applied sciences

MDPI

Review

Cybersecurity in the AI-Based Metaverse: A Survey

Mitra Pooyandeh, Ki-Jin Han and Insoo Sohn *

Division of Electronics & Electrical Engineering, Dongguk University, Seoul 04620, Republic of Korea
* Correspondence: isohn@dongguk.edu

Abstract: The Metaverse is a multi-user virtual world that combines physical reality with digital virtual reality. The three basic technologies for building the Metaverse are immersive technologies, artificial intelligence, and blockchain. Companies are subsequently making significant investments into creating an artificially intelligent Metaverse, with the consequence that cybersecurity has become more crucial. As cybercrime increases exponentially, it is evident that a comprehensive study of Metaverse security based on artificial intelligence is lacking. A growing number of distributed denial-of-service attacks and theft of user identification information makes it necessary to conduct comprehensive and inclusive research in this field in order to identify the Metaverse's vulnerabilities and weaknesses. This article provides a summary of existing research on AI-based Metaverse cybersecurity and discusses relevant security challenges. Based on the results, the issue of user identification plays a very important role in the presented works, for which biometric methods are the most commonly used. While the use of biometric data is considered the safest method, due to their uniqueness, they are also susceptible to misuse. A cyber-situation management system based on artificial intelligence should be able to analyze data of any volume with the help of algorithms. To prepare researchers who will pursue this topic in the future, this article provides a comprehensive summary of research on cybersecurity in the Metaverse based on artificial intelligence.

Keywords: Metaverse; artificial intelligence; cybersecurity; biometric

Citation: Pooyandeh, M.; Han, K.-J.; Sohn, I. Cybersecurity in the AI-Based Metaverse: A Survey. *Appl. Sci.* **2022**, *12*, 12993. https://doi.org/10.3390/app122412993

Academic Editors: Shan Jiang, Zonghu Liao and Shigang Liu

Received: 14 November 2022
Accepted: 15 December 2022
Published: 18 December 2022

1. Introduction

The Metaverse is said to be the next generation of the Internet. Through the Internet, millions of computers, servers, and other electronic devices can connect and access any type of information. Metaverses, on the other hand, are digital spaces in which people, places, and things are represented digitally. A major difference between the Internet and the Metaverse is that the Internet connects users through platforms, websites, or games, whereas the Metaverse places the user in the center of the action. You can be online without interacting with others on the Internet, but in the Metaverse, avatars or digital identities interact. Additionally, there are many similarities between the Internet and Metaverse when it comes to cyber security challenges, such as hacking accounts, phishing, malware, etc. In spite of its differences in infrastructure, Metaverse introduces new cybercrimes that differ from those that occur on the Internet. As the use of NFTs and digital currencies expands, hackers may become more attracted to these targets. The Metaverse is an immersive, multidimensional environment in which one interacts with digital content as one would with real-world content. A study on multi-layer networks [1] emphasized that the Metaverse is essentially an evolving Internet, with a dominant focus on social networking and an exponential increase in creativity driven by a decentralized ecosystem. Indeed, it is a network of 3D virtual worlds centered on social interaction. As the Metaverse develops, it is expected that it will come to reveal much more personally identifiable information about its users in the future not only to the platform but to other users as well. The formats for interaction in the Metaverse include video, audio, text, augmented reality (AR), virtual reality (VR), and extended reality (XR). The strength and depth of the Metaverse's automation derive from artificial intelligence. Using machine learning

algorithms, artificial intelligence oversees all activities in the Metaverse. With the advent of Zuckerberg's company Meta, which combines artificial intelligence and the Metaverse, most researchers have considered ways to empower the Metaverse through the combination of artificial intelligence, AR, VR, blockchain, and 5G. For example, AI can create sensible and accurate avatars from 2D images or 3D scans. Using AI technology, digital humans built in the Metaverse appear as 3D chatbots in a virtual reality world that react to various actions. There are non-player characters (NPCs), which refer to characters controlled by a set of rules or a script and not by a human user (or player). It is possible to convert natural languages into machine-readable formats using artificial intelligence. Although not much time has passed since the introduction of the virtual world and the Metaverse, there are currently many concerns in the field of cybersecurity in the Metaverse that must be urgently dealt with. Disagreements about the nature of the Metaverse and its lack of regulations have caused concern about cybersecurity, as criminals may exploit the unknown nature of the Metaverse to attack its structure. Many of the security risks that threaten Metaverse users are similar to the security risks of Internet users, such as data hacking, malware attacks, privacy problems, and spam. However, the Metaverse has created new security challenges due to its different structure; for example, virtual identities, digital currencies, and non-fungible tokens are interesting economic targets for hackers. Additionally, with the increase in the use of virtual reality glasses and headsets—which may serve as suitable access points for hackers—or augmented reality devices in which the biometric data of users are stored, they may become ideal targets for attacks. Wearable hardware, which is one of the most important components of the Metaverse, can also create new threats. Furthermore, there is also the risk of blockchain-related fraud in financial institutions. All of these are examples of security problems related to the Metaverse. Machine learning (ML) and artificial intelligence (AI) have become critical technologies in information security, as they can analyze millions of events and identify a wide variety of threats. By using artificial intelligence, the AI-based Metaverse can provide significantly improved cybersecurity solutions. However, security risks remain an important challenge for the Metaverse despite the use of artificial intelligence.

With the advent of new technologies, new issues and concerns arise, with security issues unquestionably being some of the most important, which take time and special approaches to resolve. One of the security application areas that has received significant attention in the past three decades is the Metaverse. As a new contribution, this work focuses on the security of the AI-based Metaverse.

The Metaverse will soon become a facilitator of interactions between businesses and consumers, users of social networks, and people who require health services. There will be a massive amount of data generated from these interactions. It is expected that security will be one of the most challenging aspects for them. Currently, there is no governing body or legal body that deals with privacy concerns in new technologies. In the Metaverse, two main technologies are virtual reality (VR) and augmented reality (AR), in which the former takes over the user's field of vision through a VR headset and creates immersive experiences such as voice tracking and body movement to interact with a virtual environment. In the latter case, augmented reality adds virtual overlays to the real world via a lens, such as apps or games on mobile devices. In both of these technologies, sensors are used to collect data, putting them at risk of intrusion and hacking. Therefore, privacy and security are very important issues to consider. Metaverse privacy issues include rights and ownership of users' data, extensive data collection, and a lack of security and privacy regulations. There are a few measures that will reduce privacy concerns: (1) creating a privacy policy, which usually involves identifying the user through biological data; (2) using non-fungible tokens (NFTs) to manage ownership of virtual assets; and (3) considering the penalty rules for unauthorized collection and sharing of users' data. Additionally, machine learning technology and artificial intelligence can be used to strengthen Metaverse networks against all types of attacks to reduce security concerns and reduce costs caused by data hacking. AI-based defense algorithms with a strong structure and accuracy prevent

hackers from infiltrating and damaging the network as well as stealing information and data. The world of the Metaverse would not evolve without artificial intelligence, so this article is based on this relationship. As none of the existing articles on Metaverse security have dealt with the role of artificial intelligence, we focus this article on the context of cybersecurity in the AI-based Metaverse. According to a comprehensive review of the literature dealing with Metaverse security, most articles have examined the security of Metaverse environments from a privacy-preservation perspective. In contrast, our article discusses the AI-based Metaverse as an extensible environment. Furthermore, we consider security issues related to the Metaverse in general; then, according to the criteria for defining Metaverse environments and their different applications, we examine different issues related to AI-based Metaverse security. Accordingly, refs. [2,3] discussed privacy issues related to avatars, whereas [4] briefly discussed some concepts related to data security. In [5], security problems were considered in four categories—user data, communication, scenarios, and goods—and some theoretical solutions were presented. A similar discussion of privacy problems can also be found in [6], in which blockchain was appraised as a solution for security problems, while ref. [7] also summarized concepts related to cybersecurity and briefly discussed artificial intelligence and machine learning as security tools. Consequently, our research clearly differs from the previous research. Our research in the security field focuses on cybersecurity issues. As a main reference and solution, artificial intelligence is given special attention in this article. In this work, the classification is solely based on the use of artificial intelligence and machine learning algorithms in order to consider all aspects of Metaverse security. In addition, this article comprehensively examines security issues, including identification, vulnerability to attacks, and countermeasures. On the basis of recent research, this paper explores and analyses the cybersecurity of the AI-based Metaverse. We aimed to select and summarize the best papers. Attempting to incorporate the various aspects of Metaverse applications into security research as much as possible and making the results available to other researchers were primary goals of our study. The article starts by briefly defining all of the concepts that are (directly or indirectly) related to the Metaverse and artificial intelligence in Section 2, followed by the important and challenging issues of security in Section 3. Finally, we discuss the content raised in the article in Section 4 before concluding this discussion in Section 5.

2. Basic Concepts

The Metaverse has created a new generation of the Internet by integrating technologies such as artificial intelligence (AI) and machine learning (ML), relying on federal learning (FL) frameworks and edge computing (EC) and 5G infrastructure. Metaverse communicates with users with the help of virtual reality and augmented reality. These technologies allow users to immerse themselves in the virtual world by using intermediaries such as headsets, glasses, and smartphones. In addition, avatars and digital twins are virtual characters who play the role of real people in the Metaverse. Moreover, virtual financial transactions are carried out through cryptocurrencies, and valuable art and virtual real estate are traded exclusively using watermarks and non-fungibles tokens. This vast volume of activities in the Metaverse produces a wealth of data. There are also an unlimited number of touch sensors to communicate between wearable devices, which are undoubtedly the favorite targets of hackers. Similar to the real world, the accumulation of this amount of data poses security risks and leads to privacy-preserving issues. Obviously, in order to identify fake users from real users, security protocols are needed, and in order to identify users through their unique information such as biometric data, there is a need for special priority. In the same way, to repel cyber-attacks, Metaverse uses artificial intelligence algorithms such as convolution neural networks (CNNs), support vector machines (SVMs), logistic regression, etc., and by adopting defensive strategies, it prevents hackers from accessing user information. According to this, important basic concepts related to the Metaverse and artificial intelligence are introduced in this section. We took into consideration the most

common definitions of Metaverse concepts, as different theories and definitions have been proposed by researchers in the Metaverse field.

2.1. Metaverse

The Metaverse is an immersive network of socially connected environments in a persistent multi-user platform. This Metaverse serves as a hub for education, work, and entertainment. The Metaverse has been depicted in books, movies, and video games as not just supplementing but significantly replacing real-life experiences. The Metaverse was discussed in [8], which was inspired by Stephenson's *Snow Crash* novel (1992) and is a virtual world parallel to the real world where avatars interact. Metaverse was introduced in [9] as a new form of Internet application and social platform. The Metaverse was described as the next-generation Internet in [10]. According to [11], the Metaverse consists of both real and virtual worlds, in which people are able to interact with each other through assistive objects such as immersion avatars, devices, and platforms. In addition to the Metaverse, there are various virtual, hypothetical, and fictional ideas that differ in dimension from it but are similar in concept, such as the mirror world, the universe, the multiverse, the omniverse, and the megaverse.

2.2. Extended Reality

Virtual reality (VR) technology allows us to see the real world from a different perspective than what we see through the use of computer tools. The use of this technology is widespread across many industries, including entertainment, military, manufacturing, medicine, training, and many more, creating an immersion mode for users in a computer-produced virtual environment. To develop, explore, and investigate virtual reality, researchers focused on the human sight sense. At present, attention is being paid to the senses of sight, hearing, and touch. Research is also being conducted on the taste and smell senses, such as in the Virtual Cocoon [12].

Augmented reality (AR) uses digital information in physical reality to allow users to interact with digital objects and surfaces in their environment. A key difference between augmented reality and virtual reality is that augmented reality does not create a virtual environment but rather simulates the real world. The Metaverse world can be entered using augmented reality. Artificial intelligence and augmented reality are incorporated into the Metaverse for image classification, recognize faces, process data, and recognize speech. Although AR can be developed for all five senses, most systems are based on visual input. There are three types of AR-based systems based on the registration method used: marker-based, markerless, and non-visual. Head-mounted displays are used with these systems [13]. Using augmented reality, computer-generated images, sounds, 3D models, videos, graphics, animated sequences, games, and GPS information can be added to real-world environments [14].

As part of the Metaverse, mixed reality (MR) combines the physical and digital worlds to facilitate interactivity between humans, computers, and the environment in three dimensions. This new technology has been launched with the help of advances in machine vision, graphical processing, cloud computing, and so on. Beyond this, mixed reality is also used for spatial mapping, hand tracking, eye tracking, spatial audio, and speech input. The ability to immerse users in a controlled, real, and interactive environment has led to research on engineering, medicine, and education [15].

Extended reality (XR) is a technology that includes several new and developing technologies offering an immersive digital experience. Virtual reality (VR), augmented reality (AR), and mixed reality (MR) are the three sides of extended reality. In VR, the user enters the processed world through a headset. AR allows users to see digital objects in real space, while MR allows them to interact with objects in virtual space. AR smart glasses, hologram displays, haptic, and VR headsets that are Metaverse-based can improve the user experience in extended reality. Devices of this type facilitate a wide range of physical services in the virtual world and aid users in navigating the Metaverse smoothly. XR is

still being improved and developed as a result of many advances in hardware and the increase in network efficiency that 5G brings. While XR performance continues to improve, there are still some challenges to overcome; for example, the camera on a mobile phone can only be used for one application at a time, which prevents the integration of multiple applications into a hybrid physical–digital environment [16].

2.3. Virtual Worlds

Virtual worlds and the Metaverse are considered to be the same by some researchers, while the Internet and Metaverse have been considered to be the same by others [17]. Virtual worlds are three-dimensional online social environments that are exact replicas of reality and are linked by the Internet such that users or avatars can interact with one another. Throughout these virtual worlds, avatars exchange messages and money, talk, move, and drive through demarcated three-dimensional spaces, such as educational environments, business environments, smart cities, smart factories, and virtual healthcare environments [18]. As a global platform, the virtual world connects millions of people and incorporates a wide range of technological features [19].

2.4. Second Life

Second Life is a virtual world created by Linden Lab, a U.S.-based company, in 2003, as a place for online socialization and electronic gaming [20]. Interaction and communication in Second Life are facilitated by Web 2. Essentially, Web 2.0 is a development model in which large tech companies rely on advertising to generate revenue. Using this model, companies rely heavily on selling advertising space and serving targeted advertisements to their massive user bases. Virtual economies and online games were clearly created in Web 2.0 [21]. Second Life is considered, by some researchers, to be the same as the Metaverse [22,23] and by others to be a separate platform for the following reasons: (1) Second Life was produced by Linden Lab, but Metaverse started with *Snow Crash*, and companies such as Microsoft, Meta, and Epic Games are currently attempting to implement the Metaverse; (2) in terms of the structure of the Metaverse, it is implemented in Web 3.0, while Second Life is implemented in Web 2.0; and (3) in terms of applications, Metaverse is a wide virtual world with many applications in various fields, including Internet of Things networks, media and entertainment, health care, real estate, social interaction, education, production, virtual tourism, finance, military, and transportation. On the other hand, the use of Second Life is mainly focused on online games, and virtual transactions are limited.

2.5. Avatar

An avatar is a digital representation of a real person in the Metaverse. There are two types of avatars: static, such as those used in social networking sites for profiles, which do not interact with their surroundings, and animated, which can move, speak, and perform a variety of other activities. An avatar in the Metaverse has a job and a social personality. In general, they are displayed using clothing and item symbols [24]. An avatar called Metabot was introduced in [25] by combining the name Metaverse with the word robot. An analysis of Metabots with mobility capabilities was presented in this paper. The authors designed a learning model that optimizes fuzzy controllers for Metabots using evolutionary computing techniques.

2.6. Digital Twin

In the digital world, a digital twin is an exact virtual representation of a physical object. The object is fitted with sensors to collect relevant data that are conveyed to the processing system, which then relays the data to the digital representation. By simulating the behavior of real-world objects, we can predict how they will behave in the future. The incorporation of digital twins in the Metaverse can help us to recreate the existence of the real world digitally. Digital twins and the Metaverse can be merged together and used in different areas of application, such as manufacturing, healthcare, automotive, retail and e-commerce,

smart architecture, and industrial IoT. Through the integration of digital twins, the Internet of Things, and 6G, a smart city can be created that offers new perspectives on city health and viability [26]. It must be noted that there are also many security issues associated with integrating the digital twin into the Metaverse, which must urgently be addressed. For example, in [27], combining a blockchain with a digital twin in the Metaverse can guarantee the security of the digital twin.

2.7. Cryptocurrencies

Digital currencies, sometimes called cryptocurrencies, are a form of alternative payment based on encryption algorithms. By using encryption technologies, cryptocurrencies serve both as currency and as virtual accounting systems. Bitcoin is the most well-known cryptocurrency. The introduction of Bitcoin led to the introduction of other new cryptocurrencies, including Ethereum, NFTs, USD coins, and so on, which can be integrated with other technologies such as Metaverse [28]. In order to facilitate Bitcoin transactions, a distributed ledger called a blockchain records them in consecutive blocks. Therefore, a user cannot spend their holdings twice. Using the distributed ledger, tampering can be prevented, as changes to any of the versions are detected and rejected by the other users. Another digital currency based on Bitcoin is Ethereum. Similar to Bitcoin, Ethereum [29] makes use of blockchain technology and the proof-of-work (PoW) consensus architecture to control the peer-to-peer network and reward nodes that make contributions to the community. The consensus process that cryptocurrencies utilize to confirm new transactions, add them to the blockchain, and produce new tokens is known as "proof-of-work". PoW uses mining to carry out these objectives. Digital assets, also known as non-fungible tokens (NFTs), include music, in-game goods, videos, and other media (Figure 1). They can be bought and traded using cryptocurrencies online. Unlike Bitcoin, NFTs are non-fungible assets, which are encoded or kept on the blockchain.

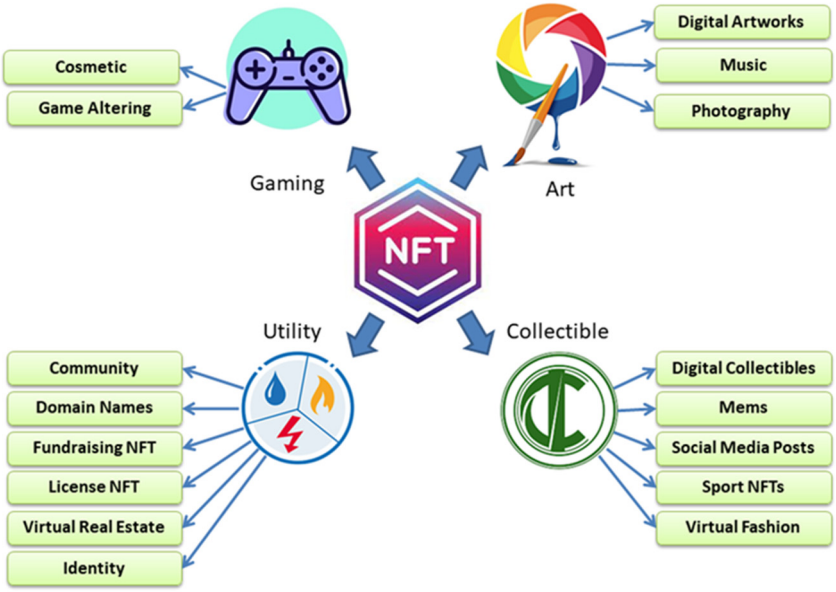

Figure 1. Classes of digital assets.

2.8. User Authentication

User authentication prevents unauthorized access to devices and networks by identifying a user's identity during user access. Different kinds of services use different methods to create passwords for their users. As different types of networks and devices present different levels of risk, authentication can be carried out in many different manners. Authentication methods such as passwords, PINs, digital signatures, biometrics, etc., can be used to prove identities. These methods can be divided into three main groups, as shown in Figure 2. As identity is the most important asset in the real world, it also plays an important

role in the virtual world. In the Metaverse, all participants must confirm their identity. Non-fungible tokens are one of the ways to perform authentication in the Metaverse [30].

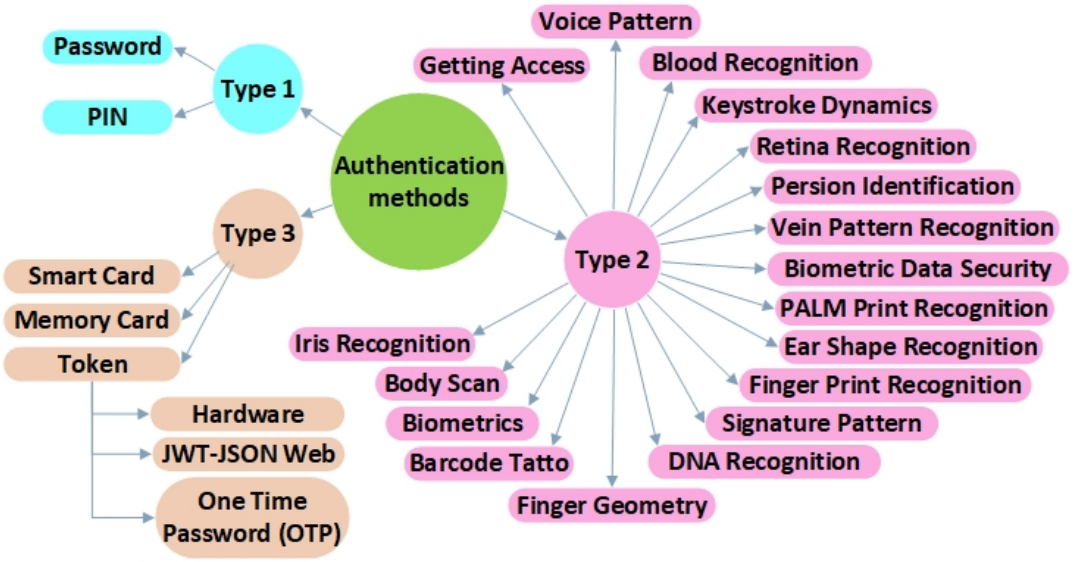

Figure 2. Three main types of authentication methods.

2.9. DeepFake

Deepfakes are fake digital images or videos that can make a person look like someone else. Deepfake technology is a type of artificial intelligence that can create convincing images, sounds, and fakes. As deepfake creates both fake content and technology, it can be seen as a collection of deep learning and fake content. There are some benign deepfake videos, but deepfakes are also responsible for a great deal of fake news, fake surveillance videos, and malicious hoaxes [31]. The three most common kinds of deepfake videos at present [32] include the fake display of a person's entire head generated using a video of the original person's head, swapping the person's face with a replacement face, and lip-syncing, in which the target person's lip image is altered to make it appear that he or she is speaking when in fact they are not. Artificial intelligence algorithms such as DNNs, CNNs, GANs, etc., can be used to achieve these goals.

2.10. Generative Adversarial Networks (GANs)

Two neural networks are trained simultaneously in a generative adversarial network: one for generation and the other for discrimination [33]. A GAN can be used both as a semi-supervised and an unsupervised learning technique. In a GAN network, the generator G acts as a forger, creating fake images identical to real ones, while the discriminator separates the real images from the fake ones. Both networks are trained simultaneously. By interacting with a trained discriminator, the generator can learn without access to real images [34].

2.11. Convolutional Neural Network (CNN)

A convolutional neural network (CNN) is a type of machine learning algorithm that consists of several hidden layers, an input layer, and an output layer. There is a connection between both nodes and a weight associated with them. A node transmits data to the next layer when its output exceeds the threshold value. Images, speech, and sound signals can be input into these convolutional neural networks. The convolution layer, pooling layer, and fully connected (FC) layer are the three main layer types. More elements of the image are identified as the number of layers increases. The convolution layer is where the majority of the calculations are made. Dimensional reduction and lowering of the number of input

parameters are the responsibilities of pooling layers. Classification is carried out using the features that were derived from the preceding layers by the fully connected (FC) layer [35].

2.12. Logistic Regression

A logistic regression algorithm estimates the probability of an event from a set of independent variables and can be used for predictive classification and analysis. There are various types of logistic regression based on categorical responses: binary logistic regression (where the response can be either zero or one), multinomial logistic regression (in which multiple responses can be present without any specific order), and ordinal logistic regression (with responses that must be arranged in a specific order). It is a supervised machine learning model that discriminates between classes based on a logarithmic function.

In addition, Scikit-learn (an open-source data analysis library) can be used to implement this model. There are many use-cases for logistic regression, such as fraud detection, predicting disease incidence in a particular population, and predicting performance decline in an organization.

2.13. Support Vector Machine (SVM)

Support vector machines (SVMs) classify data in N-dimensional space with the aid of hyperplanes, which have the same number of features. There are many hyperplanes that separate two data categories, but the goal is to find a plane maximizing the distance between the data points of both classes such that the classification accuracy is maximized. There is a loss function, called a hinge, that is used to maximize the distance between the data points and the hyperplane. If the predicted value and the actual value have the same sign, the cost is zero; otherwise, we must calculate the amount of loss. To do this, a tuning parameter must be added to the function, which balances the margin maximization and loss [36,37].

2.14. Federated Learning (FL)

Federated learning refers to the application of machine learning in a decentralized manner. The devices train a model jointly at the edge of the network, and the data are not transferred to the server but instead remain on the device. Therefore, after downloading the current model from the edge server, the device learns from the data on the device and updates the model, which is then encrypted and sent to the cloud server. FL increases network speed and bandwidth optimization as well as increasing data security. Mobile phones, self-driving cars, and other applications use FL [38].

2.15. Cyber-Attack

The act of gaining unauthorized access to a computer, network, or devices connected to networks with the goal of harming them is referred to as a cyber-attack. This type of attack can disrupt or destroy devices. It is also possible for the attacker to control, delete, or block the devices as well as stealing their data. The purpose of a cyber-attack includes obtaining financial benefits or stealing user identities for abuse. The most famous cyber-attacks are malware, phishing, man-in-the-middle, denial-of-service attacks, SQL injections, zero-day attacks, and DNS tunneling. For the identification and management of cyber-attacks and in order to repel them, they must be simulated to determine the network's weak points [39]. These attacks can be prevented by implementing strategies such as using a multi-factor identification method [40], using internal controls of organizations, backing up data, antiviruses, and so on.

2.16. Metaverse Sensors

In the Metaverse, wearable devices such as mobile phones, smartwatches, and AR/VR technologies contain important components called sensors. AR and VR technologies use sensors to detect motion or sound. As an example, VR systems use inertial measurement units (IMUs) that include accelerometers, gyroscopes, and magnetometers. By adding time,

thermal, respiration, and light sensors to the IMU, the AR system can detect the user's location and what they see or hear. A majority of headsets are equipped with sensors such as time-of-flight (ToF) cameras, vertical cavity surface-emitting lasers (VCSELs), binocular depth sensors, and structural light sensors. There are also audio-related sensors, such as directional microphones, as well as thermal sensors and forward- and rear-facing video cameras [41]. Furthermore, touch sensors can also be used to exchange information between humans and machines as a human–machine interface (HMI). Touch input is activated by these sensors (e.g., on a touchpad) [42]. In addition, many sensors are used in the context of industrial IoT, drones, healthcare [43], and so on.

2.17. Edge Computing

Edge computing refers to computing near the edge as part of a distributed computing topology. As a result of edge computing, real-time data are available to users without delay, and thus, network latency and bandwidth costs can be reduced. IoT sensors, notebooks, smartphones, security cameras, smartphones, or robotic arms in car factories can all be considered as edge devices. Servers located at the edge of a network are known as edge servers. Edge computing improves the performance of applications such as virtual reality and augmented reality, self-driving cars, smart cities, and automation systems by speeding up calculations. Artificial intelligence takes advantage of the edge computing paradigm to speed up the calculations of AI algorithms.

2.18. AI-Based Metaverse

The Metaverse consists of common infrastructures, protocols, and standards that are connected to the physical world via intermediaries but are not separate from it. AI can support all of the Metaverse's technology layers. Due to the large amount of content produced in this digital world, artificial intelligence can provide large-scale and continuous content production for Metaverse. In Metaverse environments, AI is used in areas such as chatbots. Using artificial intelligence in speech recognition, machine vision, and natural language processing, Metaverse can become easier and more practical. Digital avatars can create visual dialogue environments in the Metaverse using artificial intelligence and virtual reality. Digital twins based on artificial intelligence are used to collect and analyze a great deal of data, creating a 360-degree view of the devices. Additionally, the Metaverse can be used for education and training. Through the use of artificial intelligence, users can learn in realistic virtual environments, receive virtual teaching assistants, and participate in educational courses in the Metaverse. The future holds countless opportunities for collaboration between artificial intelligence and Metaverse since Metaverse is still in its infancy.

3. Security in Metaverse

In the same way that the Internet is facing numerous security threats, Metaverse is no exception. It is impossible to discuss the future of the Metaverse without discussing cyber security challenges. Despite the fact that Internet threats and Metaverse threats are very similar, dealing with threats in a virtual environment can be extremely challenging and expensive. There are many security challenges faced by businesses and users in the Metaverse. There are also threats such as money laundering in virtual currency exchanges, security threats in online games, art forgery, and privacy risks such as theft of personal data, impersonation, avatar ownership, and thousands of others. As biometric data are increasingly used to verify Metaverse users' identities, especially in social networks, it adds a large amount of personal information to the existing data, making it difficult to maintain and posing a threat to cyber security because they create something new. Our goal in this section is to categorize the existing security challenges based on their topics and provide researchers with interesting results.

3.1. Security in Metaverse Based on Biometric Data

A VR environment can be created with various type of visual stimuli and scenarios, which can be easily switched or repeated, while eye tracking shows exactly where the participant's attention is at any given moment of the experience and what visual elements trigger certain responses. In particular, VR experiences can be enhanced by eye tracking. According to [44], virtual reality devices store most of a user's personal information, such as account numbers and biometric information, so they are constantly at threat of being attacked by hackers. In addition, these attacks can damage the headset's vision. Many solutions have been proposed for authentication, but the most effective methods (e.g., PIN, pattern, biometric brain, and so on) require a significant amount of user time and are also highly insecure. Therefore, the authors of this study presented blinkey, a method for securing VR devices equipped with eye-tracking for user authentication. In this method, authentication is performed by blinking one's eyes according to a rhythm that is only known to the user. This is a new method of authentication that uses a passcode. Instead of numbers, letters, or characters, users blink to different rhythms. To evaluate their blinkey method, the authors discussed the effects of the following commonly seen attacks: zero-effort attack, statistical attack, shoulder-surfing attack, and credential-aware attack. Their experiments were conducted using two machine learning algorithms for classification: support vector machine (SVM) and *k*-nearest neighbors (*k*NN). They achieved an average error rate (ERR) of 4% using this method, making it effective against all types of attacks. Compared with commonly used methods on mobile devices (e.g., passwords, PINs, and pattern locks), blinkey exceeded user expectations from the perspectives of security and usability. Due to a special genetic pattern controlling the pupil's expansion and contraction, the accuracy and speed of the blinkey method are very high. In addition, the pupil size change between each blink is also as unique as a fingerprint.

An artificial-intelligence-driven deepfake is a picture, video, or audio recording that looks real but is actually a fake. Deepfakes can be created by AI technologies such as autoencoders (artificial neural networks that reconstruct the input from simpler representations) and generative adversarial networks (GANs). Metaverse users can create their own hyper-real avatars using their biometric data. However, deepfakes pose many privacy and cybersecurity challenges. Based on a deep convolutional neural network, ref. [45] has proposed a lip-based speaker authentication system that defends against severe deep fake attacks. There are usually two types of deepfakes: (1) manipulation methods (e.g., face swapping) and lip syncing and (2) visual speaker authentication (VSA) systems are vulnerable to deepfake attacks, which mimic the original user's pronunciation. It has been shown that the lips of people can be used as a biometric feature to distinguish speakers. Lip-based authentication, which has high security and can be used in most systems, contains both fixed and mobile data related to identity (i.e., the shape and appearance of the lips as well as their movement). Using VSA, the authors proposed a deep learning algorithm that can detect deepfake attacks without prior manipulation knowledge. Due to the vulnerability of static information to deepfakes, they have used dynamic information for authentication. To extract an image of the lip area from a video of a face, the authors used the Dlib detector (a detector which is used to extract the lip region from a video of a face), and to verify the spoken text, they used connectionist temporal classification (CTC). The proposed network consists of two subnets: (1) a low-level fundamental lip feature extraction subnet (FFE-Net) and (2) a high-level representative lip feature extraction and classification subnet (RC-Net). MOBIO (a data set of bimodal audio–visual data from 152 people) and GRID (including thirty-three speakers, each of whom speaks 1000 sentences containing commands, colors, prepositions, letters, numbers, and adverbs) were used as data sets. To verify whether the lip movement matches the user's speaking habit, the speaker authentication network based on dynamic talking habit (SA-DTH-Net) was used. They used three deepfake attack methods: Faceswap (FS), Deepfacelab-Quick96 (DFL), and Faceswap-GAN (FS-GAN). According to their results, detection methods based on biometric features, such as SA-DTH-Net, performed better than other detection methods,

especially in detecting fake videos produced by FS-GAN. Under the assumption that their method does not require any prior information about the deepfake spoofing method, it can be applied to defend against different kinds of deepfake attacks.

Online photos on social networks can be used to retrieve features from a user's face, which poses a serious threat. In order to create security for users, face recognition tools should be strong and efficient enough. In [46], a face authentication system was attacked, and by using images from social networks, models of the user's face were created that weaken the security of the system. They deceived liveness detectors using a VR system and specific facial movements such as smiling. One of the most common attacks on face authentication systems is VR-based spoofing. Any system that uses color images and camera movement is vulnerable to these attacks. To extract 68 2D facial landmarks, the authors used the supervised descent method (SDM). Due to a median alignment error of 2.7 pixels, they used high-fidelity pose and expression normalization (HPEN) with a 3D morphable model (3DMM). In most cases, SDM works well even on low-resolution online images. For the sample, they spoofed True Key, BioId, and KeyLemon. For indoor logins, they achieved 98% accuracy and 100% accuracy, while for outdoor logins, they achieved 96% accuracy and 100% accuracy, respectively. According to their results, this method works well if the image height is 50 pixels; however, if the image resolution is less than 30 pixels, their system does not work, as they cannot obtain useful features from the image. Furthermore, there are three features that can knock down this approach: random projection of light patterns, detection of minor skin tone fluctuations related to pulse, and the use of illuminated infrared (IR) sensors. It is possible to avoid the first two with additional adversary efforts, but the third would require significant changes to their method in order to avoid.

According to [47], in the Metaverse, human–machine interactions are fundamental, especially where augmented reality and virtual reality are combined, and sensors must be used to accomplish this. The authors used an all-in-one multi-point touch sensor (AIOM) with two electrodes to learn and recognize human–machine interactions using a deep learning method. Touch sensors are also used to protect security by enabling biometric verification, preventing the leakage of passwords. An Arduino Leonardo was used as a microcontroller in a circuit, which is connected to a computer by USB. In the AIOM, mechanical receptors convert the touch of fingers on the skin into a transient receptor potential by mimicking the function of biological sensory neural systems. Upon receiving this potential, the brain decodes it and reacts accordingly. In addition to detecting the spatial and temporal dynamics of stimulation by touching a different point, the touch sensor AIOM can detect the mechanical information of spatio-temporal dynamics. As a linear interactive control interface for playing piano, it is designed to validate linear touch sensors. Additionally, it can be used to control drones programmatically. To protect privacy, the authors also proposed a biometric approach utilizing an artificial neural network (ANN), in which the AIOM is mechanically stimulated by touch, and the mechanical signals are converted into digital signals, which are then used by neural networks to classify the features extracted from the digital signals. Key-pressing examples from three users and their dynamic characteristics were used as the training data set. There are three parameters to consider: holding time, interval, and signal magnitude. A back-propagation algorithm (BP) is used to calculate the output of each node in the ANN model. Furthermore, when entering the password of each user, the ANN model was able to identify them accurately. It was determined that about 98% of the identifications made by the algorithm were accurate based on the test results. A key component of the AI-based Metaverse is human–machine interaction, which, when combined with the variety of sensors and deep learning algorithms, greatly assists in the construction of all kinds of prosthetics, robotics, and so on.

It is important to keep in mind that privacy is one of the biggest dangers associated with augmented reality in the Metaverse. AR technologies are capable of observing what a person does, which puts their privacy at risk. Compared to other types of technology—such as social media networks—AR gathers a great deal of information about the user.

The authors in [48] described the development of an augmented reality app that uses computer vision and raw input data to deliver real-time attack guidance to an attacker's phone. To establish an attack, this method mimics the unique typing behavior of users on a smartphone without modifying the device, installing software, or using special hardware. The attacker uses their own smartphone to run this app, positioning it such that the camera can see the user's hands as they grasp their phone. By using this information, the attacker can immediately simulate the victim's input behavior by superimposing instructions over the camera stream. In order to create an augmented reality prototype, they built a simple physical model. An invader uses audio beeps to time their taps and attaches a transparent film with spatial hints to the victim's smartphone. In this study, the authors gathered 31 volunteers to test over 400 mimicking attacks. Their application utilized the OpenCV 2.4 library and Android KitKat (Android KitKat 4.4, Google, San Jose, CA, USA). Furthermore, spatial, temporal, and contact features were extracted and evaluated using an SVM classifier. Key-hold interval, inter-stroke interval, down pressure, down area, down x, and down y were the six target features identified in their study. In order to compare the results, they used both the proposed AR-based method and the audiovisual method. The data were divided into two parts for training and testing. Additionally, their data set was assessed using the zero-effort attacker model. In four minutes, they succeeded in 87% of the attacks. By using AR, the attack success rate improved from 6% to 73%. Input behavior-based biometrics can also be attacked using this method. Note that the challenge of capturing user behavior makes this attack relatively narrow.

In [49], a user authentication system called GaitLock was introduced, which is an innovative method that can identify users based on their gait signatures. While typical previous methods for authentication through walking have been based on the use of sensors or pre-defined gestures performed by the users for identification, this system uses the onboard inertial measurement units (IMUs) present in virtually all popular VR/AR headsets. To this end, the inertial signals generated during walking should be analyzed to identify unique gait patterns. To extract walking patterns, dynamic time warping (DTW) and sparse representation classifier (SRC) were combined. Dynamic-SRC is a new model proposed for recognizing gait. Sensors employed by IMUs assist in identifying and stopping attackers. In this study, internal and external threats are considered. Six different walking detection methods were compared with dynamic-SRC, including dynamic time warping with nearest neighborhood (DTW+NN), time-delay embeddings with template matching (TDE+TM), nearest neighborhood (NN), and three variations of SRC approaches including zero padding, sparse fusion, and majority voting. Finally, they assessed the performance of GaitLock against zero-effort attacks and mimicking attacks. In comparison with other user authentication methods, their results showed an increase in accuracy of about 20%. Additionally, they achieved an equal error rate (EER) of 2.9%. In this work, sparse fusion modulates the detection accuracy by fusing sparse coefficient vectors from multiple sequential step cycles at the same time in order to enhance detection accuracy, as they must have been generated by the same subject. To conduct their experiment, GaitLock was implemented on Google Glass. Both internal and external threats were considered.

In augmented reality (AR) headsets, voice-based inputs can be used to recognize the user. However, attackers with unintelligible voice commands can attack devices that do not have a voice verification system. To defend against voice-spoofing attacks, a voice-spoofing defense system for AR headsets has been proposed [50]. Two popular techniques used by older systems to identify sound are based on broadcast reverberation analysis and noise analysis. These techniques present unsatisfying performance, with a 17% false-positive rate. In order to combat voice-spoofing attacks, numerous liveness detection systems have recently been proposed. These systems use phoneme location, articulatory gestures, magnetic fields of loudspeakers, and throat voice to analyze the differences between the human voice system and loudspeakers. As all of these methods were primarily developed for smartphones, current liveness detecting technologies are generally not compatible with AR headsets. These proposed systems defend against voice

spoofing by helping the human voices be propagated both internally and externally and using a low-cost contact microphone to collect body sounds in order confirm the user's voice. Furthermore, voice spoofing can be prevented by detecting the common features in the frequency bands of human voices and/or by deploying a contact microphone on the user's head to collect body sounds in order to confirm the user's voice. The authors noted two key challenges to overcome: (1) the low signal-to-noise ratio (SNR) of the voice propagates to extract voice features from the raw time-domain signals and (2) determining a correlation between the internal body voice and the air voice of the user. The SNR issue can be resolved by transforming the raw signal into the time–frequency domain and utilizing spectrogram enhancement techniques. In order to find correlated high-energy blocks from both spectrograms, two voices are matched to estimate the correlation and similarity between them robustly. An obstruction attack was performed, in which a malicious user appears close to the normal user and issues a high-volume voice command. The next attack is the replay attack for voice-based authentication. It is assumed that an attacker can physically access a victim's headset if they are not noticed, enabling them to record the user's voice and replay it. Hidden Markov model (HMM)-based word segmentation techniques can be applied to each audio sample to segment it into different words. The proposed method has been implemented on a Raspberry Pi using an iRig HD 2 soundcard and an AXL contact microphone. Their system can correctly accept the normal user with a mean accuracy of 97% for all users and high accuracy of 92.3% for normal users. In terms of their defensive approach, they achieved mean accuracy of 99.2% and 98% against obstruction and replay attacks, respectively.

3.2. Security in Metaverse Based on Transportation Data

Drones, i.e., unmanned aerial vehicles (UAVs), are gaining popularity across a wide range of industries, including the Metaverse. Recently, a number of companies, including Walmart, Google-owned Wing, Magellan Health, and Brinker International, are experimenting with drone deliveries. Additionally, Drone Orange is currently building a giant Metaverse platform in South Korea using drones. In this massive project, drones are used to collect all the images and data. As a result, drones have become increasingly significant in the Metaverse. Drones require AI algorithms and come with many sub-challenges, such as privacy issues, identity theft, and security concerns. A fog-assisted Internet of Drones (IoD) was presented in [51]. The fog node is responsible for analyzing the vast amount of data transferred by drones in the IoD. This volume of drone data collection inevitably leads to traffic generation and privacy leakage. Federated learning (FL) has been proposed as a means of protecting drone privacy. Even so, drone privacy can still be threatened through other means, such as eavesdropping. A power control scheme for drones was investigated in this paper in order to maximize FL system security. To resolve this issue, an algorithm was designed. As part of the FL system, the drones alternately download global model parameters, train them with their own data, and then send them to a fog node, where they are collected into a new global model. In order to avoid excessive power consumption, they proposed a power control in secure FL (PCSF) algorithm, as the drone's transmission rate depends on air-to-ground and fog channels. For maximum system security, this algorithm counts all FL times, optimizes the wireless transmission power of drones, and selects the best FL time and optimal power control method. They compared their algorithm with the delay-aware algorithm (an algorithm to minimize FL time), and to determine whether their algorithm minimizes energy consumption, they also compared it with the energy-aware algorithm (an algorithm to minimize energy consumption). They considered N = 16 drones flying within a 1000 $\times$ 1000 m area. Based on the obtained results, as the number of drones increases, the security rate of the system increases. Compared to the delay-aware and energy-aware algorithms, the results of the proposed PCSF algorithm presented a greater increase in security rate. The FL training time remained the same regardless of how many drones were used. The PCSF algorithm training time was similar to that of the delay-aware algorithm but less than that of the energy-aware algorithm. The delay-aware

algorithm operates similarly to the PCSF algorithm and outperforms it, when compared to the energy-aware algorithm, in terms of security rate. On the other hand, the energy-aware algorithm uses the most energy, as its training period is the longest. Additionally, due to the eavesdropping issue, the security rate of all three methods increases as the amount of eavesdropping grows. Regarding the effect on the quality of service (QoS), the security rate in each of the three algorithms falls as the QoS rises. The system's security rate rises when the QoS is low, as more transmission power is needed to meet the QoS requirements. The results indicate that, in terms of battery capacity, security rate, and FL training time, the delay-aware algorithms are not related to improving battery capacity, as battery capacity restricts the minimum wireless transmission. However, as battery capacity increases, the security rate of the energy-aware algorithm decreases and the training time of its FL increases. Ultimately, the PCSF algorithm performed the best out of the three considered algorithms. In terms of accuracy, FL in PCSF and the delay-aware algorithm both experienced shorter training times as accuracy increased, while the energy-aware algorithm used no energy at all. This problem can be considered as a non-linear programming problem. Additionally, as eavesdroppers typically conceal their locations, increasing the channel power from the drone to the eavesdropping node is treated as a random parameter. It can be concluded that more wireless transmission power offers a higher level of system security.

Thanks to cutting-edge technology such as virtual reality, augmented reality, and the Internet of Things, automobiles should be built to be able to interact with the Metaverse. Upcoming vehicles—including planes, trains, trucks, and cars—will be based on computer platforms with the ability to receive and transmit data, on the basis of which they will perform their own functioning. Data transmission is made possible by the use of sensors, which are prone to hacking at all times. The issues surrounding safe data transmission between sensors were examined by the authors in [52]. The authors looked at how jamming and eavesdropping attacks affect wireless network sensors. In order to deal with this problem as an optimization problem based on a Stackelberg game, they took into consideration both the single-antenna model and the multi-antenna model. Jammers have been employed in numerous studies to stop attacks. However, a jammer can also be used for harm. A jammer can lower the overall power usage of a cyber–physical transportation system (CPTS). This technology was referred to as a green cyber-physical transportation system (GCPTS) by the authors. The jammer can partially prevent eavesdropping assaults in addition to interfering with sensor and controller communications, as it broadcasts noise into the GCPTS system. The authors constructed two different kinds of communication method: a single-antenna sensor, in which the information is conveyed in a single channel, and a multi-antenna sensor, in which the information is separated into several packets and delivered at various channels. They used a Stackelberg game to describe the power distribution issue, with the sensor acting as the leader and the jammer as the follower. The Stackelberg game was used to mimic the power allocation problem, which may be thought of as an optimization problem. The sensor, as the leader, has priority, as they both want to make the most of their resources. A stochastic algorithm with feedback (SAF) and a newly developed intelligent simulated annealing (RISA) algorithm were suggested to achieve the Stackelberg equilibrium (SE) strategies. The common wiretapping model (CWM), the wiretapping model with friendly jammer (WMFJ), and the wiretapping model with malicious jammer (WMMJ) were all employed in their experiment. As a result, CWM always presented the lowest capacity for concealment and the smallest expansion window. There was not much difference between WMFJ and WMMJ in terms of their secrecy capacity or level. Additionally, allied sides have the same authority and ability for secrecy. Due to the power of the friendly jammer, WMFJ had significantly higher power than WMMJ. Moreover, while WMMJ used less power, it had a relatively high secrecy capacity.

3.3. Security in Metaverse Based on Virtual Learning

An innovative use of the Metaverse is the incorporation of a virtual world in an educational setting, which investigates its viability as an additional digital tool to the

teaching–learning process in the context of a university, where the flexibility of access to synchronous and asynchronous information presents an alternative method of knowledge transmission and acquisition through technological means. In [53], social virtual reality-based learning environments (VRLEs) were studied. A risk assessment method was proposed by the authors in this paper. In particular, to study young people with autism spectrum disorder (ASD), they used social VRLEs such as vSocial. It is important for VRLEs to provide a safe environment for young people with learning disabilities. VRLEs use emotion-tracking sensors, and their data are stored in a cloud environment. Attacks on these data can lead to negative effects, such as changing content and learning results (Figure 3). VRLEs were assessed in this paper for the first time in terms of security and privacy concerns. All three aspects of security, privacy, and safety were considered. Three attack scenarios were presented in this study, each involving different aspects of security, including loss of nodes, packet sniffing, and malicious network changes. Tree structures depict attack scenarios using root nodes and leaf nodes as targets and attacker activities, which illustrate the relationship between possible system vulnerabilities and attack scenarios. Based on the likelihood of the threat occurring, the authors used this concept to analyze server threats to vSocial and risk scores. To create the tree, they use the SecurITree tool with countermeasure nodes, rate, and weights as inputs. Besides frequency rates (i.e., the number of times an attack occurs over a period of time), they also used the duration of attacks to calculate risk. Additionally, network discrepancy, packet loss, and sniffing attacks were used to attack the system, and they evaluated how these attacks impact storage, network, and VR rendering. As a result of this tree, they determined the probability of occurrence, which is a well-known measure of risk. SPS creates a risk score based on the probability of occurrence and impact of the threat. Generally speaking, the higher the risk score associated with a threat, the greater the risk. Based on the results, creating a defensive strategy for the system is made easier. Users connect to the virtual classroom using head-mounted display (HMD) devices, such as HTC Vive (HTC, New Taipei City, Taiwan) or Oculus Rift (Meta Platforms, Menlo Parks, CA, USA), through a cloud-based application hosted on the global environment for network innovations (GENI). They used Steam (an online game platform for simulation), Netlimiter (an internet traffic control tool to simulate DoS attacks), Wireshark (an open-source network protocol analyzer), and Clumsy 0.2 (a Windows-based tool for controlling network conditions). Their results indicated that any upload speed below 30 Kbps resulted in high-fidelity crashing, but the frame rate was not significantly affected. In terms of privacy, they simulated packet sniffing attacks and demonstrated that avatar information, confidential host information, and server details were completely exposed, implying that all user information could be captured and deciphered. From a safety standpoint, they demonstrated that reducing the bandwidth can result in abrupt changes in VR content. In terms of attack tree results, an ad hoc attack tree alternately under-represents system vulnerabilities, resulting in a lower risk score, where a lower risk score indicates low susceptibility to threats, necessitating stronger countermeasures. As a result, the quality of an ad hoc attack tree fails.

VRLEs were investigated from a security standpoint in [54]. The authors developed a new framework for security and privacy by employing vSocial and a new attack-fault tree (AFT) in order to demonstrate the outcomes of cyber-attacks. AFTs can be used to model security issues such as loss of confidentiality (LoC), loss of integrity (LoI), and loss of availability (LoA) scenarios as well as privacy issues such as privacy leakage. To analyze the attack model, these attack-fault trees were converted into stochastic timed automata (STA) presentations. Finally, in a VRLE session, they demonstrated how their attack-fault tree model compounds suitable design fundamentals such as hardening, diversity, redundancy, and the principle of least privilege to ensure user safety. Through the use of AFTs, they generated graphical models of different cyber-attack/fault-attack scenarios and their corresponding consequences toward a common goal of system disruption. Their goals were as follows: using their framework, they measured cybersickness, and security/privacy attacks were evaluated in the context of cybersickness in the vSocial application; according

to their results, a denial of service (DoS) attack and data leakage were the most likely causes of high levels of cybersickness in VRLE sessions. Moreover, they assessed the impact of the identified threat vectors on cybersickness levels in a social VRLE. Using the results of their previous work [53], they modeled security, privacy, and attacks using an AFT. This AFT, which includes SPS attack scenarios and causes cybersickness, is called safety-AFT. Technical issues as factors of cybersickness, such as low bandwidth and network failure scenarios, are modeled in safety-AFT. They also used the simulation tools Clumsy 0.2 and Wireshark to perform a boundary test. VRLEs use distributed wearable devices and head-mounted displays such that the user experience is sensitive to distributed denial of service attacks. The result was obtained for a DoS attack scenario executed through packet tampering, packet duplication, and packet drop affecting the server, which showed that a packet drop can disrupt the communication between the user and VRLE server by as much as 80%. Moreover, a tamper rate of 20% can crash the VRLE server for VRLE users.

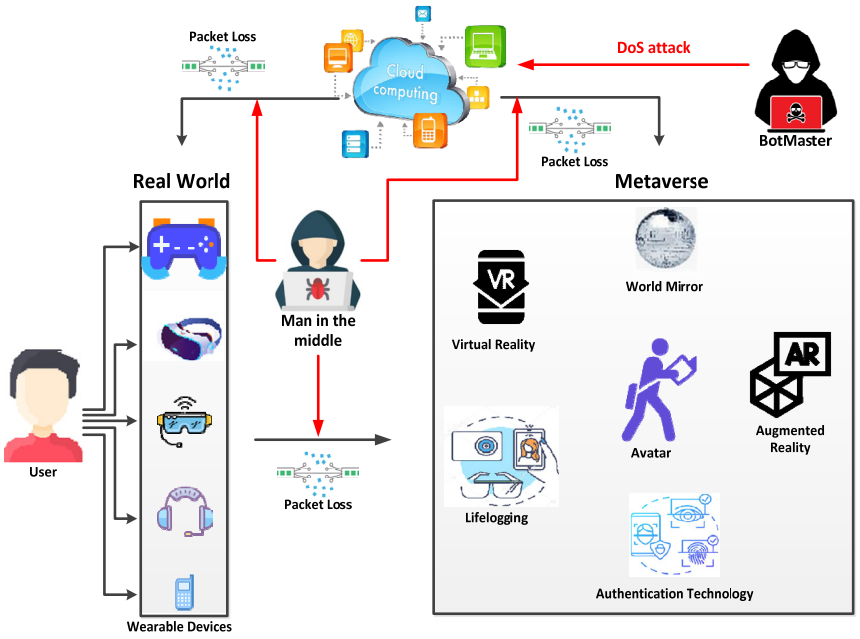

Figure 3. Common types of attacks on virtual reality learning systems.

3.4. Security in Metaverse Based on Other Data

With the use of cryptocurrency in the Metaverse, stacks would be inclined to hold digital assets and conduct daily transactions in digital tokens. Since the advent of cryptocurrencies, security problems have also drastically increased. Bitcoin is a peer-to-peer cryptocurrency system for which it is very difficult to trace its transactions, leading to an increase in illegal activities such as money laundering in the Bitcoin system. According to [55], the authors attempted to determine what combination of services actually prevents Bitcoin money laundering. A feature-based framework was introduced to identify the statistical features at three levels: networks, accounts, and transactions. The authors also described transaction models using attributed temporal heterogeneous (ATH) motifs. Furthermore, they tackled the mixed detection task as a positive and unlabeled (PU) learning problem and developed a detection model by leveraging the features that are considered. To analyze the transaction records, they created two kinds of temporal directed transaction networks: a homogeneous address–address interaction network (AAIN) and a heterogeneous transaction–address interaction network (TAIN). ATH motifs were proposed for the TAIN to analyze the complicated dynamic processes in the Bitcoin transaction network. Hybrid motifs with temporal homogeneous motifs in AAIN and ATH motifs in TAIN were employed as crucial features for detecting mixed services. The authors used three real data sets with labels from WalletExplorer, which provides label information of

addresses by making transactions with some services and observing how Bitcoin flows combine. They used logistic regression (LR) as the classifier. For the training set in one stage, they selected 70% unlabeled addresses and 70% labeled addresses in order to obtain some reliable negative instances. In stage two, they used 70% reliable negative instances as well as the labeled addresses used in stage one. For the testing set, they selected the remaining 30% reliable negative instances and 30% labeled addresses to evaluate the model. They evaluated the performance of the model in terms of TPR, FPR, and geometric mean (G-Mean) in order to evaluate its classification performance in imbalanced data sets. A comparison was made between their model and the one-class support vector machine (OCSVM), the isolation forest (IF), the decision tree (DT), and the InterScore (IS). As a result, they found that OCSVM, IF, and IS, which are unsupervised anomaly detection techniques, obtained most of the positive instances but had a higher FPR than other techniques. The IS performance was significantly differentiated in different data sets. LR and DT, as supervised techniques, presented over-fitting and relatively poor performance. The results showed that, on extremely imbalanced data sets, the PU learning framework performed better for Bitcoin mixing detection, with a TPR exceeding 91% and an FPR below 4%. Despite the good performance of the proposed method, mixing service providers might have to update their methods to avoid detection. As the detection model is based on prior information, and as the data are unlabeled, detection is difficult.

In the Metaverse, extended reality is expected to enable users to have better experiences through the use of devices such as headsets, smart glasses, haptics, and so on. A key consideration in extended reality (XR) privacy and security is protecting the vast amount of data gathered by these tools, as they are vulnerable to attack. According to [56], XR technology requires advanced human–computer interaction (HCI) devices for integration into the Metaverse. HCI devices use Internet of Things (IoT) wireless networks to communicate, in which a low-power and lossy networking protocol (RPL) is the backbone of an IPv6-based low-power and lossy network (LLN). IPv6 is a protocol that handles packets more efficiently in order to reduce the size of routing tables and increase security. An analysis of countermeasures to Sybil attacks on RPL-based networks was presented in this paper. A simulation environment with 100 nodes in 200 m of various areas was implemented using Contiki-NG and the MATLAB programming language. Additionally, two countermeasures were compared for analysis purposes. First, the Gini model—a countermeasure model based on the Gini index—was used to recognize and lessen Sybil attacks. Gini is a technique for propagating and sustaining code modifications in wireless sensor networks. In this attack, the malicious node broadcasts an destination-oriented-directed acyclic graph (DODAG) information object (DIO) with fake identities, which activates the trickle algorithm and causes the limited energy resources of genuine nodes to be depleted. On the other hand, Gini was emulated using ++OMNet, and to enable universal status awareness, a warning message was issued to every node. The second countermeasure was the ABC model, which uses a swarm-based meta-heuristic algorithm, does not have an alert system, and can identify Sybil nodes from the perspective of local nodes. Their findings indicated that the ABC model's detection performance was inferior to that of Gini but had superior performance to Gini in terms of the average expected time. Due to the nature of Sybil assaults, detection takes time. Therefore, when designing a model, detection delay and routing stability should be equally taken into account.

While the Metaverse is dependent on many cloud technologies to function, the ability for the Metaverse to successfully operate is also related to physical world events. Edge computing is a part of the physical infrastructure that can be used to enhance the safety of the Metaverse by distributing infrastructure closer to the end user and moving the compute, store, and data processing functions to the edge, enabling improved network response times and reduced network bandwidth. In [57], the authors presented a privacy-preserving framework for the wireless edge Metaverse. A Metaverse service provider (MSP) dedicates bandwidth to VR users in this framework, making access to the Metaverse from edge access points possible. To preserve privacy, a covert communication method

(exchange of data using a covert channel) is used in the downlink. By using the "covert" definition, targeted advertising is used to promote bandwidth sales and prevent competitors from making counter-offers or invaders from interrupting services. They obtained an outstanding advertising plan with the help of the Vidale–Wolfe model and Hamiltonian function. Meta immersion, a novel metric for measuring the feelings of Metaverse users, was also introduced in this work. They considered a jamming-aided covert wireless edge Metaverse access system. To recognize the necessary bandwidth for normal-quality access, the detection error probability, downlink covert rate (CR), and uplink bit-error rate (BER) were extracted under different modulations. For system implementation, an MSP with K users was considered, where the VR users use a head-mounted display (HMD) through EAPs (employee assistance programs). The authors introduced a friendly jammer to assist in communication by actively generating jamming signals to stop the data transmission detected by a malicious supervisor. In order to determine how much bandwidth an MSP should allocate to its users, a new metric to represent user feelings in the Metaverse was proposed. The user experience and service indicators included three groups: downlink data rate (which should be highly sufficient), uplink-tracking bit-error rate, and virtual experience (SK), which is influenced by their subjective behavior, such as their activity within the Metaverse, their online time, their physical health, and so on. The results of analysis based on the bit-error rate (BER) demonstrated that the interference between EAPs comes from jamming signals. With frequency division multiplexing, these signals can be ignored. User channel conditions can greatly influence the Metaverse experience, and targeted advertising contributes to the sale of acceleration bandwidth.

Generally, a watermark appears as a logo, text, or pattern on top of another image. It makes it more difficult to copy or use the original image without permission. Clearly, current NFTs used in the metaverse are not as secure as some would have you believe. The introduction of watermark technology is a game-changer since it provides much more than just basic copy-pasting protection for your NFT; it also acts as a visual indicator of which NFTs are secure to buy. According to [58], discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) are used for multiple watermarking in health applications. In this paper, to solve the authentication problem, three watermarks are used: medical Lump image, doctor signature/identification code, and the patient's diagnostic information. In order to remove noise effects, they use a backpropagation neural network (BPNN). An arithmetic compression technique and a Hamming error correction code are used to encode the signs in the signature. This algorithm performs well against a variety of signal processing attacks. For increased security, multiple watermarks are placed in the system simultaneously. However, as the number of watermarks rises the peak signal-to-noise ratio (PSNR) performance suffers and the computation time grows. The watermark is compressed using a lossless arithmetic compression method. Additionally, the Hamming error-correcting algorithm is utilized to secure the watermark of the doctor's signature and to lessen distortion. Furthermore, error correcting Hamming code (Hamming ECC) is employed to make up for the Bit Error Rate (BER) decline in the text watermark. The experiment's findings demonstrate that in the absence of an attack, the PSNR and Normalized cross-correlation (NC) values without BPNN are 43.88 and 0.9344, respectively and With BPNN, the value of NC is equal to 0.9547 (considering the gain factor of 0.01). NC is equal to 0.9888 with BPNN (assuming a gain factor of 0.08). In the absence of the BPNN algorithm, the highest NC value is obtained, which is 0.9852. A Median filtering attack yields the lowest NC value at 0.0123 and a CROP attack yields the highest BER at 47.619% and 44.7% for Symptoms and Signature watermarks, respectively. Based on these results, DTC, DWT, and SVD can be combined to achieve the best performance.

4. Discussion

Table 1 summarizes the security techniques discussed in Section 5, based on the system, vulnerability, attack type, solution, technique, metrics, and challenges. As shown

in the table, VR headsets and smartphones are the main platforms that have been used to study security performance in the Metaverse. As for the vulnerabilities in different Metaverse systems, we can see that personal information, biometric data, money laundering, user data, and learning content are the vulnerable points in available Metaverse networks, where biometric data appear to be the most vulnerable. There are many types of cybersecurity attacks that can be used to test a system's robustness. Spoofing, Sybil, DDoS, and eavesdropping attacks are some of the most common attacks. The results indicated that neural networks (NNs) and support vector machines (SVMs) are the most popular AI techniques, which have received more attention in Metaverse security protection due to the high accuracy of SVMs in classifying data into different classes as well as the efficiency and multi-tasking ability of NNs. These algorithms, which are used to extract fixed features, conduct mapping from multi-dimensional spaces to spaces with fewer dimensions.

As discussed in Section 3, AI-based AR, VR, and MR interfaces work as gateways to the Metaverse. The Metaverse is a deeper and broader concept than virtual games played online. AR, VR, MR, social media, digital currencies, and blockchain are all part of the Metaverse. All of these technologies are AI-based and heavily influence the development of the Metaverse. VR and AR technologies play a crucial role in providing users with an immersive experience in Metaverse. Sensory experiences within the Metaverse can be created using these technologies; as such, it goes without saying that VR headsets and glasses are needed in order to create these experiences in the Metaverse. In order to experience the Metaverse and enter the virtual world, users require some access devices, such as headsets for VR, smartphones or tablets for AR, and so on. The Metaverse powered by AI is also used in transportation, health care, the military (e.g., drones), smartphones, and virtual education. Avatars, robots, and digital twins are Metaverse characters that have identities similar to real-world characters, which require identity recognition systems. Metaverse objects and assets also require confirmation and identification, which can be carried out through NFTs. According to the research surveyed in this paper, user identification is one of the important security challenges in the Metaverse based on artificial intelligence, which is discussed in this study. Authentication methods that are mainly based on biometrics are the dominant methods for identification. Biometrics is a method for identifying users based on the use of their biological characteristics, which exist in different ways, including identification through fingerprints, face recognition, ear shape, eye scanning, lips movement, voice recognition, motion tracking, and so on. The use of biometrics to identify a person through the measurement and analysis of their unique physical and behavioral characteristics has gained great prominence.

Obviously, biometrics are always available to users. They can use biometric data in mobile phones, glasses, or browsers. Machine learning algorithms and artificial intelligence can be used to transform this data to create human–machine interactions. With the assumption that biometric data are unique to each person, the use of these data in user identification ensures the security of AI-based Metaverse systems. As can be seen from the results table, biometric-based identification methods provide reliable results against all types of attacks. Biometric authentication, however, does carry some risks. It should be noted that sharing biometric data with social network operators creates a greater risk for users through full control over the biometric information of users. Blockchain technology can be integrated into authentication systems based on biometric data to reduce the risk of cyber-attacks and to protect biometric data. By using blockchains, users can control their personal information. As the data cannot be changed after being placed in the ledger, it is very unlikely that identity information could be misused or stolen.

Additionally, one of the most important challenges in using biometric data for authentication is detection error. Biometric devices face two major problems: false-acceptance rates (FAR) and false-rejection rates (FRR). FAR refers to the probability of the device accepting a false user's authentication, while FRR refers to how often the device prevents an authorized user from entering. Ideally, the authorized user has a higher pattern than the unauthorized user, which means that the FAR is decreased as the is FRR increased. When

the score of the unauthorized user is higher than the minimum identification threshold, then access is allowed and vice versa: if the score of the authorized user is less than the maximum identification threshold, access is allowed. These errors may occur according to the age of users or weather and physical conditions, leading to harmful damage. As can be seen from the results in the table, the use of error correction codes is one of the most attractive ways to eliminate these errors. Using error correction codes, irregularities in a pattern can be decoded in a borderline manner such that the system receives biometric patterns without error.

Table 1. AI-based Metaverse cyber security summary.

Ref.	System	Vulnerability	Attack Type	Solution	Technique	Metrics	Challenges
[44]	VR headset	Personal information	Zero-effort, statistical attacks, shoulder-surfing	Blinkey	SVM, k-NN	FRR, FAR, ERR	Identifying the start and end points of a blinkey
[45]	Smartphone	Biometric data	FS, DFL, and FS-GAN attacks	Visual speaker authentication	DNN SA-DTH-Net	FAR, FRR, $\hat{H}$	Difficulties in recognizing speech content by lip-reading because of large vocabulary
[46]	VR face authentication	User data	Spoofing attacks	High-fidelity pose and expression normalization (HPEN)	SDM	Accuracy, and spoofing success rate	Illuminated infrared (IR) sensors
[47]	VR/AR touch sensors	Biometric data	Password leaking	Cyber security layer	ANN	Accuracy	Massive crossover electrodes, signal crosstalk, and propagation delay
[48]	AR in smartphone	User data	Zero-effort attack	SVM	SVM	ASR, FAR, TAR	Unlimited range of passwords, and different Smartphones
[49]	AR/VR headset	User data	Zero-effort and mimicking attacks	GaitLock	TDE+TM, DTW+NN, sparse fusion	EER, accuracy	implementing SRC-based approaches on Google Glass
[50]	AR headset	Biometric data	Voice spoofing, obstruction, and replay attacks	Hidden Markov model (HMM)	Hidden Markov model	Accuracy	Fake voice channels
[51]	Internet of Drones (IoD)	Drone data	Eavesdropping	PCSF	FL	QoS, security rate, training time	Computational complexity
[52]	Cyber–physical system	Transportation system data	CWM, WMFJ, and WMMJ attacks	SAF, RISA	SAF, RISA	Secrecy capacity	Eavesdropping defense with smart jammer (EDSJ) problem
[53]	VRLEs	Learning content	Network discrepancy, packet loss, and sniffing attacks	Attack tree	Attack tree	Impact of packet loss and scale of threats, risk score	Lack of policy change Control during VRLE sessions
[54]	VRLEs	Learning content	DoS attack	AFT	STA	Probability of cybersickness	Evaluation of different attacks
[55]	Bitcoin	Money laundering	Service contamination	ATH	OCSVM, IF, DT, IS	TPR, FPR	Unlabeled data make difficult detection
[56]	XR	User data	Sybil	Gini and ABC Model	Gini and ABC Model	Delay	Lack of computational information and lack of full model
[57]	Metaverse	User data	Competitive data theft	Jamming-aided covert access	Vidale–Wolfe model, Hamiltonian function	BER	Computational complexity
[58]	Watermark in healthcare	Personal information	Median filtering attack, CROP attack	DWT, DCT, and SVD	Backpropagation neural network, DWT, DCT, and SVD	BER, NC	Computational complexity

It is expected that further expansion of the Metaverse will pose countless challenges in the future. For example, with the expansion of haptic technology, the security risks in the Metaverse environment will become more real and tangible. Additionally, storing biometric data increases the risk of data leakage and misuse. It seems that, in order to overcome these problems and create a safer digital future, more research is needed in the field of creating security in the Metaverse.

5. Conclusions

The purpose of this paper was to discuss and analyze the cybersecurity of the AI-based Metaverse based on research conducted in the last few years. Our goal was to select the best papers and summarize them. As the AI-based Metaverse has not yet been considered in some aspects of security research, we attempted to consider the various aspects of Metaverse applications as much as possible and make the results available to other researchers. As mentioned earlier, in the field of cybersecurity, authentication is of great interest to researchers, and biometric methods are among the most important and widely used forms of authentication. Biometric data are very unique; thus, there is very little chance that they can be cheated. It is important to note, however, that there are also concerns, such as error detection and the possibility of biometric information being misused. Considering AI as one of the most effective solutions for complex cybersecurity problems in the Metaverse, we analyzed the role of AI in security, and it was concluded that neural network algorithms can greatly improve the attack detection accuracy. In order to conduct attack detection, authentication methods may use these algorithms. Alternatively, hackers can also make use of AI to attack the Metaverse. Various types of attacks have been described using AI algorithms in several papers. The results of this study suggest that researchers in this area face a very basic challenge regarding access to specific Metaverse data. While artificial intelligence and machine learning can help to guard against cyber-attacks, hackers can defeat security algorithms by targeting the data they use. It is also possible for hackers to use AI to break through defenses and develop mutating malware that can change its structure in order to avoid detection. In the absence of massive volumes of data and events, AI systems may produce inaccurate results and false positives. The consequences of data manipulation could be catastrophic if organizations fail to detect it, as they may struggle to recover the correct data that feed their AI systems. To develop AI-based Metaverse cybersecurity, collecting and classifying data is an attractive idea, as implicit intelligence algorithms require large data sets.

Author Contributions: Conceptualization, M.P., K.-J.H. and I.S.; methodology, M.P.; investigation, M.P., K.-J.H. and I.S.; writing—original draft preparation, M.P.; writing—review and editing, I.S.; visualization, M.P.; supervision, K.-J.H. and I.S.; project administration, K.-J.H. and I.S.; funding acquisition, K.-J.H. and I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20224000000020).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Moro Visconti, R. From Physical Reality to the Internet and the Metaverse: A Multilayer Network Valuation. *J. Metaverse* **2022**, *2*, 6–22. [CrossRef]
2. Leenes, R. Privacy in the Metaverse. In *IFIP International Summer School on the Future of Identity in the Information Society*; Springer: Boston, MA, USA, 2007; pp. 95–112.
3. Falchuk, B.; Loeb, S.; Neff, R. The social metaverse: Battle for privacy. *IEEE Technol. Soc. Mag.* **2018**, *37*, 52–61. [CrossRef]

4. Chukwunonso, A.G.; Njoku, J.N.; Lee, J.M.; Kim, D.S. Security in Metaverse: A Closer Look. In Proceedings of the Korean Telecommunications Society Conference, Seoul, South Korea, 9–11 February 2022; pp. 199–200.
5. Zhao, R.; Zhang, Y.; Zhu, Y.; Lan, R.; Hua, Z. Metaverse: Security and Privacy Concerns. *arXiv* **2022**, arXiv:2203.03854.
6. Wang, Y.; Su, Z.; Zhang, N.; Liu, D.; Xing, R.; Luan, T.H.; Shen, X. A survey on metaverse: Fundamentals, security, and privacy. *arXiv* **2022**, arXiv:2203.02662. [CrossRef]
7. Di Pietro, R.; Cresci, S. Metaverse: Security and Privacy Issues. In Proceedings of the Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Virtual, 13–15 December 2021; pp. 281–288.
8. Lee, L.H.; Braud, T.; Zhou, P.; Wang, L.; Xu, D.; Lin, Z.; Kumar, A.; Bermejo, C.; Hui, P. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv* **2021**, arXiv:2110.05352.
9. Ning, H.; Wang, H.; Lin, Y.; Wang, W.; Dhelim, S.; Farha, F.; Ding, J.; Daneshmand, M. A Survey on Metaverse: The State-of-the-art, Technologies, Applications, and Challenges. *arXiv* **2021**, arXiv:2111.09673.
10. Cheng, R.; Wu, N.; Chen, S.; Han, B. Will metaverse be next to internet? Vision, hype, and reality. *arXiv* **2022**, arXiv:2201.12894.
11. Lee, U.K.; Kim, H. UTAUT in Metaverse: An "Ifland" Case. *J. Theor. Appl. Electron. Commer. Res.* **2022**, *17*, 613–635. [CrossRef]
12. Muhanna, M.A. Virtual reality and the CAVE: Taxonomy, interaction challenges and research directions. *J. King Saud. Univ. Comput. Inf. Sci.* **2015**, *27*, 344–361. [CrossRef]
13. Daşdemir, Y. Cognitive investigation on the effect of augmented reality-based reading on emotion classification performance: A new dataset. *Biomed. Signal Process. Control.* **2022**, *78*, 103942. [CrossRef]
14. Avila, S. Implementing augmented reality in academic libraries. *Public Serv. Q.* **2017**, *13*, 190–199. [CrossRef]
15. Lopez, M.A.; Terron, S.; Lombardo, J.M.; Gonzalez-Crespo, R. Towards a solution to create, test and publish mixed reality experiences for occupational safety and health learning: Training-MR. *Int. J. Interact. Multimed. Artif. Intell.* **2021**, *7*, 212–223. [CrossRef]
16. Braud, T.; Lee, L.H.; Alhilal, A.; Fernández, C.B.; Hui, P. DiOS—An Extended Reality Operating System for the Metaverse. *arXiv* **2022**, arXiv:2201.03256. [CrossRef]
17. Nevelsteen, K.J. Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the Metaverse. *Comput. Animat. Virtual Worlds* **2018**, *9*, e1752. [CrossRef]
18. Messinger, P.R.; Stroulia, E.; Lyons, K.; Bone, M.; Niu, R.H.; Smirnov, K.; Perelgut, S. Virtual worlds—Past, present, and future: New directions in social computing. *Decis. Support Syst.* **2009**, *47*, 204–228. [CrossRef]
19. Shen, B.; Tan, W.; Guo, J.; Cai, H.; Wang, B.; Zhuo, S. A study on design requirement development and satisfaction for future virtual world systems. *Future Internet* **2020**, *12*, 112. [CrossRef]
20. Gajendra, S.; Sun, W.; Lu, Q. Communication in Second Life and E-business Opportunities: A Case Analysis. *Inf. Technol. J.* **2011**, *10*, 499–510. [CrossRef]
21. Shin, D.H. Understanding purchasing behaviors in a virtual economy: Consumer behavior involving virtual currency in Web 2.0 communities. *Interact. Comput.* **2008**, *20*, 433–446. [CrossRef]
22. Prendinger, H.; Ullrich, S.; Nakasone, A.; Ishizuka, M. MPML3D: Scripting agents for the 3D internet. *IEEE Trans. Vis. Comput. Graph.* **2010**, *17*, 655–668. [CrossRef]
23. Dominguez-Noriega, S.; Agudo, J.E.; Ferreira, P.; Rico, M. Language learning resources and developments in the Second Life metaverse. *Int. J. Technol. Enhanc. Learn.* **2011**, *3*, 496–509. [CrossRef]
24. Park, S.M.; Kim, Y.G. A Metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access* **2022**, *10*, 4209–4251. [CrossRef]
25. Arroyo, A.; Serradilla, F.; Calvo, O. Adaptive fuzzy knowledge-based systems for control metabots' mobility on virtual environments. *Expert Syst.* **2011**, *28*, 339–352. [CrossRef]
26. Allam, Z.; Bibri, S.E.; Jones, D.S.; Chabaud, D.; Moreno, C. Unpacking the '15-Minute City'via 6G, IoT, and Digital Twins: Towards a New Narrative for Increasing Urban Efficiency, Resilience, and Sustainability. *Sensors* **2022**, *22*, 1369. [CrossRef] [PubMed]
27. Lv, Z.; Qiao, L.; Li, Y.; Yuan, Y.; Wang, F.Y. BlockNet: Beyond reliable spatial Digital Twins to Parallel Metaverse. *Patterns* **2022**, *3*, 100468. [CrossRef]
28. Park, J.; Seo, Y.S. A Deep Learning-Based Action Recommendation Model for Cryptocurrency Profit Maximization. *Electronics* **2022**, *11*, 1466. [CrossRef]
29. Min, T.; Cai, W. Portrait of decentralized application users: An overview based on large-scale Ethereum data. *CCF Trans. Pervasive Comput. Interact.* **2022**, *4*, 124–141. [CrossRef]
30. Chalmers, D.; Fisch, C.; Matthews, R.; Quinn, W.; Recker, J. Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? *J. Bus. Ventur. Insights* **2022**, *17*, e00309. [CrossRef]
31. Güera, D.; Delp, E.J. Deepfake video detection using recurrent neural networks. In Proceedings of the 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 27–30 November 2018; pp. 1–6.
32. Lyu, S. Deepfake detection: Current challenges and next steps. In Proceedings of the IEEE International Conference on Multimedia & Expo Workshops (ICMEW), Taipei, Taiwan, 18–22 July 2020; pp. 1–6.
33. Yi, X.; Walia, E.; Babyn, P. Generative adversarial network in medical imaging: A review. *Med. Image Anal.* **2019**, *58*, 101552. [CrossRef]
34. Creswell, A.; White, T.; Dumoulin, V.; Arulkumaran, K.; Sengupta, B.; Bharath, A.A. Generative adversarial networks: An overview. *IEEE Signal Process. Mag.* **2018**, *35*, 53–65. [CrossRef]

35. Kaviani, S.; Sohn, I. Application of complex systems topologies in artificial neural networks optimization: An overview. *Expert Syst. Appl.* **2021**, *180*, 115073. [CrossRef]
36. Suykens, J.A.; Vandewalle, J. Least squares support vector machine classifiers. *Neural Process. Lett.* **1999**, *9*, 293–300. [CrossRef]
37. Do, T.-N. Incremental and parallel proximal SVM algorithm tailored on the Jetson Nano for the ImageNet challenge. *Int. J. Web Inf. Syst.* 2022; ahead-of-print.
38. Pooyandeh, M.; Sohn, I. Edge Network Optimization Based on AI Techniques: A Survey. *Electronics* **2021**, *10*, 2830. [CrossRef]
39. Al-Mohannadi, H.; Mirza, Q.; Namanya, A.; Awan, I.; Cullen, A.; Disso, J. Cyber-attack modeling analysis techniques: An overview. In Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 69–76.
40. Chinnasamy, P.; Deepalakshmi, P.; Dutta, A.K.; You, J.; Joshi, G.P. Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in AI-Enabled IoT System. *Mathematics* **2021**, *10*, 68. [CrossRef]
41. Ionut-Cristian, S.; Dan-Marius, D. Using Inertial Sensors to Determine Head Motion—A Review. *J. Imaging* **2021**, *7*, 265. [CrossRef] [PubMed]
42. Wu, Y.; Karakurt, I.; Beker, L.; Kubota, Y.; Xu, R.; Ho, K.Y.; Zhao, S.; Zhong, J.; Zhang, M.; Wang, X.; et al. Piezoresistive stretchable strain sensors with human machine interface demonstrations. *Sens. Actuators A Phys.* **2018**, *279*, 46–52. [CrossRef]
43. Saranya, D.; Chinnasamy, P.; Nalinipriya, G.; Jeipratha, P.N.; Wise, D.J.; Kalaiarasi, A. Adaptive Intelligence System based on the Internet of Things for Patient Monitoring in Remote Area. In Proceedings of the International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 25–27 January 2022; pp. 1–6.
44. Zhu, H.; Jin, W.; Xiao, M.; Murali, S.; Li, M. Blinkey: A two-factor user authentication method for virtual reality devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2020**, *4*, 1–29. [CrossRef]
45. Yang, C.Z.; Ma, J.; Wang, S.; Liew, A.W. Preventing deepfake attacks on speaker authentication by dynamic lip movement analysis. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1841–1854. [CrossRef]
46. Wu, J.; Liu, J.; Chen, W.; Huang, H.; Zheng, Z.; Zhang, Y. Detecting mixing services via mining bitcoin transaction network with hybrid motifs. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *52*, 2237–2249. [CrossRef]
47. Xu, Y.; Price, T.; Frahm, J.M.; Monrose, F. Virtual u: Defeating face liveness detection by building virtual models from your public photos. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 497–512.
48. Wei, C.; Lin, W.; Liang, S.; Chen, M.; Zheng, Y.; Liao, X.; Chen, Z. An All-In-One Multifunctional Touch Sensor with Carbon-Based Gradient Resistance Elements. *Nano Micro Lett.* **2022**, *14*, 131. [CrossRef]
49. Yao, J.; Ansari, N. Secure federated learning by power control for internet of drones. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 1021–1031. [CrossRef]
50. Kim, J.D.; Ko, M.; Chung, J.M. Novel Analytical Models for Sybil Attack Detection in IPv6-based RPL Wireless IoT Networks. In Proceedings of the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–9 January 2022; pp. 1–3.
51. Wang, K.; Yuan, L.; Miyazaki, T.; Chen, Y.; Zhang, Y. Jamming and eavesdropping defense in green cyber–physical transportation systems using a Stackelberg game. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4232–4242. [CrossRef]
52. Khan, H.; Hengartner, U.; Vogel, D. Augmented reality-based mimicry attacks on behaviour-based smartphone authentication. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services, Munich, Germany, 10–15 June 2018; pp. 41–53.
53. Shen, Y.; Wen, H.; Luo, C.; Xu, W.; Zhang, T.; Hu, W.; Rus, D. GaitLock: Protect virtual and augmented reality headsets using gait. *IEEE Trans. Dependable Secur. Comput.* **2018**, *16*, 484–497. [CrossRef]
54. Gulhane, A.; Vyas, A.; Mitra, R.; Oruche, R.; Hoefer, G.; Valluripally, S.; Calyam, P.; Hoque, K.A. Security, privacy and safety risk assessment for virtual reality learning environment applications. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Vegas, NV, USA, 11–14 January 2019; pp. 1–9.
55. Valluripally, S.; Gulhane, A.; Hoque, K.A.; Calyam, P. Modeling and defense of social virtual reality attacks inducing cybersickness. *IEEE Trans. Dependable Secure Comput.* **2021**, *19*, 4127–4144. [CrossRef]
56. Du, H.; Niyato, D.; Kang, J.; Kim, D.I.; Miao, C. Optimal targeted advertising strategy for secure wireless edge metaverse. *arXiv* **2021**, arXiv:2111.00511.
57. Shang, J.; Wu, J. Enabling secure voice input on augmented reality headsets using internal body voice. In Proceedings of the 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–9.
58. Zear, A.; Singh, A.K.; Kumar, P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed. Tools Appl.* **2018**, *77*, 4863–4882. [CrossRef]