Artificial Intelligence-based Cybersecurity for the Metaverse: Research Challenges and Opportunities

Abeer Awadallah, *Student Member*, Khouloud Eledlebi, *IEEE*, Jamal Zemerly, *Senior Member*, *IEEE*, Deepak Puthal, *Senior Member*, *IEEE*, Ernesto Damiani, *Senior Member*, *IEEE*, Kamal Taha, *Senior Member*, *IEEE*, Tae-Yeon Kim, Paul D. Yoo, *Senior Member*, *IEEE*, Kim-Kwang Raymond Choo, *Senior Member*, IEEE, Man-Sung Yim, and Chan Yeob Yeun, *Senior Member*, *IEEE*

***Abstract*—The *metaverse*, known as the next-generation 3D Internet, represents virtual environments that mirror the physical world. It is supported by innovative technologies such as digital twins and extended reality (XR), which elevate user experiences across various fields. However, the metaverse also introduces significant cybersecurity and privacy challenges that remain underexplored. Due to its complex multi-tech infrastructure, the metaverse requires sophisticated, automated, and intelligent cybersecurity measures to mitigate emerging threats effectively. Therefore, this paper is the first to explore Artificial Intelligence (AI)-driven cybersecurity techniques for the metaverse, examining academic and industrial perspectives. First, we provide an overview of the metaverse, presenting a detailed system model, diverse use cases, and insights into its current industrial status. We then present attack models and cybersecurity threats derived from the unique characteristics and technologies of the metaverse. Next, we review AI-driven cybersecurity solutions based on three critical aspects: User authentication, intrusion detection systems (IDS), and the security of digital assets, specifically for Blockchain and Non-fungible Tokens (NFTs). Finally, we highlight challenges and suggest future research opportunities to enhance metaverse security, privacy, and digital asset transactions.**

***Index Terms*—Artificial Intelligence, biometrics, continuous authentication, cybersecurity, Digital Twins, intrusion detection, metaverse, multimodality, NFTs**

Manuscript received xx April 2023; revised xx Month 2023; accepted xx Month 2024. Date of publication xx Month 2024; date of current version xx Month 2023. This work was supported in part by the Center for Cyber-Physical Systems, Khalifa University, under Grant 8474999137-RC1-C2PS-T5. (Corresponding authors: Abeer Awadallah and Chan Yeob Yeun).

Abeer Awadallah, Kholoud Eldelbi, Chan Yeob Yeun, Jamal Zemerly, Ernesto Damiani, and Kamal Taha are with the Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi 127788, United Arab Emirates (e-mail: 100061895@ku.ac.ae and chan.yeun@ku.ac.ae).

Tae Yeon Kim is with the Civil Infrastructure and Environmental Engineering Department, Khalifa University, Abu Dhabi 127788, United Arab Emirates. (e-mail: taeyeon.kim@ku.ac.ae).

Deepak Puthal is with the Indian Institute of Management Bodh Gaya, India. (e-mail: deepak.puthal@ieee.org).

Paul D. Yoo is with the University of London, London WC1E 7HX, United Kingdom (e-mail: p.yoo@bbk.ac.uk).

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio TX 78249, USA (e-mail: raymond.choo@fullbrightmail.org).

Man-Sang Yim is with Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea (e-mail: msyim@kaist.ac.kr).

Digital Object identifier

I. Introduction

The *metaverse* is an increasingly popular concept that is gaining significant attention from the tech industry, with its market value expected to reach 2.5 trillion US dollars by 2023 [1]. Essentially, the metaverse is the next-generation Internet, characterized by immersive three-dimensional virtual environments that mirror the physical world, where users engage in various experiences via customizable digital avatars. The term *metaverse* was coined by Neal Stephenson in his 1992 science-fiction novel Snow Crash [2], which envisioned a digital world that could be accessed in real-time via smart devices known as head-mounted displays (HMDs). Early adaptations of the metaverse were in the realm of video games, with Massively Multiplayer Online Games (MMOGs) like Second Life and Roblox enabling players to create personalized avatars, construct virtual worlds, and purchase in-game items using digital currencies. Beyond the gaming industry, the metaverse has the potential to revolutionize everyday activities in various domains, including entertainment [3], education [4], e-commerce [5], social interactions [6], healthcare [7], and tourism [8].

Advancements in technology have brought significant transformations in wireless communications and user engagement, evolving from PCs and static web environments (Web 1.0) to the current era of smart devices, Wi-Fi, applications, and the dynamic web (Web 2.0). The next phase, commonly known as Web 3.0, is expected to be user-centered and supported by emerging technologies and the future metaverse [9], as shown in Fig. 1. Digital twin technology is a core enabler of the metaverse, as it generates real-time virtual representations of physical objects, capturing precise imitations of their actions and responses within an Internet of Things (IoT) ecosystem [10]. Extended Reality (XR), which combines Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), is another important technology responsible for the creation of immersive and interactive experiences in the metaverse [11]. Other metaverse-enabling technologies include Artificial Intelligence (AI), computer vision, blockchain, edge and cloud computing, and emerging communication networks such as 5G and 6G+ [12].

Although the metaverse promises to deliver technological, economic, and social benefits, its significant digital

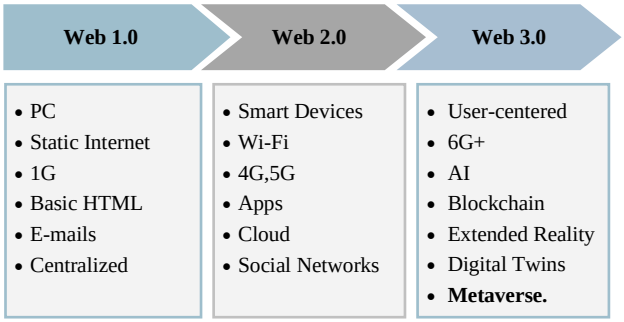

Fig. 1. Advancing from the current Internet of 2D apps into a decentralized, 3D, and immersive Internet, known as the metaverse.

transformation poses various challenges, particularly cybersecurity and privacy threats. Cybercriminals often exploit new technological trends, as evidenced during the COVID-19 pandemic, when increased online activities led to a rise in phishing attacks and fraud [13]. Moreover, technological advancements lead to evolved cybercrime, demonstrated by the rise of sophisticated AI-driven cyberattacks [14]. Therefore, integrating numerous heterogeneous technologies in the metaverse contributes to its complexity and vulnerability, likely magnifying current cyber threats. Furthermore, the metaverse's decentralized and highly interactive nature presents unique security challenges that need to be addressed.

First, the metaverse introduces significant threats to digital identity as virtual environments become more integrated into daily life [15]. As users navigate the metaverse through customizable digital avatars, verifying their true identities becomes increasingly difficult, enabling malicious actors to commit identity theft and impersonation. Deepfakes, AI-generated entities that can mimic real images, videos, and voices [16], can be utilized to create realistic but fraudulent avatars, leading to potential misuse of personal data and financial fraud. Additionally, AI-generated Non-Playable Characters (NPCs), which operate without direct human control, can complicate identity verification processes and integrity. Another identity-related issue arises with VR technology [17], where collecting biometric data such as facial features and behavioral patterns is necessary. Malicious actors can exploit vulnerabilities in authentication mechanisms, compromising this sensitive information and leading to severe privacy breaches.

Second, the dynamic nature of the metaverse poses significant network security threats. Unlike traditional networks, the metaverse consists of constantly changing virtual environments, high volumes of real-time data transmission, and interaction among numerous devices and users. This complexity increases the risk of network-based attacks, such as Denial of Service (DoS) attacks, which can cause disruptions and downtimes. Additionally, malicious actors can leverage AI techniques to target the metaverse with automated attacks that evade detection, known as Advanced Persistent Threats (APTs) [18]. Therefore, current cybersecurity measures that rely on pre-defined rules and static approaches, such as firewalls and antivirus software, are insufficient to mitigate advanced threats, especially zero-day attacks that exploit unaddressed vulnerabilities [19].

Third, the economic system of the metaverse is poised to be supported by blockchain technology, which provides a relatively secure and decentralized platform for online transactions [20]. Virtual object trading is expected to rely on cryptocurrencies and Non-fungible Tokens (NFTs), the latter being unique cryptographic identifiers that verify ownership of digital assets [21]. The market value for cryptocurrencies and NFTs is rapidly growing, with OpenSea, one of the largest NFT marketplaces, achieving a sales record of $20.37 billion in 2022 [22]. This rapid growth makes these systems attractive targets for cybercriminals. For instance, in February 2022, NFTs worth 2.9 million US dollars were stolen from the OpenSea marketplace due to phishing attacks [23]. Cybersecurity threats extend to blockchain wallets, where users store their cryptocurrency and NFTs. Attackers often use fake profiles on NFT marketplaces and impersonate other users to gain unauthorized access to blockchain wallets and NFT accounts. Therefore, exploring the risks associated with asset trading and developing solutions to mitigate these issues is necessary to ensure the security and integrity of the metaverse's economic system.

Given the scale and scope of potential threats in the metaverse, traditional cybersecurity measures are insufficient and thus require innovative solutions. Specifically, AI-driven cybersecurity techniques offer promising advantages [24],[25]. Enhanced biometric authentication, automated real-time threat detection, and cost-effective fraud detection represent areas where AI can transform security practices. As the metaverse is still in its nascent stages, existing literature mainly focuses on addressing technological limitations and realizing its full potential. While numerous survey papers investigate potential risks and propose countermeasures, more in-depth studies that mainly explore AI-based cybersecurity methods for the metaverse need to be conducted. Therefore, this comprehensive survey seeks to bridge this gap by examining AI solutions for securing the metaverse, focusing on the potential of AI in enhancing user authentication, intrusion detection, and security of asset trading within the metaverse. The contributions of this paper are summarized as follows:

1) Provide an overview of the metaverse based on academic and industrial perspectives, presenting a comprehensive system model and use cases.
2) Present attack models and discuss cybersecurity threats unique to the metaverse.
3) Review various AI-based cybersecurity solutions for the metaverse, including user authentication, intrusion detection systems (IDS), and security of digital asset trading (specifically for NFTs).
4) Identify challenges and research opportunities for building a secure metaverse environment using AI-based cybersecurity measures.

The paper is organized into six sections, as shown in Fig. 2. Section II includes a review of related surveys. Section III provides a background on the metaverse and relevant AI techniques. Attack models and cybersecurity threats of the metaverse are presented in Section IV. Section V reviews AI techniques for cybersecurity based on user authentication, intrusion detection systems (IDS), and digital asset security. Section VI summarizes the lessons learned from this survey, Section VII highlights the challenges and research opportunities, and the conclusion is presented in Section VIII.

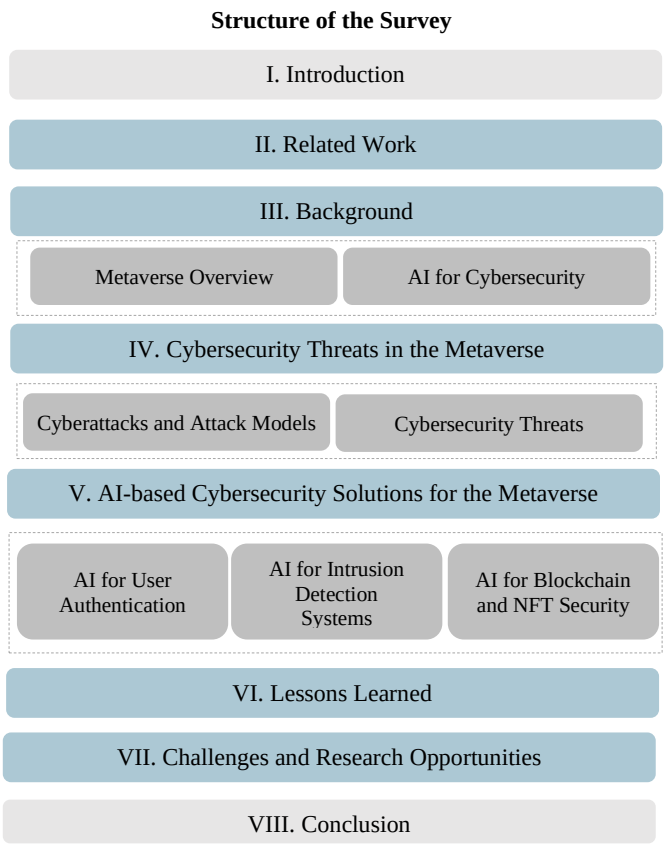

Fig. 2. Organization of the Survey.

II. RELATED WORK AND MOTIVATION

This section reviews previously published survey papers related to the metaverse. Our literature search was guided by a set of keywords, including *metaverse*, *survey*, *overview*, *review*, *cybersecurity*, *security*, *privacy*, and *threats*. We sourced papers published in English from leading academic databases and publishers such as ACM, Elsevier, IEEE, ScienceDirect, and Scopus. The reviewed survey papers, listed in Table I, are compared based on the inclusion of discussions on metaverse threats, NFTs threats, and possible cybersecurity solutions. Regarding solutions, our comparative analysis is focused on user authentication, intrusion detection systems (IDS), and NFT security, as these areas are the main contributions of our work. We employ a symbol system to categorize discussions based on depth and the inclusion of AI-based solutions, as follows:

- Comprehensive discussion (✓).
- Partial discussion (≈), indicating brief mentions or generalized discussions.
- Inclusion of AI-based solutions (*).
- Absence of AI-based solutions (–).

As observed from Table I, the papers are categorized based on their primary research focus into general overview, AI and blockchain, and cybersecurity. A notable early survey from 2013 [26] outlines foundational features of the metaverse, such as *Realism*, *Ubiquity*, *Interoperability*, and *Scalability*, but primarily addresses computational challenges rather than security concerns. Recent surveys [27]-[32] offer extensive overviews of the metaverse's development, architecture, technologies, characteristics, applications, and open challenges. Lee *et al*. [28] explore user behavior, ethical design, and data privacy challenges, highlighting examples of existing threats likely to be magnified within the metaverse. However, their examination of countermeasures is limited. For instance, user authentication and federated learning (an AI paradigm) are generally mentioned as potential research areas for metaverse security without delving into detailed discussions about their current state, limitations, or existing solutions. Metaverse threats are discussed in [30] and [31], while NFT issues are partially mentioned. The authors in [30] focus on edge computing and blockchain as solutions, but they also mention the utilization of federated learning as a privacy-preservation method and the need for robust authentication methods. The work in [31] addresses metaverse threats based on data, network, software and hardware, and mentions threats targeted at cryptocurrencies and NFTs, providing general research directions toward governing the metaverse to avoid security issues.

Several survey papers focus their research on AI and blockchain for the metaverse. In [33], [34], the authors highlight the role of AI in the metaverse, with general discussions of potential security and privacy threats. Yang *et al*. [35] investigate the integration of blockchain and AI, particularly in advancing the metaverse's development. In [36], the authors discuss the role of blockchain technology in enabling the economic system of the metaverse, highlighting its role in mitigating potential challenges. Another study [37] conducts an in-depth review of the integration of blockchain technology within the metaverse, particularly in terms of digital asset management and security aspects. It discusses various threats to the metaverse, including access control attacks, network intrusions, malware attacks, and impersonation risks. Additionally, the paper discusses NFTs as a mechanism for verifying ownership and authenticity of digital assets, briefly mentioning potential scams in NFT marketplaces. While this survey provides a broad range of strategies to address identity and digital asset management, it focuses on blockchain-based solutions. In contrast, our survey explores AI techniques for user authentication and mitigation of NFT-related threats.

The surveys focusing exclusively on cybersecurity and privacy threats in the metaverse analyze potential risks across various domains. The survey conducted by Wang *et al*. [38] is among the earliest comprehensive works to examine cybersecurity and privacy threats within the metaverse, focusing on threats related to data, privacy, identity, network, physical and social impacts, and governance. The authors offer corresponding countermeasures for each challenge, paving the path for future research in metaverse security. Another survey [39] studies potential challenges and cyber threats that might derive from implementing digital twin technology in the metaverse, focusing on blockchain-based solutions. Chen *et al*. [40] provides a discussion on metaverse threats based on five of its enabling technologies: blockchain, AR/VR, AI, cloud and IoT, and digital twins. The authors also mention integrity issues associated with NFTs.

Chow *et al*. [41] categorize security threats into authentication and identity, privacy issues, social issues, and physical threats, focusing on challenges brought by visualization technologies like VR and AR. The survey discusses the vulnerabilities of traditional authentication

TABLE I

OVERVIEW AND COMPARISON OF RELATED SURVEYS

✓: YES ×: NO ≈: PARTIALLY INCLUDED *: INCLUDES AI —: DOES NOT INCLUDE AI

Research Field	Refs.	Year	Contributions	Metaverse threats	NFT threats	Discuss solutions?	Discussed Solutions		
							User Auth.	Intrusion Detection	NFT Security
General Overview	[26]	2013	Overview of four metaverse features: Realism, ubiquity, interoperability, scalability, and highlighting computational limitations for metaverse development	×	×	×	×	×	×
	[27]	2021	A survey on metaverse development, standards, current applications, and key characteristics	≈	×	×	×	×	×
	[28]	2021	An analysis of metaverse technologies, applications, and development	✓	≈	≈	≈*	×	×
	[29]	2022	A survey on metaverse development and case studies of existing metaverse applications	≈	×	×	×	×	×
	[30]	2023	A survey on the utilization of different technologies in the metaverse	✓	≈	✓	≈–	×	×
	[31]	2022	A thorough investigation of metaverse architecture, development, applications, and impact on various sectors	✓	≈	≈	≈–	×	×
	[32]	2023	A survey on metaverse characteristics, applications, and challenges with a focus on the concept of human-centric metaverse	≈	×	≈	×	×	×
AI and Blockchain	[33]	2022	A survey on 6-G enabled edge and AI techniques in the metaverse, focusing on technological issues	≈	×	≈	×	×	×
	[34]	2022	Analysis of the role of AI in the metaverse, AI-enabled applications, and open challenges	≈	×	≈	×	×	×
	[35]	2022	A survey on the integration of AI and blockchain technologies into the metaverse and open challenges	≈	≈	×	≈–	×	≈–
	[36]	2023	Technical analysis of blockchain technology and its role in building the economic system of the metaverse	×	≈	✓	≈–	×	≈–
	[37]	2023	A survey on the role of blockchain in the metaverse, focusing on digital asset management	✓	≈	✓	✓–	×	✓–
Cybersecurity and Privacy	[38]	2022	A comprehensive survey on the metaverse and its security and privacy issues based on seven aspects	✓	≈	✓	✓–	×	×
	[39]	2022	Overview of digital twin technology for the metaverse and relevant security and privacy issues	✓	≈	≈	≈–	×	×
	[40]	2022	Overview of metaverse security and privacy issues, current solutions, and open security questions	✓	≈	≈	≈*	×	×
	[41]	2022	A Survey on cybersecurity threats in the metaverse based on visualization technologies	✓	×	✓	✓*	≈*	×
	[42]	2022	A survey on big data in the metaverse and potential security and privacy threats	✓	×	≈	≈–	×	×
	[43]	2023	A survey on security and privacy threats and solutions in the metaverse	✓	≈	✓	≈*	≈*	×
	Our Paper	**2024**	Survey on AI-based cybersecurity solutions for the metaverse, exploring user authentication, intrusion detection, asset trading, specifically for the metaverse	✓	✓	✓	✓*	✓*	✓*

methods in virtual environments. It highlights the potential of AI-driven cybersecurity measures to combat these threats, such as continuous authentication, DeepFakes (AI-generated avatars) detection, and automated monitoring for malicious activities. Sun *et al*. [42] explore security and privacy threats specifically for big data, focusing on potential cyberattacks on different layers of the metaverse. User authentication is briefly mentioned in the context of lightweight methods for metaverse security. The work in [43] also comprehensively reviews metaverse security and discusses user biometric authentication solutions. Moreover, solutions for attack detection methods are discussed, with AI-based methods mentioned as solutions.

The reviewed surveys have made substantial contributions to the field of metaverse cybersecurity. However, our distinct contributions lie in exploring AI-based solutions for metaverse cybersecurity, particularly for user authentication, IDS, and NFT security, areas not extensively covered in prior surveys. While numerous works discussed biometric and continuous authentication for the metaverse, our approach comprehensively analyzes various biometric traits, highlighting their advantages, disadvantages, and implementation for the metaverse. We also emphasize the significance of integrating multimodal and continuous authentication, comprehensively reviewing literature combining both methods in metaverse-related applications.

Furthermore, our survey is the first to investigate AI-based

solutions for detecting security breaches (IDS) specifically designed for the metaverse. We also explore how AI can help secure NFTs, moving beyond the usual discussions focusing only on blockchain technology. Furthermore, we discuss related challenges to the metaverse while considering academic and industrial perspectives, and we also examine AI algorithms, datasets, performance metrics, and the applicability of such methods in the metaverse. With this approach, we aim to offer a comprehensive overview of the current applications of AI technologies and their deployment for metaverse security. We aim to add valuable insights to the field and guide researchers interested in AI-based cybersecurity for the future metaverse.

III. Background

This section offers a preliminary background divided into two parts. First, an overview of the metaverse is provided, outlining its architecture, enabling technologies, characteristics, and industrial status. Second, general AI concepts are introduced, emphasizing their role in cybersecurity.

A. Metaverse Overview

The term *metaverse* combines 'meta' (transcending/beyond) and 'universe'. While its definition is still evolving, the metaverse is often envisioned as a 3D next-generation form of the Internet. Coined by Neal Stephenson in his 1992 novel *Snow Crash*, the metaverse is described as an immersive virtual space that reflects aspects of the real world, with users representing themselves as digital avatars [2]. Essentially, the metaverse is a cyberspace consisting of numerous virtual worlds that represent the convergence of physical and digital realities, where users engage in immersive experiences such as social communication, entertainment, education, and digital asset trading.

1) Architecture and Elements: The metaverse combines the cyber and physical worlds into a unified virtual space. Powered by Digital Twin technology, a digital replica of our reality is created, where two worlds are seamlessly interconnected and updated in real time. The overall metaverse architecture is illustrated in Fig. 3, and it primarily consists of the physical world, digital world, and the metaverse engine that consists of enabling technologies.

a) Physical World: The physical infrastructure supporting the metaverse consists of interconnected technologies, including computation units, communication networks, storage devices, and hardware. As the metaverse continues to evolve, a concrete physical architecture with detailed specifications is still being developed. However, several studies propose frameworks for the physical infrastructure of the future metaverse [44][45]. Based on these studies, we conceptualize the architecture of the physical world of the metaverse around five main elements: Human Area, Physical Layer, Communication Layer, Edge Layer, and Cloud Layer.

- **Human Area:** The metaverse mirrors the complexities of the real world, including humans, physical environments, objects, social interactions, human activities, official institutions, and governance.
- **Physical Layer:** This layer consists of hardware and technologies that collect data from the Human Area. Users access and interact with the metaverse using various end devices, such as HMDs (VR headsets and AR glasses), haptic gloves [46], motion controllers, and smart devices (wearables and smartphones). While traditional devices like personal computers (PCs), mobile devices, and tablets can access the metaverse, they do not provide a fully immersive experience. Metaverse devices (HMDs) collect diverse user data, including biometrics (eye movements, heart and brain activities, and facial expressions). Based on the Internet of Things (IoT) ecosystem, sensors deployed across physical environments collect data on atmospheric conditions, acoustics, physical movements, and features of objects and buildings, seamlessly integrating physical world dynamics into the digital space.
- **Edge Layer:** The edge layer consists of distributed and decentralized edge nodes that process data from the physical layer. Edge computing supports transmitting time-sensitive data, allowing faster data flow and reducing latency by performing real-time operations close to data sources. Additionally, edge computing enhances privacy and security by enabling local data processing and giving users control over their data [47]. The edge layer filters data and transmits the necessary packets to the cloud, ensuring an efficient infrastructure capable of handling the metaverse's dynamic and demanding ecosystem.
- **Cloud Layer:** The cloud layer is the backbone for storing and processing big data. It consists of data centers with servers and storage units responsible for the mapping of the cyber and physical worlds through data analytics [47], AI processing, data synchronization, Application Programmable Interfaces (APIs), and security measures such as authentication, identity management, firewalls, and access control.
- **Communication Layer:** This crucial layer is responsible for the seamless data exchange across multiple layers in the metaverse. Innovative networking technologies and protocols must be incorporated into the metaverse to enable reliable, secure, and high-speed data transmissions. Among these, 5G and 6G networks are anticipated to be part of the metaverse communication system due to their capability to deliver ultra-low latency and massive data throughput [48]. Software-defined networking (SDN) is another critical architectural innovation within the communication layer. SDN increases network flexibility and efficiency by separating control and data planes, allowing for more agile network management and optimized resource utilization [49]. SDN also facilitates smoother data movement across the distributed infrastructure of the metaverse.

b) Digital World: The digital world, or the virtual landscape of the metaverse, consists of an extensive network of interconnected sub-metaverse worlds. These worlds host various applications and experiences, such as entertainment, social interactions, and education. Users can navigate seamlessly between different environments and experiences without barriers.

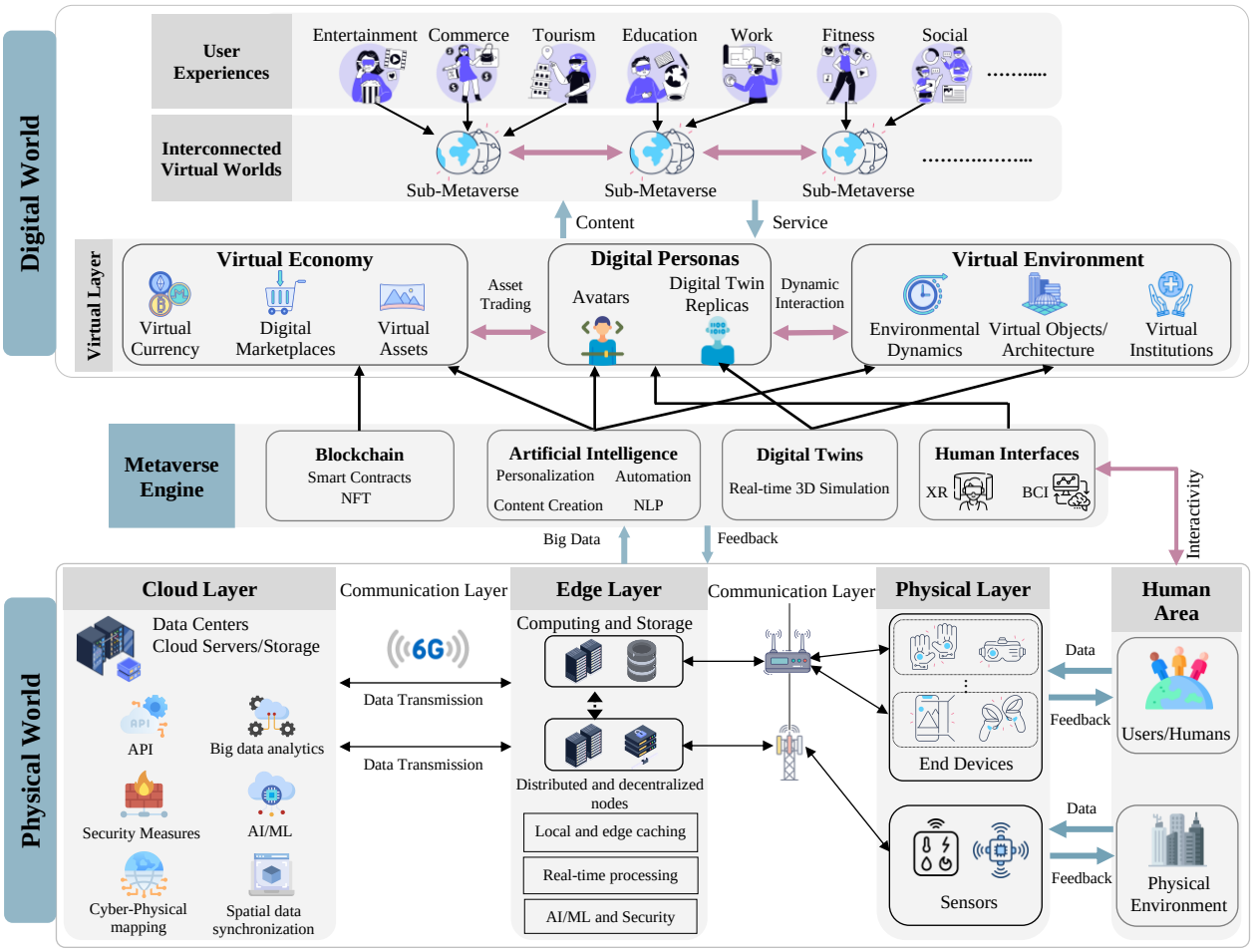

Fig. 3. A diagram of the general architecture of the metaverse, showing the elements and their connections in the physical world and digital worlds. The metaverse engine is the link layer that includes the main enabling technologies of the metaverse. Real-time and constant data flow between the physical infrastructure and the metaverse highlights the complexity and dynamic nature of the metaverse.

- **Virtual Personas:** Users represent themselves as digital avatars in the metaverse. A digital avatar is a visual illustration of a character within a digital platform, which can be created using 2D or 3D graphics to perform certain actions [50]. Since the metaverse consists of multiple worlds and applications, users can customize avatars based on their experience [51]. For example, an avatar that reflects similar physical features of a user (powered by digital twins) can be used in a work or educational environment for integrity purposes (i.e., Microsoft Mesh avatars). However, avatars can be extensively personalized in gaming platforms such as Roblox and Fortnite, offering users imaginative elements to explore.
- **Virtual Environment:** This component mirrors the physical world within the metaverse, with digital twin technology generating real-time simulations of physical entities and landscapes, including everything from institutions (such as schools and workplaces) to entire virtual cities and natural landscapes.
- **Virtual Economy:** The economic system of the metaverse is poised to be supported by blockchain technology, which provides a secure and decentralized platform for online transactions [20]. The creator-based economy allows users to generate virtual objects empowered by blockchain, cryptocurrencies, and Non-fungible Tokens (NFTs), which are cryptographic identifiers that verify ownership of digital assets on the Internet [21]. NFTs can represent any form of digital content, including images, videos, in-game items, domain names, and virtual real estate. Yilmaz *et al.* [52] found that the integration of NFTs into the metaverse offers new opportunities for digital trading and asset ownership, enriching user interactions and expanding the digital economy. VR and AR technologies enable immersive trading experiences through virtual auction houses and promote the monetization of digital art, introducing possibilities for virtual real estate and cross-platform interoperability.
- **User Experience:** Users can experience real-world activities in the metaverse with full immersion and engagement. Such experiences include gaming, entertainment (e.g., virtual concerts), tourism, education, work meetings, shopping, etc. Users can create their own content and indulge in social interactions and interactive live events without the restrictions of time and space.

2) Metaverse Engine and Enabling Technologies: The metaverse engine layer (illustrated in Fig. 3) consists of the

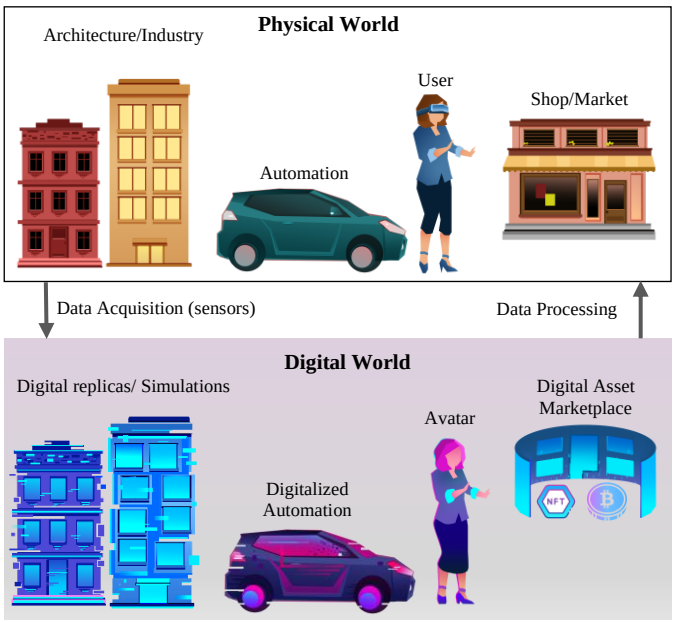

Fig. 4. Digital twin technology enables the replication of users, objects, and environments in the physical world into digital counterparts via sensors that feed real-time data to the digital space.

enabling technologies that bridge the physical and virtual worlds, such as human interfaces, AI technology, digital twins, and blockchain. This layer provides a continuous and real-time flow of data between the physical world and the metaverse. Data, especially big data from the physical world, is collected, analyzed, and processed though these technologies, enriching the virtual world with real-time feedback and interactions.

a) Digital Twin: Digital twin is an emerging technology that generates real-time virtual copies of physical objects with accurate representations of their actions and responses [53]. Data of physical elements is obtained via sensors and recreated in a digital space, building a "digital twin" of that element. AI techniques are used to simulate the effects of any changes that can occur in the real world. For a digital twin to function efficiently, information from physical sensors must be continuously gathered to ensure any changes in the physical world are reflected in the digital twin. As the metaverse is a virtual reflection of physical reality, digital twin technology is vital for creating exact replicas of elements and environments such as avatar generation, architectures, e-commerce, retail, and automation, as illustrated in Fig. 4.

b) Human Interfaces: Interfaces in the metaverse are revolutionized by emerging technologies. Extended Reality (XR), which includes Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), offers users deeply immersive environments, enhancing their sense of presence and engagement [54]. As shown in Fig. 5, VR immerses users in fully interactive digital environments, isolating them from the physical world, while AR overlays digital objects onto the real world, enhancing but not replacing the user's environment. MR merges real and virtual worlds to generate new environments where physical and virtual objects coexist in real-time, allowing users to interact with responsive elements integrated into real environments. Additionally, Brain-Computer Interface (BCI)

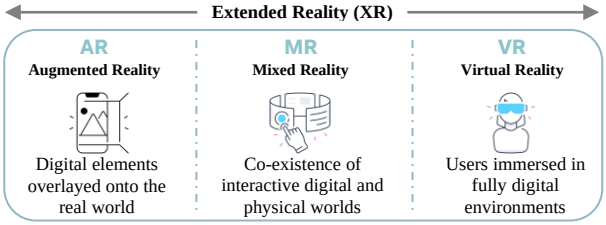

Fig. 5. Extended Reality (XR): A term describing the integration of Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), which enable immersive and interactive experience in the metaverse.

technology connects the human brain with a device to translate neural signals into commands, allowing users to control virtual elements or receive tactile feedback without physical movements [55]. The integration of XR and BCI opens new opportunities for the collection of biometric data and emotional states, which provides highly immersive, responsive, and personalized experiences for metaverse users.

c) *Artificial Intelligence*: Artificial Intelligence (AI) refers to the simulation of human intelligence in machines or computer systems, allowing them to perform tasks such as learning, problem-solving, and language understanding. AI offers the benefits of automating tasks, enhancing decision-making, improving efficiency, and unlocking insights from vast amounts of data. Table II lists several survey papers that explore the role of AI in various communication systems, highlighting the significant potential of using AI to ultimately transform industries and simplify our daily lives.

AI plays a transformative role in the metaverse [34][56]. It enables personalized experiences through sophisticated algorithms that analyze user behavior, preferences, and interactions. According to [57], AI enhances realism and user interaction via immersive content generation, intelligent interactions, conversational AI, and lifelike avatars. It also optimizes network infrastructure, improves interfaces, and advances spatial computing [57]. Moreover, AI powers natural language processing (NLP) for communication with virtual assistants and characters, making interactions more intuitive [58]. AI also supports the development of realistic scenes, non-playable characters (NPCs), and autonomous agents that can enhance storytelling and social interactions.

d) Blockchain: Blockchain is the core technology that supports decentralization, security, and transparency. It enables trustworthy transactions and ownership of digital assets via cryptocurrencies and NFTs.

e) Spatial Computing: Spatial computing is mainly responsible for the reconstruction of 3D spaces in the metaverse. It utilizes computer vision, AR, and sensors to blend digital content with the physical world with precise placement and scaling of virtual objects.

3) Key Characteristics: The metaverse is distinguished by several unique characteristics, including immersion, interoperability, decentralization, persistence, and scalability.

Immersion is the key characteristic that distinguishes the metaverse from the current Internet. Through integrating XR and haptic technologies, the metaverse creates highly engaging and realistic environments. The human senses are embedded

into the virtual space, elevating the user experience.

Interoperability allows users to seamlessly use and trade their virtual goods across virtual worlds. Achieving interoperability in the metaverse is an open challenge due to the need for global standards and protocols to ensure compatibility of virtual assets across several platforms [59].

Decentralization is another key characteristic of the metaverse. Transitioning from Web 2.0 to Web 3.0 leads to a user-centric and decentralized Internet, which is a key aspect of the metaverse. A decentralized system, opposite to a centralized one, eliminates the involvement of a third party, allowing users to control their transactions directly. This aspect, supported by blockchain technology, enhances security and data transmission in the metaverse [35].

Persistence refers to the ability of the metaverse to operate in real-time, ensuring that augmented objects and environments remain sustainable and accessible [27]. This means that AR objects placed in real-world locations will persist to exist even when not actively viewed, allowing for real-time updates visible to all metaverse users. This persistence can lead to cost and time savings, for example, by replacing physical billboards with AR technology [60].

Scalability ensures the environment can handle increasing number of users and complex interactions without degrading performance. Addressing scalability for the metaverse involves optimizing computing capabilities, network bandwidth, and the overall quality of the virtual experience.

Hyper-spatiotemporality in the metaverse refers to the enhanced and multidimensional integration of spatial and temporal elements within virtual environments, transcending the limitations of physical reality. This concept involves the manipulation and synchronization of space and time in ways that are not possible in the real world, allowing for dynamic, interactive, and immersive experiences.

4) Applications: The metaverse is revolutionizing various aspects of our daily lives, akin to how the evolution of the Internet transformed communication and interaction with technology. It offers diverse applications across entertainment, commerce, tourism, remote work, education, healthcare, and social interaction.

a) Entertainment: The metaverse is reshaping entertainment through immersive gaming, virtual events, concerts, and virtual theme parks, as highlighted by initiatives like Disney's virtual theme park project [61].

b) E-commerce: Commerce is evolving into an immersive experience where users can virtually navigate stores in real-time, exemplified by collaborations between brands like Gucci, Nike, and Roblox.

c) Tourism: Virtual tourism enriches the travel experience with various levels of interactivity based on user goals, offering digital trips for entertainment or immersive preview of travel destination [62]. The Emirates VR Experience is a VR application released by Emirates Airlines on the Oculus store, which allows users to explore the interior and services of the airline through a realistic and interactive VR experience [63].

d) Remote Work: The COVID-19 pandemic emphasized the need for effective online communication. The metaverse addresses challenges of remote work, such as social isolation [71] and reduced productivity due to lack of mobility [72], by offering immersive virtual meetings and customizable workspaces, as seen in platforms like Meta's Horizon Workrooms and Microsoft Mesh.

TABLE II
SURVEY PAPERS ON AI APPLICATIONS FOR VARIOUS

Ref	Field	Examples of discussed AI roles
[64]	6G Networks	Optimizing network efficiency, real-time decisions, fast data processing.
[65]	Smart Cities	Intelligent transportation systems, efficient urbanization and energy consumption, improved communications.
[66]	IoT and cyber-physical systems (CPS)	Adaptive network architecture, optimization of wireless technologies, federated learning for data privacy, real-time analytics.
[67]	Edge Computing	Optimizing computing offloading and resource allocation, reducing latency, adapting to dynamic workloads.
[68]	Cloud Computing	Optimizing resource allocation and server performance, creating GPU-accelerated computing
[69]	Vehicular Ad-hoc Networks	Safety applications, traffic management, routing optimization, mobility management.
[70]	Internet of Things (IoT) Systems	Operational efficiency, risk management, scalability, smart sensors and data gathering

e) Education: The metaverse enables realistic digital replicas of educational environments, offering immersive experimental learning and improved observations of students' behaviors via their emotional state and body language [73].

f) Healthcare: The metaverse is posed to enhance healthcare through telepresence, automation, remote diagnosis, and medical education/training [74], [75].

g) Social Interactions: Enhancing global communication, the metaverse facilitates rich online social interactions, allowing users to participate in activities regardless of physical distances.

h) Practice Platform: The metaverse provides a platform for realistic and controlled professional training in fields like athletics and military operations. Several studies demonstrate the potential of implementing immersive VR environments for professional training due to realistic stimulation, controlled environment, remote training, to name a few [76]-[78].

5) Metaverse Use Cases: Based on the metaverse's architecture and enabling technologies, we present two use cases that highlight examples of basic operations within it.

a) Building a Digital City: In the metaverse, a digital city is crafted by an interdisciplinary team of urban planners, architects, and digital artists. They design a city with various districts for education, entertainment, and innovation, utilizing advanced server technologies and cloud computing for infrastructure. Key elements include digital twinning of real-world locales for accurate urban simulations and integration with IoT devices to feed real-time data on weather, traffic, and environmental conditions. Through XR devices, users worldwide can explore this city, interact with its components, own virtual property, and engage in community governance. This virtual city is a dynamic platform for urban planning

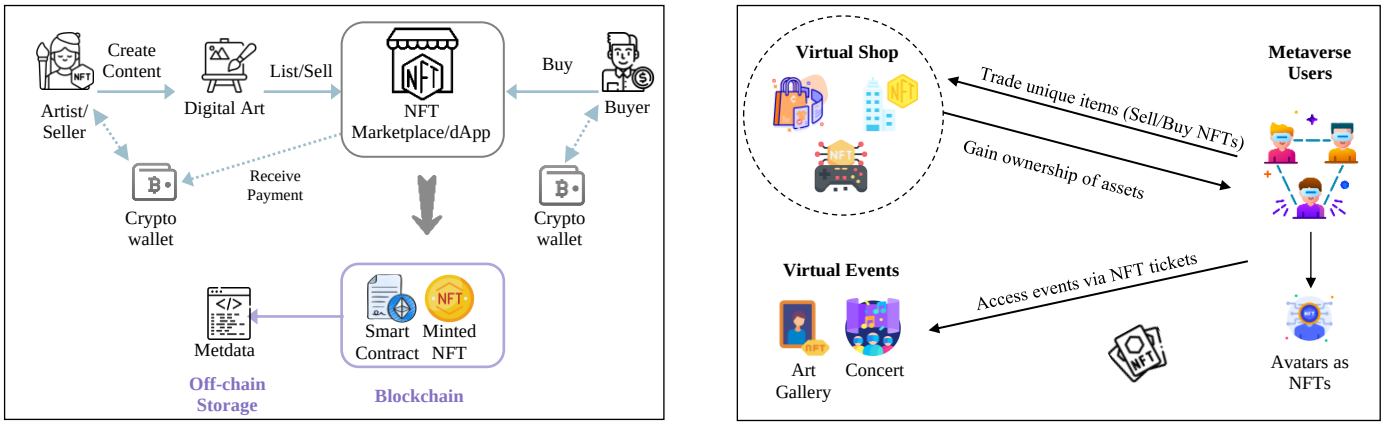

Fig. 6. Illustration of virtual asset trading withing the metaverse. Fig.6a illustrates the process of NFT creations in marketplaces and decentralized apps, highlighting the technical components and operations involved. Fig.6b illustrates a scenario where NFTs can be used in the metaverse, including using them for avatars, virtual shopping, and attending virtual events.

experiments, educational ventures, and cultural exhibitions, highlighting the seamless blend of real-world integration and virtual innovation within the metaverse.

b) Virtual Asset Trading: The metaverse is set to capitalize on blockchain technology to revolutionize asset trading, with NFTs being an example of digital assets traded in this use case, as shown in Fig. 6. Content creators (artists) can sign up to any NFT marketplace, such as OpenSea, where their accounts get linked to their cryptocurrency wallet. *MetaMask* stands out as a popular crypto wallet that allows users to interact with decentralized applications (dApps) via their Ethereum-based wallet. Once the artist lists the digital work on the NFT marketplace, it gets minted via a smart contract. The actual information (metadata) of the NFT is stored off-chain, while the buyer of an NFT, who is also required to connect their crypto wallet to the marketplace, can use or view the content of the NFT on blockchain once it is purchased (See Fig. 6a).

NFTs bring new opportunities for both metaverse users and enterprises (See Fig. 6b). With their ability to ensure ownership of virtue goods in the metaverse [79], shopping in the metaverse can be done more securely. Once an NFT-based item is purchased, users immediately get ownership of that item. Beyond asset trading, avatars can also be minted as NFTs, linking the identity of a user to that specific unique avatar, which offers a solution to impersonation problems in the metaverse [80]. Moreover, NFTs can be utilized for legal access controls within virtual worlds, enabling the creation of exclusive event tickets and managing organized virtual gatherings with specific access parameters.

6) Industries and Strategies: The global metaverse market has seen substantial investments in the tech industry. Table III lists several investing companies, highlighting their goals, current metaverse-related projects, and their publicly announced metaverse-specific security measures.

Mark Zuckerberg, the CEO of Meta, describes the metaverse as the "next chapter of the Internet" [81]. Meta's goals revolve around building user-centric and immersive experiences where users can engage in activities such as work, shopping, and learning. Zuckerberg acknowledges the need to address privacy and cybersecurity issues, open standards, interoperability, and governance. Meta has officially committed to responsible innovation to create a safe and sustainable metaverse by prioritizing user safety and privacy [82].

Microsoft envisions the metaverse as the new version of the Internet [83], focusing on the evolution of the workplace. Their online meetings platform, Mesh for Microsoft Teams, integrates MR, AI, digital twins, and holograms to create an immersive and accessible digital-physical work experience. In Teams, users can represent themselves as 3D avatars that reflect lip and head movements. Charlie Bell, the executive vice president of security, compliance, identity, and management at Microsoft, discussed potential privacy threats such as fraud and impersonation attacks [84], and called for further investigation of possible solutions.

Nvidia's metaverse strategy focuses on the economic benefits for enterprises and industries. Its platform, Omniverse, generates AI-driven 3D simulations of physical environments, aiming to provide efficient and time-saving workflows [85]. Nvidia is dedicated to integrating AI and cybersecurity in the future, as they publicly highlighted the company's role in accelerating cybersecurity applications like threat detection, zero-trust architecture, and fingerprint scanning [86].

Apple Inc. has a different perspective on the metaverse, focusing on the development of AR technology. Tim Cook, CEO of Apple, stated that his company does not embrace the term metaverse due to its vagueness. However, Cook anticipates a future where MR will be implemented in daily life activities, leading to a new technological revolution [87]. While Apple has not disclosed specific security and privacy measures, their Vision Pro XR headset utilizes iris recognition for user authentication.

Adobe Inc. aims to create virtual goods for the metaverse [88]. Adobe Experience Manager (AEM) Cloud Services employ security measures such as encryption, authentication, and auditing to protect user data [89]. Unity Technologies is collaborating with other companies to incorporate its engine as a tool for content creation in the metaverse [90]. Epic Games focuses on the consumer's perspective and experience, aiming to allow users to own and monetize their creations [91]. Regarding safety issues, Epic Games and Lego Group

TABLE III
COMPANIES INVESTING IN THE METAVERSE, THEIR APPLICATIONS, AND METAVERSE-RELATED SECURITY MEASURES

Company/ Platform	Goal/Vision	Current Applications/ Hardware	Security/Privacy Measures
Meta	Advancing from 2D screens into immersive 3D worlds, where people can engage in work, physical health, commerce, and education	- Horizon Worlds - Horizon Workrooms - Oculus Headsets	User privacy protocols
Microsoft	Building a real-presence digital representation of the physical world, focusing on the workplace and industrial usage	- Mesh for Microsoft Teams - HoloLens Headsets	- Identity management - User privacy. - Transparency - Collaborative governance
Nvidia	Applying the metaverse in industries and businesses for economics to reduce workload and save time via immersive 3D simulations of physical environments	- Omniverse	- AI for cybersecurity
Apple	Focusing on the development and implementation of MR (specifically AR) for daily-life activities	- Entertainment: Clips app - Shopping: Warby Parker and IKEA Place - Education: Apollo's Moon-Shot AR - Tourism: Museum Alive	- Iris recognition for user authentication (Vision Pro)
Adobe	Creating 3D virtual goods for a variety of experiences, such as gaming, shopping, art, virtual museums, and job training	- Adobe Substance 3D - Adobe Aero	Encryption, authentication
Unity	Utilizing multiple technologies to collaborate with other companies and build real-time immersive worlds for variant experiences	- Industrial: Hyundai's Meta-Factory - Sports: Rezzil's training app - Shopping: Samsung's digital twin store - Healthcare: Fatal Heart VR	N/A
Epic Games	Focusing on user-centered experience and ownership of virtual assets	- Unreal Engine - Fortnite	Protected virtual world for under-aged groups
Amazon	Integrating metaverse technologies for immersive shopping experiences	- Amazon AR View	N/A
Nike	Building a virtual space for immersive experiences and NFT trading	- Nikeland	N/A
MetaDubai	Leveraging multiple technologies to build a digital twin of Dubai city	- MetaDubai	N/A

announced a collaborative project to build an immersive regulated digital world for children to ensure their safety and privacy [92].

Amazon Web Service (AWS) is specialized in immersive online shopping [27], while Nike Inc. has developed *Nikeland*, a Roblox-based virtual space where users can engage in different experiences related to the brand, such as gaming, socializing, working, and NFT trading [93]. MetaDubai, an ongoing project that aims to build a digital version of Dubai city, focuses on improving the economy and developing the future metaverse via the integration of XR, AI, big data, blockchain, and cloud/edge computing.

The massive global interest in the metaverse implies its significant potential for economic growth in enterprises and businesses, as well as providing an innovative user experience for many applications. However, most companies are currently focused on technological challenges, and a few have publicly addressed cybersecurity and privacy concerns.

B. Artificial Intelligence for Cybersecurity

Artificial Intelligence (AI) aims to create systems capable of performing tasks that require human intelligence, such as learning, problem-solving, and perception. Generally, AI systems rely on algorithms to acquire knowledge and make informed decisions. The generic workflow, illustrated in Fig. 7, starts with problem definition, data acquisition and preparation, model training and development, tuning and evaluation, and then model deployment and testing against new data.

In the field of cybersecurity, AI allows for real-time detection and mitigation of security threats. AI systems process large volumes of data, identify anomalies, and automate responses to threats, enabling proactive defense mechanisms against evolving cyber threats, as reviewed in [94]-[97]. Within AI, machine learning (ML) is a core subfield extensively utilized in cybersecurity applications. ML enables computers to learn from data autonomously, identifying patterns and making decisions without human intervention. Deep Learning (DL) is an advanced branch of ML that uses multi-layered *neural networks* to simulate the complex processing of the human brain. Unlike traditional ML, which offers manual feature extraction, DL automates this process, allowing the system to learn directly from the data through the deep network of layers.

This subsection provides an overview of various ML algorithms employed in cybersecurity applications and highlights the key performance metrics required for AI-based cybersecurity systems.

1) Learning-based Algorithms for Cybersecurity: ML can be broadly categorized based on the system's learning style into Supervised Learning, Unsupervised Learning, Semi-Supervised Learning, Reinforcement Learning, and Federated Learning, as shown in Fig. 8.

a) Supervised Learning (SL): This method requires *labeled* datasets, in which the model is trained using an input object

(vector) and a corresponding output (label). The algorithm learns the mapping function from the input and output to perform tasks such as classification and regression. Common algorithms used in SL include Decision Trees (DT), Random Forest (RF), and Support Vector Machines (SVM). DT utilize a hierarchical tree structure consisting of several nodes and branches used to enable decision-making, while RF integrates multiple DT for robust accuracy. DT and RF are widely employed in cybersecurity for fraud detection [98] and phishing attacks identification [99]. SVM, known for their efficacy in classification by maximizing the margin between classes, are extensively applied in malware detection across Android platforms [100], network traffic [101], and unknown malware classification [102]. Additionally, ensemble learning is a specific method that combines multiple ML algorithms to improve model accuracy and robustness. For example, a combined DT and SVM framework proposed in [103] has shown high accuracy for malware detection within IoT ecosystems. AdaBoost and XGBoost are notable ensemble learning algorithms that have also been deployed to enhance the detection of complex threats in IoT domains [104],[105].

Artificial Neural Network (ANN) architectures like Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) are also examples of SL methods. RNNs, particularly Long-short Term Memory (LSTM) networks, can process information from previous inputs to influence the output of subsequent steps, making them ideal for analyzing time-series data or sequences of actions within cybersecurity, such as continuous monitoring of network traffic for anomaly detection. CNNs are specialized deep neural networks that excel in handling data with grid-like structures such as images. In cybersecurity, CNNs are commonly used for tasks like biometric authentication and malware image identification to detect suspicious patterns or anomalies [106].

b) Unsupervised Learning (UL): UL deals with *unlabeled data*, allowing algorithms to learn and identify patterns without human supervision.

Clustering focuses on grouping similar data points into clusters. K-Means is a common clustering algorithm that partitions a dataset into K distinct groups, with each data point assigned to the nearest mean value (centroid). In cybersecurity, log files are crucial for identifying and detecting anomalies. Clustering techniques manage the vast amounts of unstructured data from system logs, aiding in outlier detection and enhancing anomaly detection [107].

Dimensionality Reduction aims to reduce the number of input variables in a dataset to simplify it without losing important information. Principal Component Analysis (PCA) is an example of such algorithms, which finds the most significant features in a dataset that makes the data easy for 2D and 3D visualization and identifying linear combinations of variables. Autoencoders (AEs) are a type of artificial neural network used to learn efficient representations of data, which can also be used for dimensionality reduction. An AE consists of an encoder that compresses input data into a lower-dimensional form and a decoder that reconstructs the original data from the compressed representation. The goal is to minimize the difference between the input and the reconstructed output, effectively capturing the important features of the data. This makes AEs useful for dimensionality reduction. In cybersecurity, AEs detect

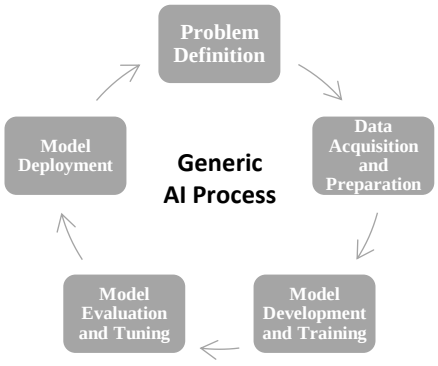

Fig. 7. Generic AI Process

anomalies or outliers in data by identifying unusual behavior in user activities or network traffic, which could indicate a cyber-attack or breach [108].

Data Generation involves creating new data points similar to a given dataset, which can be used for data augmentation, simulation, and anomaly detection. Generative Adversarial Networks (GANs) are generative models that consist of two neural networks, a generator and a discriminator, trained simultaneously to generate and discriminate between real and synthetic data, respectively. GANs are trained on given datasets and can generate synthetic data for data augmentation purposes, such as increasing dataset size or balancing class distribution, thereby improving the overall performance of the AI model. GANs enhance security by creating synthetic data for secure analysis, improving intrusion detection systems and malware detection through adversarial training. They are also used in secure image steganography to conceal data within images and in neural cryptography for encrypting biometric data [109].

*c) Semi-Supervised Learning***:** Semi-supervised learning uses both labeled and unlabeled data for training. This approach is particularly useful when acquiring a fully labeled dataset is expensive or impractical. Semi-supervised learning techniques have been employed in various cybersecurity applications, including anomaly detection [110], cyberattack detection in smart grids [111], ransomware detection [112], detection of malicious authentication attempts [113], and insider threat detection [114].

d) Reinforcement Learning (RL): In RL, an agent learns to make decisions by performing actions in an environment to achieve rewards. Two notable RL algorithms are Q-Learning and Deep Q-Networks (DQN). Q-Learning is a model-free algorithm that learns the value of actions directly, while DQN combines Q-Learning with deep neural networks for more complex decision-making. In cybersecurity, RL can be utilized to develop adaptive systems that continuously learn and optimize their detection capabilities. Several survey papers review the applications of RL in cybersecurity systems, including intrusion detection, intrusion prevention, botnet detection, identity management, etc. [115], [116].

e) Federated Learning (FL): Federated Learning is a ML paradigm where multiple decentralized devices collaboratively train a model without sharing their local data [117]. FL is extensively researched within metaverse security since it is expected to address privacy and computational efficiency issues [118]. FL is categorized into three types based on how data is distributed among participants.

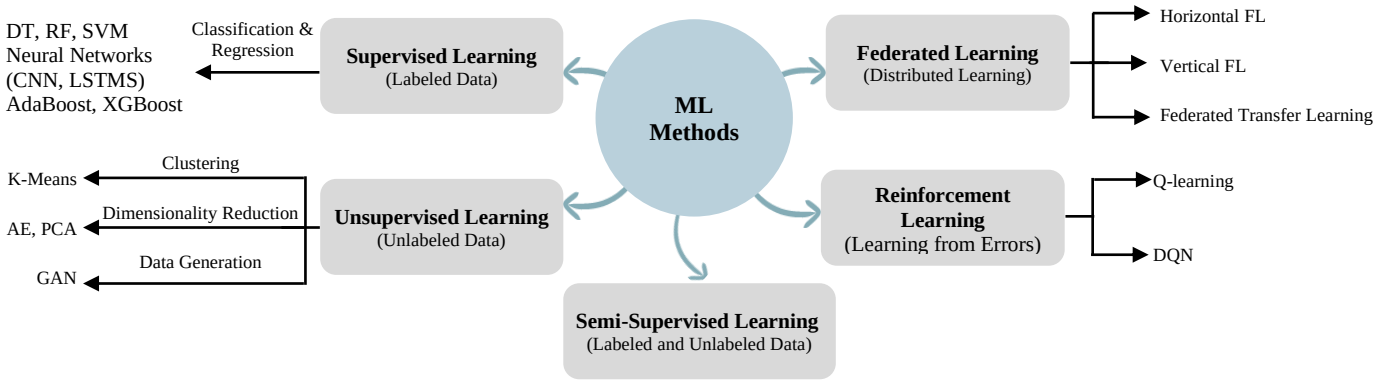

Fig. 8. Categorization of common ML methods used in cybersecurity based on model learning style.

- **Horizonal Federated Learning (HFL)**: Involves training with similar data features but from different samples.
- **Vertical Federated Learning (VFL)**: Involves training with **shared** or overlapped samples but different data features.
- **Federated Transfer Learning (FTL):** Involves training with different samples and features.

2) Performance Metrics: In ML systems, several metrics are generally used to evaluate the performance of models in cybersecurity applications.

a) Accuracy: The ratio of the correct predictions to the total number of predictions. Higher accuracy indicates a better-performing system.

b) Confusion Matrix: A summary table often used to evaluate model performance. In includes:

- **True Positive (TP):** Correctly identified legitimate actions or entities.
- **True Negative (TN):** Correctly rejected malicious actions or entities.
- **False Positive (FP):** Incorrectly identified legitimate actions or entities as malicious.
- **False Negative (FN):** Incorrectly identified malicious actions or entities as legitimate.

c) False Acceptance Rate (FAR): The probability that the system incorrectly accepts a malicious action or entity. Lower FAR is preferred to avoid security breaches.

d) False Rejection Rate (FRR): The probability that the system incorrectly rejects a legitimate action or entity. Lower FRR is preferred to ensure usability.

e) Equal Error Rate (EER): The point where FAR and FRR are equal. A lower EER indicates a more accurate system.

f) Area Under the Curve (AUC): The value quantifying overall model performance by measuring the area under the Receiver Operating Characteristic (ROC) curve. A higher AUC indicates better performance.

Effective AI training, validation, and monitoring are essential to reduce false positives and negatives, ensuring robust system security.

IV. Cybersecurity Threats in the Metaverse

Cybersecurity threats refer to malicious activities that aim to gain unauthorized access to data or cause damage to computer systems and networks. While cybercrimes have been occurring since the evolution of the Internet, they are rapidly evolving with the growth of technology. According to a report published by the Internet Crime Compliant Center (IC3) in the United States, a loss of 6.9 billion dollars was caused by cybercrime in 2021, which is an increase of 64% from 2020 [119]. Cybercriminals often target new technological trends, as exemplified by the significant increase in scam and frauds (i.e., phishing attacks) during the pandemic due to dependance on remote work [120]. With the metaverse being a new form of the Internet that integrates various innovative technologies, the attack surface increases, and current cybersecurity threats are likely to be magnified.

In this section, we examine potential risks in the metaverse from a cybersecurity perspective. First, we highlight the impact of existing cyberattacks on the metaverse and present scenarios that illustrate several potential attack models. Second, we provide a general discussion on metaverse threats according to several aspects: Data, identity, privacy, digital wellbeing, legal regulations, and NFTs.

A. Cyberattacks and Attack Models

Traditional cyberattacks, such as network-based attacks and malware injections, will continue to target the metaverse. However, their potential impact is expected to magnify due to the complex nature of the metaverse ecosystem and its deployment into daily life activities. The convergence of innovative technologies, such as XR and digital twins, introduces new threats that exploit the unique immersive and interconnected features of the metaverse, ranging from integrity issues to threatening the wellbeing of users [121],[122]. Attackers can also utilize AI techniques to launch sophisticated and automated attacks, targeting the metaverse infrastructure. These AI-driven attacks are particularly concerning as they can adapt, learn, and bypass conventional security measures [123],[124]. Some attacks may even target and exploit vulnerabilities within AI models (e.g. Data Poisoning attacks), which presents a meta-layer of security challenges requiring innovative defensive strategies. Table IV lists examples of traditional cyberattacks, immersion-based attacks, and AI-based attacks, each with their respective definition and impact on the metaverse.

Based on the metaverse architecture, use cases, and existing cyberattacks, we propose three scenarios that highlight

TABLE IV
CYBERATTACKS AND THEIR IMPACT ON THE METAVERSE

Attack Type	Cyberattack	Definition	Impact on the Metaverse
Traditional Attacks	**Denial of Service DoS/DDoS**	A cyberattack that prevents access to legitimate users due to high traffic (flood) from a compromised computer. Distributed DoS (DDoS) occurs when multiple computers are used to perform the attack	Attackers can target IoT devices connected to the metaverse to launch DDoS attacks. Service interruption in the metaverse is very costly and risky due to its significant economic impact and integration into everyday life activities.
	Malware Attacks	Malware refers to malicious software developed to infect devices and networks. Examples of malware include viruses, worms, and trojans	The multitude of devices and sensors used to access the metaverse makes them susceptible to malware attacks, compromising user privacy and security
	Ransomware Attacks	Ransomware is a type of malware that encrypts data and blocks access to computer systems until the attacker's demands are met. (Usually monetary demands)	With the expansive economy in the metaverse and the emergence of NFTs and cryptocurrency, ransomware demands can be higher and have a significant impact on both companies and individuals
	Phishing Attacks	The attacker tricks the victim by sending malicious emails and links to steal sensitive information	Phishing attacks are already causing major theft incidents in NFT marketplaces and are expected to target the intellectual property and personal information of metaverse users
	Man in The Middle (MiTM)	MiTM attacks occur when attackers position themselves between the communication of two entities to eavesdrop, alter data, or inject malicious content into the communication flow	MiTM attackers eavesdrop on user-to-user communications and transactions of virtual assets in the metaverse, leading to theft or altering of sensitive data. MiTM attackers can also disrupt data flow between the physical and virtual worlds, leading to inaccurate rendering of digital twin entities
	Masquerade Impersonation Attacks	Occurs when an attacker disguises themselves as a legitimate user to gain access to sensitive information	With digital twins and avatar generation, malicious attackers can impersonate legitimate users and potentially gain access to unauthorized information
Immersion-based Attacks	**Overlay Attacks**	In an overlay attack, malicious content is placed on top of user interface (UI) elements to deceive or harm users	Affects user perception and interaction with immersive environments, leading to manipulation, phishing, or unauthorized access to virtual resources
	Occlusion Attacks	These attacks cause disorientation of the content in an immersive environment, obstructing the user's view during a VR session	Disrupts the user experience, which can be significantly problematic for learning and work environments. It can also lead to physically harming users by causing cybersickness
AI-driven Attacks	**False Generation of Data**	AL algorithms generate synthetic, misleading content such as fake news or deepfake audio/visuals of users	Can lead to misinformation, manipulation of public opinion, impersonation of other users to gain personal information that can lead to unauthorized access
	AI-driven password attacks	Deep learning models, like GAN, can be utilized to guess passwords based on learned distributions from actual breaches, improving the success rate of password cracking attacks	Attempting to gain unauthorized access is inevitable in the metaverse. In case of a password breach, sensitive data will be put at risk (e.g. biometrics, digital goods)
	AI-Model Manipulation	Manipulation of ML models with adversarial techniques to degrade their performance (e.g., data poisoning)	The heavy reliance on AI in the metaverse can motivate attackers to target the ML algorithms or datasets used for training, compromising their effectiveness and increasing vulnerabilities to attacks

examples of possible attack models in the metaverse, including the creation of digital entities, impersonation of other users, and targeting digital goods, as illustrated in Fig. 9.

1) Scenario 1: Digital Integrity Attacks: In this scenario (based on Use Case 1 presented in Section III), a digital city is developed by an interdisciplinary team using digital twin technology and IoT. The scenario highlights three possible cyberattacks related to data integrity and information transmission: Data tempering, MiTM attack, and overlay attacks. With data tempering, the attacker exploits vulnerabilities in a sensor to compromise its accuracy via malware injections, distorting the digital twin's representation and leading to flawed urban planning decisions. MiTM attacks intercept communication channels between the physical infrastructure and its digital counterpart, altering data flow and resulting in inaccurate simulations of city models. The overlay attack introduces malicious content into the digital city that can be utilized for false advertising, manipulation, or inducing psychological effects on the users (e.g., panic).

2) Scenario 2: User Impersonation: In this scenario, the identity of a user engaging in a metaverse-based meeting is compromised through two impersonation tactics. First, a MiTM attack intercepts communications between the user and the metaverse platform, especially when the user attempts to access the meeting by providing authentication credentials. The attacker establishes a fraudulent connection to extract sensitive information, thus endangering the user's digital identity. Secondly, utilizing AI to create convincing deepfakes based on stolen data, an attacker crafts a deceptive avatar that mimics the user's facial features and voice, engaging in acts of misinformation, harassment, or reputational damage. This is particularly dangerous if the impersonated avatar holds a position of authority (e.g., a CEO or political figure), since attackers take advantage of their perceived trust to extract

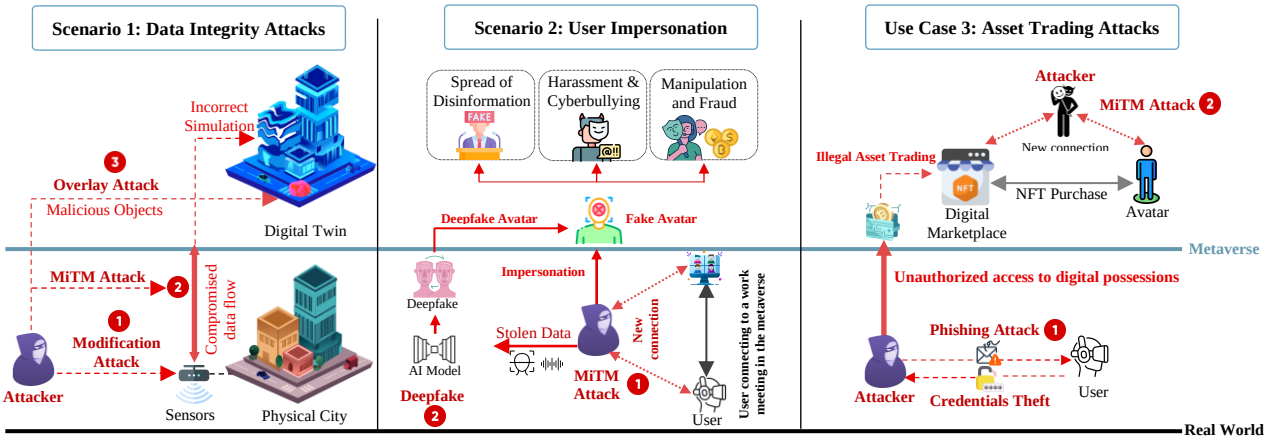

Fig 9. Attack models based on three scenarios. Scenario 1 illustrates integrity attacks on digital twin environments. Scenario 2 highlights possible attacks that can lead to user impersonation in the metaverse. Scenario 3 is set to show a combination of traditional attacks (phishing and MiTM) that can occur when metaverse users are involved in asset trading.

private information or manipulate others within the metaverse.

3) Scenario 3: Virtual Asset Trading: This scenario outlines cyberattacks that target asset trading in the metaverse. Attackers can use sophisticated phishing attacks to gain unauthorized access to users' assets, enabling them to conduct illegal transactions. Additionally, a MiTM attacker can eavesdrop on communications during asset transactions, aiming to capture sensitive information like user credentials, digital wallet details, and transaction data. Such breaches not only compromise the financial security of individuals, but it also undermines trust and integrity of the virtual marketplace's security mechanisms.

B. Emerging Threats in the Metaverse

The unique characteristics of the metaverse introduce potential cybersecurity and privacy risks, which can be generalized as follows:

1) ***Scalability:*** The metaverse allows a massive number of users to log into virtual worlds simultaneously. Thus, significant amounts of data are collected, increasing the risk of highly sensitive information.
2) ***Availability:*** DoS and ransomware attacks pose significant impact on users and enterprises due to its integration into various aspects of daily life and operations.
3) ***Interoperability:*** The presence of multiple metaverse sub-worlds increases the attack surface and raises issues concerning privacy and authentication.
4) ***Immersion:*** Biometric and behavioral information is collected via headsets, putting sensitive information at risk. Additionally, the immersive nature of the metaverse can amplify the impacts malicious behaviors such as cyberbullying.
5) ***Hyper-Spatiotemporality:*** Integrity compromises will arise as distinguishing between what is real and fake in the metaverse can become challenging.
6) ***Decentralization:*** Concerns regarding virtual asset transactions and user authentication are heightened in the decentralized environment of the metaverse, posing additional security challenges.

We discuss metaverse threats based on six aspects, as summarized in Fig. 10: Data threats, digital identity threats, privacy threats, digital well-being threats, legal and regulations issues, and security risks associated with blockchain and NFTs. The figure also illustrates how some metaverse elements are linked to potential threats.

1) Data Threats: Data security and privacy are ongoing concerns in the current Internet. Attackers target sensitive information for monetary gains, data theft, and political motives. As shown earlier in Table IV, data is vulnerable to various traditional cyberattacks aimed at damaging or stealing information. The metaverse is still susceptible to these cyberattacks due to its reliance on traditional IT hardware [125]. However, the complexity of the metaverse and the vast amount of data collected by third-party companies heighten concerns about cyberattacks and privacy issues.

In Information Security, the three principles for a secure infrastructure are confidentiality, integrity, and availability, known as the “CIA triad”. Confidentiality relates to privacy, integrity refers to data consistency, and availability ensures data accessibility at any time and place. From an attacker’s perspective, they target confidentiality through data theft, integrity via data manipulation, and availability by denying users access to computer and network systems.

a) Data Confidentiality Risks: Confidentiality in cybersecurity refers to protecting sensitive data from unauthorized access, closely tied to privacy. It ensures that only authorized users can access specific information. Data breaches are a major concern in today's Internet, and it is expected that they will amplify in the metaverse due to the amount and sensitivity of data. Data breaches occur when confidential information is exposed to unauthorized parties, significantly impacting reputation and user privacy. In some cases, data breaches can cause financial losses [126]. For instance, 165 million LinkedIn records were compromised in 2012, which led the company to compensate users who paid for services with an estimated value of 1.25 million dollars [127]. Similarly, the online game *Second Life*, one of the earliest versions of the metaverse, suffered a data breach in 2006 affecting 660 thousand users [128]. Cyberattacks like phishing and malware injections can occur in the metaverse, with potentially greater impact due to the larger amount of data at stake. Biometric information, which is permanently linked to users, poses a

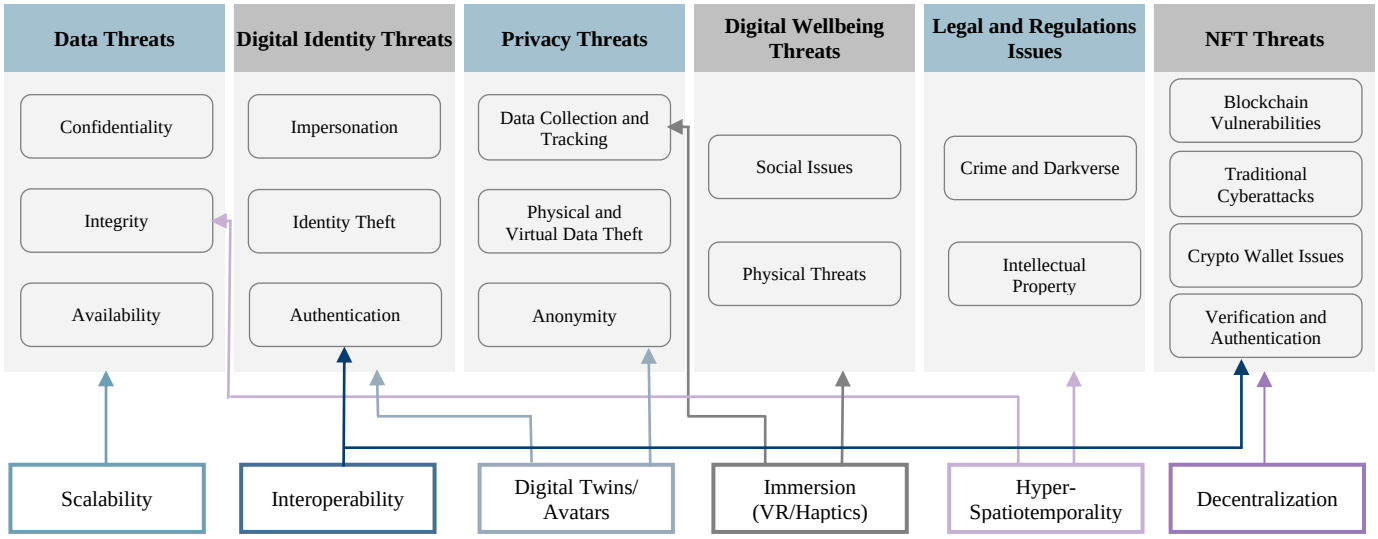

Fig. 10. Cybersecurity issues discussed in this paper are based on threats related to data, identity, privacy, digital wellbeing, legal regulations, and NFTs. The figure illustrates how some characteristics/elements of the metaverse cause such issues. Scalability is generally related to data issues as more information will be put at risk. Interoperability leads to issues in authentication and asset management, while Digital Twin technology is related to identity and anonymity issues. Immersion causes concerns regarding the data collected (biometrics) and can amplify the impact of physical and social issues on users due to the high sense of presence. Hyper-Spatiotemporality can lead to integrity and crime issues, while decentralization is mainly associated with NFTs and blockchain.

significant privacy risk if compromised, far exceeding the impact of traditional credentials loss.

b) Data Integrity Threats: Data integrity ensures that digital information is reliable, trustworthy, and uncorrupted throughout its lifecycle. Cyberattacks targeting data integrity involve data manipulation for various purposes, such as tampering with records or accessing backup data for ransomware. In the metaverse, data manipulation can have severe consequences. For example, attackers could exploit vulnerabilities in metaverse hardware or software to redirect payments or tamper with medical records, leading to false prescriptions and potential fatalities [129].

The hyper-spatiotemporal nature of the metaverse allows for extensive personalization in content creation. If wearable devices are compromised, attackers could inject malware to manipulate data. For instance, overlay attacks generate malicious content on the user's VR view, which cannot be removed and can deceive users into divulging personal information [130]. Another manipulation scenario includes misleading users by altering location directions in GPS-based applications.

c) Data Availability Threats: The third CIA triad element is availability, which aims to guarantee that information is consistently accessible to authorized users. Common cyberattacks threatening data availability include DoS and DDoS attacks, as discussed in Table IV. DoS attacks can disrupt user workflow, time, and convenience, with severe reputational and financial impacts on organizations. The metaverse, with its multi-billion-dollar market, is an attractive target for ransomware. Additionally, as a multi-application space utilizing IoT and HMDs, any weaknesses in these devices can be exploited for DoS attacks, significantly affecting healthcare, education, and work dependent on the metaverse.

2) Identity Threats: Digital identity is one of the key features of the metaverse. Users represent themselves as multiple digital avatars, which are customizable, interoperable, and sometimes valuable (e.g., if they were NFTs). Virtual assets and social interactions are also aligned with the user's identity. Thus, identity management in the metaverse is crucial, as the user's virtual identity is associated with their physical attributes, whether it is their biometrics, behaviors, connections, or possessions. Identity-related issues include identity theft, impersonation, fake AI-generated virtual objects, and user authentication.

a) Impersonation: Cybercriminals carry out impersonation attacks to imitate a legitimate user's identity to steal credentials or financial information from targeted individuals or organizations. Common impersonation tactics include manipulating email addresses to mimic the original, creating fake social media accounts, and posing as users or company executives. In the metaverse, detecting such attacks is more challenging. Attackers can use ML techniques to manipulate visuals and sounds, creating avatars that resemble specific users. For example, deepfake technology leverages deep learning techniques (i.e., encoders and GAN networks) to capture a person's facial expressions, voice, and behavior, generating realistic images or videos of that person [131].

Impersonation leads manipulation of other users, sabotaging the reputation of the impersonated user, gaining unauthorized access to assets, spreading fake news, cyberbullying, extortion, and the creation of illegal content. These activities can cause physical, psychological, political, and financial harm to both individuals and companies.

b) Identity Theft: Social network users are more susceptible to identity theft crimes as they are more willing to share their private information [132]. In 2021, identity theft increased by 20% compared to 2020 due to rapid digitalization [119]. The identity of metaverse users will include more critical information than social media applications, such as biometric data, digital assets, and secret keys, which can be obtained via

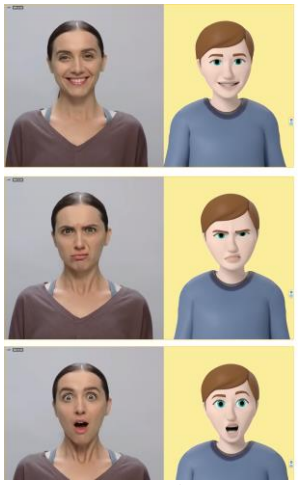

Fig. 11. Facial expressions accurately reflected onto avatars using Oculus Pro headset [138]

hacking wearable devices and phishing scams [27]. Therefore, having a user's identity stolen in the metaverse poses a significant risk. Philipp Pointner, the chief of digital identity at *Jumio*, emphasized the risks to users if their digital possessions were stolen, since they are tied to monetary value in the physical world. He called for exploring more innovative methods to protect users' digital identities [133].

c) User Authentication: Avatar authentication is necessary in the metaverse to prevent issues like impersonation and identity theft. However, two main challenges arise. First, despite the high security and better usability of utilizing biometrics for authentication systems (such as face and voice), compromising such sensitive traits poses significant risks to user privacy. Additionally, with advanced technology, attackers gain access to users' biometrics or imitate them and perform spoofing attacks, granting them false access to the system. Therefore, more robust and privacy-preserving methods are needed to safely authenticate users in the metaverse.

Second, as pointed out by Wang *et al.* [134], interoperability in the metaverse allows users to move between different platforms and domains. This calls for research on fast and efficient cross-platform authentication, which should provide a secure and user-friendly experience by allowing users to travel and use their assets across different applications without the need for reauthentication.

3) Privacy Issues: Ensuring user privacy is essential to prevent unauthorized access to sensitive information. The privacy concerns of the metaverse discussed in this paper focus on data sensitivity and theft, as well as the anonymity of avatars.

a) Sensitive Data Collection and Tracking: In the current web, organizations have access to user data for marketing purposes [135]. For example, Google's search engine utilizes web tracking technologies to learn about user preferences and customize advertisements accordingly. This trend will continue in the metaverse, but the nature of the data will be highly sensitive. Metaverse hardware can capture the user's biometric information, including eye and head movements, facial patterns, voice, and possibly brainwaves and health-related data like blood pressure, heart rate, and breathing rates. Moreover, biometrics can be utilized to detect human emotions [136], adding a new level of privacy concerns in the metaverse. For

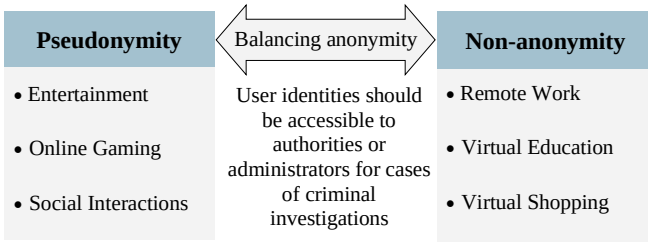

Fig. 12. Anonymity framework for metaverse users.

instance, Quest Pro VR headset, released by Meta in 2022, has high capabilities for accurately imitating the user's facial expressions, eye movements, and eye contact with other users, as shown in Fig. 11 [137],[138]. According to Meta's privacy policy [139], headset position, audio data, hand tracking, eye tracking, and facial expressions are collected to provide the user with immersive experiences. Therefore, companies investing in the metaverse are expected to implement invasive data collection in the future, putting the user's privacy at risk.

b) Date Theft in Physical and Virtual Environments: Compromised VR and IoT equipment can lead to the theft of information directly and physically related to the user, such as voice, facial features, behavioral information, brain signals, etc. Attackers can target metaverse hardware to use it as spyware, a type of malware used to track the user's physical environment to steal private information [140]. Data theft can also occur within the virtual metaverse itself. For example, AI bot avatars can target a user's avatar to monitor their behaviors, leading to impersonation attacks.

c) Anonymity: Online anonymity is a critical issue in the metaverse. While shielding one's identity is essential for protecting user privacy, it can also be exploited for harmful purposes like cyberbullying and illegal activities [141]. Anonymity in the metaverse raises concerns about the accountability of user identities, as individuals can create multiple avatars for diverse intentions. Consequently, there is a pressing need for further research to explore policies that balance users' rights to remain anonymous in specific contexts and prevent potential misuse of this feature for malicious purposes in the metaverse.

Granting full anonymity to users might be challenging. However, users can create pseudonymous avatars and accounts with optional identity verification, allowing them to remain partially anonymous or opt for verified accounts, depending on their preferences. Users can create pseudonymous avatars for unofficial applications, such as video games, art events, and virtual concerts. However, the identity of an avatar needs to be visible and represent the user's physical attributes in settings such as work, education, and virtual asset transactions. In the case of criminal activities, regardless of the activity the user is engaged in, legal authorities should be able to track the offender by having access to information about their physical identity, as proposed in Fig. 12. Policies such as real-name registration, where users are obligated to provide legal documents for authorities to use in case of any criminal investigation, can be deployed in the metaverse to manage the issue of anonymity.

4) Digital Wellbeing Threats: VR and AR are two of the key

enablers that build the metaverse. However, there are some concerns about the effect of these technologies on the psychological and physical wellbeing of users.

a) Social Issues: The flexibility, hyper-spatiotemporality, and decentralization of content creation in the metaverse allow users to control what happens rather than adhering strictly to central authorities and regulations. For example, on current social media platforms, users can create content that meets certain requirements and specifications, and interaction with others is restricted (e.g., liking a post or commenting). However, the lack of regulations and physical restrictions in the metaverse can lead to social misconduct. Negative user-to-user interactions, already prevalent on social media platforms, are inevitable in the metaverse.

From a culprit's perspective, it is more convenient to engage in harmful behaviors in the metaverse compared to the real world due to the lack of physical limitations and the relatively lower risk of getting caught. Such acts include cyberbullying, harassment, verbal abuse, and stalking, which have significant impacts on victims due to the immersion and realism of metaverse environments. Recently, a researcher reported that her avatar was physically harassed and assaulted in Meta's Horizon Worlds app. In response, Meta developed a "Personal Boundary" feature that prevents avatars from approaching within about four feet of other avatars [142].

Falchuk *et al*. [143] proposed solutions for social and behavioral issues in the metaverse, such as allowing users to clone their avatars, teleport, or activate an invisibility feature to hide their avatars in the virtual world. While these solutions contribute to user safety, their effectiveness depends on whether users can use them appropriately. Additionally, malicious users might misuse such features, causing other potential risks.

b) Physical Risks: In VR environments, immersion attacks can manipulate virtual environments and potentially lead to physical harm. For example, *chaperone* attacks occur when attackers alter the walls in the environment, putting the user's safety at risk [144]. Attackers can also manipulate the physical movement of the user without their knowledge, known as *Human Joystick attacks* [145]. Moreover, *disorientation attacks* induce dizziness and confusion in VR users [144]. Casey *at el*. [130] conducted an experiment in which these attacks were implemented using OpenVR software. The results showed that the impact of these attacks was magnified due to the immersion in VR environments. Furthermore, the authors found that VR systems, in general, are prone to cyberattacks, regardless of the hardware used. Therefore, developing secure VR systems is especially essential for the metaverse.

5) Legal and Regulation Issues: As the metaverse introduces new ways for people to interact with technology and the Internet, legal issues concerning criminal laws, intellectual property, and virtual asset regulations might arise [146].

a) Cybercrime and the Darkverse: Data theft, money laundering, fraud, assault, and crimes against children are examples of potential crimes that can take place in the metaverse. While these cybercrimes already exist on today's Internet, the immersive characteristics of the metaverse can introduce new methods for committing crimes. Trend Micro, a cybersecurity company, predicts the emergence of the *Darkverse*, a virtual dark web where criminals conduct illegal activities anonymously [147]. For instance, criminals can use XR technologies to simulate and prepare for real-world crimes and create their own marketplaces for illegal trading.

Omar Al Olama, Minister of State for Artificial Intelligence in the United Arab Emirates, discussed the Darkverse and emphasized the need for strict regulations regarding criminal activities in the metaverse, as these behaviors can significantly affect victims due to the high sense of presence [148]. Kasiyano and Kilinc [149] argue that the state of criminal activities in the metaverse is still unclear and requires further investigation to understand how criminal law and regulations can be applied in this new environment.

b) Intellectual Property: Property laws dictate ownership rights of personal property, which can include land, physical items, or intellectual property (IP) [150]. The lack of physical boundaries in the metaverse can cause uncertainty regarding IP laws since such regulations differ according to each country. Unlike physical trading, the identity of a virtual property owner might be difficult to determine due to the anonymity of users representing themselves as avatars. While NFTs play a significant role in providing proof of ownership of virtual goods online, the real identity behind the creators and consumers of assets still needs to be verified, which can affect fair use laws regarding the right to reuse copyrighted material

Another potential legal issue in the metaverse is trademark dilution, which refers to using a brand or trade name for one's commerce [151]. For example, in early 2022, NFT creator Mason Rothschild was sued by the fashion company Hermes for creating a digital asset line called "Metabirkins", which included duplications of a bag design produced by the company [152]. Cloning people's identities in the metaverse is also concerning. For instance, an avatar could represent a known public figure, leading to impersonation issues and violation of the person’s IP (in this case, their own avatar). There have been several incidents where public figures filed lawsuits against companies for using their physical features without permission [153]. Therefore, it is essential to establish laws and regulations for IP in the metaverse while considering that individuals from diverse demographics with different laws are involved.

6) NFT Threats: Recent studies have explored the potential of integrating NFTs in the metaverse [154]-[156]. Despite the advantages of NFTs in securing digital assets and enhancing relationships between consumers and brands, their market status has been inconsistent. Notably, the NFT market experienced a significant decline by the end of 2022 [157], which may be attributed to issues related to cryptocurrency liquidity and a decrease in public interest. A recent study [158] indicates that the restriction of using a crypto wallet affects users’ acceptance of NFT trading. Additionally, security concerns have been identified as a significant factor contributing to market fluctuations, highlighting the importance of addressing these issues to stabilize and grow the NFT marketplace.

Wang *et al*. [159] reviewed NFT security issues using the STRIDE security evaluation method, which stands for

Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation of Privilege. Another work by Das et al. [160] discussed the security risks of NFT marketplaces. In this paper, we highlight several cyber threats to NFTs. Table V lists several cyberattack incidents that targeted cryptocurrency and NFT platforms, highlighting the affect platforms and financial damages of such attacks.

a) Blockchain Vulnerabilities: Due to its decentralized nature, blockchain lacks a central authority that can address misconduct, making it crucial for users to confirm the credibility of parties they interact with to avoid potential fraud. Moreover, Proof of Work (PoW), a blockchain mechanism (known as the mining process), requires participants (miners) to perform computationally intensive tasks to validate transactions and receive rewards. This process introduces challenges, such as the 51% attack, where miners acquire more than half of the network's mining power, enabling double-spending [161].

b) Traditional Attacks: NFTs are susceptible to traditional cyberattacks such as DoS attacks, where the data of an NFT stored outside the blockchain is targeted to disrupt its service availability. Another common threat is phishing attacks. In February 2022, NFTs worth an estimated $1.7 million were stolen from OpenSea due to a phishing attack in which users were manipulated into signing a contract that appeared legitimate [162]. Furthermore, spoofing attacks occur when a malicious user exploits authentication vulnerabilities in marketplaces or manages to steal a user's private key, gaining illegal ownership of the NFT.

c) Smart Contract Vulnerabilities: Smart contract vulnerabilities represent a critical area of concern in blockchain security [163]. Reentrancy attacks exploit code in smart contracts to unauthorizedly execute functions. Overflow and underflow errors handling values outside intended ranges can also occur, leading to the acceptance of unauthorized transactions. Moreover, Address Attacks exploit weaknesses in the Ethereum Virtual Machine (EVM) with crafted addresses to inject address-related bugs.

d) Crypto Wallet Issues: A user's crypto wallet contains cryptocurrency used to purchase assets, which can be accessed using a private key or a passphrase. Cybercriminals attempt to gain access to the crypto wallet via malware and MiTM attacks [164]-[166].

e) Verification and Authentication: Verification during transactions is essential to ensure the legitimacy of a user's identity online. For example, online banking companies have strict regulations to verify a customer's identity by requiring specific information. In contrast, identity verification for NFTs is a concern. Das *et al.* [160] found that none of the NFT marketplaces execute robust verification measures, allowing users to register anonymously and create multiple accounts, posing an issue of tracing accounts to their respective users. Another identity-related issue for NFTs is user authentication. Das *et al*. [160] also analyzed authentication methods in several NFT marketplaces and found that most do not implement two-factor authentication, with *Nifty* being an exception and *Sorare* enabling optional authentication. Spoofing attacks exploit weak authentication mechanisms to steal a user's private key and illegally transfer their NFT ownership into their own wallets [159].

TABLE V
CYBERATTACK INCIDENTS ON NFT AND CRYPTO WALLETS

Attack	Year	Target(s)	Platform	Damages
51% Attack	2018	Bitcoin Gold [167]	Cryptocurrency	$18 million
	2021	Bitcoin SV [168]	Public Ledger	5% decrease in value
Phishing Attacks	2022	NFT Artist 'Beeple'[169]	Twitter Account	$438000
	2022	Bored Ape Yacht Club [170]	Instagram Account	$360,000
Crypto Wallet Hacks	2021	Fvckerender [171]	NFT Artist	$4 million
	2021	NFT Collector [171]	NFT Collection	$2.2 million
Spoofing	2022	The Shifters [172]	NFT Collection	$2 million

V. AI Techniques for Cybersecurity in The Metaverse

As discussed so far, the emerging risks the metaverse is expected to bring require investigating innovative solutions. Our paper focuses on reviewing the role of AI in metaverse threat mitigation based on three core aspects: Identity management, network security, and securing digital asset transactions. We investigate recent advancements, current industrial status, and limitations of existing solutions, with a particular emphasis on their applicability and implications within the metaverse framework.

Our review begins with AI-based user authentication methods, focusing on biometric multimodal and continuous authentication for the metaverse. Next, we explore AI techniques for intrusion detection systems (IDS), highlighting current challenges and reviewing state-of-the-art solutions for the metaverse. Finally, we discuss AI techniques aimed at securing blockchain and NFT transactions, acknowledging that this area is still at an early stage with many security vulnerabilities to consider. The taxonomy of this review is presented in Fig. 13, providing a general overview of how such methods can mitigate cybersecurity threats in the metaverse.

A. AI-based Biometric User Authentication

Authentication is a critical element of digital security. It protects personal information by verifying the legitimacy of users requesting access to a device, system, application, or network. Traditional password-based methods, the earliest forms of authentication, are becoming inadequate due to their vulnerability to breaches and user errors. Examples of common user errors include forgetting a password, using a weak one, or using the same password across several platforms, increasing the chance of gaining unauthorized access to user information.

The emergence of AI-based authentication mechanisms, particularly those utilizing biometrics, has significantly enhanced security and adaptability across various applications. By integrating machine learning and deep neural networks,

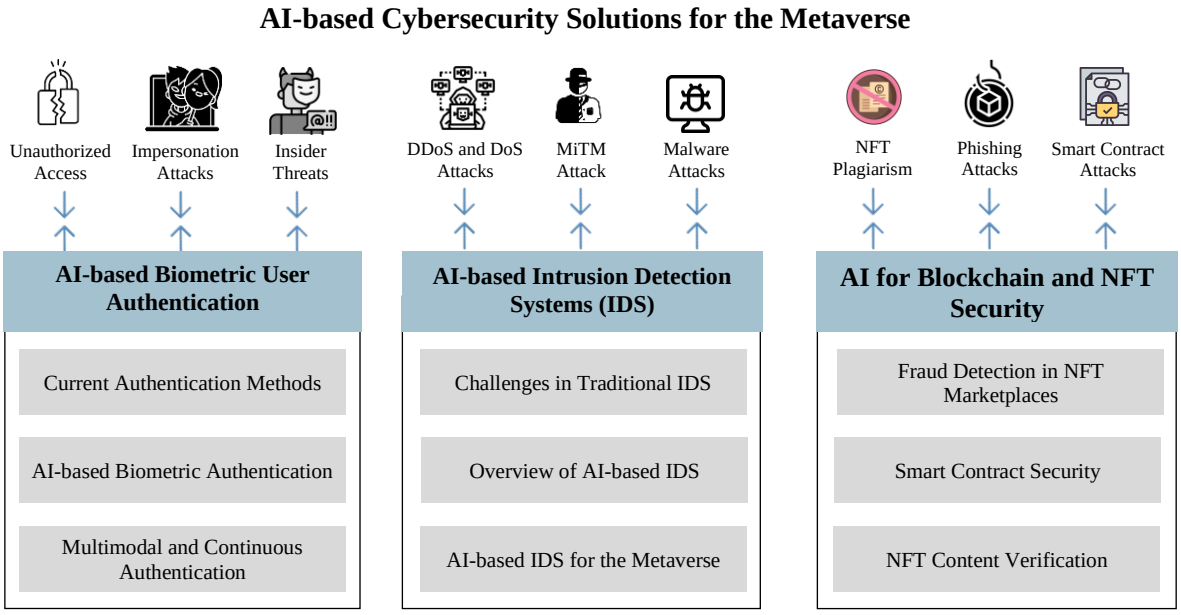

Fig.13. Taxonomy for AI-based cybersecurity solution in the metaverse. AI-based authentication utilizes biometrics and enables real-time monitoring of users' identities and behaviors, enhancing the security system against unauthorized access, impersonation and insider attacks. AI for IDS provides advanced detection mechanisms and real-time monitoring of network traffic, limiting network-related attacks and malware injections. AI for blockchain security contributes to detecting fraud attacks in NFT marketplaces, preventing smart contract attacks, and providing content verification of NFTs to detect plagiarism.

these systems can analyze unique biometric data such as iris patterns, facial features, and behavioral traits to verify user identities accurately.

In the context of the metaverse, where virtual interactions and transactions are frequent, AI-based biometric authentication offers highly secure and efficient solutions. The topic of user authentication for the metaverse has gained considerable attention from researchers. However, there is a clear need for more dedicated research into this area, especially concerning integrating AI and biometrics in the metaverse. The works in [15] and [173] examined the feasibility of employing biometric and continuous authentication within the metaverse, suggesting robust authentication methods beyond traditional face and voice recognition, such as user identification via brain and heart signals.

This survey takes a unique approach by conducting a comprehensive analysis of authentication methods with a metaverse-centric focus. We first review existing authentication schemes utilized in metaverse-related applications. We then examine the strengths and weaknesses of various biometric modalities, highlighting their current industrial status and applicability in the metaverse. Finally, we discuss the deployment of multimodal and continuous authentication, reviewing current research that combines both approaches.

1) Current Authentication Methods: User authentication is the process of validating a user requesting access to a device, network, or computer system, ensuring the protection of sensitive information from unauthorized access. This process typically begins with *identification* or *identity verification*, where the user provides evidence to confirm their claimed identity. There are three main types of authentication mechanisms categorized based on the *type of factors* utilized:

- **Knowledge-based**: Something the user knows (e.g., usernames, passwords, and PINs).
- **Possession-based**: Something the user owns (e.g., device and tokens).
- **Biometric-based**: Something the user is (e.g., facial and voice recognition).

Authentication methods can also be classified into three categories based on the *number of factors* employed:

- **Single-factor Authentication (SFA):** Relies on one type of credentials (identifier), often usernames and passwords. SFA is relatively insecure because it can be easily compromised through phishing and brute force attacks.
- **Two-factor Authentication (2FA):** Enhances security by requiring two types of credentials. An example of 2FA is One-Time Password (OTP) authentication, an automatically generated code sent to the user's device to verify a single action. While more secure than SFA, 2FA has issues such as susceptibility to SIM swapping [174], user inconvenience, and risks from lost or stolen tokens.
- **Multi-factor Authentication (MFA):** Requires two or more factors (knowledge-based, possession-based, biometric-based). MFA significantly enhances security by incorporating additional layers of protection, making it more challenging for attackers to gain unauthorized access, even in case one factor was compromised. However, MFA can still suffer from usability issues [175].

Table VI shows various verification and authentication methods used in current metaverse-related environments, mainly devices, gaming applications, and gaming platforms. Verification refers to validating the authenticity of users' information during registration, which typically involves official documents. Some mobile devices offer optional biometric authentication, like fingerprint scanning and facial recognition. Notably, the newly released Apple Vision Pro headset is the first commercially available device to incorporate

TABLE VI
VERIFICATION AND AUTHENTICATION METHODS IN EXISTING APPLICATIONS/HARDWARE

Platform	Application	ID Verification	Authentication
Devices	Apple ID	ID documents for Apple Cash or Apple Card	MFA: Optional Biometrics: Face ID and Finger ID
	Android Device	Not Applicable	MFA: Optional Biometrics: Face, Fingerprint
	Apple Vision Pro	Not Applicable	Optic ID: Iris Recognition Optional Authentication during session
Gaming and Social	Second Life	Not Applicable	2FA: Optional for sensitive information (changing passwords, transactions)
	Roblox	Age verification via personal photo and ID	2FA: Optional via authenticator apps, security keys, or emails.
	Fortnite	Not Applicable	- 2FA: Optional via authenticator apps, or emails. - Users get rewards (game assets) for enabling 2FA.
	VRChat	Not Applicable	2FA: Optional via Authentication app.
	PlayStation account	Not Applicable	2FA: Optional via authentication app or text message.
	Meta Account	Photo ID requirements for business verification	2FA: Optional
NFT Platforms	Decentraland	Not Applicable	Authentication via connecting to a crypto wallet.
	The Sandbox	Account KYC verification is optional: 1. Liveness detection (face) 2. Official ID document: passport/ID	1. SFA, or 2. Crypto wallet.

iris recognition with its Optic ID technology, allowing users to perform authentication at any given time during the session.

In gaming applications, most MMOGs provide optional 2FA, often recommended during sign-up. Users can enhance security and usability by installing authenticator apps such as Google Authenticator and Microsoft Authentication, which generate time-based one-time passwords every thirty seconds. Additionally, platforms like Roblox offer hardware-based secure authentication through security keys. As for NFT platforms, users are typically authenticated via their crypto wallets, a necessity for blockchain-based applications that involve cryptocurrency and NFT trading.

Identity verification can be optional but is sometimes necessary for certain scenarios. For instance, Meta users can verify their identity to boost business credibility, and age-restricted activities on Roblox may require official ID documents, depending on the user's country of residence. The Sandbox platform combines face recognition and official documents for optional identity verification, granting access to additional in-game activities.

According to this review, most current authentication methods are optional, with a strong reliance on 2FA. This trend is a direct response to the challenge of balancing security and usability, as the integration of additional steps and security layers can potentially disrupt the user experience, a particularly undesirable outcome in the metaverse. However, there have been significant developments in integrating biometrics in certain applications and devices, such as the Apple Vision Pro headset's iris recognition. This technology allows users to authenticate before performing sensitive tasks, like making a payment, by simply selecting the authentication option from the user interface. Despite these advancements, the metaverse presents unique challenges that necessitate further research to develop authentication methods that effectively balance usability and security while also considering privacy issues.

2) AI-based Biometric Authentication: Biometric authentication verifies users based on their unique characteristics, broadly categorized into behavioral and physical traits (see Fig. 14). Behavioral traits include patterns such as voice, gait, keystroke dynamics, and physical activities (e.g., head or hand movements). Physical attributes are biological measurements categorized as static or physiological. Static biometrics remain constant, including fingerprints, facial features, iris, retina, hand geometry, and DNA. Physiological biometrics, such as brain signals (EEG), heart signals (ECG), and blood volume changes (PPG), not only authenticate but also confirm the user's presence and vitality.

Biometrics, intrinsically linked to individuals, offer a reliable confirmation of identity. They present advantages over traditional methods like passwords, which are susceptible to loss, forgetfulness, or forgery. Advances in technology, especially in computer vision and AI, are contributing to the growth of the biometrics market, increasingly replacing conventional authentication methods [176].

a) Biometric Authentication Models and Protocol: AI-based authentication systems operate through a multi-phase process consisting of *training*, *enrollment*, and *verification* (or *authentication*) phases [177], as illustrated in Fig. 15.

Training phase: This phase precedes the deployment of the authentication system, aiming to optimize the performance of the AI model based on requirements that vary according to the application/system. Typically, the training phase consists of the following steps:

- **Data Collection:** Biometric data is systematically gathered to capture a wide range of characteristics across diverse demographics and environmental conditions. The collected dataset is segmented into distinct training and testing sets. This separation ensures that the model is trained on one subset of data and subsequently tested on a completely unseen subset to verify its predictive performance.
- **Data Preprocessing:** The dataset undergoes preprocessing techniques that aim to standardize input data and ensure

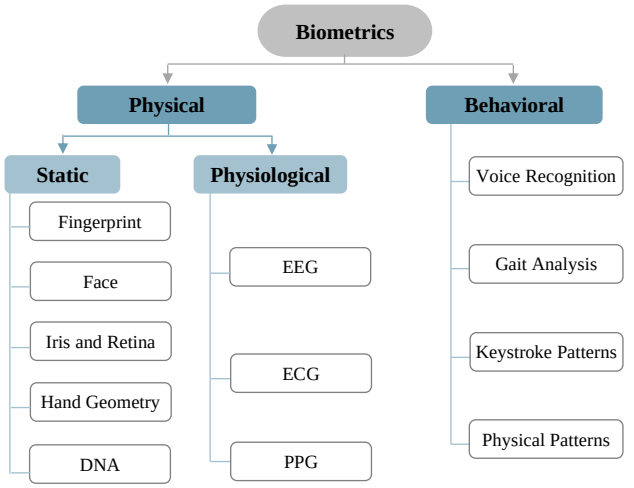

Fig. 14. Examples of biometric modalities used for user authentication.

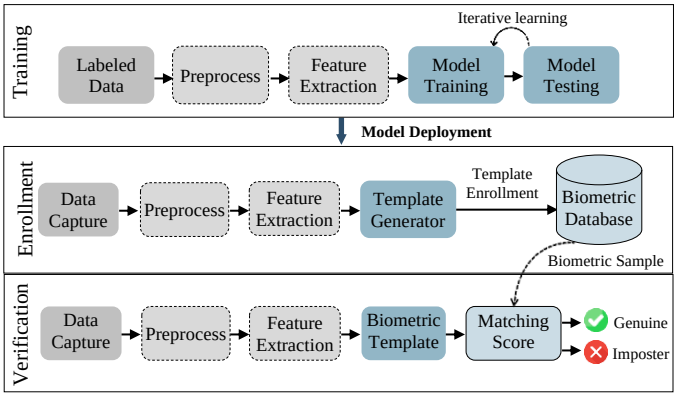

Fig.15. Generic authentication system: The training phase prepares the AI model using labeled dataset before deployment. The system utilizes the trained model and enrolls unique extracted features into a secure database. The system then verifies access requests by comparing user data with enrolled records

optimal analysis. This phase may include normalizing data to uniform sizes, cleaning noise, and enhancing quality.

- **Feature Extraction:** The system identifies and isolates specific attributes of the biometric data. Effective feature extraction ensures that each feature selected offers a distinct representation of an individual, thus laying a solid foundation for differentiating between users during the authentication process.
- **Model Training:** Techniques such as supervised learning are typically used, where models are trained on labeled data (training set) to learn the correlation between biometric features and individual identities. ML Algorithms like SVM, RF, and Logistic Regression (LR) are commonly employed for their efficiency in classification tasks [177]. DL models like CNNs (image data) and RNNs (time-series data like voice signals) are also used for their ability to handle complex patterns.
- **Model Testing and Evaluation**: The final step is to test and validate the trained model using new data unseen by the model during the training phase (testing set). This step is crucial to evaluate the model's performance in real-world scenarios (Refer to Section III-2 for details on performance metrics). Ongoing testing and periodic re-training with updated data are necessary to maintain the model's performance and adaptability to changes.

Enrollment Phase: During this phase, a user's biometric data is captured using the sensor designated for the specific biometric trait being measured. The system employs the preprocessing and feature extraction methods developed and refined in the training phase to process this new data. The resulting features are securely stored in a database, forming the reference **biometric template** for the user. During this phase, the user must engage in typical activities, as this ensures the sensor's readings accurately reflect the user's natural behavior, enhancing the system's reliability and performance.

Verification Phase: When the user attempts to access the system, their biometric data is captured. This new input data undergoes the same preprocessing and feature extraction process to ensure consistency and accuracy. The system then compares these extracted features against the stored biometric templates in the database. A matching score is generated by the trained AI model, which determines the user's legitimacy. Access is granted if the AI model recognizes the data with sufficient confidence based on thresholds established during the training and validation phases. It is worth noting that for each biometric modality, diffident pre-processing and feature extraction techniques are used.

b) Biometric Modalities: Several survey papers have thoroughly investigated biometric authentication modalities, providing insights into their strengths and vulnerabilities [180]-[185]. In our paper, we investigate a combination of biometrics while focusing on their deployment in the metaverse. Note that when discussing metaverse deployment in this section, we refer to the full immersive experience achieved by innovative technologies and hardware such as XR and haptics, so any 2D smart devices or applications are not considered. Table VII provides an overview of each biometric method in terms of security aspects, applicability in the metaverse, possible challenges, and relevant existing products and/or research.

Fingerprint recognition is a leading form of biometric authentication due to its robust security, ease of use, and short verification times [184]. Initially used in forensic applications to identify individuals, it has expanded to various consumer sectors, including unlocking digital devices, securing personal storage lockers, and automotive systems. The technology identifies unique minutiae patterns within fingerprints, which are captured via specialized sensors. Integrating fingerprint scanning into VR technologies, particularly VR gloves, is an underexplored area. However, ongoing advancements in haptic technology by companies like *Meta* and *TESLA* suggest promising avenues for research. Including fingerprint scanners in VR gloves could lead to seamless authentication methods that can enhance usability in the future metaverse.

Facial recognition automatically verifies a user's identity by analyzing their facial features from images, videos, or real-time captures. Initially, the face is detected using cameras combined with various ML algorithms, followed by an analysis and measurements of unique facial features [185]. Research on facial recognition In VR applications mostly focuses on identifying facial expressions and emotions [186]. However, a significant challenge in VR facial recognition is the face occlusion caused by the HMD, which can hinder full facial

TABLE VII
OVERVIEW OF BIOMETRIC AUTHENTICATION SYSTEMS AND THEIR APPLICABILITY IN THE METAVERSE

Biometric Modality	Description	Applicability in the Metaverse	Relevant Products
Fingerprint Recognition	Captures unique patterns of the finger, known as minutiae	Applicable if sensors are implemented in VR gloves	NA
Facial Recognition	Analyses distinct facial features	Applicable: Partial facial occlusion due to VR headsets is a challenge. However, ongoing research is dedicated to tackle this issue, making facial recognition possible in the future metaverse.	Modular Codec Avatars
Iris Recognition	Scans the unique patterns in the coloured part of the eye	Available: gaze tracking is already implemented in HMDs	*Pixsur* Iris Recognition Optic ID (Apple)
EEG Signals	Identifies users based on their brain activity in certain scenarios	Applicable: The integration of EEG sensors into a metaverse headset might be possible in the future, considering the extensive research into BCI for the metaverse and single-channel EEG authentication	Emotive headsets
ECG Signals	Identifies users based on unique patterns in heart activity	Applicable: ECG is already deployed into wearable devices for mounting users' health, which can also be used for authentication	TESLA Glove Wearable Devices
PPG Signals	Measures cardiac signals and volumetric blood flow changes	Applicable: PPG authentication is applicable in the metaverse since it can be measured with wearable sensors (e.g. TESLA suit)	TESLA Suit Wearable Devices
Voice Recognition	Analyses voice signals to extract a voiceprint	Available: Microphones exist in all hardware devices, so voice recognition would be easily implemented in the metaverse	All HMDs

recognition. To address this problem, Ciftci *et al*. [187] developed a real-time, depth-based recognition framework that focuses on mouth gestures visible beneath VR headsets using a novel 3D edge map technique. Similarly, Houshmand and Khan [188] utilized transfer learning with pre-trained models like *VGG* and *ResNet*, which were fine-tuned on datasets modified to simulate the occlusion caused by VR headsets. Wen *et al*. [189] also reviews this issue and highlight advancements like Modular Codec Avatars and inward-facing cameras in VR headsets to capture facial expressions effectively despite partial face coverage. Therefore, facial recognition can be implemented in the metaverse to enable more realistic avatars, enhance social interactions, identify user emotions, and potentially identify and authenticate users.

Iris recognition identifies users based on the unique patterns of the iris, which is the colored tissue around the eye's pupil. Iris recognition is considered one of the most efficient biometric systems for several reasons, such as the uniqueness of the two irises, data stability, and low verification time [190], [191]. In iris recognition, images of the user's eye are acquired using cameras with infrared illumination, which aim to highlight the detailed texture of the iris for a more accurate performance. Low image resolution and distortion can negatively affect the performance of the iris recognition system [192]. However, several studies investigated methods to tackle such issues. For instance, Ribeiro *at el*. [193] showed that utilizing CNNs can help balance edge preservation and the smoothness of images, providing good performance for iris recognition systems in mobile devices and images taken from a distance. Another recent study [194] proposed a deblurring method that aims to enhance the quality of the images for accurate iris recognition results. Regarding VR applications, *Shanghai Pixsur Smart Technology Co., Ltd* has launched an iris recognition algorithm and hardware that captures images of the iris for VR and AR headsets [195]. Similarly, as mentioned earlier, Apple has released Optic ID, which uses high-performance eye-tracking with LEDs and infrared cameras to provide secure and intuitive authentication. Optic ID adapts to various lighting conditions and works with prescription lenses, ensuring accurate performance. That said, iris recognition is potentially suitable for user authentication in the metaverse due to its robustness and applicability in HMDs.

EEG-based authentication is an emerging verification technique that relies on capturing the brain activities. As discussed in Section III, the Brain-Computer Interface (BCI) is a technology that enables direct communication between the brain and external devices by interpreting brain signals to perform specific commands [196]. In the metaverse, BCI is presumed to play a significant role in user interactivity, as the stimulation of the brain can replicate immersive sensory experiences [197]. EEG is a BCI application defined as recordings of the neural activities in the brain generated from internal or external stimuli, and they are recorded via electrodes, known as channels, placed on the scalp [198]. Depending on the application, EEG systems can vary in the number of channels used, ranging from a single channel up to 256. Five main frequency bands of EEG waveforms can help provide information about the mental and behavioral states of the user, including delta, theta, alpha, sigma, and beta [199]. Moreover, Event-Related Potentials (ERPs) are very small voltages generated in the brain structures in response to specific events or stimuli, and they can be useful in classifying the emotional states of the user [200].

As an authentication method, EEG has gained interest due to its characteristics. EEG signals differ for each individual even if they perform the same task, and repeating the task for the same individual does not change the corresponding signals. Therefore, EEG signals attain the uniqueness and stability factors required for authentication. EEG outperforms other static biometric traits like fingerprint and iris recognition

because brain signals are not easily exposed to the attacker, making them extremely difficult to capture and forge. They also depend on the user's emotions, so they cannot be invoked under force [201]. Moreover, EEG supports liveness detection, a method to ensure that the biometric sample is obtained from a live person and not a spoof attack [201]. The pattern and features of EEG signals correspond differently according to the activity the individual is undertaking.

Emotive Inc. is a tech company that produces headsets for EEG brain interface, which has been used for biometric research. Their collection of hardware includes multi-channel devices, the maximum being a 32-channel headset. *Muse Inc*. and *OpenBCI* are other companies that also provide special headsets for EEG collection. Most works utilize multiple channels of EEG data to achieve high accuracy and a relatively low-time process. However, this technique can be impractical in the metaverse due to the high cost, obstruction of user mobility, and overall convivence. Studies in [202], [203], and [204] investigated single-channel EEG with deep learning techniques and achieved an accuracy of 80%, 86%, and 97-98%, respectively. Balancing security and usability for user authentication in the metaverse is essential. Since HMDs are the main hardware used to provide a fully immersive experience in the metaverse, there is potential for metaverse users to use EEG-based authentication if compatible devices are designed. On another note, Li *et al*. [205] found that the performance of EEG authentication is not affected by whether the brainwaves are collected via 2D or VR-based visuals. Thus, collecting EEG signals in virtual environments would not be an issue.

ECG-based authentication verifies the user's identity based on the heart's electrical activity, known as Electrocardiogram (ECG) readings. ECG is often used to monitor and evaluate patients' medical conditions in real time and detect cardiovascular issues [206]. In addition to ECG being a diagnostic tool, researchers are investigating its potential for identification and authentication applications. Like EEG, ECG is more resistant to cyberattacks than other biometrics since they are very difficult to forge. ECG contains unique patterns for each individual, such as the variations in the amplitude and distances between heart pattern waves [207]. ECG is also applicable for liveness detection and continuous authentication. Several recent studies [208]-[210] proposed ECG authentication systems and achieved high accuracies of 98-99%, 99.05%, and 100%, respectively.

In the medical field, specifically in hospitals, ECG is recorded using electrodes attached to the chest area and limbs (wrists, ankles). This process is relatively complex as it requires special preparations of the patient's skin, and multiple electrodes are used in addition to an external monitor for high-accuracy results [207]. Alternatively, wearable devices have functionalities for recording ECG, including smartwatches, patches, and sensors embedded in clothing [211]. Notably, the new *TESLA Glove* by *TESLA* incorporates ECG monitoring to gather biometric information like the user's heart rate, enhancing its functionality for real-time physical reaction assessments during XR experiences. This innovative use of ECG in VR gloves presents a promising research opportunity for seamless authentication in the metaverse. Wearable devices are ideal for ECG authentication in the metaverse, as they are portable and can provide real-time results without disrupting the user's experience. Uwaechia and Ramli [207] pointed out that despite the good performances of ECG authentication in research, these studies are conducted in controlled environments with datasets obtained from medical databases that perform intensive user preparation data collection. Thus, the authors argue that for wearable devices, the quality of acquired data will be of much lower quality, which is an issue that can be solved if ECG is implemented in a multimodal authentication system [212].

PPG-based authentication is emerging as a non-invasive method for verifying identities through Photoplethysmography, which measures blood flow changes via optical sensors [213]. This technique is reliable due to the complexity of duplicating an individual's unique cardiovascular pattern, offering a robust defense against spoofing attacks. However, Li *et al*. [214] highlight several challenges currently faced by PPG technology, such as signal accuracy issues caused by motion and varying ambient lighting conditions. Ongoing research is actively addressing these challenges, aiming to refine PPG into a more reliable component of multimodal and continuous authentication systems [215],[216].

PPG technology is readily implementable in wearable devices, as the TESLA suit exemplifies. This suit utilizes PPG sensors to monitor vital signs such as heart rate and blood oxygen levels, which are crucial for health monitoring during interactive experiences. This capability enhances safety by alerting users to potential health issues in real time and integrates seamlessly with user authentication processes in the metaverse. Such dual functionality of the TESLA suit shows the potential of PPG to provide both secure and immersive user experiences in virtual environments.

Voice recognition systems receive and analyze sound signals to verify a user based on their voiceprint. A voiceprint includes unique patterns such as the shape and movement of the mouth while speaking, airways, and soft-tissue cavities [217]. A voice sample can be captured using a microphone, so a voice authentication system would not require complex hardware. Voice assistants are examples of existing voice recognition applications, which include *Siri*, *Amazon Echo*, and *Google Home*. Despite its advantages, voice recognition can be affected by unstable environments (noise) and medical throat conditions. Sound samples can also be easily faked using a recording. Hence, it is important to implement liveness detection to ensure the user is the one who is providing the voice sample.

3) Multimodal and Continuous Authentication: Despite the high level of security that biometrics provide, there are still possible attacks that can target the system, which can be mitigated when deploying the concept of multimodality and continuous authentication.

a) Multimodal Authentication: Biometric authentication methods can be classified based on the number of traits used in the system: *unimodal* and *multimodal*. One modality is utilized in unimodal systems, whereas multimodal techniques integrate two or more biometric factors [218]. In biometric systems, fusion techniques are employed to enhance the accuracy and reliability of authentication by integrating data from multiple sources, as shown in Fig. 16. These techniques can be categorized into four main levels: **sensor-level**, **feature-level**,

score-level, and **decision-level** fusion. *Sensor-level* fusion involves combining raw data from different sensors before any processing, which can enrich the data quality and detail. *Feature-level* fusion merges the extracted features from multiple biometric sources, creating a comprehensive feature set that is more informative and discriminative. *Score-level* fusion combines the matching scores from several classifiers corresponding to different modalities, often using strategies like weighted sums or statistical methods to refine the overall score. Lastly, *decision-level* fusion aggregates the final decisions from multiple biometric systems, using methods such as majority voting or consensus theory to arrive at a final authentication verdict. Each fusion level has its own advantages and limitations, which can depend on the system requirements.

While unimodality is easier and less expensive to build, its main drawback is that it can be a single point of failure in the system. Other issues can arise from using a single biometric trait, including [219]:

- **Vulnerability to spoof attacks:** These attacks refer to deceiving a system through impersonating the biometric traits. For example, images or videos of a user can be forged (DeepFake) and fake fingerprints made of silicon or rubber can deceive a fingerprint recognition system. EEG signals can also be faked if intruders use advanced technologies (GAN models) [201].
- **Noisy data:** Data acquisition might be inaccurate in abnormal or unstable conditions. For example, high anxiety levels can affect the ECG readings, and images taken from a wrong angle can affect a facial recognition system. This issue affects FRR and FAR.
- **Non-universality:** Some biometrics might not be compatible with all users. For example, faded or burnt fingerprints might work poorly for fingerprint detection, and certain eye conditions can affect iris recognition [184].

Multimodal authentication systems merge a group of biometric factors, which helps overcome the limitations caused by single biometric techniques. Thus, multimodality outperforms unimodality as follows [219]:

- **Protection against spoofing attacks:** The integration of multiple biometric traits increases the protection of the system against spoofing attacks because manipulating and forging of all modalities at once is significantly difficult.
- **Reliability and accuracy:** Multimodal systems provide better accuracy, reduce errors, and eliminate the issue of single-point-of-failure in the system.
- **Flexibility:** If certain biometric cannot be obtained from the user, the other biometrics can be used for authentication, solving the issue of non-universality in unimodal systems.

Multimodal authentication addresses the limitations of unimodal systems, making it crucial for user authentication in the metaverse. By combining different biometrics, it compensates for the weaknesses of individual identifiers, enhancing security and usability. This approach adapts flexibly to various devices used in the metaverse, such as HMDs, haptic gloves, smartphones, and smart glasses, offering a seamless and convenient user experience.

b) Real-time Continuous Authentication: Traditional

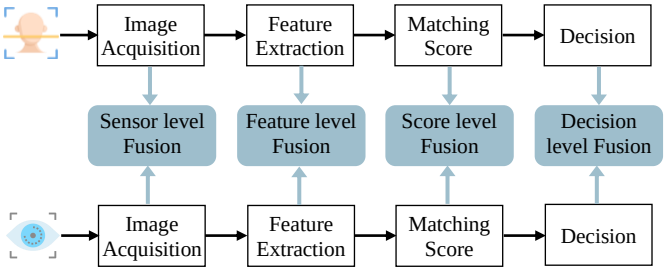

Fig. 16. Fusion techniques in multimodal authentication can occur at the sensor level, feature extraction level, score level, and decision level.

authentication methods like SFA, 2FA, and MFA are typically one-time based. Thus, they do not ensure that the user remains authenticated throughout the session, allowing malicious individuals to gain unauthorized access during periods of user inactivity [220]. Continuous Authentication (CA), powered by AI and biometric technologies, addresses this issue by providing ongoing verification of the user's identity, which helps to reduce unauthorized access, credential stuffing, and phishing attacks. This system operates seamlessly in the background, requiring no repeated credential inputs from the user, thus enhancing both security and usability.

Advantages of Continuous Authentication in the Metaverse: Integrating CA with multimodal systems offers significant benefits in the metaverse. Firstly, CA enhances security by promptly detecting unauthorized access or session hijacking, reducing impersonation risks [221]. For example, if a user's account in an NFT marketplace is compromised, a well-integrated multimodal CA system would quickly detect anomalies in the user's biometric data, such as unusual EEG signal patterns, and lock the account before further malicious activities occur. This prompt response necessitates reauthentication, preventing the attacker from further access. Secondly, CA can enhance usability. As users navigate multiple virtual worlds, they do not need to re-enter their credentials, preserving their experience's continuity. For instance, an avatar can be automatically authenticated during transitions from a virtual meeting to a virtual shopping center without any action required by the user. Moreover, continuous monitoring of user behavior, such as real-time ECG signal analysis by wearable devices, can enhance safety by detecting potential health issues during critical activities like virtual driving, thereby contributing to a safer metaverse environment.

Existing Work on Multimodal and Continuous Authentication: Various works on CA utilize behavioral attributes, physiological traits, or a combination of both. Ryu *et al.* [222] review works that combine multimodality with CA. They found that most researchers prefer behavioral attributes for CA because they do not require additional hardware, are less intrusive to collect, cost-effective, and require less computational complexity. However, the authors also found that combining behavioral and physiological biometrics provides better performance and measurability, which is practically feasible in the metaverse since its enabling technologies and hardware are variant, allowing the integration of different types of biometrics.

We review several recent studies on CA systems (Table VIII), categorized based on the hardware used: Touch-based devices, wearable devices, and HMDs, all part of the future

TABLE VIII
EXISTING WORKS ON MULTIMODAL AND CONTINUOUS AUTHENTICATION

Hardware	Ref.	Biometric Modalities	AI Techniques	Fusion Technique	Performance
Mobile Devices	[223] 2018	**Behavioural:** Gait and keystroke dynamics	Multilayer Perceptron (MLP) outperformed other algorithms	Feature Level Fusion	Accuracy: 99.11% FAR: 0.684% FRR: 7%, EER: 1%
	[224] 2020	**Combination:** Face recognition and movement of phone	SVM	Score Level Fusion	Accuracy: 98.53% FAR: 5.86%, FRR: 0.33%
	[225] 2021	**Behavioural:** Multiple activities.	DL techniques (Novel model: DeepConvLSTM)	Feature Level Fusion	Accuracy and EER are calculated for each activity
Wearable Devices	[226] 2020	**Combination:** EEG, Gait, Breathing audio signals.	K-Nearest Neighbours (kNN), RF, SVM	Feature Level Fusion	Accuracy: 93% F1 score: 93%, FPR <0.08
	[227] 2022	**Physiological:** ECG and Finger vein	Combination of DL and ML	Feature and Score Level Fusions	EER: Feature level: 0.12%, Score level: 1.40%
	[228] 2022	**Physiological:** ECG and PPG (Photoplethysmography)	- CNN for feature extraction -LSTM for CA - ML algorithms for classification	Feature level Fusion	Accuracy: 99.8% EER = 0.16
Head Mounted Displays	[229] 2019	**Combination:** EEG and Eye Tracking	- SVM for EEG - RF for eye tracking	Score Level Fusion	FAR: 23.6%FRR: 29.2%
	[230] 2020	**Physiological:** Iris and periocular biometrics	Deep Learning (CNN)	Score Level Fusion	ERR: 0.0586
	[231] 2021	**Behavioural**: Head movements, hand gestures.	KNN, SVM, RF, AdaBoost	Feature Level Fusion	Accuracy: 92.67% EER: 11%
	[232] 2020	**Behavioural**: Physical movements, head pose, gaze.	KNN	Feature Level Fusion	Accuracy: 98.6%
	[233] 2020	**Combination**: EOG signals: Physiological: eyelid features, RPE, eye globe size and shape Behavioural: eye movement and fixation.	SVM	Feature Level Fusion	EER: 3.55%, 4.97%.

metaverse essential gear. The table summarizes the biometrics used in each work, AI methods, fusion techniques, and performance metrics.

In mobile devices, built-in accelerometers, gyroscopes, and magnetometers capture and analyze user behaviors. Lamiche *et al*. [223] utilized accelerometers in smartphones to measure the user's gait and keystroke dynamics for their CA systems. As the user walks, data is collected under different scenarios, such as having the device in their pockets, holding the phone, and answering a call. The proposed system achieved an overall good performance, even when tested under realistic conditions, such as uneven grounds, wearing high heels, and various fatigue levels. In [225], the authors also deployed behavioral attributes using three datasets that contain activities such as walking, sitting, standing, eating, typing, writing, and combinations of reading and sitting. Using a DL network with CNN and LSTM, the authors outperformed other baseline DL algorithms. Wang *et al*. [224] implemented face recognition and phone movement for CA, obtaining high classification metrics using SVM.

Several studies investigated ECG with other biometrics for CA in wearable devices. In [226], gait and breathing audio signals were integrated with ECG. In [227], the authors proposed a multimodal CA system with ECG and finger vein. Their work showed that EER is significantly less with multimodal feature-level fusion than unimodal authentication and score-level fusion. Ahamd *et al*. [228] fused ECG and PPG for a device-level authentication system, focusing on healthcare IoT devices. According to their findings, ECG authentication outperformed PPG and ECG-PPG. However, the multimodal ECG-PPG system still achieved a high performance with an accuracy of 99.8% and an EER of 0.16.

HMDs typically include sensors for eye tracking and head movement tracking. User authentication in HMDs widely studied using behavioral and physiological biometrics, such as head movement [234], eye movement [235], and iris recognition [236]. However, only a few works implemented multimodality with real-time authentication for XR applications, as shown in the table. Krishna *et al*. [229] integrated EEG signals and eye tracking, leveraging inter-user differences to enhance user authentication and incorporating the SVM and RF classifiers. Bhalla *et al*. [231] utilized behavioral biometrics for AR headsets, such as head movement and hand gestures, and Olade *et al*. [232] integrated physical movements with head and eye gaze patterns. While these two works show promising results and potential for behavioral biometrics in VR/AR applications, their main limitation is that they are application-specific, which is not feasible for a CA system in the metaverse. In [230], a CA system is implemented for AR/VR applications using iris and periocular recognition while considering low computation resources. The experiments have shown acceptable results even when using a computationally light model. Finally, Luo *et al*. [233] explored the use of electrooculography signals (EOG) for CA, which are typically captured to study eye movements. EOG contains both physiological (eyelid features, Retinal Pigment Epithelium (RPE), eye globe size and shape) and behavioral (eye movement and fixations) features. The proposed system achieved relatively low computational time and can provide

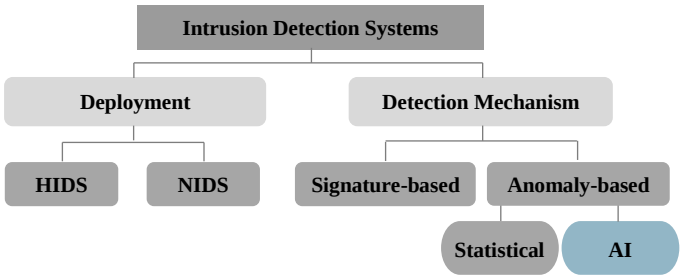

Fig. 17. Intrusion detection categorization based on deployment and detection mechanisms.

both security and usability for users.

Current research highlights the potential for using multimodal biometrics and continuous authentication in the metaverse, focusing on security and usability. However, studies often explore limited modalities and are application-specific, only partially suitable for the diverse metaverse environments. Future work should test these systems in realistic settings to ensure they are adaptable and robust across various metaverse applications.

B. Intrusion Detection Systems in the Metaverse

The metaverse utilizes next-generation technologies to enable seamless high-speed communication structures, such as 6G, intelligent sensing, multi-access edge computing (MEC), and digital twins [48]. Integrating such advanced technologies requires innovative research into network security to handle the metaverse's complex ecosystem. Intrusion Detection Systems (IDS) are central to any cybersecurity framework as they monitor digital and network systems for unusual activities that violate security policies. IDS alerts network administrators if anomalies are identified, allowing prompt action against potential attacks [237], which can provide proper threat mitigation in the metaverse.

IDS can be categorized based on environmental deployment and detection mechanism, as shown in Fig. 17. In terms of deployment, there are two primary types of IDS:

- *Network Intrusion Detection Systems (NIDS)*: NIDS monitor network traffic for signs of intrusion or malicious activity. They are typically placed at strategic points within a network to analyze packets and identify abnormal behaviors. NIDS can detect attacks at the network level, such as DDoS, intrusion attempts, malware propagation, and MitM attacks.
- *Host Intrusion Detection Systems (HIDS)*: HIDS are typically installed directly on individual hosts to monitor system logs, files, and activities. HIDS can detect unauthorized access and malware activity.

Intrusion detection can also be categorized based on the detection process (Fig. 17): *Signature-based* detection and *Anomaly-based* detection. Signature-based techniques use a database of existing attack patterns. During detection, the network traffic being analyzed is compared with the database, which generates an alarm in case of matching. This method minimizes false alarm rates and is relatively less complex [238]. However, one of its major limitations is its inability to detect emerging or zero-day attacks, making it insufficient for metaverse security.

Anomaly-based detection, on the other hand, constructs

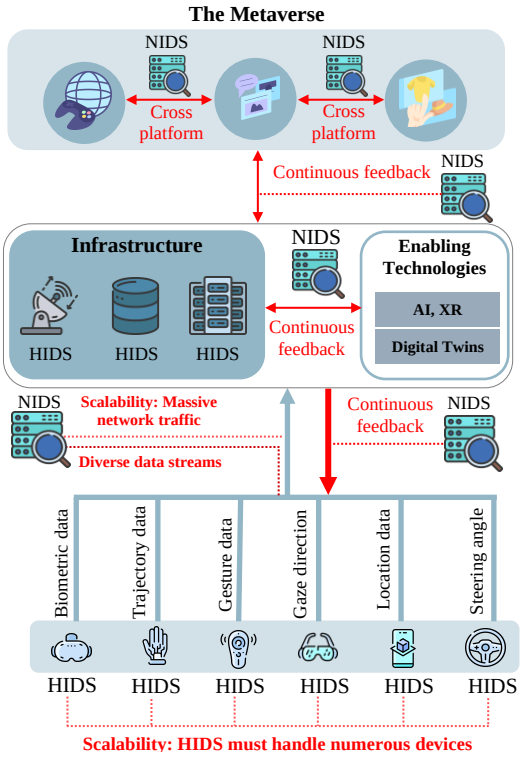

Fig. 18. Challenges of NIDS and HIDS implementation in the metaverse in terms of scalability, diverse data, continuous detection, and cross-platform detection.

patterns of normal traffic via algorithms and advanced models that rely on datasets, detecting "malicious" traffic that does not conform to normal behavior. Therefore, anomaly-based IDS has a stronger defense mechanism and adaptability, which has more potential to be deployed in the metaverse. Several types of anomaly-based methods exist, such as statistical techniques and AI algorithms. The scope of this paper is focused on reviewing AI-based IDS.

In this section, we first address the unique challenges of implementing IDS within the metaverse and then discuss the role of AI in enhancing IDS performance. We then review existing IDS solutions designed specifically for the metaverse, comprehensively analyzing their contributions and limitations

1) IDS Challenges in the Metaverse: Several challenges are associated with current IDS solutions, including management of alerts, false positives and negatives, and response time [239]. Implementing IDS within the metaverse presents novel challenges, specifically traditional systems such as static firewalls and signature-based methods. Fig. 18 illustrates a high-level representation of possible IDS implementation (NIDS and HIDS) in the metaverse, pinpointing the following challenges:

Scalability*:* Truong *et al*. [240] highlight that traditional IDS encounter scalability issues due to the vast number of end devices and monitoring points within the metaverse. The extensive network traffic demands that NIDS scale effectively, while HIDS must ensure the security of each device/server [240], making current IDS solutions insufficient for metaverse security.

Diverse Data Streams: Data of various types are collected from different sources to empower the metaverse, including IoT

device sensors, real-time updates from the physical world, user interactions, spatial data (information related to position, movement, and orientation within a three-dimensional space), 3D models, virtual assets, audio streams, textual data, and non-structured data [241]. The diversity and complexity of such data inputs are considered a challenge for traditional IDS, as they must be capable of analyzing and protecting a vast array of information sources to maintain the integrity of the metaverse environments and users' privacy.

Dynamic and Real-time Detection: The metaverse's dynamic nature leads to the constant evolution of its virtual environments and real-time data synchronization. For instance, digital twin technology requires continuous updates from real-world data sources to converge the digital and virtual worlds [242]. User interactions and content generation in the metaverse also evolve, requiring IDS to adapt quickly to these changes.

***Cross-platform Security*:** The interoperability of the metaverse allows users to interact with diverse virtual environments, assets, and experiences via moving across multiple meta-worlds [243]. Consequently, having diverse platforms with unique architecture and user interaction models can pose a challenge for IDS, especially when detecting abnormalities. Some behaviors can be considered normal on one platform and might be anomalous on another, which complicates the establishment of behavior baselines for IDS. Therefore, it can be challenging for IDS to maintain consistent security policies within the metaverse, which demands innovative solutions requiring high interoperability, adaptability, threat intelligence collaboration [244], and standards.

Table IX compares these challenges within diverse environments relevant to the metaverse, showing how growth in technology increases the complexity and factors involved in implementing IDS. The comparison is conducted between traditional networks, IoT networks, and the metaverse. Traditional networks represent the foundational digital infrastructure that enables enterprises and organizations to operate. IoT, on the other hand, is one of the core building elements of the metaverse, characterized by its vast network of interconnected devices and sensors, which introduces more security challenges. The table addresses additional factors such as user interactions, decentralization, and the threat landscape, all of which are areas where expertise and research can make a significant impact.

As pointed out by Ooi *et al*. [245], integrating physical and virtual spaces amplifies the need for IDS to adapt to new vulnerabilities and safeguard the seamless user experience against sophisticated cyber threats. Thus, the development of advanced, scalable, and efficient IDS solutions is paramount in the evolving landscape of the metaverse.

2) Overview of AI-based Intrusion Detection Systems: In the context of the rapid technological advancement and the emergence of sophisticated cyberattacks, the research area of AI-based IDS, particularly in complex network infrastructures, is of paramount importance. The deployment of AI in intrusion detection offers numerous advantages over traditional methods, including adaptability to emerging threats and dynamic behaviors, detection of day-zero attacks, effective pattern recognition for threat detection in large data volumes, real-time response, reduced false alerts, and overall enhanced prediction accuracy [246].

TABLE IX
COMPARISON OF IDS CHALLENGES IN TRADITIONAL IT AND IOT NETWORKS WITH THE METAVERSE

Challenge	Traditional Networks	IoT Networks	The Metaverse
Scalability	Essential, but uniform	High, dependant on device capabilities	Extremely high due to rapidly growing virtual spaces
Data Diversity	Primarily structured data, less variation	High, variant data types and formats	Enormous diversity due to additional sources such as VR, user interactions, virtual assets
Connectivity	Predictable and static	Dynamic (ad-hoc and intermittent)	Highly dynamic
Real-time Detection	Important for critical systems	Critical for real-time response to sensors and control devices	Crucial to maintain user experience and security
Cross-platform Security	Less complex	Challenges in device-to-device communication security	Complex due to interoperability with various platforms and devices
User Interaction	Relies on access control and network policies	Varies due to the diversity of user and device interaction	Highly complex due to varied, immersive interactions
Decentralization	Low, mostly centralized networks	Typically centralized, but growing use of decentralized approaches	Significant, the metaverse is posed to rely on decentralized tech
Threat Landscape	Traditional cybersecurity threats	Traditional cybersecurity threats and device-specific vulnerabilities	More AI-based sophisticated attacks and advanced persistent threats (APT)

Numerous survey papers examine the employment of AI techniques in IDS. Table X summarizes the key findings and limitations of the latest comprehensive surveys, aiming to provide readers with up-to-date insights into the application of various AI methods in IDS.

Abdallah *et al*. [247] focus on supervised ML techniques, concluding that RF achieves the highest accuracy while AdaBoost has the lowest performance. The authors discuss one challenge: IDS requires large datasets to predict abnormalities, which might need to be more efficient with ML algorithms. Darley *et al*. [248] highlight the importance of utilizing ML algorithms for intrusion detection in IoT systems, as they have shown promising results. However, the authors discuss some challenges related to IoT systems regarding computation capabilities, storage demands, and scalability issues. Khan *et al*. [249] highlight cyber-attacks emerging with IoT, such as DoS, device failures, sniffer attacks, and unauthorized access. The authors conclude that deep learning techniques are highly

TABLE X
SUMMARY OF RECENT SURVEY PAPERS THAT INVESTIGATE AI FOR IDS

Ref.	Year	Research Focus	Key Findings	Challenges and Limitations
[247]	2022	IDS using supervised ML techniques	1) Supervised ML techniques have promising results for IDSs. 2) Work with RF achieved the highest accuracy of 99.9%. 3) Feature selection in supervised ML is critical and affects the performance of the model.	1) Data imbalance affects the performance. 2) IDS require large datasets, which might not be feasible with ML algorithms.
[248]	2022	ML-based IDS in IoT systems	1) ML techniques are effective in intrusion detection. 2) Data preprocessing is essential and has high impact on IDS performance.	1) Imbalanced datasets. 2) Scalability issues in IoT. 3) IoT requires high computation demands and storage.
[249]	2022	DL for IDS of IoT	1) DNNs achieve high accuracies and low loss rates. (99.91%) 2) Image-based DL (DCNN) were introduced for anomaly detection and classification, also achieving 99% accuracy rates 3) Two-Stage DL (TSDL) was developed for the prevention of new attack variation, achieving high accuracy (99.96%) 4) Datasets affect the performance of the models.	1) Imbalanced datasets. 2) IoT challenges such as real-time updates, computational restrictions, complexity, and privacy concerns.
[250]	2023	AI/ML for NIDs	1) ML improves the efficiency of IDSs. 2) Datasets play a crucial part in determining IDS efficiency. 3) Compared to ML, DL techniques significantly improve IDS accuracy. However, they require high computation resources and time.	1) Many works use outdated datasets. 2) Class imbalance in datasets leads to lower detection rates. 3) Lack of real-world testing. 4) IDS design for IoT is challenging.
[251]	2023	ML, DL, ensemble learning	1) DL achieves higher accuracy in IDS comapred to ML. 2) Feature reduction is imporatned in AI-based IDS.	1) Most owrks focus on the accuracy metric. 2) Most works do not explore multiple classication 3) Noisy data affect IDS 4) Time complexity and CPU utlization

effective in intrusion detection, with neural networks (DNN) achieving remarkable accuracies. However, several challenges are discussed, such as computational constraints and privacy concerns in DL-based IoT intrusion detection.

Vanin *et al*. [250] focus on reviewing AI-based NIDS in IoT, covering both ML and DL algorithms. This study shows that while DL methods achieve higher accuracies for IDS than ML, they require additional computational resources and training time. Moreover, the authors discuss IoT challenges, highlighting that IoT devices primarily operate on wireless networks and often consist of sensor nodes that generate substantial data. These nodes typically have limited computing capabilities. Therefore, creating effective IDS solutions for IoT necessitates the development of lightweight systems that demand fewer computational resources and can efficiently process smaller data volumes for threat detection.

One of the most recent surveys [252] provides a review of AI-enabled intrusion detection for smart digital infrastructures, discussing ML, DL, and ensemble learning methods. The author emphasizes the need for research on AI-based IDS to focus on enhancing current solutions in terms of prediction accuracy to adapt to emerging technologies and systems such as cyber-physical systems, IoT networks, smart cities, digital twins, and the metaverse.

These survey papers illustrate the significant potential that AI methods hold in enhancing IDS. However, examining the challenges and limitations, all these papers highlight two primary concerns: computational restrictions and imbalanced datasets. These challenges present a notable research gap in metaverse-based IDS, given that the metaverse demands access to high-quality datasets and requires efficient security measures to provide a seamless user experience.

3) AI-based Solutions for Metaverse IDS: Several works investigate intrusion detection within the metaverse, as summarized in Table XI. Since numerous studies propose AI frameworks for intrusion detection in various applications (e.g., web-based, IoT, critical infrastructure, vehicle networks), it is important to identify the specific solutions these metaverse-based papers propose, which is shown in the "Motivation and Relevance to the Metaverse" column in the table. Additionally, the table highlights the AI technique(s) used for each work, datasets, performance metrics, and limitations.

Most research in IDS for the metaverse is motivated by tackling challenges associated with its enabling technologies, such as IoT, 5G, and blockchain. Ding *et al*. [253] emphasize the importance of IoT and 5G in building the future metaverse, which requires real-time data processing to bridge the physical and virtual worlds. Consequently, the attack surface and vulnerabilities are magnified. The authors proposed a hybrid model integrating DAE, GAN, and RF to enhance metaverse security and prevent disruptions. This model, designed to achieve high classification accuracies and produce true predictions and speed, significantly advances efficient IDS. Using the InSDN dataset [254], DAE is deployed for feature dimensionality reduction, optimizing the model's efficiency and convergence speed. GAN enhances the imbalanced dataset by increasing training samples, while RF is used for classification.

The model is evaluated for binary classification (normal and abnormal network traffic) and multi-class classification to predict attack types. The proposed model outperforms other DL models, including CNN, LSTM, and CNN-LSTM, in both binary and multi-class classifications, yielding significantly lower error predictions. However, it is important to note that the training time for binary classification is double that of LSTM,

TABLE XI
SUMMARY OF STUDIES ON AI-BASED IDS FOR THE METAVERSE

Ref.	IDS Type	Motivation and Relevance to the Metaverse	AI Techniques	Dataset	Performance Metrics	Limitations/Future Work
[253] 2022	Anomaly Detection	The metaverse is based on 5G and IoT, making it complex and in need for real-time detection	Hybrid (ML/DL) DAE, GAN, RF	InSDN	For binary and multiple classifications: - Acc: 99.8% & 99.6% - Recall: 99.9% and 99.6% - Prec: 99.8% and 99.5% - Time: 613s and 623s	- GAN is unstable - Training time is high compared to LSTM - Dataset limited in size
[255] 2023	IDS for IoT	The metaverse requires fast cyberthreat mitigation methods since it is driven by emerging technologies that require real-time solutions	User-plane machine learning inference with RF	ToN-IoT	Results in Python and Switch (best model): - F1 Score: 99.28% - 99.27% - TPR: 99.93%-99.93% - FPR: 0.74% – 0.77% - TNR: 99.26% - 99.23% - FNR: 0.07% - 0.07% - Latency: 73-91 ns	- Centralized - Privacy concerns - Best performing RF model has the most complex configurations - FPR can be further improved
[256] 2023	MetaCIDS: Collaborative IDS	MetaCIDS: A framework to secure the large-scale, distributed, and decentralized (blockchain) metaverse, while also addressing privacy concerns	FL, MLP	CIC-IDS2017	- Accuracy: 99.05% - Precision: 0.99 - Recall: 0.99 - F1 score: 0.99 - False Negaives: 5 to 15	- The model cannot collect labelled data for new attacks - Issue of data heterogeneity in decentralized training
[257] 2023	MetaCIDS: Collaborative IDS	Integration of FL, blockchain and AI to enhance security and privacy of IDS in the metaverse	Attention-based DAE, FL	CSE-CIC-IDS2018, CIC-IDS2017, NSL-KDD, UNSW-NB15	Accuracy: 95-99%	- Low performance against the NSL-KDD dataset - Diverse attacks in diverse devices
[258] 2023	IDS	High data volume from IoT and sensitive data from digital twins requires privacy-preserving and efficient IDS for the metaverse + imbalanced datasets issue	FL, meta-learning, Clustering RL ResNet-9	UNSW-NB-15, NSL-KDD	- F1 Score: 83.69 - AUC: 83.05 - Recall: 78.96 - Precision: 89.03	- Performance metrics can still be improved. - Lack of investigation of resource utilization.
[259] 2023	Anomaly Detection for Healthcare	Sensitive nature and unique data challenges in healthcare for the metaverse requires efficient and cost-friendly IDS	LSHiForest	SMTP and HTTP datasets	Accuracy Time cost AUC F1 score	Future work includes optimizing the model update process and improving data distribution estimation techniques for enhanced detection accuracy.
[260] 2023	IDS for IoT	- Securing IoT - Ensuring integrity - Advanced solutions for future metaverse	DT, RF, XGBoost	NSL-KDD, UNSW-NB15, CIC-IDS2017	Acc >99% for all datasets	Future work: - Test on datasets with more classes. - Analyse time utilization. - Investigate hybrid AI techniques. - Evaluate on diverse dataset.
[261] 2024	NIDS	Integrating explainable AI for NIDS in metaverse-based learning environments aims to ensure secure and transparent cybersecurity measures	DNN, XAI (SHAP and LIME)	EdgelloT, CICoT2023, UNSW-NB15	DNN-based NISA for metaverse learning platforms. Achieved high accuracy for binary classification	- Limited datasets - Specific to learning environments

which is a significant limitation given the criticality of speed in metaverse security solutions.

Bütün *et al*. [255] address the fast-response challenge with a novel approach that deploys ML (RF) algorithms in the user plane for real-time intrusion detection within SDN-based metaverse environments. This approach, which outperforms traditional methods operating in the control plane, is a significant leap in the field. It efficiently forwards data packets and achieves real-time detection without any delays associated with control plane processing. The research's novelty lies in its evaluation of the model at both software and hardware levels, employing Intel Tofino programmable switches and the P4

programming language to test the model against the ToN-IoT dataset. Several RF models with different configurations were evaluated, achieving accuracies that exceed 99%. The results also showed that the model has a minimal hardware resource consumption of below 5% and latency below 100ns. While this work offers promising insights into securing the future metaverse network, there are aspects that are not considered, such as the decentralized nature of the metaverse and potential privacy concerns.

Considering the distributed and decentralized aspects of the metaverse, several works combine blockchain with AI solutions [256],[257]. Troung and Le [256] present *MetaCIDS*, a collaborative IDS that leverages federated learning (FL) and blockchain technology to enhance the security and privacy of the decentralized metaverse. *MetaCIDS* utilizes FL to enable decentralized and collaborative intrusion detection, allowing metaverse devices to contribute to a shared intelligence model without compromising user data privacy. To further enhance privacy, differential privacy noise is added during the training process to minimize the exposure of sensitive information.

Additionally, a token-based incentive system is incorporated, and users are rewarded for participating in the training process and verifying alerts. These tokens serve as virtual currency, which can motivate metaverse users to indulge in and enhance intrusion detection training on their local devices. The role of AI is demonstrated through an attention-based Multi-Layer Perceptron (MLP) model that achieved an accuracy rate of 99% in identifying intrusion attacks. *MetaCIDS* was robust against several attacks, including fake alerts, DDoS, privacy attacks, zero-day attacks, and poisoning attacks.

Despite the model's high efficiency, the authors highlight a significant challenge posed by the lack of metaverse-specific datasets, emphasizing the need for future research in metaverse security. *MetaCID* cannot be trained on unlabeled data or collect labeled data for new attack types, making the system insufficient for real-world scenarios in the metaverse. However, the authors address these limitations in their next work [257], roposing an improved MetaCIDS version incorporating semi-supervised learning. The model integrates attention-based techniques with DAE, wherein the latter serves as an unsupervised learning module that can extract features from the network data without needing labeled data. The extracted models then pass through an attention-based weighting module, which assigns importance to features based on their relevance to intrusion detection. Subsequently, a lightweight neural network classifier is designed to evaluate the model against four datasets (see Table XI). Results show that *MetaCIDS* outperformed other models in multi-class and zero-day attack detection. It also demonstrated scalability and resilience against various attacks, providing a robust solution for metaverse security.

He *et al*. [258] recognize that digital twin-enabled 6G devices operating within the metaverse are vulnerable to security and privacy risks. Specifically, the authors highlight data-related IDS challenges within the heterogenous metaverse environment, namely the imbalance of classes in IDS datasets and non-independent and identically distributed (non-IID) data. To address these issues, the authors proposed a federated meta-learning approach that deploys FL for privacy preservation and meta-learning (a subfield of ML that aims to train models to self-adapt to new environments with minimal data) for tackling imbalanced datasets.

A meta-sampler is designed and optimized through reinforcement learning (RL) techniques to learn a sampling strategy and select effective data samples during training. It is worth noting that the meta-sampler is trained without needing access to the client's local data, thus ensuring data privacy protection. Additionally, a federated clustering algorithm is proposed to address the issue of non-IID data problems by dynamically clustering and ranking client-side models, leading to improved model performance. Through comprehensive experiments conducted on two datasets, it was found that the proposed model outperformed baselines in terms of accuracy and stability while also maintaining privacy.

Wu *et al*. [259] also address data-related issues in the metaverse, focusing on healthcare applications. The authors present a novel 6G-enabled Data Stream Anomaly Detection (DS AD) approach tailored for healthcare analytics within the metaverse, focusing on addressing cybersecurity challenges such as DDoS, probe, and port scanning attacks. Given the unique characteristics of medical data streams in the metaverse, including infiniteness, correlation, and distribution change, traditional static data anomaly detection algorithms must improve accuracy and efficiency. Thus, the proposed DS AD method integrates a sliding window model update and change detection mechanisms into the LSHiForest framework. This structure employs hash functions to partition data spaces to identify anomalies efficiently.

The core innovation lies in DS AD's ability to process data in one pass using a sliding window that stores the latest data, thus addressing the issue of data infiniteness. The model employs hash functions via LSHiForest to map data points, considering the correlations within the data stream. A change detection mechanism is introduced at the end of each sliding window to determine the necessity of model updates, ensuring the model remains accurate over time despite changes in data distribution. The effectiveness of DS AD is validated through extensive experiments on SMTP and HTTP datasets, demonstrating superior accuracy and efficiency compared to traditional methods. This approach not only enhances the detection of anomalies in healthcare data streams within the metaverse but also does so with consideration for the computational constraints of the 6G network, ensuring a high level of detection efficiency.

In [260], the authors deployed ensemble learning methods (XGBoost) on several intrusion detection datasets, achieving accuracies of over 99% for all of them. A recent study [261] introduced the integration of deep neural networks (DNN) with Explainable AI (XAI) for a network intrusion detection system designed specifically for mitigating threats in metaverse-based learning environments. In designing their model, the authors utilized a DNN architecture known for its automatic feature learning process, scalability, and accelerated training. The model is evaluated against IoT datasets for training and evaluation, achieving a high accuracy rate of 99.9% in establishing a secure learning environment. By incorporating explainable AI methods like SHAP and LIME, the model provides transparent and trustworthy explanations for its predictions, enhancing the understanding and trustworthiness of the NIDS in the context of the metaverse.

TABLE XII
AI-BASED FRAUD DETECTION FOR NFTS

Ref.	Year	Addressed Issue	Contribution	Dataset	Method(s)	Limitations
[262]	2022	Fraudulent Activity (Wash Trading, Pump and Dump)	A time series classification model to identity and predict fraudulent activity based on NFT collections.	NFT transactional data [263]	Clustered MCNN	- Model cannot predict new frauds. - Small labeled data.
[264]	2023	Wash Trading accounts	Systematic categorization of NFT user (trader) behaviours to identify potential fraud using ML.	Data collected includes transaction detailed from OpenSea	K-mean clustering	- Limited labels. - Small sample. - Limited data source. - Limited to wash trading accounts.
[265]	2023	Phishing, Pre-mint, and Rugpull Scams	An ML classifier tool that detects fraudulent NFT projects on Twitter.	Tweets that promote NFT projects	Random Forest	- Small dataset. - Focused on specific blockchains.
[266]	2023	Anomality Detection	A classifier model to predict anomalies in the Top Shot NFT platform.	Transactions in Top Shot (collectibles information)	Linear Regression	- Dataset is up to 2021. - Absence of ground truth labels. - Platform-specific.

C. Blockchain and NFT Security

Blockchain technology is highly associated with the future metaverse due to its potential in digital asset management [37], data privacy [267], and interoperability [268]. Several studies discuss the integration of blockchain technology with AI to enhance the security and interoperability of data in the metaverse [35][269][270]. This survey investigates the utilization of AI techniques to solve security issues in blockchain, focusing mainly on NFTs. To our knowledge, [271] is the first work to discuss AI deployment for NFT security. The authors highlight the integration of AI-based solutions with the International Financial Reporting Standard (IFRS) guidelines in NFT minting and transactions. Specifically, they suggest that AI solutions should be incorporated for smart contract creation, valuation, and verification, and ML techniques should be utilized for fraud detection.

This section reviews existing literature that uses AI techniques for NFT fraud detection, smart contracts security, and NFT verification. We then summarize how these solutions and identity verification can help enhance NFT transactions within the metaverse.

1) NFT Fraud Detection: The issue of fraud in NFT marketplaces is rising, as was discussed in Section V. Utilizing AI technology can limit such by detecting anomalies that indicate fraudulent activities. Several studies have demonstrated the efficiency of using AI for fraud detection in blockchain and cryptocurrency transactions. A recent example is the research conducted by Bhowmik *et al*. [272], in which the authors compare several ML algorithms to detect fraudulent transactions in the blockchain, concluding that AdaBoost, SVM, and RF classifiers achieved the best results with accuracies of 97%. Ashfaq *et al*. [273] integrated ML algorithms (XGboost and RF) and blockchain to design a model that can predict the legitimacy of blockchain transactions. It was tested against double-spending and Sybil attacks and proved robust against them.

Research on fraud detection for NFTs has emerged recently (See the summary in Table XII). In [262], the authors utilized a time-series classification model to predict whether a given collection of NFTs is legitimate (whitelisted) or suspicious (blacklisted), aiming to identify fraudulent activities such as Pump & Dump and Wash Trading. The dataset used in this study includes transactional information collected from NFT marketplaces (e.g., OpenSea and AtomicHub) [263]. The authors deployed K-means clustering and a Multiple Convolutional Neural Network (MCNN), previously developed by [274], because it provides enhanced feature extraction capabilities compared to other models, achieving an overall accuracy of 71.1%.

2) AI for Smart Contract Security: Smart contracts are utilized in blockchain for minting and holding the metadata of NFTs, making them susceptible to security threats and cybercriminal attacks, as was discussed in Section V. Considering the serious impact and financial loss that such risks can cause, multiple studies attempted to enhance the security of smart contracts, specifically through the deployment of AI techniques. By training ML algorithms on datasets of known vulnerabilities, the model learns to identify patterns or anomalies in smart contract code, resulting in detecting security flaws before they are exploited. Moreover, the adaptive nature of ML systems supports continuous monitoring of potential breaches and ensures that smart contracts can evolve in response to new threats. Jiang *et al*. [275] conducted a comprehensive survey investigating ML algorithms for smart contract security, focusing on reviewing supervised, unsupervised, semi-supervised, and reinforcement learning methods. It was found that supervised learning is the most used technique for detecting vulnerabilities in smart contracts due to its high predictive accuracy and applicability. Its main disadvantage is that it requires large amounts of labeled data to perform effectively. Furthermore, the authors suggest combining ML with statistical methods for future research in smart contract security.

Krichen [276] also conducted a comprehensive survey on applying AI techniques in enhancing smart contract security. The author compared classical and AI-based techniques,

TABLE XIII
STUDIES ON AI METHODS FOR NFT CONTENT VERIFICATION

Ref	Year	Methodology	AI Algorithm(s)	Dataset	Challenges and Limitations
[277]	2022	Integrates blcokchain and deep learning for NFT content verification.	VAE for feature compression and content protection	MNIST dataset	1) Study used a non-NFT dataset. 2) Scalability issues.
[278]	2023	Deep learning-based approach to detect plagiarism in NFT images	EfficientNet-B0 DNN with Triplet Semi-Hard Loss fuction	Public NFT dataset images	1) Specific dataset. 2) Limited to image-based NFTs.
[279]	2024	A verfification framework for NFT images based on quantum blockchain and deep learning.	ConNeXt deep learning model	Public NFT dataset	1) Specific dataset. 2) Computational and scalability issues.

highlighting the advantages of using AI for securing smart contracts, such as high accuracy and scalability. AI models can also analyze the smart contract code to detect and fix flaws and identify ambiguities and inconsistencies within the contract via a natural language processing (NLP) algorithm. The author also highlights the role of deep learning models, such as LSTM, ANN, and RNN, for vulnerability detection. Graph-based approaches, such as temporal message propagation networks, are also reviewed, highlighting their role in defining irregularities in financial transition in the blockchain. The author outlines significant challenges that must be addressed for AI-based smart contract security, including adversarial attacks, data privacy, scalability, and interoperability.

3) Content Verification: Verifying the legitimacy of the contents of an NFT is a pressing concern. Despite each token having a distinct identifier, the digital asset linked to an NFT may face duplication or plagiarism issues. Given the niche area of NFT research, especially in cybersecurity solutions, only a few papers attempted to investigate this problem, as summarized in Table XIII. Kimura *et al*. [277] proposed a distributed authenticity verification scheme integrating blockchain technology and deep learning. The study addresses blockchain poisoning, where malicious data aims to compromise blockchain integrity, focusing on NFTs as they are increasingly susceptible to such threats due to their growing popularity and market value. The authors analyzed the process from digital content creation to NFT distribution, identifying two main attack vectors: fake attacks and reuse attacks. A decentralized verification scheme was proposed to mitigate these attacks. Variational Auto Encoder (VAE) - a generative deep learning model- was incorporated to create a compressed representation of the original content, which serves as an irreversible transformation of content to ensure the confidentiality of the data and authenticity of NFTs without compromising privacy. This compressed representation is then used in a distributed verification scheme that involves a "verification game", in which blockchain participants collectively verify the authenticity of the content proposed for NFT minting. The authors highlighted the issue of content policies in NFT trading, emphasizing the need for clear guidelines regarding content use and licensing.

A recent study [278] proposed an NFT image plagiarism detection method using an advanced deep learning approach. The authors utilized *EfficientNet-B0*, a highly efficient deep learning architecture optimized for accuracy and computational efficiency. Coupled with the Triplet Semi-Hard Loss function, the system is trained to distinguish between original and plagiarized NFT images. The study utilized a publicly available NFT-Classifier dataset from Kaggle, which includes images from popular NFT collections. The method was tested against other models like *Resnet50*, *DenseNet*, and *MobileNetV2*, showing superior performance in terms of loss and accuracy. A notable limitation of this work is the reliance on a specific dataset that only partially represents the diversity of NFT images across different platforms and collections. Additionally, the study focuses on image-based plagiarism detection and does not consider other forms of content plagiarism within the NFT ecosystem, such as audio or video files.

The study in [279] highlighted the vulnerabilities of classical cryptographic schemes that can be broken by quantum computing. The authors proposed a novel solution combining quantum-resistant technologies with deep learning to protect NFT content against emerging threats. The proposed framework utilized *ConvNext*, a deep learning model distinguished by its optimized architecture. Through experimental evaluations, the study demonstrated the effectiveness of the proposed method in terms of accuracy, scalability, and resilience against quantum threats.

4) General Framework: In addition to the possible solutions discussed so far, the deployment of an efficient biometric continuous authentication system in the metaverse provides robust verification of the identities participating in NFT trading (sellers and buyers), preventing any potential imposters from engaging in unauthorized transactions. Moreover, mutual authentication schemes can be incorporated into the NFT marketplace to verify the transactions between users and marketplaces, ensuring that both entities are legitimate. Fig. 19 illustrates an overview of a general framework that demonstrates the application of various AI methods for enhancing security in NFT transactions within the metaverse, including biometric continuous user authentication, mutual authentication, detection of fraudulent activities in NFT trading, plagiarism detection and content verification of NFTs, and finally smart contract security.

VI. Summary and Lessons Learned

In this section, we highlight the key lessons learned from this survey, providing an overall summary of the main sections.

A. Lessons Learned from Metaverse Security Overview

1) Existing Literature: Since the metaverse is still an

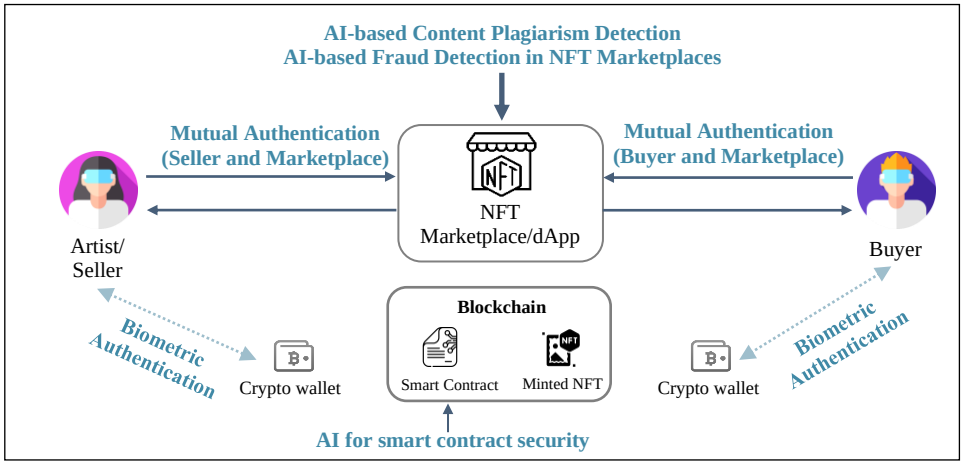

Fig. 19. AI can be deployed for NFT security as follows. Robust authentication systems (biometric and real-time) provide identity verification for the seller and buyer when they trade on an NFT platform or when they access their crypto wallets, preventing unauthorized access and impersonation attacks. AI models can also be deployed to verify the content of an NFT before it is listed on the marketplace. Furthermore, fraud detection can occur within the NFT platform to alert users of potential scams. Lastly, AL techniques can help prevent attacks directed at smart contracts.

emerging concept, most existing surveys and research are focused on investigating technological solutions for achieving the envisioned metaverse. Several notable survey papers [134] [43] comprehensively review the plausible security and privacy threats of the metaverse. However, there are still limitations in academic works that propose solutions to such risks. Moreover, further research is still needed to explore innovative solutions, such as AI, that can handle the complex and dynamic nature of the future metaverse.

2) Industrial Solutions: Many companies invest in the metaverse, but only a few publicly address cybersecurity and privacy concerns. For example, Meta has acknowledged the critical need to focus on privacy, open standards, and governance as integral parts of their metaverse strategy. Similarly, Microsoft has initiated discussions about identity-related threats and emphasized the importance of collaborative approaches to overcome these challenges effectively. However, standards, policies, and legal concepts still need to be considered to ensure the safety and privacy of users and enterprises indulging in the metaverse.

3) Security and Privacy Issues: The metaverse presents unique cybersecurity challenges and significant privacy risks due to its expansive scalability, multi-tech integration, and extensive user data collection. Specifically, sensitive information such as user biometric and behavioral data collected through head-mounted displays (HMDs) introduces vulnerabilities that could compromise user privacy. Additionally, users enter the metaverse as customizable digital avatars and interact with other avatars that could be other human users or AI-generated virtual assistants, which raises concerns related to impersonation, integrity, and anonymity. The highly immersive nature of the metaverse also increases the impact of malicious behavior, such as cyberbullying and harassment [143], which affects the digital wellbeing of users. Other potential attacks target the safety of users, such as altering the walls of the virtual environment, manipulate the physical movement of users without their knowledge (Human Joystick attack), and disorientation attacks that can induce dizziness for virtual reality (VR) users.

4) NFTs in the Metaverse: Non-fungible tokens (NFTs) have gained considerable attention in discussions about the metaverse's economic framework [37][154][280]. NFTs are unique cryptographic identifiers that offer promising means to establish digital asset ownership, supported by the security of blockchain technology. However, given the substantial market value of cryptocurrencies and NFTs, they have become prime targets for cybercriminals. Security risks associated with NFTs include fraudulent activities in digital marketplaces, social engineering attacks, vulnerabilities in smart contracts, instances of NFT plagiarism, and the absence of proper authentication mechanisms in NFT marketplaces.

B. Lessons Learned from AI-based User Authentication

1) Authentication for Metaverse-related Applications: Most platforms rely on optional two-factor authentication (2FA). While 2FA represents an improvement in security over traditional single-factor methods, it remains vulnerable to cyberattacks and inadequate for the security demands of the metaverse, considering the high risk of compromising users' digital identity (personal information, biometric data, digital assets). Additionally, NFT marketplaces lack robust user authentication and verification mechanisms, leaving them susceptible to security vulnerabilities, such as Man in the Middle attacks, phishing attacks, and hacking of crypto wallets.

2) Biometric Authentication: The metaverse offers unique opportunities for advanced biometric technologies. Metaverse hardware, like head-mounted displays (HMDs), collect biometric data such as facial features, head movements, and body movements to enable the generation of realistic avatars and immersive experiences. Since biometrics are already part of the metaverse ecosystem, it offers opportunities to utilize them for user authentication. Several studies have shown the potential of using biometric attributes in identifying and verifying users, including physical and behavioral traits like facial features, iris, retina, gait, and keystroke patterns. Additionally, physiological signals, such as EEG, are part of the Brain-Computer Interface (BCI) research dedicated to the metaverse. They have also been utilized for user authentication, making them suitable as identifiers in the future

metaverse. ECG and PPG (measurements of heart activity) are also biometric identities used for user authentication, and like EEG, they are relatively robust against spoofing attacks and can provide liveness detection.

3) Multimodal and Continuous Authentication: Multimodal and continuous authentication can significantly enhance security and user experience within the metaverse. By integrating multiple biometric modalities, multimodal authentication effectively counters risks associated with single biometric systems, such as spoof attacks and data inaccuracies, increasing the overall robustness of security frameworks. Continuous authentication further builds on this by maintaining user verification throughout the session, which is crucial for preventing unauthorized access post-initial login. Recent research shows potential in integrating multimodality with continuous authentication. However, further investigations are needed on how they can be applied in the metaverse while considering computational requirements, usability, and privacy.

C. Lessons Learned from AI-based Intrusion Detection Systems

1) Intrusion Detection Challenges in the Metaverse: he metaverse presents unique challenges for Intrusion Detection Systems (IDS) due to its expansive scale and the diverse array of data it encompasses, from IoT device sensors to virtual interactions and 3D models. This diversity and scale necessitate scalable IDS solutions that can process a broad array of information efficiently to ensure comprehensive security. Moreover, the metaverse's dynamic nature—with its continuous data updates and evolving virtual spaces—requires IDS that can adapt in real time. Additionally, the interoperability feature of the metaverse allows users to move seamlessly across various virtual environments, which introduces further security challenges. IDS must effectively manage security across different platforms, each with potentially varying user behavior and interaction norms. The decentralized nature of the metaverse complicates security management even further, requiring innovative IDS solutions that can operate effectively within a decentralized architecture while ensuring user privacy and data integrity.

2) AI Solutions for Intrusion Detection Systems: The integration of AI into IDS has shown promising enhancements, particularly in terms of detection accuracy and operational efficiency. AI techniques enable the detection of complex attack patterns and support the handling of large-scale data environments. However, the reliance on AI also introduces challenges such as the need for large and diverse datasets, computational intensity, and potential issues with data privacy. Future research needs to focus on optimizing AI-driven IDS in terms of computational demands, data management, and privacy preservation to ensure they are suitable for the expansive and multifaceted metaverse.

D. Lessons Learned from AI for Blockchain and NFT Security

Integrating blockchain technology with AI holds immense potential for shaping the future metaverse, offering enhanced security, data management, and interoperability [37][267]. Incorporating AI techniques for NFT transactions can significantly reduce risks and ensure the trustworthiness of NFT marketplaces. For example, several works used ML techniques to detect fraudulent activities in NFT marketplaces, enhancing the security and integrity of NFT transactions [262],[264]. Moreover, AI methods can identify vulnerabilities in smart contracts, contributing to their improved security and reliability [275],[276]. Lastly, ensuring the uniqueness and security of data content within NFTs is a critical concern. Therefore, the deployment of DL models showed effective performance in detecting duplication and plagiarism, which is needed in the NFT market and future metaverse to ensure the integrity of NFTs and the rights of content creators.

VII. Challenges and Research Opportunities

This section highlights research challenges and future research opportunities.

A. Research Challenges

1) Privacy Concerns: The metaverse presents several privacy issues regarding data and personal information. As users immerse themselves in this digital realm, they generate significant data, including their movements, interactions, and preferences. This data can be collected and analyzed by metaverse platforms and potentially shared with third parties for various purposes, such as targeted advertising or user profiling [146]. Concerns about data privacy in the metaverse revolve around the potential for unauthorized data collection, surveillance, and the risk of personal information falling into the wrong hands. Additionally, the anonymity often associated with the metaverse can give rise to instances of cyberbullying and harassment, raising further privacy and safety concerns for users [281],[282]. The metaverse, like any innovative technology, brings significant privacy concerns. The vast user data expected to be collected increases privacy risks, not to mention that collecting biometrics is an essential part of the metaverse since this data is needed for enabling the immersive virtual environments making up the metaverse. Additionally, the deployment of AI, despite its significant advantages, also has privacy concerns since training AI algorithms requires datasets, which puts them at risk

Addressing these privacy concerns in the metaverse requires a comprehensive approach, especially when implementing AI techniques for cybersecurity, including biometrics. While AI can be crucial in detecting and preventing cyber threats in the metaverse, it also introduces privacy issues, particularly in handling biometric data. AI systems may inadvertently access and analyze sensitive biometric information during cybersecurity operations, potentially exposing private details to unauthorized entities. The deployment of biometric authentication methods in the metaverse raises concerns about the storage and protection of biometric templates, as any breach could have lasting consequences for users.

2) Limitations in Datasets: The quality of datasets is crucial for AI systems, as it directly influences the accuracy and reliability of the resulting models. Several challenges arise regarding collecting, processing, and utilizing datasets intended for AI models in the metaverse.

User Authentication: In the metaverse, user authentication heavily relies on biometric data to verify identities uniquely.

However, the challenge arises from limited datasets, often needing to be more diverse to train AI models effectively. This lack of diversity can result in models that fail to recognize less common biometric traits, leading to higher false rejection rates. Moreover, small datasets may need to adequately represent the range of variations in biometric data caused by different environmental conditions or user behaviors.

Intrusion Detection Systems (IDS): The challenge for IDS in the metaverse is training AI models on datasets that comprehensively represent the diverse ways a system can be attacked or compromised. The importance of this aspect is highlighted by the fact that limited datasets might not encompass the full spectrum of attack vectors, particularly newer or more sophisticated strategies that have yet to be widely documented, such as zero-day attacks or novel exploitation techniques.

NFT Security: AI models in NFT security must detect and prevent fraud, such as duplication attempts or unauthorized transfers. Limited datasets can restrict the training of these models by not providing enough examples of fraud patterns or the variety of legitimate transactions. This limitation can result in higher false positives, where legitimate transactions are flagged as suspicious, or worse, false negatives, where fraudulent activities go undetected. The unique nature of NFTs requires datasets that are not only large but also rich with varied and complex transaction data to train accurate and reliable models.

3) Adversarial Attacks on AI Models: AI models, integral to the functionality and security of the metaverse, face significant risks from targeted attacks, such as data poisoning. This type of threat involves maliciously altering training data to affect the learning process of AI models, leading to compromised outputs or decisions. For example, data poisoning could target AI-based biometric systems such as facial recognition [283] and voice authentication [284], manipulating them to incorrectly verify user identities and potentially allowing unauthorized access to sensitive areas or user accounts. Data poisoning attacks can also target physiological biometric systems such as EEG [285] and ECG [286]. Another critical concern is the poisoning attacks on federated learning (FL) systems, where the decentralized nature of FL poses unique vulnerabilities [287]. In FL, malicious participants can send model updates derived from mislabeled data, which, as studies have shown, can cause substantial drops in classification accuracy and recall. These attacks could be particularly damaging in the metaverse, where AI needs to operate reliably across diverse and dynamic virtual environments.

B. Research Opportunities and Future Directions

1) AI and Biometrics for Metaverse Security: Given that biometrics are essential in supporting the metaverse for realistic avatar generation, XR interactions, health applications, and Brain-Computer Interfaces (BCI), there is a research opportunity to also investigate their deployment for security and safety of metaverse users.

User Authentication: A common application is biometric authentication, which has already been implemented in smart devices (facial recognition), HMDs (iris recognition), and voice recognition in banking applications. However, research is still needed on metaverse-specific datasets that cater to the diverse range of metaverse users and applications. Given the importance of user experience, particularly as the metaverse integrates into daily activities and works, investigating continuous and seamless authentication methods is crucial as it can provide high security without disrupting user activity, ideally operating in the background. Considering the computational limitations of emerging metaverse hardware like XR headsets, VR gloves, and VR suits, it is vital to design AI biometric systems using lightweight methods compatible with current hardware specifications and requirements.

Insider Threat Detection: Insider threats—malicious actions by individuals with system access—are particularly critical for enterprises and national infrastructure, making insider threat detection a significant research area. While still niche, studies have explored using biometric modalities to monitor users in critical infrastructure to detect and prevent insider threats [288]. AI can identify anomalies indicating malicious activities or unauthorized access by analyzing patterns in movement, speech, and interactions within the environment. This capability is essential for mitigating risks associated with insider threats, where seemingly legitimate users might exploit their access for harmful purposes. Research into using EEG for insider threat detection has also shown promising results [289].

Emotion Recognition: AI-driven emotion recognition systems can autonomously discern human emotional states, offering valuable applications in mental health assessment, behavior tracking, and marketing strategies. These systems can evaluate student engagement in virtual learning environments, improve healthcare outcomes, and enhance safety by monitoring driver behavior and detecting potential threats. Various biometric modalities, including facial expressions, EEG, and ECG, can reflect emotions [186],[290]. Facial emotion recognition can be adapted for avatars in the metaverse, while EEG and ECG signals can provide objective emotional insights, particularly in VR environments.

2) Exploring Network Security for the Metaverse: As the metaverse continues to evolve, it is imperative to emphasize ongoing research and development in network security. The dynamic and complex nature of the metaverse presents unique challenges. Therefore, it is essential to focus on several key research areas. Firstly, implementing real-time network traffic monitoring solutions is crucial to detect and respond promptly to emerging threats within this interconnected virtual space. Secondly, integrating AI-driven firewall technologies can enhance the metaverse's security posture by autonomously identifying and mitigating potential vulnerabilities and attacks. Furthermore, developing robust threat intelligence systems tailored to the metaverse environment is essential for proactive defense. Given the increasing adoption of 5G networks, the metaverse will benefit from dedicated research into DDoS mitigation strategies optimized for the high-speed, low latency demands of 5G. Additionally, the security of Internet of Things (IoT) devices and virtual environments within the metaverse warrants dedicated attention, as these endpoints represent potential entry points for cyber threats. In summary, advancing research in these areas is pivotal to ensuring robust cybersecurity within the metaverse.

3) AI for NFT Security and NFT for Metaverse Security:

Integrating AI and NFTs within the metaverse presents a significant research opportunity, particularly in enhancing security and user experience. AI can be used to develop more sophisticated security protocols for NFT transactions, potentially reducing fraud and phishing attacks. Furthermore, AI could assist in automating the verification of NFT authenticity and provenance, adding a layer of trust to transactions. There is also potential to explore how AI can optimize NFT metadata to enhance searchability and interoperability within the metaverse ecosystems.

4) Privacy-preservation: To address privacy concerns in the metaverse, it is essential to explore innovative strategies that can ensure the protection of user data, and that can also handle AI training in a way that limits, and ideally prevents, the possibility of data leakages or data breaches. In general, metaverse platforms should limit data collection to those that are extremely necessary for the required functionality. This strategy is related to regulations and legal standards that should be set up by the authorities. In terms of research opportunities on the other hand, there are several research areas that can be explored to tackle privacy concerns in the metaverse.

Homomorphic Encryption: Encryption refers to a method that converts data into another form of unreadable text or a secret code that hides the meaning of information to protect it. Researchers can explore emerging forms of encryption that can balance security with the high performance required for real-time virtual interactions in the metaverse. *Homomorphic encryption (HE)*, for instance, enables computations to be performed on encrypted data without having to decrypt it, allowing for privacy preservation during processing. In their comprehensive review, Yang *et al*. [291] discuss the application of HE in biometric systems, highlighting its ability to protect data without affecting the systems' recognition accuracy, and discussing challenges to consider such as computational complexity and management of keys.

Privacy-Preserving Biometrics: As biometrics become integral to the metaverse for various applications, developing methods to ensure data privacy is essential. Arman *et al*. [292] provides a comprehensive review on privacy-preserving technologies for biometrics that are worth investigating for the metaverse, such as cryptography, hashing algorithms, and biometric template protection. Notable examples of such techniques discussed in the paper are: *1) Cancelable biometrics*, which distorts data features to prevent intruders from accessing the original biometric information. *2) Differential Privacy (DP)*, a statistical technique that adds controlled random noise to data or its extracted features to obscure individual identities. is another technique that can be used to protect biometric templates in AI systems. While it is not restricted to biometrics.

VIII. Conclusion

The metaverse is an emerging concept described as the future 3D Internet, where users engage in various experiences and interact with others online as digital avatars in an immersive virtual environment. Many companies are investing in the metaverse, aiming to achieve an immersive, decentralized, interoperable, scalable, and multi-technological cyber-physical world that revolutionizes the way people interact with technology. Despite the significant opportunities of the metaverse for various applications, there are cybersecurity concerns that need to be addressed. The technological innovation and vast economy of the metaverse will increase surface attack and attract cybercriminals. This paper highlighted potential cybersecurity threats related to data, identity, user privacy, digital wellbeing, legal regulations, and NFTs based on the characteristics and enabling technologies of the metaverse, highlighting current cyberattack incidents and demonstrating how they can be magnified in the metaverse. The dynamic nature of the metaverse requires advanced techniques to mitigate evolving cyber threats. Therefore, we investigated several AI techniques for cybersecurity and privacy in the metaverse, focusing on user authentication, intrusion detection systems, and blockchain security. According to our findings, most applications and devices provide optional two-factor authentication, which is inefficient for the metaverse. Therefore, we proposed a multifactor, multimodal, and continuous authentication system for metaverse users, in which various biometric identifiers are utilized. The novelty in our system is that it integrates multiple biometrics and utilizes EEG and ECG to provide liveness check and constant validation of metaverse users and NFT transactions. Furthermore, AI techniques hold potential for intrusion detection in the metaverse. However, there are still limitations and research directions to consider when it comes to network security within the metaverse. Finally, we highlighted the potential of AI for securing blockchain and NFT transactions via fraud detection, maintaining smart contract security, and content verification of NFT. As the metaverse continues to grow, the use of AI techniques will become increasingly important for enhancing security and protecting users from a range of security threats.

Acknowledgment

Fig. 4 was designed by Salma Awadallah, a professional illustrator (e-mail: salmawadallah@gmail.com).

References

[1] R. Moro-Visconti and A. Cesaretti, "The Metaverse," in Digital TokenValuation, Cham: Springer Nature Switzerland, 2023, pp. 199–240. doi: 10.1007/978-3-031-42971-2_7.

[2] N. Stephenson, *Snow Crash*. United States: Bantam Books, 1992.

[3] X. Niu and W. Feng, "Immersive entertainment environments-from theme parks to metaverse," in *Proc. International Conference on Human-Computer Interaction, Cham*, Switzerland, 2022., pp. 392–403. doi: 10.1007/978-3-031-05463-1_27.

[4] G.-J. Hwang and S.-Y. Chien, "Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective," *Computers and Education: Artificial Intelligence*, vol. 3, p. 100082, 2022, doi: 10.1016/j.caeai.2022.100082.

[5] K. Baskaran, "Customer Experience in the E-Commerce Market Through the Virtual World of Metaverse," in *Handbook of Research on Consumer Behavioral Analytics in Metaverse and the Adoption of a Virtual World, IGI Global*, 2023, pp. 153–170. doi: 10.4018/978-1-6684-7029-9.ch008.

[6] T. Hennig-Thurau, D. N. Aliman, A. M. Herting, G. P. Cziehso, M. Linder, and R. V. Kübler, "Social interactions in the metaverse: Framework, initial evidence, and research roadmap," *J Acad Mark Sci*, vol. 51, no. 4, pp. 889–913, Jul. 2023, doi: 10.1007/s11747-022-00908-0.

[7] R. Chengoden et al., "Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions," *IEEE Access*, vol. 11, pp. 12765–12795, 2023, doi: 10.1109/ACCESS.2023.3241628.

[8] C. Koo, J. Kwon, N. Chung, and J. Kim, "Metaverse tourism: conceptual framework and research propositions," *Current Issues in Tourism*, vol. 26, no. 20, pp. 3268–3274, Oct. 2023, doi: 10.1080/13683500.2022.2122781.

[9] C. Chen et al., "When Digital Economy Meets Web3.0: Applications and Challenges," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 233–245, 2022, doi: 10.1109/OJCS.2022.3217565.

[10] S. Mihai et al., "Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2255–2291, 2022, doi: 10.1109/COMST.2022.3208773.

[11] J. Ratcliffe, F. Soave, N. Bryan-Kinns, L. Tokarchuk, and I. Farkhatdinov, "Extended Reality (XR) Remote Research: a Survey of Drawbacks and Opportunities," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, May 2021, pp. 1–13. doi: 10.1145/3411764.3445170.

[12] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, "Characterising the Digital Twin: A systematic literature review," *CIRP J Manuf Sci Technol,* vol. 29, pp. 36–52, May 2020, doi: 10.1016/j.cirpj.2020.02.002.

[13] M. Chawki, "Cybercrime in the Context of COVID-19," in *Intelligent Computing: Proceedings of the 2021 Computing Conference*, vol. 3, Springer International Publishing, 2021, pp. 986–1002, doi: 10.1007/978-3-030-80129-8_65.

[14] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review," *Applied Artificial Intelligence*, vol. 36, no. 1, Dec. 2022, doi: 10.1080/08839514.2022.2037254.

[15] A. M. Awadallah, E. Damiani, J. Zemerly, and C. Y. Yeun, "Identity Threats in the Metaverse and Future Research Opportunities," in 2023 *International Conference on Business Analytics for Technology and Security (ICBATS)*, IEEE, Mar. 2023, pp. 1–6. doi: 10.1109/ICBATS57792.2023.10111122.

[16] Y. Mirsky and W. Lee, "The Creation and Detection of Deepfakes," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1–41, Jan. 2022, doi: 10.1145/3425780.

[17] S. Kulal, Z. Li, and X. Tian, "Security and privacy in virtual reality :A literature review," *Issues In Information Systems*, vol. 23, no. 2, pp. 185–192, 2022, doi: 10.48009/2_iis_2022_125.

[18] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891.

[19] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: a systematic literature review," *Artificial Intelligence Review*, vol. 56, no. 10, pp. 10733–10811, Oct. 2023, doi: 10.1007/s10462-023-10437-z.

[20] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Blockchain Integration in the Era of Industrial Metaverse," *Applied Sciences*, vol. 13, no. 3, p. 1353, Jan. 2023, doi: 10.3390/app13031353.

[21] M. Fortnow and Q. Terry, *The NFT Handbook: How to Create, Sell and Buy Non-Fungible Tokens*, 1st ed. Hoboken, NJ: Wiley, 2021

[22] B. White, A. Mahanti, and K. Passi, "Characterizing the OpenSea NFT Marketplace," in *Companion Proceedings of the Web Conference*, 2022, pp. 488–496. doi: 10.1145/3487553.3524629.

[23] S. Bhujel and Y. Rahulamathavan, "A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces," *Sensors*, vol. 22, no. 22, p. 8833, Nov. 2022, doi: 10.3390/s22228833.

[24] L. Chan et al., "Survey of AI in Cybersecurity for Information Technology Management," in *2019 IEEE Technology & Engineering Management Conference (TEMSCON),* IEEE, Jun. 2019, pp. 1–8. doi: 10.1109/TEMSCON.2019.8813605.

[25] L. LAZIĆ, "Benefit From AI in Cybersecurity," in *The 11th International Conference on Business Information Security (BISEC-2019)*, 2019.

[26] J. D. N. Dionisio, W. G. Burns, and R. Gilbert, "3D virtual worlds and the metaverse: Current status and future possibilities," *ACM Comput Surv*, vol. 45, no. 3, Jun. 2013, doi: 10.1145/2480741.2480751.

[27] H. N. Wang et al., "A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges," *arXiv* preprint arXiv:2111.09673, 2021.

[28] L.-H. Lee et al., "All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda," *arXiv*, [Online]. Available: http://arxiv.org/abs/2110.05352

[29] S. M. Park and Y. G. Kim, "A Metaverse: Taxonomy, Components, Applications, and Open Challenges," *IEEE Access*, vol. 10, pp. 4209–4251, 2022, doi: 10.1109/ACCESS.2021.3140175.

[30] M. Xu et al., "A Full Dive Into Realizing the Edge-Enabled Metaverse: Visions, Enabling Technologies, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 656–700, 2023, doi: 10.1109/COMST.2022.3221119.

[31] 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, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102542.

[32] R. Yang, L. Li, W. Gan, Z. Chen, and Z. Qi, "The Human-Centric Metaverse: A Survey," in Companion Proceedings of the ACM Web Conference 2023, New York, NY, USA: ACM, Apr. 2023, pp. 1296–1306. doi: 10.1145/3543873.3587593.

[33] L. Chang et al., "6G-enabled Edge AI for Metaverse: Challenges, Methods, and Future Research Directions," *arXiv*, 2022, [Online]. Available: http://arxiv.org/abs/2204.06192

[34] T. Huynh-The, Q.-V. Pham, X.-Q. Pham, T. T. Nguyen, Z. Han, and D.-S. Kim, "Artificial Intelligence for the Metaverse: A Survey," *arXiv*, 2022, [Online]. Available: http://arxiv.org/abs/2202.10336

[35] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing Blockchain and AI with Metaverse: A Survey," *arXiv*, 2022, [Online]. Available: http://arxiv.org/abs/2201.03201

[36] T. Huynh-The et al., "Blockchain for the metaverse: A Review," *Future Generation Computer Systems*, vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/j.future.2023.02.008.

[37] V. T. Truong, L. Le, and D. Niyato, "Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey," *IEEE Access*, vol. 11, pp. 26258–26288, 2023, doi: 10.1109/ACCESS.2023.3257029.

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

[39] S. B. Far and A. I. Rad, "Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges," *arXiv,* Apr. 2022, [Online]. Available: http://arxiv.org/abs/2204.11343

[40] Z. Chen, J. Wu, W. Gan, and Z. Qi, "Metaverse Security and Privacy: An Overview," Nov. 2022, [Online]. Available: http://arxiv.org/abs/2211.14948

[41] 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, p. 11, Dec. 2022, doi: 10.3390/jimaging9010011.

[42] J. Sun, W. Gan, Z. Chen, J. Li, and P. S. Yu, "Big Data Meets Metaverse: A Survey," *arXiv,* Oct. 2022, [Online]. Available: http://arxiv.org/abs/2210.16282

[43] Y. Huang, Y. J. Li, and Z. Cai, "Security and Privacy in Metaverse: A Comprehensive Survey," *Big Data Mining and Analytics*, vol. 6, no. 2, pp. 234–247, Jun. 2023, doi: 10.26599/BDMA.2022.9020047.

[44] N. Aung, S. Dhelim, L. Chen, H. Ning, L. Atzori, and T. Kechadi, "Edge-Enabled Metaverse: The Convergence of Metaverse and Mobile Edge Computing," *Tsinghua Sci Technol*, vol. 29, no. 3, pp. 795–805, Jun. 2024, doi: 10.26599/TST.2023.9010052.

[45] T. Q. Duong, D. Van Huynh, S. R. Khosravirad, V. Sharma, O. A. Dobre, and H. Shin, "From Digital Twin to Metaverse: The Role of 6G Ultra-Reliable and Low-Latency Communications with Multi-Tier Computing," *IEEE Wirel Commun*, vol. 30, no. 3, pp. 140–146, Jun. 2023, doi: 10.1109/MWC.014.2200371.

[46] G. Huisman, "Social Touch Technology: A Survey of Haptic Technology for Social Touch," *IEEE Trans Haptics*, vol. 10, no. 3, pp. 391–408, 2017, doi: 10.1109/TOH.2017.2650221.

[47] H. Fan, J. Gao, Y. Xu, G. Fortino, and W. Qi, "Metaverse Driven Edge-Fogging-Cloud Network for Complex Human Activity Recognition Using Sensors Fusion," *in 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)*, IEEE, Sep. 2023, pp. 1–6. doi: 10.1109/iMETA59369.2023.10294545.

[48] F. Tang, X. Chen, M. Zhao, and N. Kato, "The Roadmap of Communication and Networking in 6G for the Metaverse," *IEEE Wirel Commun*, vol. 30, no. 4, pp. 72–81, Aug. 2023, doi: 10.1109/MWC.019.2100721.

[49] L. Qi, S. Dou, Z. Guo, C. Li, Y. Li, and T. Zhu, "Low Control Latency SD-WANs for Metaverse," in 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), IEEE, Jul. 2022, pp. 266–271. doi: 10.1109/ICDCSW56584.2022.00057.

[50] K. L. Nowak and J. Fox, "Avatars and computer-mediated communication: A review of the definitions, uses, and effects of digital representations," *Review of Communication Research*, 2018, doi: 10.12840/issn.2255-4165.2018.06.01.015.

[51] Meta, The Metaverse and How We'll Build It Together -- Connect 2021, (Oct. 28, 2021). Accessed: Feb. 11, 2021. [Online Video]. Available: https://youtu.be/Uvufun6xer8

[52] M. Yilmaz, T. Hacaloğlu, and P. Clarke, "Examining the Use of Non-fungible Tokens (NFTs) as a Trading Mechanism for the Metaverse," *European Conference on Software Process Improvement*, Cham, Switzerland: Springer International Publishingm 2022, pp. 18–28. doi: 10.1007/978-3-031-15559-8_2.

[53] M. Liu, S. Fang, H. Dong, and C. Xu, "Review of digital twin about concepts, technologies, and industrial applications," *J Manuf Syst*, vol. 58, pp. 346–361, Jan. 2021, doi: 10.1016/j.jmsy.2020.06.017.

[54] L. Adriana Cárdenas-Robledo, Ó. Hernández-Uribe, C. Reta, and J. Antonio Cantoral-Ceballos, "Extended reality applications in industry 4.0. – A systematic literature review," *Telematics and Informatics*, vol. 73, p. 101863, Sep. 2022, doi: 10.1016/j.tele.2022.101863.

[55] S. Bularka and A. Gontean, "Brain-Computer Interface review," *in 2016 12th International Symposium on Electronics and Telecommunications, ISETC 2016 - Conference Proceedings, Institute of Electrical and Electronics Engineers Inc.*, Dec. 2016, pp. 219–222. doi: 10.1109/ISETC.2016.7781096.

[56] S. S. Thakur, S. Bandyopadhyay, and D. Datta, "Artificial Intelligence and the Metaverse: Present and Future Aspects," *The Future of Metaverse in the Virtual Era and Physical World*. Cham: Springer International Publishing, 2023, pp. 169–184. doi: 10.1007/978-3-031-29132-6_10.

[57] A. Dubey, N. Bhardwaj, A. Upadhyay, and R. Ramnani, "AI for Immersive Metaverse Experience," in *Proceedings of the 6th Joint International Conference on Data Science & Management of Data (10th ACM IKDD CODS and 28th COMAD)*, New York, NY, USA: ACM, Jan. 2023, pp. 316–319. doi: 10.1145/3570991.3571045.

[58] D. Solska, "Traversing the Metaverse: the new frontiers for computer-mediated communication and natural language processing," *Forum Filologiczne Ateneum*, no. 1(10)2022, pp. 27–38, Dec. 2022. doi: 10.36575/2353-2912/1(10)2022.027.

[59] B. S. Rawal, A. Mentges, and S. Ahmad, "The Rise of Metaverse and Interoperability with Split-Protocol," in *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)*, IEEE, Aug. 2022, pp. 192–199. doi: 10.1109/IRI54793.2022.00051.

[60] S. Butler, "Persistent AR Explained: Why It's the Key to the Metaverse," *How-To Geek*. Accessed: Oct. 23, 2022. [Online]. Available: https://www.howtogeek.com/788486/persistent-ar-explained-why-its-the-key-to-the-metaverse/

[61] R. Faughnder, "Disney 'metaverse' begins to take shape," *Tech Xplore*. Accessed: Dec. 24, 2022. [Online]. Available: https://techxplore.com/news/2022-04-disney-metaverse.html

[62] D. Gursoy, S. Malodia, and A. Dhir, "The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions," *Journal of Hospitality Marketing and Management*, vol. 31, no. 5, pp. 527–534, 2022. doi: 10.1080/19368623.2022.2072504.

[63] Emirates Airlines, "Emirates launches first airline virtual reality app in Oculus store, the world's most popular VR platform," *Emirates Airlines*. Accessed: Nov. 12, 2022. [Online]. Available: https://www.emirates.com/media-centre/emirates-launches-first-airline-virtual-reality-app-in-oculus-store-the-worlds-most-popular-vr-platform/

[64] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2494–2528, 2023. doi: 10.1109/COMST.2023.3315374.

[65] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of Artificial Intelligence and Machine learning in smart cities," *Comput Commun*, vol. 154, pp. 313–323, Mar. 2020. doi: 10.1016/j.comcom.2020.02.069.

[66] B. A. Salau, A. Rawal, and D. B. Rawat, "Recent Advances in Artificial Intelligence for Wireless Internet of Things and Cyber–Physical Systems: A Comprehensive Survey," *IEEE Internet Things J*, vol. 9, no. 15, pp. 12916–12930, Aug. 2022. doi: 10.1109/JIOT.2022.3170449.

[67] H. Hua, Y. Li, T. Wang, N. Dong, W. Li, and J. Cao, "Edge Computing with Artificial Intelligence: A Machine Learning Perspective," *ACM Comput Surv*, vol. 55, no. 9, pp. 1–35, Sep. 2023. doi: 10.1145/3555802.

[68] R. Pasumarty, R. Praveen, and M. T. R, "The Future of AI-enabled servers in the cloud- A Survey," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Nov. 2021, pp. 578–583. doi: 10.1109/I-SMAC52330.2021.9640925.

[69] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs)," *Vehicular Communications*, vol. 34, p. 100403, Apr. 2022. doi: 10.1016/j.vehcom.2021.100403.

[70] S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review," *IEEE Sens J*, vol. 21, no. 22, pp. 24920–24932, Nov. 2021. doi: 10.1109/JSEN.2021.3055618.

[71] T. Galanti, G. Guidetti, E. Mazzei, S. Zappalà, and F. Toscano, "Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement, and stress," *J. Occup. Environ. Med.*, vol. 63, no. 7, pp. E426–E432, Jul. 2021, doi: 10.1097/JOM.0000000000002236.

[72] R. Ratan, D. B. Miller, and J. N. Bailenson, "Facial Appearance Dissatisfaction Explains Differences in Zoom Fatigue," *Cyberpsychol. Behav. Soc. Netw.*, vol. 25, no. 2, pp. 124–129, Feb. 2022, doi: 10.1089/cyber.2021.0112.

[73] S. K. Jagatheesaperumal, K. Ahmad, A. Al-Fuqaha, and J. Qadir, "Advancing Education Through Extended Reality and Internet of Everything Enabled Metaverses: Applications, Challenges, and Open Issues," Jun. 2022. [Online]. Available: http://arxiv.org/abs/2207.01512

[74] R. Chengoden et al., "Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions," vol. 4, 2016, doi: 10.1109/ACCESS.2017.DOI.

[75] G. Bansal, K. Rajgopal, V. Chamola, Z. Xiong, and D. Niyato, "Healthcare in Metaverse: A Survey On Current Metaverse Applications in Healthcare," *IEEE Access*, pp. 1–1, Nov. 2022, doi: 10.1109/ACCESS.2022.3219845.

[76] H. Liu, Z. Wang, C. Mousas, and D. Kao, "Virtual Reality Racket Sports: Virtual Drills for Exercise and Training," in *2020 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, IEEE, Nov. 2020, pp. 566–576, doi: 10.1109/ISMAR50242.2020.00084.

[77] F. Pallavicini, L. Argenton, N. Toniazzi, L. Aceti, and F. Mantovani, "Virtual Reality Applications for Stress Management Training in the Military," *Aerosp. Med. Hum. Perform.*, vol. 87, no. 12, pp. 1021–1030, Dec. 2016, doi: 10.3357/AMHP.4596.2016.

[78] S. G. Wheeler, H. Engelbrecht, and S. Hoermann, "Human Factors Research in Immersive Virtual Reality Firefighter Training: A Systematic Review," *Front. Virtual Real.*, vol. 2, Oct. 2021, doi: 10.3389/frvir.2021.671664.

[79] E. Cetinic and J. She, "Understanding and Creating Art with AI: Review and Outlook," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 18, no. 2, May 2022, doi: 10.1145/3475799.

[80] A. Duggal, M. Gupta, and D. Gupta, "Significance of NFT Avatars in Metaverse and their Promotion: Case Study," *Scientific Journal of Metaverse and Blockchain Technologies*, vol. 1, no. 1, pp. 28–36, 2023, doi: 10.36676/sjmbt.v1i1.04.

[81] M. Zuckerberg, "Founder's Letter, 2021," Meta. Accessed: Sep. 12, 2022. [Online]. Available: https://about.fb.com/news/2021/10/founders-letter/

[82] Meta, "Privacy Policy," 2023. [Online]. Available: https://www.meta.com/legal/privacy-policy/. [Accessed: Jul.10, 2024].

[83] Microsoft, "What is Microsoft's Metaverse?," (Nov. 03, 2021). Accessed: Sep. 19, 2022. [Online Video]. Available: https://youtu.be/Qw6UCwCt4bE

[84] C. Bell, "The metaverse is coming. Here are the cornerstones for securing it.," Mar. 2022.

[85] NVIDIA Studio, "What is NVIDIA's Omniverse?," (Feb. 01, 2022). Accessed: Aug. 17, 2022. [Online Video]. Available: https://youtu.be/dvdB-ndYJBM

[86] Nvidia, "Modernize Cybersecurity with AI," https://www.nvidia.com/en-us/industries/cybersecurity/.

[87] J. Porter, "Tim Cook is latest CEO to question the 'metaverse,'" *The Verge*. Accessed: Feb. 01, 2023. [Online]. Available: https://www.theverge.com/2022/10/3/23384708/tim-cook-metaverse-skeptical-meta-ar-vr-headset

[88] Adobe, "Metaverses and other shared immersive experiences.," Adobe. Accessed: Jan. 01, 2023. [Online]. Available: https://www.adobe.com/content/dam/cc/us/en/metaverse/metaverse-whitepaper-and-immersive-experiences.pdf

[89] "Cloud Service Security Overview," *Adobe Experience Manager Cloud Service Documentation*. [Online]. Available: https://experienceleague.adobe.com/en/docs/experience-manager-cloud-service/content/security/cloud-service-security-overview. [Accessed: 19-December-2023].

[90] CNBC Television, "We're the underlying tool set for creating the metaverse: Unity CEO," (Nov. 10, 2021). Accessed: Feb. 01, 2032. [Online Video]. Available: https://youtu.be/1rRIL8wzihg

[91] VentureBeat, "Why We Need an Open Metaverse," (Jan. 22, 2022). Accessed: Dec. 12, 2022. [Online Video]. Available: https://vimeo.com/764001039

[92] Epic Games, "The LEGO Group and Epic Games Team Up to Build a Place for Kids to Play in the Metaverse," Epic Games. Accessed: Sep. 12, 2022. [Online]. Available: https://www.epicgames.com/site/en-US/news/the-lego-group-and-epic-games-team-up-to-build-a-place-for-kids-to-play-in-the-metaverse

[93] B. Marr, "The Amazing Ways Nike Is Using The Metaverse, Web3 And NFTs," *Forbes*. Accessed: Mar. 01, 2023. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2022/06/01/the-amazing-ways-nike-is-using-the-metaverse-web3-and-nfts/?sh=71cf60af56e9

[94] F. Noorbehbahani and M. Saberi, "Ransomware Detection with Semi-Supervised Learning," *in 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE)*, IEEE, Oct. 2020, pp. 024–029. doi: 10.1109/ICCKE50421.2020.9303689.

[95] Z. Zhang et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 55, no. 2, pp. 1029–1053, Feb. 2022, doi: 10.1007/s10462-021-09976-0.

[96] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey," *IEEE Access*, vol. 10, pp. 93575–93600, 2022, doi: 10.1109/ACCESS.2022.3204171.

[97] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022, doi: 10.1109/ACCESS.2022.3204051.

[98] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE, May 2018, pp. 371–390. doi: 10.23919/CYCON.2018.8405026.

[99] M. R. Dileep, A. V Navaneeth, and M. Abhishek, "A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, Feb. 2021, pp. 1025–1028. doi: 10.1109/ICICV50876.2021.9388431.

[100] A. Ahmed Fazal and M. Daud, "Detecting Phishing Websites using Decision Trees: A Machine Learning Approach," *International Journal for Electronic Crime Investigation*, vol. 7, no. 2, Jul. 2023, doi: 10.54692/ijeci.2023.0702155.

[101] H. Han, S. Lim, K. Suh, S. Park, S. Cho, and M. Park, "Enhanced Android Malware Detection: An SVM-Based Machine Learning Approach," in *2020 IEEE International Conference on Big Data and Smart Computing (BigComp)*, IEEE, Feb. 2020, pp. 75–81. doi: 10.1109/BigComp48618.2020.00-96.

[102] B. Liu et al., "An Approach Based on the Improved SVM Algorithm for Identifying Malware in Network Traffic," *Security and Communication Networks*, vol. 2021, pp. 1–14, Apr. 2021, doi: 10.1155/2021/5518909.

[103] I. Shhadat, B. Bataineh, A. Hayajneh, and Z. A. Al-Sharif, "The Use of Machine Learning Techniques to Advance the Detection and Classification of Unknown Malware," *Procedia Comput. Sci.*, vol. 170, pp. 917–922, 2020, doi: 10.1016/j.procs.2020.03.110.

[104] A. Mustafa Hilal et al., "Malware Detection Using Decision Tree Based SVM Classifier for IoT," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 713–726, 2022, doi: 10.32604/cmc.2022.024501.

[105] R. K. Pareriya, P. Verma, and P. Suhana, "An Ensemble Xgboost Approach for the Detection of Cyber-Attacks in the Industrial IoT Domain," in *Big Data Analytics in Fog-Enabled IoT Networks*, Boca Raton: CRC Press, 2023, pp. 125–140. doi: 10.1201/9781003264545-6.

[106] R. Golchha, A. Joshi, and G. P. Gupta, "Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things," *Procedia Comput. Sci.*, vol. 218, pp. 1752–1759, 2023, doi: 10.1016/j.procs.2023.01.153.

[107] P. Dixit and S. Silakari, "Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review," *Comput. Sci. Rev.*, vol. 39, p. 100317, Feb. 2021, doi: 10.1016/j.cosrev.2020.100317.

[108] M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber, "System log clustering approaches for cyber security applications: A survey," *Comput. Secur.*, vol. 92, p. 101739, May 2020, doi: 10.1016/j.cose.2020.101739.

[109] H. S. Mavikumbure, C. S. Wickramasinghe, D. L. Marino, V. Cobilean, and M. Manic, "Anomaly Detection in Critical-Infrastructures using Autoencoders: A Survey," in *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, Oct. 2022, pp. 1–7. doi: 10.1109/IECON49645.2022.9968505.

[110] I. K. Dutta, B. Ghosh, A. Carlson, M. Totaro, and M. Bayoumi, "Generative Adversarial Networks in Security: A Survey," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, Oct. 2020, pp. 0399–0405. doi: 10.1109/UEMCON51285.2020.9298135.

[111] M. E. Villa-Pérez, M. Á. Álvarez-Carmona, O. Loyola-González, M. A. Medina-Pérez, J. C. Velazco-Rossell, and K.-K. R. Choo, "Semi-supervised anomaly detection algorithms: A comparative summary and future research directions," *Knowl. Based Syst*, vol. 218, p. 106878, Apr. 2021, doi: 10.1016/j.knosys.2021.106878.

[112] A. Dairi, F. Harrou, B. Bouyeddou, S.-M. Senouci, and Y. Sun, "Semi-supervised Deep Learning-Driven Anomaly Detection Schemes for Cyber-Attack Detection in Smart Grids," *Power systems cybersecurity: Methods, concepts, and best practices*. Cham: Springer International Publishing, 2023, pp. 265–295. doi: 10.1007/978-3-031-20360-2_11.

[113] G. Kaiafas, C. Hammerschmidt, S. Lagraa, and R. State, "Auto Semi-supervised Outlier Detection for Malicious Authentication Events," 2020, pp. 176–190. doi: 10.1007/978-3-030-43887-6_14.

[114] D. C. Le, N. Zincir-Heywood, and M. Heywood, "Training regime influences to semi-supervised learning for insider threat detection," in *2021 IEEE Security and Privacy Workshops (SPW)*, IEEE, May 2021, pp. 13–18. doi: 10.1109/SPW53761.2021.00010.

[115] M. Sewak, S. K. Sahay, and H. Rathore, "Deep Reinforcement Learning for Cybersecurity Threat Detection and Protection: A Review," 2022, pp. 51–72. doi: 10.1007/978-3-030-97532-6_4.

[116] A. M. K. Adawadkar and N. Kulkarni, "Cyber-security and reinforcement learning — A brief survey," *Eng Appl Artif Intell*, vol. 114, p. 105116, Sep. 2022, doi: 10.1016/j.engappai.2022.105116.

[117] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated Learning for Internet of Things: A Comprehensive Survey," *Institute of Electrical and Electronics Engineers Inc.*, Jul. 01, 2021, doi: 10.1109/COMST.2021.3075439.

[118] Y. Chen, S. Huang, W. Gan, G. Huang, and Y. Wu, "Federated Learning for Metaverse: A Survey," in *Companion Proceedings of the ACM Web Conference 2023*, New York, NY, USA: ACM, Apr. 2023, pp. 1151–1160. doi: 10.1145/3543873.3587584.

[119] Federal Bureau of Investigation, "Internet Crime Report," 2021. [Online]. Available: www.ic3.gov.

[120] H. S. Lallie et al., "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," Jun. 2020, doi: 10.1016/j.cose.2021.102248.

[121] J. Happa, M. Glencross, and A. Steed, "Cyber Security Threats and Challenges in Collaborative Mixed-Reality," *Frontiers in ICT*, vol. 6, Apr. 2019, doi: 10.3389/fict.2019.00005.

[122] S. Valluripally, A. Gulhane, K. A. Hoque, and P. Calyam, "Modeling and Defense of Social Virtual Reality Attacks Inducing Cybersickness," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 6, pp. 4127–4144, Nov. 2022, doi: 10.1109/TDSC.2021.3121216.

[123] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," *Journal of Information Security and Applications*, vol. 57, p. 102722, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.

[124] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The Emerging Threat of AI-driven Cyber Attacks: A Review," *Applied Artificial Intelligence*, vol. 36, no. 1, Dec. 2022, doi: 10.1080/08839514.2022.2037254.

[125] N. Huq, R. Reyes, P. Lin, and M. Swimmer, "METAVERSE OR METAWORSE?"

[126] F. Khan, J. H. Kim, R. Moore, and L. Mathiassen, "Data Breach Risks and Resolutions: A Literature Synthesis Completed Research Full Papers," 2019.

[127] S. Zulfqar, "Companies That Encountered a Data Breach Horror Story," *Scoopearth*. Accessed: Jan. 04, 2023. [Online]. Available: https://www.scoopearth.com/companies-that-encountered-a-data-breach-horror-story/

[128] E. Auchard, "Second Life suffers security breach," *NBC News*. Accessed: Dec. 15, 2022. [Online]. Available: https://www.nbcnews.com/id/wbna14783327

[129] A. K. Pandey et al., "Key Issues in Healthcare Data Integrity: Analysis and Recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020, doi: 10.1109/ACCESS.2020.2976687.

[130] P. Casey, I. Baggili, and A. Yarramreddy, "Immersive Virtual Reality Attacks and the Human Joystick," *IEEE Trans Dependable Secure Comput*, vol. 18, no. 2, pp. 550–562, Mar. 2021, doi: 10.1109/TDSC.2019.2907942.

[131] P. Neekhara et al., "Adversarial Threats to DeepFake Detection: A Practical Perspective." [Online]. Available: https://deepfakeattacks.github.io/

[132] E. Holm and M. Helen, "Social networking and identity theft in the digital society," 2014. [Online]. Available: http://epublications.bond.edu.au/law_pubs/722

[133] P. Pointner, "Smart, Reusable and Secure: The Future of Digital Identity," *Jumio*. Accessed: Nov. 19, 2022. [Online]. Available: https://www.jumio.com/smart-reusable-secure-digital-identity/

[134] Y. Wang et al., "A Survey on Metaverse: Fundamentals, Security, and Privacy," Mar. 2022, doi: 10.1109/COMST.2022.3202047.

[135] K. D. Martin and P. E. Murphy, "The role of data privacy in marketing," *J Acad Mark Sci*, vol. 45, no. 2, pp. 135–155, Mar. 2017, doi: 10.1007/s11747-016-0495-4.

[136] A. Dzedzickis, A. Kaklauskas, and V. Bucinskas, "Human emotion recognition: Review of sensors and methods," *MDPI AG*, Feb. 01, 2020, doi: 10.3390/s20030592.

[137] Meta, "Meta Connect Keynote 2022," (Oct. 11, 2022). Accessed: Jan. 10, 2023. [Online Video]. Available: https://youtu.be/hvfV-iGwYX8

[138] VR Quickie, "Joe Rogan Tells Mark Zuckerberg His New Quest Pro VR Headset is Creepy," (Aug. 31, 2022). Accessed: Jan. 12, 2023. [Online Video]. Available: https://youtu.be/rgh3ELuDZGY

[139] Meta, "Supplemental Meta Platforms Technologies Privacy Policy," Accessed: Mar. 08, 2023. [Online]. Available: https://www.meta.com/legal/quest/privacy-policy/?ref=shareable&utm_source=srt.facebook.com&utm_medium=dollyredirect

[140] V. Rohokale and R. Prasad, "Cyber Security for Intelligent World with Internet of Things and Machine to Machine Communication," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 23–40, 2015, doi: 10.13052/jcsm2245-1439.412.

[141] H. Webb, N. Savage, and P. Millard, "Arguments For Anonymity," 2015.

[142] BBC, "Female avatar sexually assaulted in Meta VR platform, campaigners say," *BBC News*, May 25, 2022. Accessed: Jan. 17, 2023. [Online]. Available: https://www.bbc.com/news/technology-61573661

[143] B. Falchuk, S. Loeb, and R. Neff, "The Social Metaverse: Battle for Privacy," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, Jun. 2018, doi: 10.1109/MTS.2018.2826060.

[144] A. Giaretta, "Security and Privacy in Virtual Reality -- A Literature Survey," Apr. 2022. [Online]. Available: http://arxiv.org/abs/2205.00208

[145] W. J. Tseng et al., "The Dark Side of Perceptual Manipulations in Virtual Reality," in *Conf. Hum. Factors Comput. Syst. - Proc.*, Assoc. Comput. Mach., Apr. 2022, doi: 10.1145/3491102.3517728.

[146] C. B. Fernandez and P. Hui, "Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse," Mar. 2022. [Online]. Available: http://arxiv.org/abs/2204.01480

[147] Trend Micro, "Into the Darkverse: Exploring the Dark Side of the Metaverse," Aug. 08, 2022. Accessed: Aug. 11, 2022. [Online Video]. Available: https://youtu.be/mcYCvOHhr90

[148] World Economic Forum, "Shaping a Shared Future: Making the Metaverse | Davos | #WEF22," May 25, 2022. Accessed: May 12, 2022. [Online Video]. Available: https://youtu.be/XZAjv3MbCK4

[149] S. Kasiyanto and M. R. Kilinc, "Legal Conundrums of the Metaverse," *J. Cent. Bank. Law Inst.*, vol. 1, no. 2, May 2022, doi: 10.21098/jcli.v1i2.25.

[150] P. Ian Hargreaves, "Digital Opportunity: A Review of Intellectual Property and Growth: An Independent Report by Professor Ian Hargreaves," 2011.

[151] M. Conrad, "Non-Fungible Tokens, Sports, and Intellectual Property Law Issues: A Case Study Applying Copyright, Trademark, and Right of Publicity Law to a Non-Traditional Ownership Vehicle," *J. Leg. Aspects Sport*, vol. 32, no. 1, pp. 132–152, Feb. 2022, doi: 10.18060/26091.

[152] M. Yoder and A. Opensea, "An 'OpenSea' of Infringement: The Intellectual Property Implications of NFTs," 2022.

[153] "The Right of Publicity: Likeness Lawsuits Against Video Game Companies," *Berkeley Technol. Law J.* Accessed: Mar. 12, 2023. [Online]. Available: https://btlj.org/2014/12/the-right-of-publicity-likeness-lawsuits-against-video-game-companies/.

[154] R. Belk, M. Humayun, and M. Brouard, "Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3, and Wild Markets," *J. Bus. Res.*, vol. 153, pp. 198–205, Dec. 2022, doi: 10.1016/j.jbusres.2022.08.031.

[155] K. Christodoulou, L. Katelaris, M. Themistocleous, P. Christodoulou, and E. Iosif, "NFTs and the Metaverse Revolution: Research Perspectives and Open Challenges," 2022, pp. 139–178, doi: 10.1007/978-3-030-95108-5_6.

[156] Y. Dong and C. Wang, "Copyright protection on NFT digital works in the Metaverse," *Security Saf.*, vol. 2, p. 2023013, Jun. 2023, doi: 10.1051/sands/2023013.

[157] D. Chun, "When the NFT Hype Settles, What Is Left beyond Profile Pictures? A Critical Review on the Impact of Blockchain Technologies in the Art Market," *Arts*, vol. 12, no. 5, p. 181, Aug. 2023, doi: 10.3390/arts12050181.

[158] Q. Xie, S. Muralidharan, and S. M. Edwards, "Who will buy the idea of non-fungible token (NFT) marketing? Understanding consumers' psychological tendencies and value perceptions of branded NFTs," *Int. J. Advert.*, pp. 1–29, Sep. 2023, doi: 10.1080/02650487.2023.2262859.

[159] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," May 2021. [Online]. Available: http://arxiv.org/abs/2105.07447.

[160] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding Security Issues in the NFT Ecosystem," Nov. 2021. [Online]. Available: http://arxiv.org/abs/2111.08893.

[161] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula, and Z. Cai, "A survey on blockchain systems: Attacks, defenses, and privacy preservation," *High-Confid. Comput.*, vol. 2, no. 2, Jun. 2022, doi: 10.1016/j.hcc.2021.100048.

[162] R. Brandon, "$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users," *The Verge*. Accessed: Jul. 12, 2022. [Online]. Available: https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft.

[163] S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart Contract: Attacks and Protections," *IEEE Access*, vol. 8, pp. 24416–24427, 2020, doi: 10.1109/ACCESS.2020.2970495.

[164] R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, Institute of Electrical and Electronics Engineers Inc., Jan. 2017, pp. 143–148. doi: 10.1109/CCAA.2016.7813706.

[165] M. A. Ferrag et al., "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.

[166] H. Rezaeighaleh and C. C. Zou, "Deterministic sub-wallet for cryptocurrencies," in *Proc. 2019 2nd IEEE Int. Conf. on Blockchain, Blockchain 2019*, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 419–424, doi: 10.1109/Blockchain.2019.00064.

[167] R. Sharma, "Bitcoin Gold Hack Shows 51% Attack Is Real," *Investopedia*. Accessed: Jan. 12, 2023. [Online]. Available: https://www.investopedia.com/news/bitcoin-gold-hack-shows-51-attack-real/

[168] P. Nahar, "What are 51% attacks in cryptocurrencies?," *The Economic Times*. Accessed: Mar. 12, 2023. [Online]. Available: https://economictimes.indiatimes.com/markets/cryptocurrency/what-are-51-attacks-in-cryptocurrencies/articleshow/85802504.cms?from=mdr

[169] C. Porterfield, "Beeple's Followers Lose $438,000 To Phishing Scam After NFT Artist's Twitter Gets Hacked," *Forbes*. Accessed: Mar. 12, 2023. [Online]. Available: https://www.forbes.com/sites/carlieporterfield/2022/05/23/beeples-followers-lose-438000-to-phishing-scam-after-nft-artists-twitter-gets-hacked/?sh=1dbc967d1332

[170] C. Townsend, "Bored Ape Yacht Club hacked, loses $360,000 worth of NFTs in phishing attack," *Mashable Middle East*. Accessed: Mar. 12, 2023. [Online]. Available: https://me.mashable.com/tech/17283/bored-ape-yacht-club-hacked-loses-360000-worth-of-nfts-in-phishing-attack

[171] N. Kshetri, "Scams, Frauds, and Crimes in the Nonfungible Token Market," *Computer (Long Beach Calif)*, vol. 55, no. 4, pp. 60–64, Apr. 2022, doi: 10.1109/MC.2022.3144763.

[172] Ola, "Doctor Troller of The Shifters NFT Says Hackers Stole $2M from Discord Members," *NFT Evening*. Accessed: Mar. 12, 2023. [Online]. Available: https://nftevening.com/doctor-troller-of-the-shifters-nft-says-hackers-stole-2m-from-discord-members/

[173] K. Eledlebi et al., "Cyber-Security Measure and Application Opportunities in the Metaverse Environment," in *Breakthroughs in Digital Biometrics and Forensics*, Cham: Springer International Publishing, 2022, pp. 213–240, doi: 10.1007/978-3-031-10706-1_10.

[174] M. Kim, J. Suh, and H. Kwon, "A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures," in *2022 IEEE/ACIS 7th Int. Conf. on Big Data, Cloud Computing, and Data Science (BCD)*, IEEE, Aug. 2022, pp. 240–245, doi: 10.1109/BCD54882.2022.9900510.

[175] A. Ometov et al., "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1–31, Mar. 2018, doi: 10.3390/cryptography2010001.

[176] M. P. Manggala, I. Wahidah, and A. T. Hanuranto, "Security And Usability of User Authentication for Fintech Data Protection in Indonesia," in *2022 Int. Conf. on Decision Aid Sciences and Applications (DASA)*, IEEE, Mar. 2022, pp. 546–550, doi: 10.1109/DASA54658.2022.9765272.

[177] L. Hernández-Álvarez et al., "Biometrics and Artificial Intelligence: Attacks and Challenges," in *Breakthroughs in Digital Biometrics and Forensics*, Cham: Springer International Publishing, 2022, pp. 213–240, doi: 10.1007/978-3-031-10706-1_10.

[178] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," *in 2013 IEEE Int. Conf. on Computational Intelligence and Computing Research*, IEEE, Dec. 2013, pp. 1–7, doi: 10.1109/ICCIC.2013.6724278.

[179] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 112505–112519, 2019, doi: 10.1109/ACCESS.2019.2932400.

[180] S. W. Shah and S. S. Kanhere, "Recent Trends in User Authentication - A Survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019, doi: 10.1109/ACCESS.2019.2932400.

[181] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimed Tools Appl*, vol. 79, no. 37–38, pp. 27721–27776, Oct. 2020, doi: 10.1007/s11042-020-09197-7.

[182] S. Arora and M. P. S. Bhatia, "Challenges and opportunities in biometric security: A survey," *Information Security Journal: A Global Perspective*, vol. 31, no. 1, pp. 28–48, Jan. 2022, doi: 10.1080/19393555.2021.1873464.

[183] M. Papathanasaki, L. Maglaras, and N. Ayres, "Modern Authentication Methods: A Comprehensive Survey," *AI, Computer Science and Robotics Technology*, vol. 2022, pp. 1–24, Jun. 2022, doi: 10.5772/acrt.08.

[184] M. M. H. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, "Overview of fingerprint recognition system," in *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, Institute of Electrical and Electronics Engineers Inc., Nov. 2016, pp. 1334–1338, doi: 10.1109/ICEEOT.2016.7754900.

[185] I. D. Raji and G. Fried, "About Face: A Survey of Facial Recognition Evaluation," 2021. [Online]. Available: www.aaai.org

[186] C. N. W. Geraets et al., "Virtual reality facial emotion recognition in social environments: An eye-tracking study," *Internet Interv*, vol. 25, Sep. 2021, doi: 10.1016/j.invent.2021.100432.

[187] U. Ciftci, X. Zhang, and L. Tin, "Partially occluded facial action recognition and interaction in virtual reality applications," in *2017 IEEE International Conference on Multimedia and Expo (ICME)*, IEEE, Jul. 2017, pp. 715–720, doi: 10.1109/ICME.2017.8019545.

[188] B. Houshmand and N. Mefraz Khan, "Facial Expression Recognition Under Partial Occlusion from Virtual Reality Headsets based on Transfer Learning," in *2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM)*, IEEE, Sep. 2020, pp. 70–75, doi: 10.1109/BigMM50055.2020.00020.

[189] L. Wen, J. Zhou, W. Huang, and F. Chen, "A Survey of Facial Capture for Virtual Reality," 2022, Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ACCESS.2021.3138200.

[190] P. Kaur, K. Krishan, S. K. Sharma, and T. Kanchan, "Facial-recognition algorithms: A literature review," *Med Sci Law*, vol. 60, no. 2, pp. 131–139, Apr. 2020, doi: 10.1177/0025802419893168.

[191] R. Saini and N. Rana, "COMPARISON OF VARIOUS BIOMETRIC METHODS," 2014. [Online]. Available: www.sciencepublication.org

[192] M. Jenadeleh, M. Pedersen, and D. Saupe, "Blind quality assessment of iris images acquired in visible light for biometric recognition," *Sensors (Switzerland)*, vol. 20, no. 5, Mar. 2020, doi: 10.3390/s20051308.

[193] E. Ribeiro, A. Uhl, and F. Alonso-Fernandez, "Iris super-resolution using CNNs: Is photo-realism important to iris recognition?," *IET Biom*, vol. 8, no. 1, pp. 69–78, Jan. 2019, doi: 10.1049/iet-bmt.2018.5146.

[194] S. Jamaludin, N. Zainal, and W. M. D. W. Zaki, "Deblurring of noisy Iris images in Iris recognition," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 156–159, Feb. 2021, doi: 10.11591/eei.v10i1.2467.

[195] "AR/VR Headset," *Pixsur*.

[196] R. Ajmeria et al., "A Critical Survey of EEG-Based BCI Systems for Applications in Industrial Internet of Things," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 184–212, 2023, doi: 10.1109/COMST.2022.3232576.

[197] H. Y. Zhu, N. Q. Hieu, D. T. Hoang, D. N. Nguyen, and C.-T. Lin, "A Human-Centric Metaverse Enabled by Brain-Computer Interface: A Survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024, doi: 10.1109/COMST.2024.3387124.

[198] T. Bin Shams, M. S. Hossain, M. F. Mahmud, M. S. Tehjib, Z. Hossain, and M. I. Pramanik, "EEG-based Biometric Authentication Using Machine Learning: A Comprehensive Survey," *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 20, no. 2, pp. 225–241, Jun. 2022, doi: 10.37936/ecti-eec.2022202.246906.

[199] H. Nee. Oon, A. Saidatul, and Z. Ibrahim, "Analysis on Non-Linear Features of Electroencephalogram (EEG) Signal for Neuromarketing Application," in *2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA)*, pp. 1–8, 2018.

[200] C. A. Frantzidis, C. Bratsas, C. L. Papadelis, E. Konstantinidis, C. Pappas, and P. D. Bamidis, "Toward Emotion Aware Computing: An Integrated Approach Using Multichannel Neurophysiological Recordings and Affective Visual Stimuli," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 3, pp. 589–597, May 2010, doi: 10.1109/TITB.2010.2041553.

[201] A. Jalaly Bidgoly, H. Jalaly Bidgoly, and Z. Arezoumand, "A survey on methods and challenges in EEG based authentication," *Elsevier Ltd*, Jun. 01, 2020, doi: 10.1016/j.cose.2020.101788.

[202] M. Zeynali and H. Seyedarabi, "EEG-based single-channel authentication systems with optimum electrode placement for different mental activities," *Biomed J*, vol. 42, no. 4, pp. 261–267, Aug. 2019, doi: 10.1016/j.bj.2019.03.005.

[203] M. A. Hendrawan, P. Y. Saputra, and C. Rahmad, "Identification of optimum segment in single channel EEG biometric system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 3, pp. 1847–1854, Sep. 2021, doi: 10.11591/ijeecs.v23.i3.pp1847-1854.

[204] Universitas Pembangunan Nasional "Veteran" Jawa Timur and Institute of Electrical and Electronics Engineers, "Proceedings, 2021 IEEE 7th Information Technology International Seminar (ITIS): October 6th-8th, 2021, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia," *IEEE*, 2022, pp. 307–311, doi: 10.1109/ITIS57155.2022.10010103.

[205] S. Li, S. Savaliya, L. Marino, A. M. Leider, and C. C. Tappert, "Brain Signal Authentication for Human-Computer Interaction in Virtual Reality," in *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, 2019, pp. 115–120, doi: 10.1109/CSE/EUC.2019.00031.

[206] J. S. Arteaga-Falconi, H. al Osman, and A. el Saddik, "ECG Authentication for Mobile Devices," *IEEE Trans Instrum Meas*, vol. 65, no. 3, pp. 591–600, Mar. 2016, doi: 10.1109/TIM.2015.2503863.

[207] A. N. Uwaechia and D. A. Ramli, "A Comprehensive Survey on ECG Signals as New Biometric Modality for Human Authentication: Recent Advances and Future Challenges," *Institute of Electrical and Electronics Engineers Inc.*, 2021, doi: 10.1109/ACCESS.2021.3095248.

[208] Z. Zhao, Y. Zhang, Y. Deng, and X. Zhang, "ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation," *Comput Biol Med*, vol. 102, pp. 168–179, 2018, doi: 10.1016/j.compbiomed.2018.09.027.

[209] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, "ECG Biometric Authentication: A Comparative Analysis," *IEEE Access*, vol. 8, pp. 117853–117866, 2020, doi: 10.1109/ACCESS.2020.3004464.

[210] H. Hwang, H. Kwon, B. Chung, J. Lee, and I. Kim, "Ecg authentication based on non-linear normalization under various physiological conditions," *Sensors*, vol. 21, no. 21, Nov. 2021, doi: 10.3390/s21216966.

[211] M. R. Bogdanov, A. S. Filippova, G. R. Shakhmametova, and N. N. Oskin, "Biometric Authentication Based on Electrocardiogram," in *Biometric Systems*, M. Sarfraz, Ed., Rijeka: IntechOpen, 2020, ch. 2, doi: 10.5772/intechopen.91172.

[212] S. K. Kim, C. Y. Yeun, E. Damiani, and N. W. Lo, "A machine learning framework for biometric authentication using electrocardiogram," *IEEE Access*, vol. 7, pp. 94858–94868, 2019, doi: 10.1109/ACCESS.2019.2927079.

[213] G. V, V. K, S. T, S. S, I. Niranjana. M, and A. L. L R, "PPG Based Biometric Authentication System," in *2024 International Conference on Science Technology Engineering and Management (ICSTEM)*, IEEE, Apr. 2024, pp. 1–5, doi: 10.1109/ICSTEM61137.2024.10561095.

[214] L. Li et al., "A Survey of PPG's Application in Authentication," *Comput Secur*, vol. 135, p. 103488, Dec. 2023, doi: 10.1016/j.cose.2023.103488.

[215] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, "TrueHeart: Continuous Authentication on Wrist-worn Wearables Using PPG-based Biometrics," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, IEEE, Jul. 2020, pp. 30–39, doi: 10.1109/INFOCOM41043.2020.9155526.

[216] H. A. Aly and R. Di Pietro, "PulseOblivion: An Effective Session-Based Continuous Authentication Scheme Using PPG Signals," *IEEE Access*, vol. 11, pp. 124213–124227, 2023, doi: 10.1109/ACCESS.2023.3329993.

[217] "Voice Authentication," *Aware, Inc.* [Online]. Available: https://www.aware.com/voice-authentication/. [Accessed: 09-Jan-2024].

[218] S. K. Choudhary and A. K. Naik, "Multimodal Biometric Authentication with Secured Templates — A Review," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, Apr. 2019, pp. 1062–1069, doi: 10.1109/ICOEI.2019.8862563.

[219] U. Gawande and Y. Golhar, "Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques," *Int J Biom*, vol. 10, no. 2, pp. 142–175, 2018, doi: 10.1504/IJBM.2018.091629.

[220] A. F. Baig and S. Eskeland, "Security, privacy, and usability in continuous authentication: A survey," *MDPI*, Sep. 01, 2021, doi: 10.3390/s21175967.

[221] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in Internet of Things environment," *Elsevier B.V.*, Nov. 01, 2020, doi: 10.1016/j.comcom.2020.09.006.

[222] R. Ryu, S. Yeom, S. H. Kim, and D. Herbert, "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review," *Institute of Electrical and Electronics Engineers Inc.*, 2021, doi: 10.1109/ACCESS.2021.3061589.

[223] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," *J Ambient Intell Humaniz Comput*, vol. 10, no. 11, pp. 4417–4430, Nov. 2019, doi: 10.1007/s12652-018-1123-6.

[224] S. Wang, J. Yuan, and S. Chen, "Quality-based Score Level Fusion for Continuous Authentication with Motion Sensor and Face," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, New York, NY, USA: ACM, Jan. 2020, pp. 58–62, doi: 10.1145/3377644.3377647.

[225] S. Mekruksavanich and A. Jitpattanakul, "Deep learning approaches for continuous authentication based on activity patterns using mobile sensing," *Sensors*, vol. 21, no. 22, Nov. 2021, doi: 10.3390/s21227519.

[226] W. Cheung and S. Vhaduri, "Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data," in *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 2020, pp. 587–592, doi: 10.1109/BioRob49111.2020.9224356.

[227] B. A. El-Rahiem, F. E. A. El-Samie, and M. Amin, "Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein," in *Multimedia Systems*, Springer Science and Business Media Deutschland GmbH, Aug. 2022, pp. 1325–1337, doi: 10.1007/s00530-021-00810-9.

[228] F. Ahamed, F. Farid, B. Suleiman, Z. Jan, L. A. Wahsheh, and S. Shahrestani, "An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services," *Future Internet*, vol. 14, no. 8, Aug. 2022, doi: 10.3390/fi14080222.

[229] V. Krishna, Y. Ding, A. Xu, and T. Höllerer, "Multimodal Biometric Authentication for VR/AR using EEG and Eye Tracking," in *Adjunct of the 2019 International Conference on Multimodal Interaction*, ICMI 2019, Association for Computing Machinery, Inc, Oct. 2019, doi: 10.1145/3351529.3360655.

[230] F. Boutros, N. Damer, K. Raja, R. Ramachandra, F. Kirchbuchner, and A. Kuijper, "Iris and periocular biometrics for head mounted displays: Segmentation, recognition, and synthetic data generation," *Image Vis Comput*, vol. 104, Dec. 2020, doi: 10.1016/j.imavis.2020.104007.

[231] A. Bhalla, I. Sluganovic, K. Krawiecka, and I. Martinovic, "MoveAR: Continuous Biometric Authentication for Augmented Reality Headsets," in *CPSS 2021 - Proceedings of the 7th ACM Cyber-Physical System Security Workshop*, Association for Computing Machinery, Inc, May 2021, pp. 41–52, doi: 10.1145/3457339.3457983.

[232] I. Olade, C. Fleming, and H. N. Liang, "Biomove: Biometric user identification from human kinesiological movements for virtual reality systems," *Sensors (Switzerland)*, vol. 20, no. 10, May 2020, doi: 10.3390/s20102944.

[233] S. Luo, A. Nguyen, C. Song, F. Lin, W. Xu, and Z. Yan, "OcuLock: Exploring Human Visual System for Authentication in Virtual Reality Head-mounted Display," *Internet Society*, Feb. 2020, doi: 10.14722/ndss.2020.24079.

[234] M. Sivasamy, V. N. Sastry, and N. P. Gopalan, "VRCAuth: Continuous Authentication of Users in Virtual Reality Environment Using Head-Movement," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2020, pp. 518–523, doi: 10.1109/ICCES48766.2020.9137914.

[235] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous Authentication Using Eye Movement Response of Implicit Visual Stimuli," *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 1, no. 4, pp. 1–22, Jan. 2018, doi: 10.1145/3161410.

[236] F. Boutros, N. Damer, K. Raja, R. Ramachandra, F. Kirchbuchner, and A. Kuijper, "On Benchmarking Iris Recognition within a Head-mounted Display for AR/VR Applications," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, 2020, pp. 1–10, doi: 10.1109/IJCB48548.2020.9304919.

[237] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4150.

[238] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Comput Commun*, vol. 49, pp. 1–17, Aug. 2014, doi: 10.1016/j.comcom.2014.04.012.

[239] M. Aljanabi, M. A. Ismail, and A. H. Ali, "Intrusion Detection Systems, Issues, Challenges, and Needs," *International Journal of Computational Intelligence Systems*, vol. 14, no. 1, p. 560, 2021, doi: 10.2991/ijcis.d.210105.001.

[240] V. T. Truong and L. B. Le, "Security for the Metaverse: Blockchain and Machine Learning Techniques for Intrusion Detection," *TechRxiv*, May 2023.

[241] H. Zhang, S. Lee, Y. Lu, X. Yu, and H. Lu, "A Survey on Big Data Technologies and Their Applications to the Metaverse: Past, Current and Future," *Mathematics*, vol. 11, no. 1, p. 96, Dec. 2022, doi: 10.3390/math11010096.

[242] Z. Lv, S. Xie, Y. Li, M. S. Hossain, and A. El Saddik, "Building the metaverse using digital twins at all scales, states, and relations," *Virtual Reality & Intelligent Hardware*, vol. 4, no. 6, pp. 459–470, Dec. 2022, doi: 10.1016/j.vrih.2022.06.005.

[243] A. Havele, N. Polys, W. Benman, and D. Brutzman, "The Keys to an Open, Interoperable Metaverse," in *The 27th International Conference on 3D Web Technology*, New York, NY, USA: ACM, Nov. 2022, pp. 1–7. doi: 10.1145/3564533.3564575.

[244] K. Rantos, A. Spyros, A. Papanikolaou, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem," *Computers*, vol. 9, no. 1, p. 18, Mar. 2020, doi: 10.3390/computers9010018.

[245] B. C. Ooi et al., "The Metaverse Data Deluge: What Can We Do About It?," in *2023 IEEE 39th International Conference on Data Engineering (ICDE)*, IEEE, Apr. 2023, pp. 3675–3687. doi: 10.1109/ICDE55515.2023.00296.

[246] M. Markevych and M. Dawson, "A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI)," *International conference KNOWLEDGE-BASED ORGANIZATION*, vol. 29, no. 3, pp. 30–37, Jun. 2023, doi: 10.2478/kbo-2023-0072.

[247] E. E. Abdallah, W. Eleisah, and A. F. Otoom, "Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey," *Procedia Comput Sci*, vol. 201, pp. 205–212, 2022, doi: 10.1016/j.procs.2022.03.029.

[248] O. G. Darley, A. A. Adenowo, and A. I. O. Yussuff, "Machine Learning Intrusion Detection as a Solution to Security and Privacy Issues in IoT: A Systematic Review," *FUOYE Journal of Engineering and Technology*, vol. 7, no. 2, pp. 148–156, Jun. 2022, doi: 10.46792/fuoyejet.v7i2.802.

[249] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions," *Security and Communication Networks*, vol. 2022, pp. 1–13, Jul. 2022, doi: 10.1155/2022/4016073.

[250] P. Vanin et al., "A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning," *Applied Sciences*, vol. 12, no. 22, p. 11752, Nov. 2022, doi: 10.3390/app122211752.

[251] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI based intrusion detection system," *Measurement: Sensors*, vol. 28, p. 100827, Aug. 2023, doi: 10.1016/j.measen.2023.100827.

[252] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection," *J Ind Inf Integr*, vol. 36, p. 100520, Dec. 2023, doi: 10.1016/j.jii.2023.100520.

[253] S. Ding, L. Kou, and T. Wu, "A GAN-Based Intrusion Detection Model for 5G Enabled Future Metaverse," *Mobile Networks and Applications*, vol. 27, no. 6, pp. 2596–2610, Dec. 2022, doi: 10.1007/s11036-022-02075-6.

[254] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: A Novel SDN Intrusion Dataset," *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.

[255] B. Bütün, A. T.-J. Akem, M. Gucciardo, and M. Fiore, "Fast Detection of Cyberattacks on the Metaverse through User-plane Inference," in *2023 IEEE International Conference on Metaverse Computing, Networking and*

Applications (MetaCom), IEEE, Jun. 2023, pp. 350–354. doi: 10.1109/MetaCom57706.2023.00067.

[256] V. Truong and L. B. Le, "MetaCIDS: A Metaverse Collaborative Intrusion Detection System based on Blockchain and Federated Learning," *TechRxiv*, 2023.

[257] V. T. Truong and L. B. Le, "MetaCIDS: Privacy-Preserving Collaborative Intrusion Detection for Metaverse based on Blockchain and Online Federated Learning," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 253–266, 2023, doi: 10.1109/OJCS.2023.3312299.

[258] S. He, C. Du, and M. S. Hossain, "6G-enabled Consumer Electronics Device Intrusion Detection with Federated Meta-Learning and Digital Twins in a Meta-Verse Environment," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023, doi: 10.1109/TCE.2023.3321846.

[259] X. Wu, Y. Yang, M. Bilal, L. Qi, and X. Xu, "6G-Enabled Anomaly Detection for Metaverse Healthcare Analytics in Internet of Things," *IEEE J Biomed Health Inform,* pp. 1–10, 2024, doi: 10.1109/JBHI.2023.3298092.

[260] A. H. Farooqi, S. Akhtar, H. Rahman, T. Sadiq, and W. Abbass, "Enhancing Network Intrusion Detection Using an Ensemble Voting Classifier for Internet of Things," *Sensors*, vol. 24, no. 1, p. 127, Dec. 2023, doi: 10.3390/s24010127.

[261] 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*, vol. 25, p. 101046, Apr. 2024, doi: 10.1016/j.iot.2023.101046.

[262] A. Leppla, J. Olmos, and J. Lamba, "Fraud Pattern Detection of NFT Markets," *SMU Data Science Review*, vol. 6, no. 2, 2022.

[263] M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the NFT revolution: market trends, trade networks, and visual features," *Sci Rep*, vol. 11, no. 1, p. 20902, Oct. 2021, doi: 10.1038/s41598-021-00053-8.

[264] M. Song, Y. Liu, A. Shah, and S. Chava, "Abnormal Trading Detection in the NFT Market," May 2023.

[265] S. S. Roy, D. Das, P. Bose, C. Kruegel, G. Vigna, and S. Nilizadeh, "Unveiling the Risks of NFT Promotion Scams," *ArXiv*, 2023.

[266] K. Pelechrinis, X. Liu, P. Krishnamurthy, and A. Babay, "Spotting anomalous trades in NFT markets: The case of NBA Topshot," *PLoS One*, vol. 18, no. 6, p. e0287262, Jun. 2023, doi: 10.1371/journal.pone.0287262.

[267] S. M. Y. Aks et al., "A Review of Blockchain for Security Data Privacy with Metaverse," in *2022 International Conference on ICT for Smart Society (ICISS)*, IEEE, Aug. 2022, pp. 1–5, doi: 10.1109/ICISS55894.2022.9915055.

[268] A. S. Rajawat et al., "Enhancing Security and Scalability of Metaverse with Blockchain-based Consensus Mechanisms," in *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE, Jun. 2023, pp. 01–06, doi: 10.1109/ECAI58194.2023.10194035.

[269] O. Bouachir, M. Aloqaily, F. Karray, and A. Elsaddik, "AI-based Blockchain for the Metaverse: Approaches and Challenges," in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, IEEE, Sep. 2022, pp. 231–236, doi: 10.1109/BCCA55292.2022.9922509.

[270] H. Jeon, H. Youn, S. Ko, and T. Kim, "Blockchain and AI Meet in the Metaverse," in *Blockchain Potential in AI*, IntechOpen, 2022, doi: 10.5772/intechopen.99114.

[271] M. Akpan and H. U. Ukwu, "Comprehensive analysis of non-fungible tokens valuation and accounting under IFRS: Challenges and artificial intelligence implications," *Risk Governance and Control: Financial Markets and Institutions*, vol. 13, no. 3, pp. 8–21, Aug. 2023, doi: 10.22495/rgcv13i3p1.

[272] M. Bhowmik, T. Sai Siri Chandana, and B. Rudra, "Comparative Study of Machine Learning Algorithms for Fraud Detection in Blockchain," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, IEEE, Apr. 2021, pp. 539–541, doi: 10.1109/ICCMC51019.2021.9418470.

[273] T. Ashfaq et al., "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism," *Sensors*, vol. 22, no. 19, p. 7162, Sep. 2022, doi: 10.3390/s22197162.

[274] Z. Cui, W. Chen, and Y. Chen, "Multi-Scale Convolutional Neural Networks for Time Series Classification," Mar. 2016.

[275] F. Jiang et al., "Enhancing Smart-Contract Security through Machine Learning: A Survey of Approaches and Techniques," *Electronics (Basel)*, vol. 12, no. 9, p. 2046, Apr. 2023, doi: 10.3390/electronics12092046.

[276] M. Krichen, "Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence," *Computers*, vol. 12, no. 5, p. 107, May 2023, doi: 10.3390/computers12050107.

[277] K. Kimura, M. Imamura, and K. Omote, "A Distributed Authenticity Verification Scheme Using Deep Learning for NFT Market," in *Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications*, New York, NY, USA: ACM, Dec. 2022, pp. 40–49, doi: 10.1145/3581971.3581977.

[278] A. T. Prihatno, N. Suryanto, S. Oh, T.-T.-H. Le, and H. Kim, "NFT Image Plagiarism Check Using EfficientNet-Based Deep Neural Network with Triplet Semi-Hard Loss," *Applied Sciences*, vol. 13, no. 5, p. 3072, Feb. 2023, doi: 10.3390/app13053072.

[279] A. T. Prihatno, N. Suryanto, H. T. Larasati, Y. E. Oktian, T.-T.-H. Le, and H. Kim, "A New Frontier in Digital Security: Verification for NFT Image Using Deep Learning-Based ConvNeXt Model in Quantum Blockchain," 2024, pp. 79–90, doi: 10.1007/978-981-99-8024-6_7.

[280] T. R. Gadekallu et al., "Blockchain for the Metaverse: A Review," Mar. 2022, *[Online]. Available: http://arxiv.org/abs/2203.09738*

[281] R. di Pietro and S. Cresci, "Metaverse: Security and Privacy Issues," 2021, *[Online]. Available: https://www.facebook.com/watch/live/?ref=watch*

[282] R. Zhao, Y. Zhang, Y. Zhu, R. Lan, and Z. Hua, "Metaverse: Security and Privacy Concerns," Mar. 2022, *[Online]. Available: http://arxiv.org/abs/2203.03854*

[283] C.-T. Chan, S.-H. Huang, and P. P. Choy, "Poisoning attacks on face authentication systems by using the generative deformation model," *Multimed Tools Appl*, vol. 82, no. 19, pp. 29457–29476, Aug. 2023, doi: 10.1007/s11042-023-14695-5.

[284] K. Li, C. Baird, and D. Lin, "Defend Data Poisoning Attacks on Voice Authentication," *IEEE Trans Dependable Secure Comput*, pp. 1–16, 2024, doi: 10.1109/TDSC.2023.3289446.

[285] Z. Zhang, S. Umar, A. Y. Al Hammadi, S. Yoon, E. Damiani, and C. Y. Yeun, "Data Poisoning Attacks on EEG Signal-based Risk Assessment Systems," Feb. 2023.

[286] N. Karimian, D. Woodard, and D. Forte, "ECG Biometric: Spoofing and Countermeasures," *IEEE Trans Biom Behav Identity Sci*, vol. 2, no. 3, pp. 257–270, Jul. 2020, doi: 10.1109/TBIOM.2020.2992274.

[287] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data Poisoning Attacks Against Federated Learning Systems," 2020, pp. 480–501, doi: 10.1007/978-3-030-58951-6_24.

[288] M. N. Al-Mhiqani et al., "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations," *Applied Sciences*, vol. 10, no. 15, p. 5208, Jul. 2020, doi: 10.3390/app10155208.

[289] A. Y. Al Hammadi et al., "Novel EEG Sensor-Based Risk Framework for the Detection of Insider Threats in Safety Critical Industrial Infrastructure," *IEEE Access*, vol. 8, pp. 206222–206234, 2020, doi: 10.1109/ACCESS.2020.3037979.

[290] Z. Ahmad and N. Khan, "A Survey on Physiological Signal-Based Emotion Recognition," *Bioengineering*, vol. 9, no. 11, p. 688, Nov. 2022, doi: 10.3390/bioengineering9110688.

[291] W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics," *Sensors*, vol. 23, no. 7, p. 3566, Mar. 2023, doi: 10.3390/s23073566.

[292] S. M. Arman, T. Yang, S. Shahed, A. Al Mazroa, A. Attiah, and L. Mohaisen, "A Comprehensive Survey for Privacy-Preserving Biometrics: Recent Approaches, Challenges, and Future Directions," *Computers, Materials & Continua*, vol. 78, no. 2, pp. 2087–2110, 2024, doi: 10.32604/cmc.2024.047870.

Abeer Awadallah is currently a Ph.D. student in the electrical engineering and computer science department and a member of the Center for Cyber Physical Systems (C2PS) at Khalifa University, United Arab Emirates. She received the B.Sc. degree in electrical engineering at United Arab Emirates University in 2017, and the M.Sc. degree in computing with digital media at the University of Sussex in 2019. She previously worked in projects related to e-learning, website design, Human-computer Interaction (HCI), gamification, and 3D modelling. Her research interests include cybersecurity, artificial intelligence, AI-based cybersecurity, metaverse, biometrics, and emotion recognition.

Khouloud Eledlebi received the B.Sc. degree in communication engineering from KUST, in 2013, the M.Sc. degree in electrical and computer engineering, in 2015, and the Ph.D. degree in electrical and computer engineering, in 2019. She is currently a Postdoctoral Fellow at Khalifa University and an Active Member of Cyber Security and Physical Systems (C2PS). Her research interests include cyber-security, AI and ML for IoT devices, cognitive radio networking, nanotechnology, and low-power semiconductor devices as she is trained in the modeling of nanoscale device and wireless-sensor network optimization and possesses expertise in several evolutionary computing methods.

Mohamed Jamal Zemerly (Senior Member, IEEE) received the M.Sc. degree from University College Cardiff, Wales, and the Ph.D. degree from The University of Birmingham, U.K., in 1986 and 1989, respectively. Since 1989, he was with various U.K. universities, such as UCL, Warwick, and Westminster, and then moved to Khalifa University of Science and Technology, in 2000, where he is currently an Associate Professor. He was the Research Program Chair (and ex-Computer Engineering Program Chair) of the Electrical and Computer Science Department for the M.Sc. degree. He has published over 100 journal and conference papers as well as eight book chapters. He is also the ex-Co-Editor-in-Chief of the IJRFIDSC journal of the Infonomics Society. His research interests include ubiquitous computing, augmented reality, image processing and computer vision, context aware mobile systems, and information security. He was the Co-Program Chair of the ICITST Conference Series for the years 2011 and 2012. He was also the Co-Chair of the same conference, from 2014 to 2015.

Deepak Puthal (Member, IEEE) is a passionate researcher specializing in Cyber Security, Blockchain, Edge Computing, IoT, and Generative Adversarial Networks, with over 150 scientific publications (h-index: 45+). His pioneering work has earned him numerous international accolades, such as the 2023 IEEE Computer Society Smart Computing STC Middle-Career Award and the 2019 Best IEEE ComSoc Young Researcher Award for the EMEA Region, and many more. He has received eight Best Paper Awards and is an IEEE Distinguished Speaker. He has secured over $2.5 million in research grants from public and private agencies. Currently, he is an Associate Professor in IT Systems and Analytics at IIM Bodh Gaya, following previous positions at the University of Technology Sydney (UTS), Newcastle University, and Khalifa University. His Ph.D. from UTS earned him the IEEE Distinguished Doctoral Dissertation Award.

Ernesto Damiani (Senior Member, IEEE) is currently a Full Professor with the Universitàdegli Studi di Milano, Italy, the Senior Director of the Robotics and Intelligent Systems Institute, and the Director of the Center for Cyber Physical Systems (C2PS), Khalifa University, United Arab Emirates. He is also the Leader of the Big Data Area, Etisalat British Telecom Innovation Center (EBTIC) and the President of the Consortium of Italian Computer Science Universities (CINI). He is also part of the ENISA Ad-Hoc Working Group on Artificial Intelligence Cybersecurity. He has pioneered model-driven data analytics. He has authored more than 650 Scopus-indexed publications and several patents. His research interests include cyber-physical systems, big data analytics, edge/cloud security and performance, artificial intelligence, and Machine Learning. He was a recipient of the Research and Innovation Award from the IEEE Technical Committee on Homeland Security, the Stephen Yau Award from the Service Society, the Outstanding Contributions Award from IFIP TC2, the Chester-Sall Award from IEEE IES, the IEEE TCHS Research and Innovation Award, and a Doctorate Honoris Causa from INSA-Lyon, France, for his contribution to big data teaching and research.

Kamal Taha (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Texas at Arlington, Arlington, TX, USA. From August 2008 to August 2010, he was an instructor of computer science with the University of Texas at Arlington. From 1996 to 2005, he was an Engineering Specialist for Seagate Technology, USA, Seagate is a leading computer disc drive manufacturer in the U.S. Since 2010, he has been an Associate Professor with the Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, UAE. He has more than 90 refereed publications that have appeared in prestigious top ranked journals, conference proceedings, and book chapters. More than 20 of his publications have appeared in IEEE Transactions journals. His research interests span bioinformatics, information forensics and security, information retrieval, data mining, databases, and defect characterization of semiconductor wafers, with an emphasis on making data retrieval and exploration in emerging applications more effective, efficient, and robust. He is a Member of the Program Committee, Editorial Board, and Review panel for a number of international conferences and journals, some of which are IEEE and ACM journals.

Tae Yeon Kim is an Associate Professor of Civil Infrastructure and Environmental Engineering at Khalifa University. Prior to joining Khalifa University, he was an acting instructor in Mechanical Engineering at the University of Washington in Seattle and a postdoctoral fellow and research associate in mechanical engineering at McGill University. Dr.

Kim has industrial experience as a senior engineer at Samsung Electronics. He received his Ph.D. in Civil and Environmental Engineering at Duke University in 2007. Dr. Kim's research interest is computational mechanics, additive manufacturing, and structural health monitoring of various materials and structures. He is particularly active in developing sensing systems for non-destructive evaluation of cementitious materials and fiber reinforced composites, computational methods for solid and fluid mechanics, the design for 3d printing of cementitious materials and durability and strength of cementitious materials with micro/nano reinforcements in hot climate conditions. Dr. Kim has published over 50 publications in journals, book chapters, and conference proceedings. He has served as the principal/co-principal investigator in more than 10 projects sponsored by Khalifa University and Abu Dhabi government agencies. Dr. Kim is a member of the advanced digital & additive manufacturing (ADAM) center and emirates nuclear technology center (ENTC) at Khalifa University.

Paul D. Yoo (Senior Member, IEEE) has held academic and research positions at esteemed institutions such as Cranfield (Defence Academy of the UK), Sydney (USyd) and South Korea (KAIST). He was trained originally as a data scientist with degrees from the University of Sydney, Australia, and has since published over ninety papers in prestigious journals and conferences. He has also been the recipient of over US$ 2.5 million in project funding, and various national and international awards for his work in advanced data analytics, machine learning and secure systems research. These accolades include the IEEE Outstanding Leadership Award, Rozetta Award (formerly CMCRC), Emirates Foundation Research Award, and the ICT Fund Award. Most recently, he was awarded the Samsung award for his research on protecting IoT devices using a machine-learning approach [news], Research England's Global Challenge Research Fund (GCRF). Paul serves as an Associate Editor for several high-ranked journals, including ACM Computing Surveys (Q1), IEEE Transactions on Sustainable Computing (Q1) and IEEE Access (Q1). He has previously served as an Editor for IEEE COMML (Q1) in the areas of big data and machine learning from 2014 to 2019. He is also affiliated with the University of Sydney and Korea Advanced Institute of Science and Technology (KAIST) as a Visiting Professor. Paul is a Senior Member of the IEEE and a Fellow of HEA.

Kim-kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio. He was a recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), and the best paper awards from IEEE Systems Journal in 2021, IEEE Computer Society's Bio-Inspired Computing STC Outstanding Paper Award for 2021, IEEE DSC 2021, IEEE Consumer Electronics Magazine for 2020, Journal of Network and Computer Applications for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015. He is the Founding Co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research and Practice, the Founding Chair of IEEE TEMS Technical Committee on Blockchain and Distributed Ledger Technologies, an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021–2023), and a Web of Science's Highly Cited Researcher (Computer Science in 2021 and Cross-Field in 2020).

Man-sung Yim received the B.S. and M.S. degrees in nuclear engineering from Seoul National University (SNU), Seoul, Republic of Korea, in 1981 and 1983, respectively, the Ph.D. degree in nuclear engineering from the University of Cincinnati, Cincinnati, OH, USA, in 1987, and the S.M. and Sc.D. degrees in environmental health science from Harvard University, Cambridge, MA, USA, in 1991 and 1994, respectively. He is currently the Associate Vice President of international office in Korea Advanced Institute of Science and Technology (KAIST), the Professor with the Department of Nuclear and Quantum Engineering, KAIST, and the Director of Nuclear Nonproliferation Education and Research Center (NEREC). His current research interests include nuclear fuel cycle, nuclear waste management, nuclear safety, and nuclear nonproliferation.

Chan Yeob Yeun (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in information security from the Royal Holloway, University of London, in 1996 and 2000, respectively. After his Ph.D. degree, he joined Toshiba TRL, Bristol, U.K., and later became the Vice President at the Mobile Handset Research and Development Center, LG Electronics, Seoul, South Korea, in 2005. He was responsible for developing mobile TV technologies and related security. He left LG Electronics, in 2007, and joined ICU (merged with KAIST), South Korea, until August 2008, and then the Khalifa University of Science and Technology, in September 2008. He is currently a Researcher in cybersecurity, including the IoT/USN security, cyber-physical system security, cloud/fog security, and cryptographic techniques, an Associate Professor with the Department of Electrical Engineering and Computer Science, and the Cybersecurity Leader of the Center for Cyber-Physical Systems (C2PS). He also enjoys lecturing for M.Sc. cyber security and Ph.D. engineering courses at Khalifa University. He has published more than 140 journal articles and conference papers, nine book chapters, and ten international patent applications. He also works on the editorial board of multiple international journals and on the steering committee of international conferences.