by using a large open-source dataset that contains all types of network traffic features [59]. Although they are effective, these methods rely on datasets that might not comprehensively reflect the complexity of metaverse traffic, highlighting the need for further extensive real-world testing. In [60], enhanced blockchain-based zero-trust security models were simulated and compared with standard security systems, and the results were evaluated on the basis of several metrics, mainly in terms of intrusion detection rates, response times to security breaches, etc. These studies, which were undertaken under newly established network infrastructures, illustrate how blockchain technology, along with zero-trust architectures, could safeguard the Metaverse. While the theoretical foundations are strong, the limited experimental validation highlights the need for further practical investigations to validate these findings.

5.1.2 AI-Driven Cybersecurity and Metaverse Threats

Advancing cybersecurity is increasingly dependent on offering reliable and transparent explanations for threat detection mechanisms that help analyse and understand anomalous behavior via normal behavior patterns. A method for detecting cyber threats in metaverse-based learning systems[61], which uses explainable AI and deep learning approaches, was proposed by . This is done by evaluating common model interpretability methods (SHAP, LIME), which is in itself a solution to a sore point in virtual education. However, its effectiveness might be limited by the absence of precise descriptions of the dataset properties, generalizability of its results, and validity metrics. Other studies [62] exploited known techniques from the past on modern devices and yielded similar exciting discoveries. This was aimed at both improving the security of virtual reality and conducting sociotechnical research in this area. The same study offered a variety of analytical and attack tools, evaluation datasets, representative vulnerability signatures, and exploitation examples, which were helpful to scientific and professional communities in developing virtual reality apps in safe ways. Nevertheless, the methodology has not yet been empirically validated , and more research is needed to validate the relevance of the heuristic. [63] listed five areas through which usability can be improved: user education, securing devices and networks, managing data privacy and identity, and protecting digital assets. It outlined a unified framework for cybersecurity in the post-Internet era, with a mission to improve cybersecurity generally, enact security and trust, protect the data rights of users, and educate users on the risks involved. Although the framework is strong, with real-world data and case studies, it is even stronger. Additionally, with the emergence of new threats, needs to be updated regularly for it to be effective. From a cultural perspective, another study [51] investigated the variables that affect cybersecurity behaviors in collectivistic contexts, providing insights influenced by differences in technology infrastructure and cultural factors. The results were pertinent to the metaverse context of the Malaysian background, which showed the background culture barrier. Ensuring ethical standards and examining these factors in different contexts, such as the developed world and the developing world, are important. In [64], a two-phase security architecture in which a lightweight cryptographic protocol with fuzzy logic and convolutional neural network (CNN) techniques were used for biometric authentication was suggested. There are privacy issues and vulnerability to spoofing attempts in this approach, which extensively uses biometric data. Additionally, her protocol has a high computational cost with respect to combining a CNN and fuzzy logic, which may violate the claim of being lightweight. The system also does not solve scalability and interoperability issues that result from the decentralized nature of the Metaverse. In [65], security features in mobile clouds and different types of wormhole attacks in the Metaverse were examined. The optimization focus covered statistical techniques such as the sequential probability ratio test (SPRT) for wormhole detection. The fuzzy weighted zero inconsistency (FWZIC) technique was improved in [66] by applying hexagonal fuzzy numbers to process weight assignment to components of industrial control systems (ICPSs). Although this is a novel approach, the findings might lack real-world relevancy without comparisons to industry performance standards. The relevance of the study could be improved through incorporating practitioner feedback.

Finally, one study [67] evaluated the ability of the Metaverse to offer educational and training opportunities in the cybersecurity domain. However, it fails to address challenges such as people on board, technical limitations and scaling the virtual environment. Additionally, the quantification of learning outcomes and a detailed comparison with conventional CTF methodologies could add more insight.

5. 2. AI-Driven Security and IoT Applications

This subsection discusses cybersecurity in terms of deep learning and AI-driven threat detection.

5.2.1. Deep Learning in Cybersecurity and IoT

A framework utilizing quantization-aware training (QAT) deep learning models has been developed for detecting dark web traffic to increase efficiency and accuracy [68]. To enhance interpretability, the framework implements explainable AI approaches such as SHAP and LIME. However, the dependence on limited datasets makes the accuracy and applicability of the insights to various contexts questionable. Moreover, the complexity of models requires considerable computational resources, which limits their application in low-resource IoT systems.

In metaverse environments, a deep learning-based intrusion detection system (metaverse-IDS) was also proposed to recognize twelve types of IoT attacks [69]. By employing CNNs, this system is able to achieve high accuracy in the detection of attacks, providing security and privacy across complex networks that interlink the metaverse and Internet of Things. While it has its strength, it mainly follows several benchmark datasets, which limits its use in the real world. The findings may be more reliable if comparisons are expanded to include a wider array of models. In this context, a deep learning-based method for channel estimation for next-generation wireless networks is proposed, with a focus on reducing the computational cost and improving the accuracy of the estimation [70]. While the paper presents meaningful insights into deep learning models' susceptibility to adversarial attacks in channel estimation, it could further contribute by probing more of the existing adversarial attack methods alongside possible self-examining defenses. In [71], an AI-based framework utilizing ECG and EEG signals for biometric authentication in digital environments, such as the Metaverse, was proposed. The proposed system provides versatility by enabling the authentication of a varying number of users without the need to retrain the model. Although the framework was novel, they needed to analyse the practical challenges associated with such a framework, such as data requirements or technical complexities, which could accompany real-world applications.

5.2.2 AI-Driven Threat Detection

The investigation of user sentiment about the Metaverse through sentiment analysis techniques, including machine learning and natural language processing (NLP), explores user-generated content from social media platforms to gain insights into individuals' thoughts, feelings, and emotions regarding the Metaverse [72]. This understanding is important not only for providing enterprises and service providers with useful insights to optimize user experiences but also for overcoming misunderstandings of metaverse adoption and user response. This study increases its relevance by validating sentiment analysis against 300,000 tweets, generating a robust dataset. However, the adequacy of the findings across different cultures is difficult, making the implications of the findings less generalized. Future works should consider the use of qualitative analyses, more elaborate demographic studies, and flesh out longitudinal approaches to provide additional understanding. Although there are limitations to the methods and results of this study, the overall contribution to the field is impactful, and a consideration of these limitations would add even more relevance to its findings. Using spatiotemporal user behaviors as a medium to conceal backdoor triggers and actions introduces a new security concern, especially for behavior-oriented decision-makers in the Metaverse [73]. Simple rule-based decision makers for metaverse scenarios introduce a significant security risk when data-driven, behavior-oriented decision makers utilizing deep neural networks are introduced. Such networks bring new threats, such as backdoor attacks, in violation of the privacy and technical security of metaverse systems, which further complicates their practical development. Another study [74] investigated potential risks by analysing user interactions with avatars in the Metaverse, which led to the creation of the simplified avatar relationship association with nonlinear gradient (SARANG) model. This model describes the full infrastructure and data flow at the moment a user interacts with the Metaverse. A breadth of literature [75] relevant to metaverse security outlines different imperatives for privacy and security around which minimizing risks can be established in a virtual ecosystem. In addition, a cascaded architecture was created using long short-term memory (LSTM) and gated recurrent unit (GRU) neural networks to build the most suitable model to overcome the peculiar attacks of the 6G-enabled Metaverse [76]. By bolstering intrusion detection, this model helps promote cybersecurity and protect privacy. Critique may be directed at oversimplifying the nuances of intrusion detection by focusing solely on LSTM and GRU models attempting to identify the relevant security dynamics. Additionally, the lack of large-scale implementation tests limits the context validity of the performance of the model in uncontrolled environments. A systematic security analysis of Metaverse based on the well-known STRIDE threat model was subsequently presented [77]. This paper identifies potential threats to the Metaverse and provides mutual mitigations. Nevertheless, it provides theoretical insights but lacks validation from the real world and would have benefited from empirical evidence.

5.3. Metaverse and Virtual Realities

This subsection discusses cybersecurity in terms of privacy in the metaverse and applications of AI and blockchain in virtual realities.

5.3.1. Frameworks and Privacy in the Metaverse

In recent studies, various approaches have been proposed to increase the security and privacy of the metaverse environment. For example, a cost-effective, decentralized multiauthority privacy protection mechanism for social media is described that is traceable and reversible [78]. However, the scalability and possible processing overhead critical to practical metaverse applications have not been thoroughly examined in this study, indicating a need for further empirical investigation. On the other hand, another study proposed a novel framework for health monitoring in the metaverse, using advanced encryption standards (AES) encryption to protect data. Although this method of encryption is reliable, it can mask other important measures, such as data latency and the scale of systems [79]. The global components of the VR world are explicitly described, with potential threats and vulnerabilities caused by a combination of these components analysed [80]. As part of the related work on security improvement, a deep learning-based intrusion detection system is proposed for virtual reality networks with interpretable analysis to enable security analysts to comprehend the model's behavior [81]. On the one hand, the limited dataset on which this study relies may not address the broad spectrum of threats that arise in VR environments, thereby limiting the generalizability of its findings. In addition to SHAP being able to interpret the model, using a different or more advanced interpretability approach may help the user better understand the reasoning behind the model decision.

From another angle, an embedded smart healthcare system was implemented in Metaverse, which focuses on human–computer interaction, wearable biomedical devices, and the digital security of such systems [82]. While the concept in this study is quite forward-thinking, it could use more in-depth thoughts on practical barriers in the healthcare arena, such as privacy concerns surrounding users and technological limitations. Moreover, a decentralized identity management system of the Metaverse is proposed to eliminate personally identifiable information (PIIs) leakage and other cyberspace threats of these associated platforms [83]. The paper is a technologically agnostic approach and follows an empowerment framework wherein users should always have control of their identity but does not provide sufficient insights into integrating the solution into existing metaverse to see what is the alignment with current needs and use cases in identity management. To solve the privacy issue of federated learning during the training of avatars in the Metaverse, one work introduces an incentive-based differential privacy federated learning model [84]. However, the study addresses only select threats and uses standard datasets that do not implement real-world conditions. Pioneering Battlefield Threats Projects need to be extended, with thorough threat analysis and diverse patterns of assessment as part of plans to bootstrap the framework to facilitate usability and stability improvements.

Finally, an antidisguise authentication mechanism based on the first impression model for metaverse avatars is proposed. The idea is to assist avatar authentication by storing and recalling the first meeting situation [85]. To protect against the adversarial manipulation of these first impressions, this paper devises a chameleon-based sign encryption mechanism and a ciphertext authentication protocol. Nonetheless, the limited real-world applicability and absence of thorough performance measures over a range of scenarios within the study, in addition to privacy issues associated with large-scale data collection and processing, indicate areas for improvement to make these technologies more useful in practice.

5.3.2. Applications of AI and Blockchain in Virtual Realities

A sharding-based blockchain framework specific to the Metaverse, called "Meta Shard," was proposed in [86]. Through this framework, we seek to establish a lightweight consensus algorithm termed "proof-of-engagement", which is used by both data consumers and providers of computational resources. Even if simulations yield high accuracy, the system needs to adapt to different practical issues described below, i.e., to ensure that this also works in the real world, a more detailed security analysis needs to be conducted. Conversely, [87] studied the incorporation of blockchain with the "zero-trust" approach of the security model, which relies on the new age of modern network scripting infrastructure. The study compared the operation of blockchain-based security systems with that of conventional security systems and used the results to establish that the adoption of the enhanced security model for the Metaverse is theoretically essential but lacks experimental proof in the real environment.

Similarly, the authors of [88] introduced the ParaDefender system to address new security attacks in the Metaverse. This system works on parallel intelligence, the integration of artificial cyberspace and parallel execution, which allows the interaction of artificial and real cyberspace to be synchronized on the basis of security requirements. The work in [89], on the other hand, presented another model to optimize engineering control tools while utilizing digital twin capabilities and other components of "CPMMS" to solve open issues in this area. This method is novel, yet its prototype has no empirical validation and provides little discussion about scalability and integration in various manufacturing settings, which could limit its applicability.

6. DISCUSSION

This section focuses on four key aspects related to Cybersecurity in the Metaverse: motivations, challenges, limitations, and recommendations (see Figure 4).

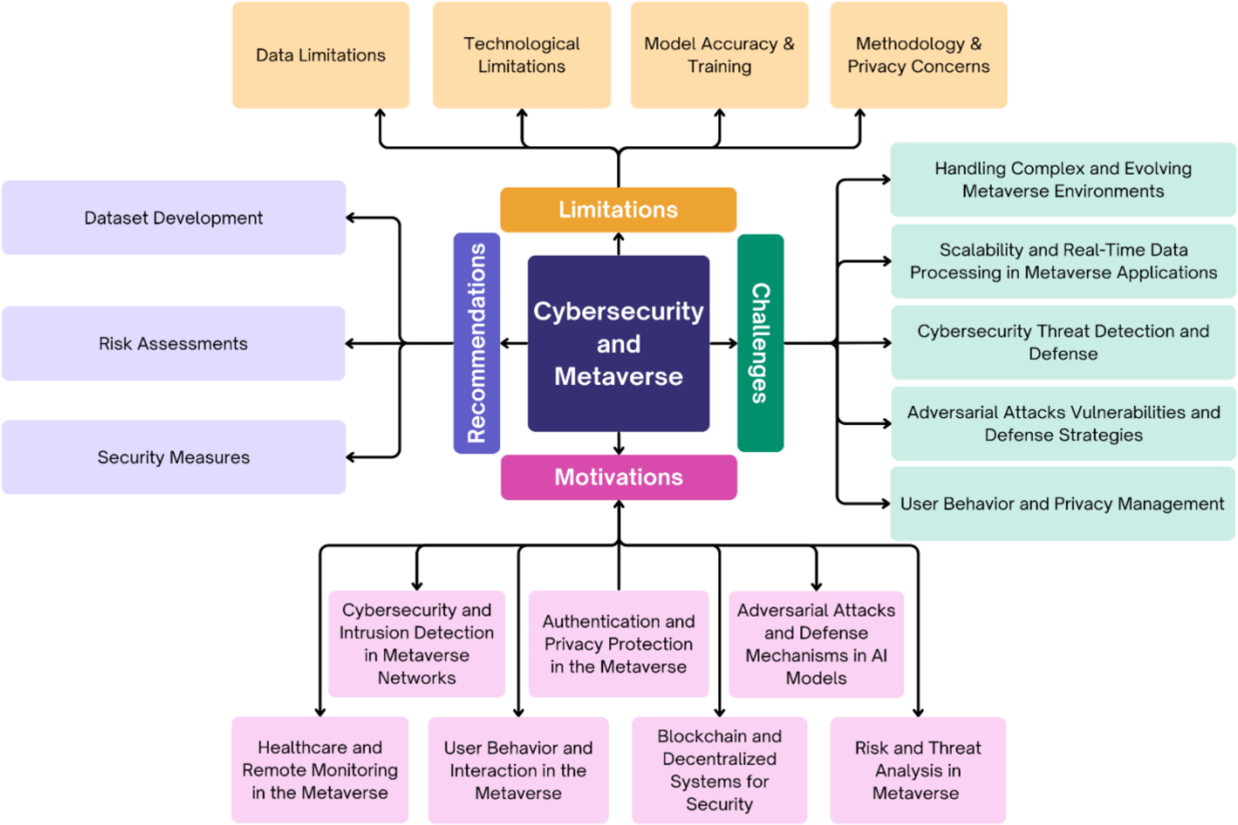

Data Limitations
Technological Limitations
Model Accuracy & Training
Methodology & Privacy Concerns
Limitations
Dataset Development
Risk Assessments
Security Measures
Recommendations
Cybersecurity and Metaverse
Challenges
Handling Complex and Evolving Metaverse Environments
Scalability and Real-Time Data Processing in Metaverse Applications
Cybersecurity Threat Detection and Defense
Adversarial Attacks Vulnerabilities and Defense Strategies
User Behavior and Privacy Management
Motivations
Cybersecurity and Intrusion Detection in Metaverse Networks
Authentication and Privacy Protection in the Metaverse
Adversarial Attacks and Defense Mechanisms in AI Models
Healthcare and Remote Monitoring in the Metaverse
User Behavior and Interaction in the Metaverse
Blockchain and Decentralized Systems for Security
Risk and Threat Analysis in Metaverse

Fig. 4: Discussion Taxonomy of Cybersecurity and Metaverse Applications

6.1 Motivations

This subsection discusses the significant motivations for cybersecurity and metaverse integration.

6.1.1. Cybersecurity and Intrusion Detection in Metaverse Networks

With its inherent linkages to IoT devices and 6G networks, Metaverse's rapid development has ushered in a new era of cyber security threats. Because these environments produce immense amounts of data and enable highly complex user interactions, they naturally increase the threat from cyberattacks. The existing intrusion detection systems (IDSs) have been proven ineffective in meeting the unique requirements of these networks, and tailored and novel approaches need to be developed [69]. In addition, the dependence of educational institutions on metaverse learning platforms underscores the need for a strong cybersecurity mechanism. They are sensitive because their data, particularly user data, are sensitive, their need for virtual space interaction is also essential, and these platforms are vulnerable to cyber threats. To protect these platforms, advanced detection mechanisms that can adapt to new attack vectors are needed [61]. Similarly, there are security challenges that pertain to 6G-enabled metaverse environments. While the high-speed and low-latency nature of the 6G networks greatly enables immersive environments of the Metaverse, it also exposes such environments to new threats that are hardly mitigated by existing security measures [76]. A further concern is the vulnerabilities of virtual reality networks, which are the foundation of many experiences in the Metaverse. These networks are becoming more vulnerable to nonimmersive attacks, jeopardizing the security and integrity of virtual habitats. Problems can lead developers to create more challenges on the basis of vulnerabilities while they are developing. Additionally, the increasing number of IoT applications in Metaverse has created challenges, such as deep web traffic detection and wormhole attacks. These issues call for improved IDS strategies for the protection of the metaverse ecosystem integrated IoT [65], [68]. The multidimensionality of the Metaverse also calls for a robust investigation into its privacy and security elements. As mobile applications proliferate and malware becomes more prevalent, maintaining a secure and trusted virtual space becomes paramount. There have been great improvements in metaverse technology, yet there is still a lingering divide between the advancement of virtual environments and countermeasures to protect these environments from breaches. Despite the important role of technology in determining attacks, technology is often conveniently left out of the narrative, which deserves attention for threats such as virtual-reality-synthesized attacks that merge the dimensions of so-called 'virtual' and 'actual' [75], [77]. Despite countless innovations in the aforementioned areas, the Metaverse still pales in comparison to how the internet actually works because technological capabilities continue to outweigh cybersecurity practices. To bridge this gap, it is necessary to proactively improve the research and development of intrusion detection and threat mitigation. Focusing on security, in tandem with innovation, will create a more robust and trustworthy metaverse ecosystem [88].

6.1.2. Authentication and Privacy Protection in the Metaverse

With the exponential growth of the metaverse and increasing reliance on the Internet of Things (IoT), the demand for strong, scalable user authentication systems to protect users against escalating digital threats has never increased. Recent research has suggested that unique biometric signals, such as electrocardiograms (ECGs) and electroencephalograms (EEGs), could be harnessed for developing AI-based systems to offer increased digital security [71]. Moreover, protecting users' health data, particularly with respect to wearable biomedical devices, is a high priority. Making these devices able to operate in the Metaverse renders possibilities for novel human–computer interactions but also requires developed protocols to ensure the security of health-related data in complex digital environments [78].

Securing interactions in the transverse environment poses significant challenges to the safety of personal data. A suggested solution is to use blockchain within metaverse platforms to enable users to interact freely while being confident in the security of their data [58]. Moreover, to better ensure metaverse security features, these authors present a two-phase security structure, which adopts fuzzy logic and CNN methods to perform biometric authentication, followed by the use of lightweight cryptographic protocols [64]. With Metaverse becoming more promising, there is an evident need for structured work to ensure that a safe ecosystem is formed to provide the confidentiality, integrity, and privacy of users' PIIs. These efforts play a vital role in building trust and preserving digital identities [83]. A different novel approach to verification in the Metaverse uses the idea of "first impressions" in real life to authenticate identity. One study proposed an antidisguise authentication system in which the first encounter of avatars is recorded and remembered to authenticate users. A chameleon-based signcryption mechanism was built in conjunction with a ciphertext authentication protocol that helps avoid forgery or replacement of the first impression where the public verification of encrypted identities is guaranteed [85].

6.1.3. Adversarial Attacks and Defense Mechanisms in AI Models

The rapid evolution of next-generation wireless networks and Metaverse has also introduced several challenges of a different kind, especially with respect to defending against new threats. One important problem that exists is that the deep learning models used in channel estimation for future wireless networks are increasingly complex and vulnerable. These vulnerabilities make critical systems vulnerable to potential adversarial attacks; thus, mitigation methods are needed to make these types of models more robust [70]. Moreover, the metaverse provides unique risks with behavior-driven decision-making algorithms. An existing study emphasized the danger of spatiotemporal backdoor attacks, which train user behaviors to bypass traditional input–output attacks. This approach also allows some backdoor triggers and actions to be invisible to human judgments, leading to an undiscovered class of physical threats and natural threats to decision-making systems in autonomous environments [73].

6.1.4. Healthcare and Remote Monitoring in the Metaverse

The expanding capabilities of the Metaverse have paved the way for innovative applications in both healthcare and cybersecurity education. The metaverse's applications in health monitoring look interesting, with one of the first frameworks being proposed to assist with IoT-based remote patient monitoring and virtual consultations. To achieve this, the framework leverages modern encryption algorithms such as AES-256, thus providing the security of sensitive medical data during transmission, which is one of the major concerns among digital healthcare entities [79]. Integrating the Esantem smart health care system in Metaverse also presents some prospects and challenges. This paper investigates the adaptation of traditional healthcare services to the Metaverse, the improved ability of human–computer interaction, and the secure transmission of medical data retrieved from wearable biomedical devices in virtual circumstances. These advancements highlight the strength of the Metaverse in enabling healthcare transformation by providing secure and interactive solutions for patients [82]. To further advance education and training in cybersecurity, the Metaverse is being evaluated as a pedagogical platform. Researchers have explored the utility of the Metaverse as a testing environment through practical case studies, comparing the execution of capture flag (CTF) exercises in metaverse versus physical settings. This exploration highlights the potential of Metaverse as an immersive and scalable medium to train the next generation of cybersecurity practitioners [67].

6.1.5. User Behavior and Interaction in the Metaverse

The rapid evolution of the Metaverse has spurred growing interest in its potential to transform various societal aspects, including communication, relationships, and economic frameworks. As an increasing number of people are exploring the metaverse, it is imperative to rectify key security and optimization concerns so that the metaverse can seamlessly blend into people's daily lives [72]. One major area of concern is user authentication. On the basis of the approach of first impressions when we interact physically, an antidisguise authentication system is proposed. In this method, the framework stores and remembers the first meeting scenarios of the avatars in the Metaverse to ascertain the authentication correctly. To enhance the security of profile linking, the system is based on a chameleon-based signcryption mechanism and a ciphertext authentication protocol, guaranteeing that encrypted profiles can be publicly verified and preventing the adversary from either forging or substituting the first impression [85]. It is therefore important in the field of cybersecurity behavior to identify factors that drive users to do something in collectivistic environments. Almost all of these factors are determined by culture and regional technology infrastructure differences. The goal of this study is to identify the factors that enhance cybersecurity behavior across various environments [51]. A major challenge is to optimize engineering practices in the Metaverse. Effectively controlling engineering tools can be achieved via a model that incorporates digital twin features and combines them with other elements of Cyber-Physical Metaverse Manufacturing Systems (CPMMS), as proposed in the literature. This model is still open and allows overcoming the questions whose state of the art could have had an impact on the development of efficient and robust engineering solutions in virtual environments [89].

6.1.6. Blockchain and Decentralized Systems for Security

Metaverse application development and operations rely heavily on blockchain technology since it provides exceptional security and transparency while ensuring seamless verification of virtual assets. Create trustworthiness in assets, data and boundaries of use. By utilizing the decentralized nature of blockchain, metaverse platforms can add a layer of security for virtual transactions, resulting in secure, transparent, and tamper-proof features, with trust built between users and stakeholders [59].

6.1.7. Risk and Threat Analysis in the Metaverse

As Metaverse has expanded and during the growth of IoT applications, new cybersecurity issues have arisen. To address one vivid and concrete concern, wormhole attacks can be used to exploit vulnerabilities in communication protocols to intercept or manipulate data transmissions. These dangers necessitate the implementation of more sophisticated systems, such as statistical-based intrusion detection systems, to secure reliable engagement in the Metaverse. Automated detection solutions in a metaverse environment are critical for protecting user data against malware attacks and limiting this access [65].

6.2 Challenges

As Metaverse integrates advanced technologies such as the IoT, biometric systems, and digital twin capabilities, several key challenges emerge that demand innovative solutions to ensure a secure and efficient virtual environment.

6.2.1. Handling Complex and Evolving Metaverse Environments

The Metaverse is an ever-growing digital ecosystem that poses its own set of cybersecurity challenges that stem from its complexity and scale. One major concern is the enormous amount of data produced by networks and broad network interactions. Traditionally, intrusion detection systems (IDSs) have not sufficiently fulfilled the particular security requirements of metaverse-IoT environments, which has led to various cyberattacks on these systems [69]. In addition, with the introduction of 6G-based metaverse settings, security risks are surging, which demands inventive solutions that surpass standard security measures. The integration of advanced techniques such as deep learning for intrusion detection has been suggested as a means to address these issues effectively [76]. Owing to its decentralized nature, blockchain technology is recognized as a key driver of metaverse security, providing transparency and security while ensuring virtual asset verification. However, the journey of scaling the blockchain is full of hurdles, especially in terms of complex management of distributed systems [86]. With the increasing number of metaverse spaces, the variety of user interactions and decentralized apps poses many cybersecurity threats. New threats include social engineering attacks where the attacker exploits a user's social instincts to gain sensitive data and vulnerabilities of decentralized applications that, despite improvements in the decentralization of the service, can become a target for attackers [63].

6.2.2. Scalability and Real-Time Data Processing in Metaverse Applications

One significant challenge is the development of scalable and robust authentication systems that can cater to the complex and dynamic nature of the Metaverse. Integrating unique biometric signals, ECGs and EEGs will enhance user authentication and may lead to highly secured and scalable user identity management in this new reality [71]. Blockchain technology has been proposed as an answer to various data security and privacy problems. It builds a platform that allows users to participate without worrying about data theft by allowing connections on a decentralized and safe connection. On the other hand, the challenges of introducing blockchain into metaverse platforms need to be explored to guarantee smooth functioning and scalability [58]. Moreover, security issues for the detection of dark web traffic in IoT networks are urgent. With the development of the Metaverse, it is critical to secure the data flow and defend against malicious activities (e.g., hidden traffic) to uphold user trust and system integrity [68]. The Metaverse is also revolutionizing the healthcare industry. IoT-based telemetry services for remote patient monitoring and virtual consultations employ encryption protocols such as the AES-256 protocol to safeguard sensitive health data. Although these frameworks provide security in practice by monitoring health in virtual spaces, challenges, including data interoperability and scalability of such systems, are not very well addressed [79]. Likewise, the deployment of platforms such as the Esantem Smart Healthcare System in the Metaverse demonstrates the necessity of transforming traditional healthcare procedures into the virtual realm. These include mining valuable insights from immutable and verifiable data and novel human–computer interactions to mitigate concerns about wearable biomedical devices that can improve the performance of healthcare systems [82]. Finally, digital twin technology in cyber-physical manufacturing systems (CPMMS) highlights the need to optimize control engineering tools. As such, creating complete models that apply these technologies to solve real-time monitoring, data synchronization, and decision-making problems are important steps toward establishing the Metaverse as an innovation space [89].

6.2.3. Cybersecurity Threat Detection and Defense

The fast-paced development of Metaverse poses several cybersecurity issues that need real-time and concrete solutions. One such challenge is the gradual reliance on and popularity of metaverse learning environments, given the urgent need for applicable cybersecurity approaches. Their dependence exposes deep flaws in these systems, which store vast amounts of sensitive information and mediate sophisticated interactions, creating numerous potential attack surfaces [61]. Other serious threats of nonimmersive attacks by VR networks are rising threats. These attacks take advantage of vulnerabilities in VR architectures, threats that can destroy the user's experience and threaten sensitive information [81]. The threat of wormhole attacks is another problem that cannot be ignored and is definitely urgent, taking into consideration the sky-rocketing new mobile apps coming in the metaverse decentralized IoT layer. This is a significant point to support the importance of automated malware detection mechanisms because traditional methods do not cope with the changing and complex nature of threats in the Metaverse ecosystem [65]. Furthermore, the rapid expansion of the Metaverse has intensified concerns regarding the confidentiality, integrity, and privacy of personally identifiable information (PII). The development of a secure metaverse that safeguards such information has become a primary focus, necessitating the implementation of frameworks that enhance cybersecurity and privacy in virtual environments [75]. Finally, the increasing complexity of metaverse systems calls for comprehensive analyses based on threat models to identify security vulnerabilities and develop effective mitigation strategies. These efforts aim to build a trustworthy metaverse capable of resisting evolving cybersecurity threats while maintaining user confidence [64].

6.2.4. Adversarial Attack Vulnerabilities and Defense Strategies

As a large software environment, the fully reactive metaverse system is burdened by daunting challenges in terms of security, privacy and efficiency. One of the major problems is the mapping function between resources and channel characteristics, which does not generalize well without overfitting training samples, which is one of the main reasons why deep learning algorithms are sensitive to adversarial attacks, which leads to poorer performance [70]. To the forcing point, uncertain human behavior modelling in autonomous systems such as the metaverse leads to vulnerabilities to spatiotemporal backdoor attacks that prompt sequential behavioral data manipulation to diminish decision-making processes in behavior-based systems [73]. The traditional security architecture ignores the fact that the interactive, connected and on-demand workings of the metaverse require more dynamic, lightweight solutions, including biometric-based cryptographic authentication with fuzzy logic for adaptive, accurate, and on-the-fly security and decision making [64]. Moreover, privacy protection remains a pressing concern, as centralized models for safeguarding user data in social metaverse settings limit user control, making them susceptible to privacy breaches and misuse. This highlights the need for decentralized, traceable, and revocable mechanisms to ensure data security and user empowerment [71]. Addressing these challenges requires a robust and innovative approach to enhance trust and resilience in metaverse ecosystems.

6.2.5. User behavior and privacy management

The Metaverse presents various unique challenges that must be addressed to ensure secure and private user experiences. One of the main problems is that avatars in virtual worlds tend to be rudimentary digital objects, which may allow attackers to easily misrepresent their appearance. This generates a need for antidisguise authentication systems that use avatars' insights into their first impressions to spot and avoid impersonation [85]. In addition, although Metaverse has immense potential, its user adoption rate is still fairly low because of concerns about data privacy and security threats, which undermines the degree of trust in user engagement. Hence, effective sentiment analysis using machine learning approaches is important for understanding people’s sentiments and worries in such settings [72]. Barriers to cybersecurity behavior, such as identity theft and loss of digital assets, must also be addressed to protect users in the Metaverse [51]. Despite it being a significantly growing technology, there is a lack of research regarding the security and privacy aspects of metaverse. This provides an important gap toward building an integrated strategy to protect our users, as they explore these increasingly troubling navigation spaces [75]. Moreover, with the rapid development of technology and the agile mechanism of Metaverse, comprehending the behavior of users and designing suitable protection mechanisms have become much more complicated [63]. Furthermore, owing to decentralized and web applications in the Metaverse, existing approaches to network-based and centralized security models cannot be adopted, which means that the requirements for an efficient, scalable, and sustainable identity management solution for the Metaverse remain vital concerns [83]. Therefore, these challenges urgently indicate the need for novel security strategies and approaches that address specific requirements in the context of metaverse environments, together with the education of users so that they can take steps to mitigate risks and safeguard their data.

6.3. Limitations

This subsection explores limitations in the integration of cybersecurity and the metaverse.

6.3.1. Data limitations

Studies on metaverse systems have many limitations in terms of technical, security and other factors; these limitations restrict these systems from modelling effective solutions under complex and heterogeneous virtual spaces. In the first case, some studies used unstructured data to measure user intention instead of actual behaviors, giving rise to potentially superficial conclusions that fall short of encapsulating user sentiments or reactions [72], [83]. Furthermore, one of the practical challenges in predicting all security vulnerabilities is the inherent dependence on conceptual frameworks owing to the rapidly evolving nature of the metaverse. This lack of implementation of the frameworks implies that it is challenging to accurately predict how users will misbehave [61], [71]. Moreover, certain security frameworks may depend on particular datasets, which do not encompass the entire spectrum of network traffic in authentic metaverse settings, thereby limiting the generalizability of the findings [76]. The absence of a specific dataset for cybersecurity for virtual reality is another challenge to overcome in terms of source; this lack of data sometimes limits models and makes them unable to handle a wide variety of threats [81]. However, the handling of sensitive data in a digital twin environment presents challenges, and the integration of IT/OT systems increases the complexity of integration together with innovation and performance [68]. In future studies, more threats may emerge along with the continued evolution of the Metaverse along with the ethical dilemmas and psychological impact of extended exposure to virtual worlds [75]. This can also limit the generalizability of the results to other applications because the deployment of a specific application in the 5G network's physical layer will create problems in extending the results to other applications [70]. Furthermore, the standardization of the doctor–patient interface in smart healthcare systems in the Metaverse context is an urgent issue in consideration of privacy concerns [82]. Finally, future research should focus on replicating cybersecurity exercises with larger participant samples and on the use of automation techniques to increase efficiency [67].

6.3.2. Technological limitations

The dynamic development of technologies within the Metaverse gives rise to a considerable challenge in gaining a comprehensive understanding of the security threats in these environments. This complexity is compounded by the reliance on conceptual frameworks that serve well in theory but often prove inadequate for tangible, real-world applicability, rendering them ineffective in addressing actual security challenges [63]. Moreover, to improve the effectiveness of and degree of trust in metaverse platforms, future studies should investigate user attitudes toward the most trustworthy technology tools in the Metaverse. Researchers can gain insights into the factors influencing the usage and acceptance of metaverse technologies by employing trust theory, social theories, and technology acceptance models [66].

6.3.3. Model accuracy and training

Metaverse technology has evolved at breakneck speed, creating a severe challenge for comprehensive cybersecurity. According to the first source, one of the issues noted is the necessity of suitable training programs to provide practitioners with the relevant skills to counter emerging threats within the Metaverse [82] Likewise, the dependency on AI-based simulations (e.g., CARLA and AIRSIM) to validate backdoor weaknesses highlights the changing landscape of security challenges in these systems [73]. Moreover, in the case of the Metaverse, interactions between avatars driven by AI and avatars driven by humans may lead to even more complexity regarding the security and authentication of the user interactions [85]. Such restrictions illustrate the requirement for more pragmatic frameworks that consider the specific security challenges accompanying metaverse and IoT integration, which traditional measures cannot effectively cover.

6.3.4. Methodology & privacy concerns

Challenges in integrating metaverse privacy protection into the real world are still evolving. One of the approaches is a decentralized, traceable, and revocable CP-ABE scheme [78] that overcomes these challenges, which allows the tracing of malicious users and revocation of privacy when conditions change. However, further exploration of fuzzy set environments could optimize these models, as seen in the suggestion to extend the FWZIC method by incorporating circular intuitionistic fuzzy sets [89]. Enhancing Scheme Adaptability to Dynamic and Complex Metaverse: This facilitates the adaptability of privacy protection schemes in a dynamic and complex Metaverse. In addition, an issue that is still open is the understanding of the drivers of cybersecurity behavior in the Metaverse. We suggest conducting longitudinal studies to evaluate how user behaviors change over time, taking into consideration variables such as cybersecurity culture, digital literacy or personality traits that can have important influences on cybersecurity outcomes [51].

These constraints highlight the complexity of building robust privacy and security frameworks for the Metaverse. Future research should continue to refine methods for privacy protection, enhance behavioral understanding, and explore new fuzzy environments to ensure more effective and adaptable cybersecurity measures.

6.4. Recommendations

This subsection provides recommendations for integrating cybersecurity and the metaverse.

6.4.1. Dataset development

As the metaverse continues to evolve, there is a need to explore new methods for solving complex problems to facilitate the development of cybersecurity frameworks. Many recommendations push for advanced deep learning models to identify combat of emerging-type attacks and ponder whether predictions should typically be performed in the cloud or at the edge. Combined with new encryption methods, this approach can greatly improve the security of intrusion detectors deployed in practice on the basis of actual data recorded on realistic networks [69]. In the same vein, the efficiency of biometric authentication is subject to the availability of representative datasets for more precise models and neural networks for more accurate and refined authentication of new users [71]. Equally, the need to build datasets representing the rapidly evolving threat landscape is critical, and adapting detection systems to future challenges [81]. Furthermore, the appropriate implementation of metaverse-based smart healthcare systems requires guard against cyber attacks and the privacy of medical data [82]. To identify backdoor attacks, the requirements for mechanisms that comprehend spatial and temporal features throughout sequential data are still urgent and can withstand advanced threats more effectively [73].

6.4.2. Risk Assessments

The cybersecurity issues of Metaverse involve multiple approaches that range from those driven by advanced systems, collaborative structures, and user-oriented methodologies. User Trust and Engagement: Longitudinal studies examining user sentiment in a variety of geographic areas, together with privacy-preserving marketing strategies, can help increase trust and engagement among users [72]. To address these emerging threats, collaboration between industries to ensure strong cybersecurity standards, as well as the integration of state-of-the-art technologies such as blockchain and AI, are needed [63], [76]. Advanced techniques such as intrusion detection systems, adversarial training techniques, and federated learning are needed to mitigate security risks in real time [57], [70]. Adhering to strict implementation protocols is paramount to avoid vulnerabilities such as improper management of login credentials and command delegation errors, as described in recent case studies [67]. Moreover, the unique characteristics of the Metaverse, such as decentralization and immersive realism, demand scalable, interoperable, and zero-trust security models to address its inherent complexities [65], [78], [84]. Future research should focus on improving blockchain technologies and exploring innovative solutions for managing the dynamic and heterogeneous nature of the Metaverse, ensuring both user autonomy and robust cybersecurity [58]. This integrated approach will be critical to navigating the evolving landscape of the Metaverse securely [89].

6.4.3. Security Measures

This research encourages the advancement of feature selection techniques to increase the accuracy of threat detection models, alongside the progress of explainable AI techniques such as SHAP and LIME, to unravel the decision-making of models and build trust in their implementation in an IoT landscape [68]. Nonetheless, centralized privacy protection models still face several issues, such as reducing computational and storage costs, avoiding single points of failure, and securely revoking malicious users' authorizations [78]. Furthermore, the lack of technical challenges related to the interoperability of IoT, AR, and VR technologies ultimately delays the development of a successful Metaverse [66], [79]. Furthermore, research highlights users' tendency to trust avatars with familiar appearances and voices, increasing the risk of deception if the "friend" is fake. This necessitates advanced authentication systems to prevent such fraud [85]. Finally, future work should focus on evaluating federated learning models and privacy-preserving techniques across diverse metaverse settings. Expanding research to defend against a broader range of attacks and conducting a more in-depth analysis of privacy preservation in federated learning, particularly concerning avatars, is also recommended [84].

7. GAPS, OPEN ISSUES AND SOME INNOVATIVE KEY SOLUTIONS

This section aims to identify gaps in the field for future studies, potentially benefiting researchers. Each subsection focuses on a specific gap and highlights areas lacking in applying cybersecurity in the context of the metaverse. The following subsections present noteworthy figures, tables, and analyses that provide an overview of the latest advancements in cybersecurity for metaverses found in the literature.

7.1. AI Directions in the Metaverse

In this section, we link the branches of AI to each metaverse, as presented in Section 4. We have explained six main branches of AI (ML, DL, XAI, fuzzy logic, and decision-making) on the basis of their coverage in scientific research. Table 1 displays the AI techniques used in the literature to which they were applied in previous studies.

TABLE I. AI TECHNIQUES AND THEIR RESPECTIVE APPLICATIONS IN THE METAVERSE

Ref.	AI Direction	Method Used	Metrics Used
[84]	DL	neural network	N/A
[59]	ML and DL	Logistic Regression XGBoost DNN	Precision, Recall, F1-score, and Accuracy
[66]	Decision making	MCDM (FWZIC · ARAS)	N/A
[73]	DL	MLP-D, RNN-D, ARNN-D, Tran-D, EAtt-D, GEA-D	COLLISION RATESPEED, EPISODE REWARDS, RUNNING DURATIONS, LONGITUDINAL DRIVING DISTANCE
[64]	Fuzzy logic and DL	CNN	Accuracy, precision, recall, F1-score
[72]	ML	SVM, Doc2Vec, RNN, and CNN	Accurcy
[69]	DL	CNN, KPCA	accuracy , precision , recall , FNR
[61]	DL	DNN	accuracy
[71]	DL	CNN	precision, recall, F1-score
[76]	DL	LSTM-GRU	Accuracy
[81]	DL	CNN	accuracy, precision, recall, f1-score
[57]	ML	DTMN	accuracy, precision, recall, and F1 scores
[70]	DL	CNN	N/A
[68]	DL, XAI	CNNs-GRU-FCN	accuracy

N/A is not applicable.

According to the information presented in Table 1, the analysis of AI techniques used in the context of metaverse and the areas that are covered only in scientific research are as follows:

- **ML** methods focused on categorization in the Metaverse include doc2vec, SVM [72], XGBoost, and logistic regression [59]. Despite their effectiveness, ML applications are less common than DL due to scalability issues when handling the massive volumes of data generated in the Metaverse.
- **DL**: Due to its proficiency in managing intricate tasks within the Metaverse, DL is the dominant research field. Studies have utilized DL models, including CNNs [64][69][71][81][70], RNNs [73], DNNs [59][61], and neural networks [84], for applications such as biometric-based authentication, cybersecurity, and intrusion detection. Hybrid models such as CNNs-GRU-FCN [68] and advanced architectures such as LSTM-GRU [76] are employed for tasks requiring robustness or sequence prediction, such as intrusion detection in 6G-enabled environments. Domain-specific DL models, such as MLP-D, RNN-D, and Tran-D [73], are applied to behavior-oriented decision-making and autonomous driving. However, there is a gap in consistent performance assessment, as some studies omit metrics such as accuracy, precision, recall, and F1 score, which are commonly used to evaluate DL models.
- **Explainable AI (XAI)**: With models such as the CNN-GRU-FCN, XAI [68] emerges as a crucial element for improving interpretability. XAI is used in only one study, despite its potential highlighting a lack of transparency and reliability in AI solutions for critical applications such as intrusion detection and cybersecurity.
- **Fuzzy Logic**: Only one study highlighted the potential of fuzzy logic for improving accuracy and robustness in security applications by combining it with DL (CNN) [64]. This field is unexplored, however, as one study makes use of fuzzy logic to manage uncertainty in dynamic metaverse settings.

- **Decision Making**: In two studies, decision-making frameworks (FWZIC-ARAS) [66] and (IvSFRS–FWZIC) [89] are utilized to assess privacy models for metaverse tools. The limited use of decision-making frameworks indicates a gap in leveraging these approaches for broader evaluations, such as comparing multiple models or addressing diverse privacy challenges in the Metaverse.

Fig. 5 shows the connections between various AIs and the metaverse.

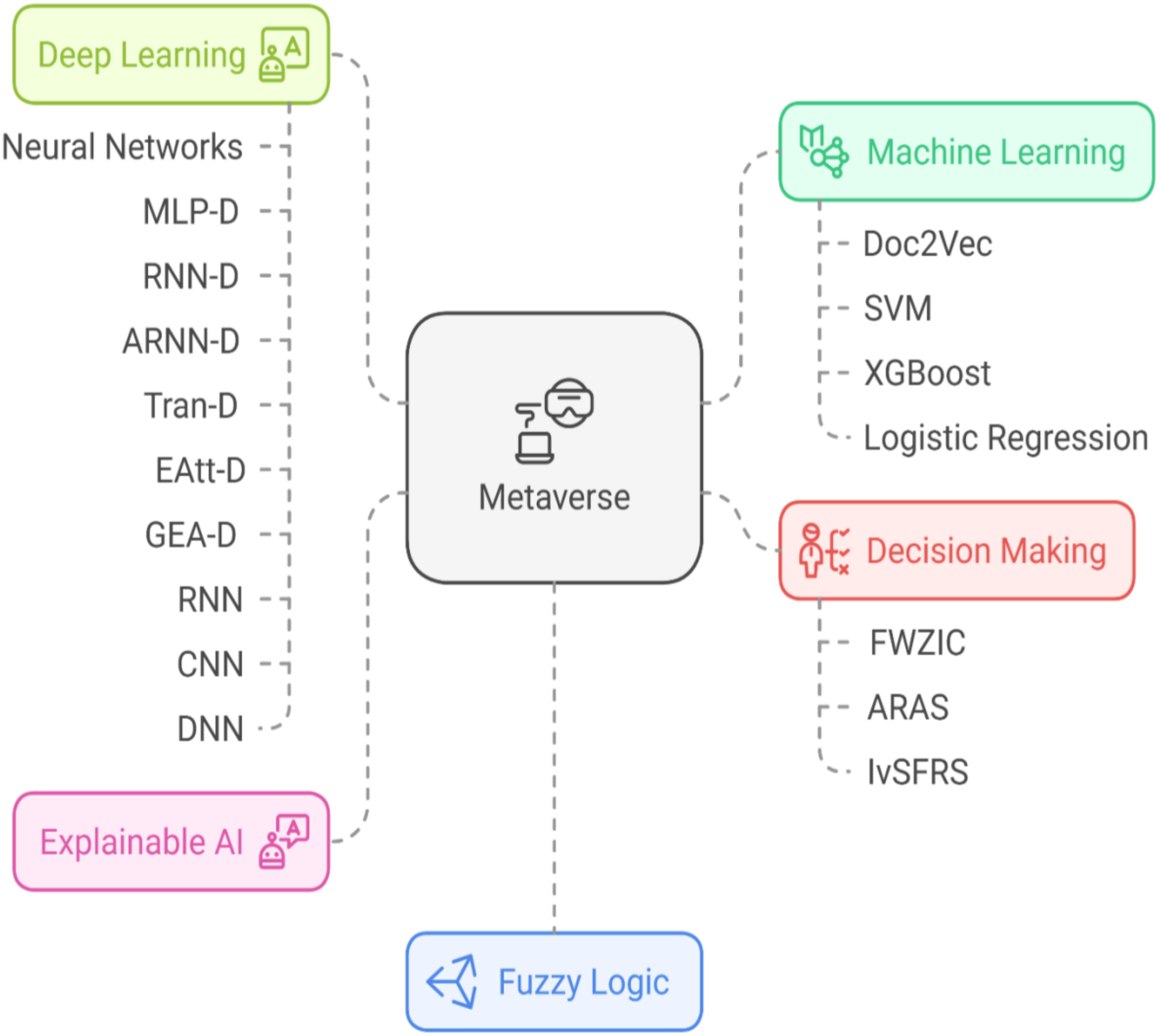


Fig. 5. AI branches used in Metaverse.

By reviewing Fig. 5, we can pinpoint a number of areas that need more investigation. The metaverse has not received much attention in AI applications. Despite their potential risks to cybersecurity and their great significance, these topics are still largely studied. This scant coverage points to the need for more research, and studies on these metaverse subjects could deepen our knowledge and assist scientists in creating practical AI-based solutions. These results may guide future studies, motivating researchers to investigate and use AI methods in a wider variety of metaverses, including those that have not yet been thoroughly investigated. By doing so, we can increase our understanding and create stronger AI solutions to lessen the effects of the metaverse and protect the data.

7.2. Availability of Metaverse Datasets

Datasets are essential for training AI models that assist data protection in the Metaverse. The data sources can offer important insights into how much harm the Metaverse has caused, including to users' security. These datasets can be used to train AI models to recognize and categorize damaged data so that prompt and efficient actions can be taken. However, throughout this systematic review, many papers required specific information regarding the datasets they used. It is frequently necessary to include essential information, such as the dataset's data type and the quantity and makeup of its many data types (see Table 2).

Furthermore, some studies have specified the precise dataset sizes that were utilized to test and train their AI models. Evaluating the appropriateness and generalizability of the models created is challenging because of this lack of information. Furthermore, it is important to consider the validity of the training data. Validation and homogeneity are two important factors in this context. Validation guarantees that the dataset is appropriate for training AI models and appropriately depicts real-world situations. Because homogeneity guarantees data consistency, the model can be effectively generalized across many contexts. It is also critical to consider whether the dataset utilized in a study was gathered privately or publicly. For study findings to be transparent and reproducible, the source of the dataset must be mentioned.

TABLE 2. METAVERSE DATASETS USED WITH AI.

Ref.	Description of the dataset	Size of the dataset	Link of the dataset (if it is available)	Is the legally collected dataset?	Public/Private
[84]	MNIST: a subset of a larger set available from NIST	21.00 MiB	https://www.tensorflow.org/datasets/catalog/mnist	√	Public
[59]	Labeled Network Traffic flows	N/A	https://www.kaggle.com/datasets/jsrojas/labeled-networktraffic-flows-114-applications	√	Public
[73]	Researchers for the NGSIM program collected detailed vehicle trajectory data on southbound US 101, also known as the Hollywood Freeway, in Los Angeles, CA, on June 15th, 2005.	171 KB	https://www.fhwa.dot.gov/publications/research/operations/07030/index.cfm	√	Public
[64]	The objective of employing this dataset was to explore the potential of hand tremor is a novel behavioral biometric trait for security applications.	4879 samples	N/A	N/A	Private
[72]	The data used in the study consists of tweets from the social media platform Twitter, collected from all countries during the period from January 2020 to August 2022. The tweets selected contain the word "metaverse" to analyze individuals' sentiments toward the use of the metaverse.	300,000 tweets	N/A	√	Public
[69]	1st dataset: Numerous AI-based cybersecurity applications, including intrusion detection systems, threat intelligence, malware detection, fraud detection, privacy preservation, digital forensics, adversarial machine learning, and threat hunting, can be validated and tested using this dataset.	N/A	https://research.unsw.edu.au/projects/toniot-datasets	√	Private

	2nd dataset: In the UNSW Canberra Cyber Range Lab, a realistic network environment was designed in order to create the BoT-IoT dataset. Both regular and botnet traffic were present in the network environment. The source files for the dataset are offered in a variety of formats, such as the generated argus files, the original PCAP files, and CSV files. To aid in the classification procedure, the files were divided into assault categories and subcategories.	N/A	https://research.unsw.edu.au/projects/bot-iot-dataset	√	Private
[61]	This work employs standard and most recent IoT cybersecurity datasets that represent modern IoT network features, since the Metaverse is expected to rely on massive IoT connectivity	61 features and15 classes	https://ieee-dataport.org/documents/edge-iiotset-new-comprehensive-realistic-cyber-security-dataset-iot-and-iiot-applications	√	Public
[63]	Various types of data that are handled in the context of cybersecurity in the Metaverse.	N/A	N/A	√	Public
[71]	The dataset extracted from ECG-ID includes 90 users, with each contributing 10 to 35 samples, while the dataset extracted from PTB includes 290 users, each providing 6 samples only. In both datasets, the features were standardized Authorized licensed to include 5-second samples recorded at 500 Hz, ensuring a fair comparison.	10 to 35 samples	https://physionet.org/content/ecgiddb/1.0.0/ https://physionet.org/content/ptbdb/1.0.0/	√	Public
[76]	The dataset is composed of 11 distinct classes representing various types of network activities, both normal and malicious.	116 samples	N/A	√	Public
[81]	The CIC-IDS2017 dataset comprises traffic data collected over five days, featuring various attack types (such as DoS and DDoS) alongside normal traffic.	Benign traffic: 654,771 samples DoS Hulk: 158,804 samples DDoS: 5,897 samples	https://www.unb.ca/cic/datasets/ids-2017.html	√	Puplic
[57]	The data used in the study encompasses performance metrics and behavioral patterns of various machine learning models applied to detect cyber threats within the Digital Twin Metaverse Network (DTMN) environment.	N/A	N/A	√	Private
[70]	It was generated through a reference example in the MATLAB 5G Toolbox, which	N/A	https://www.mathworks.com/products/5 g.html	√	puplic

	is titled "Deep Learning Data Synthesis for 5G Channel Estimation." This example is utilized to generate a dataset for channel estimation using Convolutional Neural Networks (CNN) in the context of fifth-generation wireless networks.				
[68]	It is specifically designed for studying and analyzing dark web traffic in the context of cybersecurity. This dataset includes data collected from various environments, encompassing both malicious and legitimate network traffic, making it useful for developing threat detection models.	N/A	https://www.unb.ca/cic/datasets/malmem-2020.html	√	Public

N/A: Not Applicable

7.3. Metaverse-based ML/DL Techniques

ML and DL approaches have several advantages in the metaverse environment, but they also present difficulties. Obtaining large quantities of high-quality data to train AI and ML algorithms is one of the main challenges. Data collection, categorization, and annotation can be expensive and time-consuming. Furthermore, the accuracy and dependability of the models may be impacted by biases or noise in the data [90]. However, hazard analysis has undergone significant changes as a result of the explosive expansion of the big data industry and improvements in machine learning and deep learning approaches. These developments are intended to reduce the devastating effects of the metaverse and encourage practical mitigating techniques. In examining the intricate connections between metaverse elements and cybersecurity. We analysed metaverse methods to identify gaps in the use of ML and DL approaches in earlier research. The 18 techniques that we have used are the neural network (NN), logistic regression (LR), extreme gradient boosting (XGBoost), deep neural network (DNN), multilayer perceptron (MLP), recurrent neural network (RNN), ARNN, Tran, EAtt, generalist embodied agent (GEA), convolutional neural network (CNN), SVM support vector machine (SVM), doc2vec, kernel principal component analysis (KPCA), long short-term memory (LSTM), gated recurrent units (GRUs) and fully convolutional networks (FCNs). We investigated the points where each metaverse and the algorithms in use intersected to find the gaps. This made it easier for us to determine which algorithms have not previously been used in earlier research, which suggests that they could be the subject of future investigations. The algorithms utilized in different metaverses are highlighted in Fig. 6.

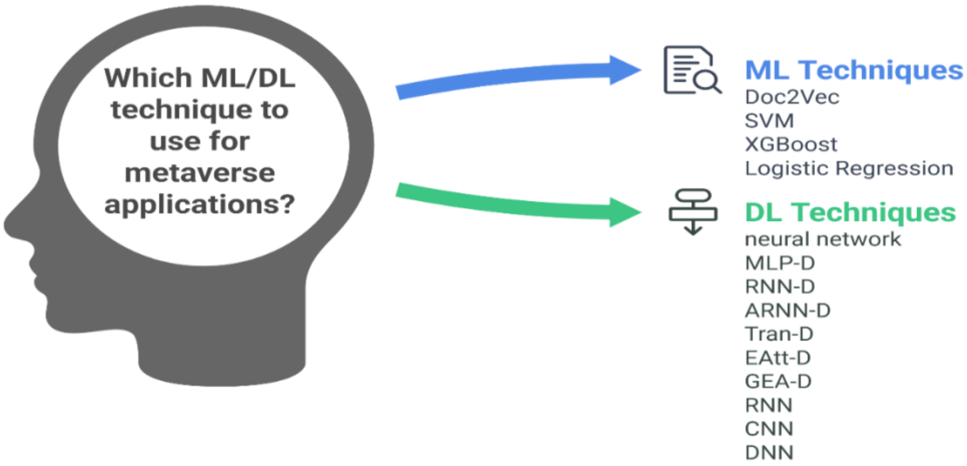


Fig. 6. The contributions of ML/DL techniques are metaverse.

Future researchers can learn from these findings, which show that ML and DL approaches have not yet been thoroughly investigated for certain metaverses. Researchers can advance knowledge and create better metaverse management solutions by concentrating on untested algorithms. However, a number of techniques have not yet been applied in earlier AI literature on the metaverse. These techniques include restricted Boltzmann machines (RBMs), bidirectional encoder representations from transformers (BERT), bidirectional long short-term memory (Bi-LSTM), and hybrid models such as the SVM-DNN. These approaches might be investigated in future research to compare and enhance outcomes or create new applications.

7.4. Metaverse and Quantum Techniques

Technology has advanced significantly during the past few decades, which has changed socioeconomic situations and living standards. When the upcoming cutting-edge technologies are completely operational, the entire process will undergo a revolution. Cutting-edge technologies such as Web 3.0 and Metaverse require extremely fast internet, powerful computers, and unbeatable security. Traditional computer techniques are limited and unable to meet demand, even in the face of growing demand. Quantum computing offers hope for resolving these issues [91]. There are intriguing opportunities to improve virtual environments, increase security, and enable new types of engagement at the nexus of quantum technology and the Metaverse. There is much potential for improving virtual environment functionality, security, and user experiences through the incorporation of quantum techniques into the Metaverse. The application of quantum technology in the Metaverse could revolutionize user interaction and engagement in digital spaces as it develops. An outline of the ways in which quantum methods can impact the creation and perception of the Metaverse. This section covers Quantum's uses in the Metaverse, real-world applications, and limitations.

7.4.1 Real-World Applications for Quantum and Metaverse

As a sophisticated extension of the more general Metaverse notion, the real-time Metaverse is a state-of-the-art element of the current digital revolution. The next development in virtual worlds is real-time Metaverse, which turns static digital landscapes into dynamic, interactive areas that are constantly updated using data from the actual world. The real-time Metaverse incorporates real-time changes in the real world as they occur, going beyond the standard metaverse's prebuilt, static environments where users can interact, work, play, and explore [92]. This change opens new opportunities by fusing the digital and physical worlds to produce more engaging and dynamic experiences. The real-time Metaverse's core instantly synchronizes digital and real-world settings and activities. Advanced sensor technologies and other inputs that continuously gather and transmit data from the physical environment are used to do this. These sensors provide powerful data processing systems with vital information on the geometry, motion, and visual features of an environment [93]. The combination of the Metaverse and quantum technologies creates new opportunities for real-world applications in a variety of sectors.

1. Quantum key distribution (QKD) can be used by virtual markets to guarantee that user transactions are secured and safe from prying eyes.
2. Training simulations can use quantum computing to more correctly model complicated circumstances in fields such as medicine and aviation.
3. More realistic interactions and behaviors can result from virtual beings using quantum algorithms to optimize their decision-making processes.
4. Quantum-enhanced rendering algorithms can produce more definition graphics in real time for video games and virtual tourism platforms.
5. To lower the risk of identity theft, users can use quantum cryptography to confirm their identities in virtual worlds.
6. Using quantum computing, researchers from all around the world can collaborate in a virtual lab and examine large, complicated datasets at once.
7. To find inefficiencies and streamline procedures, manufacturing sectors can use the Metaverse to model their production lines.

7.4.2 Enhanced Features for Integrating Quantum and Metaverse Applications

- **Computing for Improved Visuals:** Real-time rendering of high-quality graphics requires complex computations that can be greatly accelerated by quantum computing. More realistic and engaging virtual Metaverse worlds could result from integrating quantum and Metaverse [91]. Visuals in virtual worlds could undergo a revolution with the combination of quantum computing and the metaverse, improving realism, interaction, and user experience in general. The complex computations needed to produce high-quality visuals can be processed far more quickly by quantum algorithms than by traditional computers. This can result in the creation of immersive settings by generating complex scenes in real time with a large number of polygons, sophisticated lighting, and realistic texturing [94].

- **Calculating Trustworthy Communication:** By providing devices with safe routes of communication and safeguarding private information and interactions, quantum communication techniques such as supersingular isogeny key encapsulation (SIKE) and QKD might improve security in the Metaverse**.** However, with developments in quantum computing and Metaverse integration, high-performance communication has a bright future. Data storage, transport, and computation can be completely transformed via quantum computing. Research into energy-efficient technologies seeks to lessen the environmental impact of high-performance communications, while the combination of Metaverse and quantum technologies will spur advances across multiple disciplines in trustworthy communications [93].
- **Effective Cryptography:** Securing transactions and identity verification—both essential for virtual economies within the Metaverse—can be ensured by putting quantum cryptographic techniques such as Dilithium, FALCON, SPHINCS, etc., for signatures and Kyber, NTRUEncrypt, Saber, etc., for encryption into practice [95]. However, with the growth of the Metaverse, the Internet of Things network has expanded with new "things," such as mixed reality devices, and it is unclear what privacy and security issues might surface in the expanded IoT network with Metaverse items. Furthermore, standard cryptographic techniques may be threatened by quantum computing, which is why postquantum cryptography is crucial for protecting identity, trust and verifiability, privacy and confidentiality, digital property rights, DeFi platforms, and metaverse transactions. Quantum-resistant cryptography must be used to protect the integrity of the Metaverse. To safeguard the Metaverse, postquantum cryptography technologies are being explored in this area [43].
- **Scalable Distributed Network**: Large-scale simulations and interactions in the Metaverse can be processed efficiently and be scalable with the help of distributed quantum computing resources. Security, performance, and user experience can all be greatly improved by incorporating quantum technology into scalable distributed networks for the Metaverse. Developers may build strong infrastructures that support the Metaverse's dynamic and immersive character by utilizing the special powers of quantum computing and communication. Across dispersed networks, quantum entanglement may enable instantaneous data transport. By drastically lowering latency, this can improve interactions and experiences in the metaverse in real time. Scalable processing capacity throughout the metaverse is made possible by the use of distributed quantum computing resources. This makes it possible to carry out intricate calculations for AI, simulations, and graphics rendering in an efficient manner, supporting an increasing number of users and surroundings [96].
- **Facilitating Improved AI:** The Metaverse's AI capabilities can be strengthened by quantum algorithms such as quantum machine learning (QML), opening the door to more complex virtual agents, improved personalization, and improved user experiences. Artificial intelligence (AI) systems' learning, data processing, and user interaction can all be greatly enhanced by the metaverse's incorporation of quantum technology. Models can be trained on large datasets more quickly because of the ability of quantum algorithms to speed up machine learning procedures. AI-driven features in the metaverse are enhanced as a result of increased prediction accuracy and the capacity to learn from increasingly intricate data patterns. A better comprehension and production of human language can be facilitated by the development of more complex NLP models via quantum computing. This enhances user pleasure and engagement by allowing more organic interactions between users and AI agents in the metaverse [97].

7.4.3 Open Issues for Integrating Quantum and Metaverse

Considerations of Technology: Since current quantum technologies are still in their infancy, there may be substantial technical obstacles to their widespread use in the Metaverse. Numerous applications are possible for the application of quantum technologies in the Metaverse environment. Nonetheless, it is thought to be most practical when implemented for security purposes and for calculations to improve the machine learning algorithm and achieve the necessary level of heuristic optimization [98].

Hardware requirements: One of the primary obstacles to quantum systems and the metaverse is hardware. Moreover, there is still little commercial and scientific interest in quantum-enabled consumer devices for Metaverse access. In addition, it is thought that the Metaverse must resemble the real world, which is characterized by a wide range of senses, including scent, wind, and slickness, in addition to sight and hearing. It becomes essential to include sensor technology to improve the Metaverse's realism of the metaverse to real-world experiences. Hardware advancement is the main barrier to quantum technologies. Currently, essential quantum mechanical properties are achieved via natural principles such as electron spins or photon polarization, which act as qubits. Qubit error correction requires a great deal of investigation. Unlike error correction for conventional bits, the procedure of error correction for qubits involves extensive complexity because of the intrinsic quantum principle of "no cloning" [91].

Complexity of Integration: Careful planning and research are necessary to assure compatibility when combining quantum techniques with current metaverse technologies [91]. Owing to issues with qubit stability and error rates, current quantum computers are still in their infancy. However, this limits the scalability and feasibility of implementing quantum solutions in the Metaverse. The complexity of current architectures must be significantly altered to integrate quantum systems with current Metaverse platforms and applications. However, ensuring smooth interoperability can be challenging and time-consuming. Furthermore, constructing the specialized networking and cryogenic systems required to support quantum computing is expensive and difficult. Organizations must, however, make significant investments in new technologies, which may make entry difficult.

Accessibility for Users: For broad adoption, users can continue to utilize quantum-enhanced functionality without needing extensive technical understanding. Although there are many advantages to combining quantum technology with metaverse technology, there are also a number of important issues that need to be resolved. First, for people who are not familiar with these ideas, the complexity of quantum technologies may result in a steep learning curve. Nonetheless, users—particularly those with little technical expertise—may find it challenging to explore and use metaverse platforms successfully. Second, creating user-friendly interfaces with quantum features can be challenging and overwhelming. However, complicated user interfaces may deter participation and user interest. Third, the cost of creating and maintaining quantum technology may restrict the range of usable applications. Third, the cost of creating and maintaining quantum technology may restrict the range of usable applications. Smaller developers, however, might find it difficult to produce reasonably priced solutions, which would reduce the variety of possibilities that are available. Fourth, individuals in disadvantaged areas might not have easy access to the tools (such as fast internet and sophisticated technology) needed to interact with quantum-enhanced metaverse platforms. However, doing so may widen the digital gap and prevent some groups from taking part [99].

Data Compatibility: The possibility of metaverse and quantum integration as a single, connected digital cosmos is hampered by the incompatibility of data. A concentrated effort must be made to create and implement common data standards and protocols to address these problems. To guarantee that data can be easily processed and utilized across many systems, these standards specify how information should be formatted, stored, and transferred. The quantum and Metaverse can offer a more seamless and integrated experience by attaining data interoperability, which allows users to move between settings with ease and utilize their digital assets throughout the ecosystem. The two most crucial components of data compatibility are data integration and common formats. With respect to data compatibility, integrating quantum technology with metaverse technology presents significant challenges. This includes the capacity to efficiently handle, move, and use data in both conventional and quantum systems. The first difficulty is that Metaverse produces a vast array of data, such as environmental simulations, user interactions, and 3D models. Data are processed differently in quantum systems. For quantum and classical systems to interact seamlessly, similar data formats and standards must be established. The second difficulty is that managing data is made more difficult by the need for specialized storage systems for quantum data, which are different from ordinary databases. For integration to be successful, hybrid storage systems that can manage both classical and quantum data are needed [100].

Moral Concerns: There are ethical, security, and data privacy issues that need to be addressed when using quantum technology in the Metaverse. Several ethical issues are caused by the combination of quantum technology with the metaverse, which may have a large influence on user experiences and social standards. To customize experiences, the metaverse depends on gathering many data, which may result in invasive monitoring techniques. However, users may feel that their privacy has been violated, which could make them dislike the platform and be reluctant to participate completely. Furthermore, there are moral concerns around user tracking given the possibility that quantum technology could improve surveillance capabilities. However, users may be concerned about being watched all the time, which can restrict their ability to express themselves freely and prevent genuine connections. Moreover, users might not be completely aware of the consequences of using quantum-enhanced devices and the data they consume. However, unethical issues pertaining to user autonomy and decision-making may arise from a lack of informed consent. Furthermore, sophisticated AI systems driven by quantum computing have the ability to forecast and modify human behavior. Nonetheless, this presents ethical concerns regarding the degree to which consumers are swaying or forced to make particular decisions or purchases [101].

7.5. Ethical considerations

The most important aspect of scientific study in AI is ethics. There are several real-world uses for language processing and analysis, whether spoken or written. As a result, an increasing number of natural language processing (NLP)-based applications are being created. Signal processing, machine learning, psychology, and grammar are all integrated into NLP. In addition to categorization, it is frequently used for text and speech recognition [102]. To ascertain the ethics, bias, and ramifications of AI-generated material in the domains of computer vision, image processing, and NLP [103]–[105], however, a thorough examination is necessary. Ethical issues (including privacy) are becoming increasingly difficult to handle with every new AI category [106], [107]. Fairness concerns in ML-based algorithm design have been a crucial issue of interdisciplinary research for over 20 years, particularly in computer science research [108], [109]. In the field of research on human–computer interaction, algorithmic fairness has attracted attention because of growing concerns regarding the use and deployment of AI-based technologies [110]. Algorithm fairness is defined as an algorithm's rationale for making decisions that are fair, just, accurate and unbiased [111].

Fair algorithm design is a difficult and crucial task that requires meticulous attention to detail in both development and implementation. This necessitates the creation of impartial models that produce equal results across diverse demographic groups, as well as the recognition that technology decisions in supervised learning have social ramifications that must be considered [108]. As a result, the researchers in [108] identified four major rationales for furthering XAI research: explaining algorithm-generated results, controlling system behavior, developing models, and extending knowledge. Fairness requires the development of unbiased models that deliver equitable outcomes across different demographic groupings. Scientifically speaking, this requires a multidimensional approach. Some things must be considered. First, at the data collection stage, insurance that is representative and inclusive of the dataset should be considered to capture various viewpoints and experiences. Stringent testing procedures should next be developed to assess the model's performance across various subpopulations. Demographic parity, equalized odds, and disproportionate impact are all ways to quantify fairness. Furthermore, continuous monitoring and change are needed to address emerging concerns about fairness. AI algorithms can be made more fair by adopting these strategies, which promote inclusion and equity in their applications [110].

On the other hand, growing social concerns about the development of AI algorithms have resulted in increased scientific and legal considerations focused on the fairness of AI systems to attain AI safety and ethical solutions [111]. An example of such considerations is the concept of an AI-related method, which was incorporated into public health law on August 2, 2021, by Bioethics Act legislation, which requires a specific algorithmic designer to explain it to staff who use it for prevention, diagnosis, or care [108]. The first Conference on fairness, accountability, and transparency, which demonstrated an increased awareness of the need for ethical and technical advancement in the scientific computer science community, was held in 2018 and was affiliated with the ACM in 2019. In addition, the ACM Conference on Computing and Sustainable Societies was established in 2020 [110]. Researchers have investigated how people perceive the fairness, accountability, and transparency (FATs) of Facebook newsfeed algorithms. In conclusion, all of the research has concluded that it would be beneficial to better legislate the explainability of algorithmic decisions in various countries by setting explicit and realistic goals. Therefore, we researched this element of AI and determined the following holes that require additional work:

- **Trustworthiness Analysis for Metaverse Applications:** Metaverse success is strongly dependent on trustworthiness, especially when it combines virtual settings with real-world applications. Ensuring secure and reliable systems is critical for increasing user confidence and safety. This can be accomplished by improving data integrity via blockchain technology, privacy-preserving techniques, and decentralized identification frameworks. Robust simulation models, transparent algorithms, and explainable AI techniques are critical for ensuring reliability. Engaging stakeholders and verifying virtual experiences against real-world criteria ensures that metaverse solutions are viable and meet user expectations and ethical standards.
- **Trustworthiness Analysis for Hybrid Metaverse Systems:** To address the different needs of users, hybrid metaverse systems that combine physical and virtual interactions must undergo careful trustworthiness examination. Studies highlight the integration of cutting-edge technologies such as AI, IoT, and AR/VR to ensure smooth interoperability. While these developments have great potential, rigorous study reveals the need to assess scalability, data privacy, and ethical concerns. Real-world applicability, user-centric design, and system effectiveness in increasing engagement and decision-making are critical. Furthermore, cultivating adaptability, inclusivity, and community participation is critical for addressing difficult events, and ensuring the metaverse is a secure and equitable space for all users.

7.6. New Insights into Cybersecurity and Metaverse

Cybersecurity in the Metaverse signals a moment of realization that challenges have arisen, demanding entirely new solutions [28]. Conventional techniques cannot provide secure protection in immersive virtual environments when digital identity, financial transactions, and personal data are at an even greater risk [29]. The application of artificial intelligence and blockchain and the implementation of zero-trust infrastructure have been reviewed to ensure that the Metaverse has become much more secure; however, some major gaps remain [58]. Some of the key problems include privacy risks for biometric data, which could be a part of the IoT-associated weaknesses influencing the application of the Metaverse, and possible adversarial AI attacks targeted at ecosystem components [64], [71], [74]. The diverse security mechanisms already proposed by experts raise questions about actual implementation and scalability [76], especially with respect to decentralized identity management, adaptive intrusion detection, and privacy-preserving cryptographic schemes, because the metaverse ecosystem remains safe and resilient [83], [87].

The following are key insights:

1. The necessity for adaptive and AI-based secure models:
   - Traditional cybersecurity measures cannot address complex, evolving threats in the Metaverse [69].
   - AI-enabled threat detection (e.g., deep learning, explainable AI) is required for anomaly detection and predictive security [68], [76].
   - Adversarial attacks targeting AI-based decision-making systems constitute an impending risk [73].
2. Blockchain and Zero-Trust for Metaverse Security:
   - Blockchain technology provides decentralization and transparency but faces the real challenge of scalability [58].
   - Zero trust is needed to secure decentralized applications in the Metaverse [87].
   - To properly secure transactions, better cryptographic protocols are warranted [64].
3. Privacy and identity management challenges:
   - The enormous amount of biometric and behavior data gathered from the metaverse poses considerable privacy concerns [71].
   - Decentralized identity management (DID) systems propose robust user authentication [83].
   - Auth models from initial impressions hold promise, but additional provenance/affirmation must take place [85].
4. Vulnerabilities of Metaverse Fundamental Applications:
   - Immersive cyberattacks have increased the degree of touchiness of VR and AR networks [81].
   - Advanced Wormhole attacks can still be placed into mobile Metaverse applications [65].
   - The establishment of the IoT in Metaverse needs high-level intrusion detection systems, without a doubt [68].
5. Cybersecurity in Healthcare and Remote Monitoring in the Metaverse:
   - In terms of benefits, AI-based healthcare monitoring has both pros and cons [82].
   - Medical data should be safely encrypted via devices such as AES-256 [79].
   - Wearable biomedical devices receive an exhilarating new entry, as biomedical wearables may usher in privacy concerns inside the Metaverse [71].

8. PERSPECTIVES ON THE METAVERSE

As the metaverse continues to grow, it redefines how individuals interact, work, and engage in digital environments. While a predominant concern remains cybersecurity, there are wider implications that touch beyond data protection. The blending of AI, blockchain, and immersive virtual experiences creates both opportunities and challenges that merit increased scrutiny. Scholars and stakeholders are starting to think comprehensively about new questions concerning the ethical, socioeconomic, and psychological implications of the Metaverse. Although existing studies do not specifically cover these insights, they provide a more complete perspective on their future implications. Below, some of the perspectives

- The Metaverse can radically change education and professional training, providing immersive and interactive experiences to learners. Future medical professionals, engineers, and scientists can train in ultrarealistic simulations, reducing the risk involved with real-world training. Despite its appeal, there is a genuine concern that this will reduce hands-on experience, thereby devaluing real-world training. This results in a workforce that is less grounded and not adequately prepared to address unpredictable real-world challenges.
- Will AI Shape Governing the Metaverse? AI will continue to remain the linchpin for many tasks, including the moderation of content, the enforcement of rules, and the design of users experienced in the coming metaverse. However, as much as the delegation of governance to AI has raised ethical questions about decision-making, bias,

and control—the very question of who ensures transparency and fairness in AI-governed environments? If AI is in a position to say what is and is not permissible, does that endanger digital freedom? Future policies will need to find the right balance between safety and personal freedom with respect to virtual environments.
- Extended engagement into the Metaverse might change the human cognitive process through the dependency on digital stimulation. Problems may develop, such as lower attention spans, less efficient retention in memory, and emotional alienation from reality. Digital addiction, which is a concern, may be a more serious issue since the immersive nature of such worlds may allow users to escape reality even better.

The Metaverse is much more than a technological innovation; it embodies a shift of paradigms concerning how we engage with the world. Cybersecurity lies, of course, at its core, but greater considerations of the implications of the Metaverse for society, psychology, the economy, and governance must be urgently addressed. As researchers, developers, and policymakers shape this new reality, we must anticipate and address these challenges such that the Metaverse becomes an inclusive, ethical, and sustainable digital world.

9. CONCLUSION

As the Metaverse continues to develop, it presents unprecedented opportunities intertwined with significant cybersecurity challenges. This study performs a systematic literature review of the current literature on metaverse cybersecurity, highlighting prominent threats, defensive measures, and future prospects. The analysis indicated that cybersecurity challenges within the Metaverse reach far beyond simply broad network security; it denotes an array of privacy and adversarial AI attacks, identity management on the basis of decentralization, and authentication mechanisms that are scalable in nature. The results reinforce the urgent requirement for next-generation security setups, which include AI-based threat detection, blockchain-based trust mechanisms, and dynamic intrusion detection. The study also revealed that proactive security policies, collaboration among industries, and continued research aimed at realizing solutions for these emerging challenges are equally important. Despite efforts at the conception of security levels in the Metaverse, many gaps continue to exist regarding the real-world validation of proposed models, the scalability of the works, and ethical challenges concerning digital identity and data privacy. To ensure secure and trustworthy metaverse strategies, future research must focus on the development of robust, scalable, and adaptive cybersecurity strategies, from creating better AI-based security models through enhancing privacy-preserving directives to operational interoperability between virtual security and physical security infrastructures. Additionally, integrating quantum computing technologies into metaverse security frameworks could offer novel solutions to complex cryptographic challenges and enhance resilience against future quantum-enabled cyber threats. If the Metaverse does come to intertwine itself within our digital society, the advances in rescuing some of these issues would be both integral, in establishing a secure and inclusive virtual ecosystem, and simple for users, organizations, and governments alike.

Conflicts of interest

The authors declare no conflicts of interest.

Funding

None.

Acknowledgement

None.

References

[1] L. Nautiyal, P. Malik, and A. Agarwal, "Cybersecurity System: An Essential Pillar of Smart Cities," in *Computer Communications and Networks*, Z. Mahmood, Ed. Cham: Springer International Publishing, 2018, pp. 25–50. doi: 10.1007/978-3-319-76669-0_2.

[2] B. (Brad) Nadji, "Data Security, Integrity, and Protection," in *Signals and Communication Technology*, vol. Part F3121, S. McClellan, Ed. Cham: Springer Nature Switzerland, 2024, pp. 59–83. doi: 10.1007/978-3-031-61117-9_4.

[3] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," *Appl. Sci.*, vol. 11, no. 10, 2021, doi: 10.3390/app11104580.

[4] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

[5] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Comput. Sci.*, vol. 3, no. 2, p. 127, 2022, doi: 10.1007/s42979-022-01020-4.

[6] W. K. Mohammed, M. A. Taha, and S. M. Mohammed, "A Novel Hybrid Fusion Model for Intrusion Detection Systems Using Benchmark Checklist Comparisons," *Mesopotamian J. CyberSecurity*, vol. 4, no. 3, pp. 216–232, 2024, doi: 10.58496/MJCS/2024/024.

[7] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, 2023, doi: 10.3390/su151813369.

[8] M. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," *Mesopotamian J. CyberSecurity*, vol. 2023, pp. 57–63, 2023, doi: 10.58496/MJCS/2023/010.

[9] D. Dave, G. Sawhney, P. Aggarwal, N. Silswal, and D. Khut, "The New Frontier of Cybersecurity: Emerging Threats and Innovations," in *2023 29th International Conference on Telecommunications (ICT)*, 2023, pp. 1–6. doi: 10.1109/ICT60153.2023.10374044.

[10] M. Subhi, O. F. Rashid, S. A. Abdulsahib, M. K. Hussein, and S. M. Mohammed, "Anomaly Intrusion Detection Method based on RNA Encoding and ResNet50 Model," *Mesopotamian J. CyberSecurity*, vol. 4, no. 2, pp. 120–128, 2024.

[11] D. H. Tahayur, and M. Al-Zubaidie, "Enhancing electronic agriculture data security with a blockchain-based search method and e-signatures," Mesopotamian Journal of CyberSecurity, 4(3), 1-21, 2024, doi: 10.58496/MJCS/2024/012.

[12] M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," *Discov. Internet Things*, vol. 1, no. 1, p. 7, 2021, doi: 10.1007/s43926-020-00001-4.

[13] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, 2022, doi: 10.3390/electronics11020198.

[14] H. Wang *et al.*, "A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14671–14688, 2023, doi: 10.1109/JIOT.2023.3278329.

[15] S. Mystakidis, "Metaverse," *Encyclopedia*, vol. 2, no. 1, pp. 486–497, 2022, doi: 10.3390/encyclopedia2010031.

[16] Y. K. Dwivedi *et al.*, "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *Int. J. Inf. Manage.*, vol. 66, p. 102542, 2022, doi: 10.1016/j.ijinfomgt.2022.102542.

[17] S. Y. Mohammed, M. Aljanabi, and T. R. Gadekallu, "Navigating the Nexus: A systematic review of the symbiotic relationship between the metaverse and gaming," *Int. J. Cogn. Comput. Eng.*, vol. 5, pp. 88–103, 2024, doi: https://doi.org/10.1016/j.ijcce.2024.02.001.

[18] A. Awadallah *et al.*, "Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities," *IEEE Commun. Surv. Tutorials*, p. 1, 2024, doi: 10.1109/COMST.2024.3442475.

[19] M. Uddin *et al.*, "Exploring the convergence of Metaverse, Blockchain, and AI: A comprehensive survey of enabling technologies, applications, challenges, and future directions," *WIREs Data Min. Knowl. Discov.*, vol. 14, no. 6, p. e1556, 2024, doi: https://doi.org/10.1002/widm.1556.

[20] S. E. Bibri and Z. Allam, "The Metaverse as a virtual form of data-driven smart cities: the ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society," *Comput. Urban Sci.*, vol. 2, no. 1, p. 22, 2022, doi: 10.1007/s43762-022-00050-1.

[21] K. J. Brakas, "Measuring the Extent of Cyberbullying Comments in Facebook Groups for Mosul University Students," vol. 5, no. 2, pp. 337–348, 2025.

[22] Z. Allam, A. Sharifi, S. E. Bibri, D. S. Jones, and J. Krogstie, "The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures," *Smart Cities*, vol. 5, no. 3, pp. 771–801, 2022, doi: 10.3390/smartcities5030040.

[23] A. Koohang *et al.*, "Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation," *J. Comput. Inf. Syst.*, vol. 63, no. 3, pp. 735–765, May 2023, doi: 10.1080/08874417.2023.2165197.

[24] F. Kamil, H. Mihna, M. A. Habeeb, L. A. E. Al-seedi, Y. L. Khaleel, and D. A. Mohammed, "Bridging Law and Machine Learning : A Cybersecure Model for Classifying Digital Real Estate Contracts in the Metaverse," pp. 35–49, 2025.

[25] 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, 2023, doi: 10.26599/BDMA.2022.9020047.

[26] T. Parlar, "Data Privacy and Security in the Metaverse BT - Metaverse: Technologies, Opportunities and Threats," F. S. Esen, H. Tinmaz, and M. Singh, Eds. Singapore: Springer Nature Singapore, 2023, pp. 123–133. doi: 10.1007/978-981-99-4641-9_8.

[27] P. Sachdeva and A. Mitra, "Chapter 2 - Navigating the complex terrain: An in-depth analysis of the challenges of the metaverse," in *Exploring the Metaverse*, D. Koundal and N. Kumar, Eds. Academic Press, 2025, pp. 17–30. doi: https://doi.org/10.1016/B978-0-443-24132-1.00002-8.

[28] M. Ali, F. Naeem, G. Kaddoum, and E. Hossain, "Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions," *IEEE Commun. Surv. Tutorials*, vol. 26, no. 2, pp. 1238–1278, 2024, doi: 10.1109/COMST.2023.3347172.

[29] S. Bindewari, A. Raghav, and R. Tiwari, "Chapter 10 - Introduction of cyber security with metaverse: Challenges and applications," in *Exploring the Metaverse*, D. Koundal and N. Kumar, Eds. Academic Press, 2025, pp. 139–164. doi: https://doi.org/10.1016/B978-0-443-24132-1.00010-7.

[30] P. Ruiu, M. Nitti, V. Pilloni, M. Cadoni, E. Grosso, and M. Fadda, "Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds," *Multimodal Technol. Interact.*, vol. 8, no. 6, 2024, doi: 10.3390/mti8060048.

[31] M. Balzano and G. Marzi, "At the Cybersecurity Frontier: Key Strategies and Persistent Challenges for Business Leaders," *Strateg. Chang.*, vol. n/a, no. n/a, doi: https://doi.org/10.1002/jsc.2622.

[32] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.

[33] Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, and A. K. Jaiswal, "A systematic literature review on the cyber security," *Int. J. Sci. Res. Manag.*, vol. 9, no. 12, pp. 669–710, 2021.

[34] M. Bartsch and S. Frey, *Cybersecurity best practices*. Springer, 2018.

[35] V. Adewopo, B. Gonen, N. Elsayed, M. Ozer, and Z. S. Elsayed, "Deep learning algorithm for threat detection in hackers forum (deep web)," *arXiv Prepr. arXiv2202.01448*, 2022.

[36] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Front. Big Data*, vol. 7, p. 1497535, 2024.

[37] J. LeClair, S. Abraham, and L. Shih, "An interdisciplinary approach to educating an effective cyber security workforce," in *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, 2013, pp. 71–78.

[38] S. Abdelkader *et al.*, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks," *Results Eng.*, vol. 23, p. 102647, 2024, doi: https://doi.org/10.1016/j.rineng.2024.102647.

[39] S. E. Bibri, "The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society," *Smart Cities*, vol. 5, no. 3, pp. 832–874, 2022, doi: 10.3390/smartcities5030043.

[40] I. V Bajić, T. Saeedi-Bajić, and K. Saeedi-Bajić, "Metaverse: A Young Gamer's Perspective," in *2023 IEEE 25th International Workshop on Multimedia Signal Processing (MMSP)*, 2023, pp. 1–6. doi: 10.1109/MMSP59012.2023.10337702.

[41] D. B. Rawat and H. El Alami, "Metaverse: Requirements, Architecture, Standards, Status, Challenges, and Perspectives," *IEEE Internet Things Mag.*, vol. 6, no. 1, pp. 14–18, 2023, doi: 10.1109/IOTM.001.2200258.

[42] Y. Wang *et al.*, "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 319–352, 2023, doi: 10.1109/COMST.2022.3202047.

[43] M. Tukur *et al.*, "The metaverse digital environments: a scoping review of the challenges, privacy and security issues," *Front. big Data*, vol. 6, p. 1301812, 2023.

[44] G. Kabanda, C. T. Chipfumbu, and T. Chingoriwo, "A Cybersecurity Model for a Roblox-based Metaverse Architecture Framework," *Br. J. Multidiscip. Adv. Stud. Eng. Technol.*, vol. 3, no. 2, pp. 105–141, 2022, doi: 10.37745/bjmas.2022.0048.

[45] M. Pooyandeh, K. J. Han, and I. Sohn, "Cybersecurity in the AI-Based Metaverse: A Survey," *Appl. Sci.*, vol. 12, no. 24, 2022, doi: 10.3390/app122412993.

[46] P. Jaipong, S. Siripipattanakul, P. Sriboonruang, and T. Sitthipon, "A Review of Metaverse and Cybersecurity in the Digital Era," *Int. J. Comput. Sci. Res.*, vol. Advanced online publication, 2022, doi: 10.25147/ijcsr.2017.001.1.122.

[47] T. N. Nguyen, "Toward Human Digital Twins for Cybersecurity Simulations on the Metaverse: Ontological and

Network Science Approach," *JMIRx Med*, vol. 3, no. 2, p. e33502, Apr. 2022, doi: 10.2196/33502.

[48] I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, "Metaverse applications in smart cities: Enabling technologies, opportunities, challenges, and future directions," *Internet of Things*, vol. 23, p. 100884, 2023, doi: https://doi.org/10.1016/j.iot.2023.100884.

[49] Y. W. Chow, W. Susilo, Y. Li, N. Li, and C. Nguyen, "Visualization and Cybersecurity in the Metaverse: A Survey," *J. Imaging*, vol. 9, no. 1, 2023, doi: 10.3390/jimaging9010011.

[50] M. Al-Emran and M. Deveci, "Unlocking the potential of cybersecurity behavior in the metaverse: Overview, opportunities, challenges, and future research agendas," *Technol. Soc.*, vol. 77, 2024, doi: 10.1016/j.techsoc.2024.102498.

[51] M. Al-Emran *et al.*, "Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA)," *Comput. Human Behav.*, vol. 159, 2024, doi: 10.1016/j.chb.2024.108315.

[52] M. Al-kfairy, A. Alomari, M. Al-Bashayreh, O. Alfandi, and M. Tubishat, "Unveiling the Metaverse: A survey of user perceptions and the impact of usability, social influence and interoperability," *Heliyon*, vol. 10, no. 10, May 2024, doi: 10.1016/j.heliyon.2024.e31413.

[53] P. Radanliev, "Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing," *Front. Blockchain*, vol. Volume 7-2024, 2024, doi: 10.3389/fbloc.2024.1359130.

[54] A. S. Albahri *et al.*, "A systematic review of trustworthy artificial intelligence applications in natural disasters," *Comput. Electr. Eng.*, vol. 118, p. 109409, 2024.

[55] Y. L. Khaleel, M. A. Habeeb, A. S. Albahri, T. Al-Quraishi, O. S. Albahri, and A. H. Alamoodi, "Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods," *J. Intell. Syst.*, vol. 33, no. 1, 2024, doi: 10.1515/jisys-2024-0153.

[56] G. G. Shayea, M. H. M. Zabil, M. A. Habeeb, Y. L. Khaleel, and A. S. Albahri, "Strategies for protection against adversarial attacks in AI models: An in-depth review," *J. Intell. Syst.*, vol. 34, no. 1, p. 20240277, 2025, doi: 10.1515/jisys-2024-0277.

[57] M. S. Hossain, M. S. Islam, and M. A. Rahman, "A Cyber Range Framework for Emulating Secure and Private IT/OT Consumer Service Verticals Towards 6G," *IEEE Trans. Consum. Electron.*, pp. 1–1, 2024, doi: 10.1109/TCE.2024.3387055.

[58] S. Jebri, A. Ben Amor, and S. Zidi, "A seamless authentication for intra and inter metaverse platforms using blockchain," *Comput. Networks*, vol. 247, p. 110460, 2024, doi: 10.1016/j.comnet.2024.110460.

[59] V. Murgai, V. R. R. Lolabhattu, R. Stimpson, E. Tripathi, and S. Chickala, "Securing the Metaverse: Traffic Application Classification and Anomaly Detection," in *Proceedings - 2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2024*, 2024, pp. 111–117. doi: 10.1109/WoWMoM60985.2024.00031.

[60] I. Ud Din, K. Habib Khan, A. Almogren, M. Zareei, and J. Arturo Perez Diaz, "Securing the Metaverse: A Blockchain-Enabled Zero-Trust Architecture for Virtual Environments," *IEEE Access*, vol. 12, pp. 92337–92347, 2024, doi: 10.1109/ACCESS.2024.3423400.

[61] E. C. Nkoro, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Detecting cyberthreats in Metaverse learning platforms using an explainable DNN," *Internet of Things (Netherlands)*, vol. 25, p. 101046, 2024, doi: 10.1016/j.iot.2023.101046.

[62] M. Vondráček, I. Baggili, P. Casey, and M. Mekni, "Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses," *Comput. Secur.*, vol. 127, p. 102923, 2023, doi: 10.1016/j.cose.2022.102923.

[63] M. Alauthman, A. Ishtaiwi, A. Al Maqousi, and W. Hadi, "A Framework for Cybersecurity in the Metaverse," 2024. doi: 10.1109/ICCR61006.2024.10532868.

[64] B. B. Gupta, A. Gaurav, and V. Arya, "Fuzzy logic and biometric-based lightweight cryptographic authentication for metaverse security," *Appl. Soft Comput.*, vol. 164, 2024, doi: 10.1016/j.asoc.2024.111973.

[65] S. Y. Kuo, F. H. Tseng, and Y. H. Chou, "Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism," *Futur. Gener. Comput. Syst.*, vol. 143, pp. 179–190, 2023, doi: 10.1016/j.future.2023.01.017.

[66] N. A. Husin, A. A. Abdulsaeed, Y. R. Muhsen, A. S. Zaidan, A. Alnoor, and Z. R. Al-mawla, "Evaluation of Metaverse Tools Based on Privacy Model Using Fuzzy MCDM Approach," *Lect. Notes Networks Syst.*, vol. 895 LNNS, pp. 1–20, 2023, doi: 10.1007/978-3-031-51716-7_1.

[67] J. N. Al-Karaki, M. Omar, A. Gawanmeh, and A. Jones, "Advancing CyberSecurity Education and Training: Practical Case Study of Running Capture the Flag (CTF) on the Metaverse vs. Physical Settings," in *2023 International Conference on Intelligent Metaverse Technologies and Applications, iMETA 2023*, 2023, pp. 1–7. doi: 10.1109/iMETA59369.2023.10294722.

[68] E. C. Nkoro, C. I. Nwakanma, J. M. Lee, and D. S. Kim, “Bit-by-Bit: A Quantization-Aware Training Framework with XAI for Robust Metaverse Cybersecurity,” in *6th International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2024*, Feb. 2024, pp. 832–837. doi: 10.1109/ICAIIC60209.2024.10463374.

[69] T. Gaber, J. B. Awotunde, M. Torky, S. A. Ajagbe, M. Hammoudeh, and W. Li, “Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks,” *Internet of Things (Netherlands)*, vol. 24, p. 100977, 2023, doi: 10.1016/j.iot.2023.100977.

[70] F. O. Catak, M. Kuzlu, E. Catak, U. Cali, and O. Guler, “Defensive Distillation-Based Adversarial Attack Mitigation Method for Channel Estimation Using Deep Learning Models in Next-Generation Wireless Networks,” *IEEE Access*, vol. 10, pp. 98191–98203, 2022, doi: 10.1109/ACCESS.2022.3206385.

[71] R. Aljaberi, M. Alawi, K. El Edlebi, J. Zemerly, and C. Yeun, “AI-Driven Scalable Authentication Framework Using ECG and EEG Biometrics for Enhanced Digital Security,” in *Proceedings of the 15th Annual Undergraduate Research Conference on Applied Computing on "AI for a Sustainable Economy.” URC 2024*, Apr. 2024, pp. 1–7. doi: 10.1109/URC62276.2024.10604554.

[72] T. Natarajan, P. Pragha, K. Dhalmahapatra, and D. R. Veera Raghavan, “Unveiling metaverse sentiments using machine learning approaches,” *Kybernetes*, 2024, doi: 10.1108/K-11-2023-2268.

[73] Y. Yu, J. Liu, H. Guo, B. Mao, and N. Kato, “A Spatiotemporal Backdoor Attack Against Behavior-Oriented Decision Makers in Metaverse: From Perspective of Autonomous Driving,” *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, pp. 948–962, Apr. 2024, doi: 10.1109/JSAC.2023.3345379.

[74] A. D. Sarang, M. A. Alawami, and K.-W. Park, “MV-Honeypot: Security Threat Analysis by Deploying Avatar as a Honeypot in COTS Metaverse Platforms,” *C. Model. Eng. Sci.*, 2024, doi: 10.32604/cmes.2024.053434.

[75] S. Salloum, K. Tahat, D. Tahat, A. Mansoori, and R. Alfaisal, “Delving Into the Security & Privacy of the Metaverse Matrix,” in *Proceedings - 2023 10th International Conference on Social Networks Analysis, Management and Security, SNAMS 2023*, Nov. 2023, pp. 1–5. doi: 10.1109/SNAMS60348.2023.10375463.

[76] B. B. Gupta, A. Gaurav, V. Arya, and K. T. Chui, “LSTM-GRU Based Efficient Intrusion Detection in 6G-Enabled Metaverse Environments,” in *Proceedings - 2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2024*, Jun. 2024, pp. 118–123. doi: 10.1109/WoWMoM60985.2024.00032.

[77] M. I. Hossain and R. Hasan, “Threat Model-based Security Analysis and Mitigation Strategies for a Trustworthy Metaverse,” in *Proceedings - 2023 IEEE International Conference on Metaverse Computing, Networking and Applications, MetaCom 2023*, 2023, pp. 33–40. doi: 10.1109/MetaCom57706.2023.00021.

[78] S. Zhang, Y. Wang, E. Luo, Q. Liu, K. Gu, and G. Wang, “A traceable and revocable decentralized multi-authority privacy protection scheme for social metaverse,” *J. Syst. Archit.*, vol. 140, p. 102899, 2023, doi: 10.1016/j.sysarc.2023.102899.

[79] Z. K. Mohammed *et al.*, “A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption,” *Appl. Soft Comput.*, vol. 158, p. 111588, 2024, doi: 10.1016/j.asoc.2024.111588.

[80] O. Nnamonu, M. Hammoudeh, and T. Dargahi, “Metaverse Cybersecurity Threats and Risks Analysis: The case of Virtual Reality Towards Security Testing and Guidance Framework,” in *Proceedings - 2023 IEEE International Conference on Metaverse Computing, Networking and Applications, MetaCom 2023*, Jun. 2023, pp. 94–98. doi: 10.1109/MetaCom57706.2023.00028.

[81] U. U. Izuazu, D. S. Kim, and J. M. Lee, “Unravelling the Black Box: Enhancing Virtual Reality Network Security with Interpretable Deep Learning-Based Intrusion Detection System,” in *International Conference on ICT Convergence*, 2023, pp. 928–931. doi: 10.1109/ICTC58733.2023.10392826.

[82] C. Dilibal and Y. Tur, “Implementation of Developed Esantem Smart Healthcare System in Metaverse,” in *ISMSIT 2022 - 6th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings*, Oct. 2022, pp. 1027–1031. doi: 10.1109/ISMSIT56059.2022.9932849.

[83] F. Fiaz, S. M. Sajjad, Z. Iqbal, M. Yousaf, and Z. Muhammad, “MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms,” *Futur. Internet*, vol. 16, no. 5, 2024, doi: 10.3390/fi16050176.

[84] Y. Bai *et al.*, “ISPPFL: An incentive scheme based privacy-preserving federated learning for avatar in metaverse,” *Comput. Networks*, vol. 251, p. 110654, 2024, doi: 10.1016/j.comnet.2024.110654.

[85] Z. Zhang, K. Yang, Y. Tian, and J. Ma, “An Anti-Disguise Authentication System Using the First Impression of Avatar in Metaverse,” *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 6393–6408, 2024, doi: 10.1109/TIFS.2024.3410527.

[86] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, Y. Xiao, D. Niyato, and E. Dutkiewicz, “MetaShard: A Novel

Sharding Blockchain Platform for Metaverse Applications,” *IEEE Trans. Mob. Comput.*, vol. 23, no. 5, pp. 4348–4361, May 2024, doi: 10.1109/TMC.2023.3290955.

[87] X. Tu, R. Ala-Laurinaho, C. Yang, J. Autiosalo, and K. Tammi, “Architecture for data-centric and semantic-enhanced industrial metaverse: Bridging physical factories and virtual landscape,” *J. Manuf. Syst.*, vol. 74, pp. 965–979, 2024, doi: 10.1016/j.jmsy.2024.05.016.

[88] J. Han *et al.*, “ParaDefender: A Scenario-Driven Parallel System for Defending Metaverses,” *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 53, no. 4, pp. 2118–2127, 2023, doi: 10.1109/TSMC.2022.3228928.

[89] N. Mourad *et al.*, “Decisioning-Based Approach for Optimising Control Engineering Tools Using Digital Twin Capabilities and Other Cyber-Physical Metaverse Manufacturing System Components,” *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3212–3221, 2024, doi: 10.1109/TCE.2023.3326047.

[90] A. S. Tejani, Y. S. Ng, Y. Xi, and J. C. Rayan, “Understanding and Mitigating Bias in Imaging Artificial Intelligence,” *Radiographics*, vol. 44, no. 5, 2024, doi: 10.1148/rg.230067.

[91] E. A. Tuli, J.-M. Lee, and D.-S. Kim, “Integration of Quantum Technologies into Metaverse: Applications, Potentials, and Challenges,” *IEEE Access*, vol. 12, pp. 29995–30019, 2024, doi: 10.1109/ACCESS.2024.3366527.

[92] M. Z. Aloudat *et al.*, “Metaverse Unbound: A Survey on Synergistic Integration Between Semantic Communication, 6G, and Edge Learning,” *IEEE Access*, vol. 13, pp. 58302–58350, 2025, doi: 10.1109/ACCESS.2025.3555753.

[93] M. Hatami, Q. Qu, Y. Chen, H. Kholidy, E. Blasch, and E. Ardiles-Cruz, “A Survey of the Real-Time Metaverse: Challenges and Opportunities,” *Futur. Internet*, vol. 16, no. 10, 2024, doi: 10.3390/fi16100379.

[94] S. Park, H. Baek, and J. Kim, “Spatio-Temporal Multi-Metaverse Dynamic Streaming for Hybrid Quantum-Classical Systems,” *IEEE/ACM Trans. Netw.*, vol. 32, no. 6, pp. 5279–5294, 2024, doi: 10.1109/TNET.2024.3453067.

[95] T. G. Tregi; and M. Al-Zubaidie, “Enhancing Traffic Data Security in Smart Cities Using Optimized Quantum-Based Digital Signatures and Privacy-Preserving Techniques,” *Mesopotamian J. CyberSecurity*, vol. 5, no. 1, pp. 256–272, 2025, doi: 10.58496/MJCS/2025/017.

[96] D. Gurung, S. R. Pokhrel, and G. Li, “Quantum Federated Learning for Metaverse: Analysis, Design and Implementation,” *IEEE Trans. Netw. Serv. Manag.*, p. 1, 2025, doi: 10.1109/TNSM.2025.3552307.

[97] Y. Xu, Y. Gao, M. Wang, and X. Zhu, “Human-Guided Metaverse Synthesis for Quantum Dots: Advancing Nanomaterial Research through Augmented Artificial Intelligence,” *ACS Appl. Mater. Interfaces*, vol. 16, no. 34, pp. 45207–45213, Aug. 2024, doi: 10.1021/acsami.4c09842.

[98] H.-J. Kwon, A. El Azzaoui, and J. H. Park, “MetaQ: A Quantum Approach for Secure and Optimized Metaverse Environment,” *Human-centric Comput. Inf. Sci.*, vol. 12, no. 42, 2022, doi: 10.22967/HCIS.2022.12.042.

[99] U. Khalid, M. S. Ulum, A. Farooq, T. Q. Duong, O. A. Dobre, and H. Shin, “Quantum Semantic Communications for Metaverse: Principles and Challenges,” *IEEE Wirel. Commun.*, vol. 30, no. 4, pp. 26–36, 2023, doi: 10.1109/MWC.002.2200613.

[100] E. A. Tuli, J.-M. Lee, and D.-S. Kim, “Leveraging quantum blockchain for secure multiparty space sharing and authentication on specialized metaverse platform,” *Sci. Rep.*, vol. 14, no. 1, p. 25776, 2024, doi: 10.1038/s41598-024-74213-x.

[101] M. Emu, S. Choudhury, and K. Salomaa, “Stochastic Resource Optimization for Metaverse Data Marketplace by Leveraging Quantum Neural Networks,” *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 3, pp. 2613–2623, 2024, doi: 10.1109/TNSM.2024.3389048.

[102] V. Dogra *et al.*, “A Complete Process of Text Classification System Using State-of-the-Art NLP Models,” *Comput. Intell. Neurosci.*, vol. 2022, no. 1, p. 1883698, 2022, doi: https://doi.org/10.1155/2022/1883698.

[103] Y. Abdelgadir Mohamed, A. H. H. M. Mohamed, A. Khanan, M. Bashir, M. A. E. Adiel, and M. A. Elsadig, “Navigating the Ethical Terrain of AI-Generated Text Tools: A Review,” *IEEE Access*, vol. 12, pp. 197061–197120, 2024, doi: 10.1109/ACCESS.2024.3521945.

[104] F. K. H. Mihna, M. A. Habeeb, Y. L. Khaleel, Y. H. Ali, and L. A. E. Al-Saeedi, “Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence,” *Mesopotamian J. CyberSecurity*, vol. 4, no. 1, pp. 4–16, 2024, doi: 10.58496/MJCS/2024/002.

[105] M. A. Habeeb, Y. L. Khaleel, and A. S. Albahri, “Toward Smart Bicycle Safety: Leveraging Machine Learning Models and Optimal Lighting Solutions,” in *Proceedings of the Third International Conference on Innovations in Computing Research (ICR’24)*, 2024, pp. 120–131.

[106] Y. L. Khaleel, M. A. Habeeb, and G. G. Shayea, “Integrating Image Data Fusion and ResNet Method for Accurate Fish Freshness Classification,” *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 4, p. 21, 2024.

[107] A. S. Albahri, Y. L. Khaleel, and M. A. Habeeb, “The Considerations of Trustworthy AI Components in

Generative AI; A Letter to Editor," *Appl. Data Sci. Anal.*, vol. 2023, pp. 108–109, 2023, doi: 10.58496/adsa/2023/009.

[108] T. Kirat, O. Tambou, V. Do, and A. Tsoukiàs, "Fairness and explainability in automatic decision-making systems. A challenge for computer science and law," *EURO J. Decis. Process.*, vol. 11, p. 100036, 2023, doi: 10.1016/j.ejdp.2023.100036.

[109] Y. L. Khaleel, M. A. Habeeb, and T. O. C. EDOH, "Limitations of Deep Learning vs. Human Intelligence: Training Data, Interpretability, Bias, and Ethics," *Appl. Data Sci. Anal.*, vol. 2025, pp. 3–6, 2025, doi: 10.58496/ADSA/2025/002.

[110] N. van Berkel, Z. Sarsenbayeva, and J. Goncalves, "The methodology of studying fairness perceptions in Artificial Intelligence: Contrasting CHI and FAccT," *Int. J. Hum. Comput. Stud.*, vol. 170, p. 102954, 2023, doi: 10.1016/j.ijhcs.2022.102954.

[111] E. D. Villacis Calderon, T. L. James, and P. B. Lowry, "How Facebook's newsfeed algorithm shapes childhood vaccine hesitancy: An algorithmic fairness, accountability, and transparency (FAT) perspective," *Data Inf. Manag.*, p. 100042, 2023, doi: 10.1016/j.dim.2023.100042.