IoT

*Review*

# Exploring the Confluence of IoT and Metaverse: Future Opportunities and Challenges

**Rameez Asif * and Syed Raheel Hassan**

School of Computing Sciences, University of East Anglia, Norwich Research Park, Norwich NR4 7TJ, UK
* Correspondence: rameez.asif@uea.ac.uk

**Abstract:** The Internet of Things (IoT) and the metaverse are two rapidly evolving technologies that have the potential to shape the future of our digital world. IoT refers to the network of physical devices, vehicles, buildings, and other objects that are connected to the internet and capable of collecting and sharing data. The metaverse, on the other hand, is a virtual world where users can interact with each other and digital objects in real time. In this research paper, we aim to explore the intersection of the IoT and metaverse and the opportunities and challenges that arise from their convergence. We will examine how IoT devices can be integrated into the metaverse to create new and immersive experiences for users. We will also analyse the potential use cases and applications of this technology in various industries such as healthcare, education, and entertainment. Additionally, we will discuss the privacy, security, and ethical concerns that arise from the use of IoT devices in the metaverse. A survey is conducted through a combination of a literature review and a case study analysis. This review will provide insights into the potential impact of IoT and metaverse on society and inform the development of future technologies in this field.

**Keywords:** blockchain; metaverse; Internet of Things; security; privacy; artificial intelligence

**Citation:** Asif, R.; Hassan, S.R. Exploring the Confluence of IoT and Metaverse: Future Opportunities and Challenges. *IoT* **2023**, *4*, 412–429. https://doi.org/10.3390/iot4030018

Academic Editor: Amiya Nayak

Received: 13 February 2023
Revised: 5 September 2023
Accepted: 6 September 2023
Published: 12 September 2023

## 1. Introduction

The Internet of Things (IoT) is a dynamically emerging technology that is redefining our interactions with our surroundings [1,2]. IoT is a network of physical devices, automobiles, buildings, and other items that are linked to the internet and capable of collecting and sharing data [3]. These devices have sensors, actuators, and communication capabilities that allow them to gather and transfer data in real time. The growing number of linked devices is one of the key trends in IoT [4]. According to recent research, there are reportedly over 30 billion linked devices in the world, with that figure anticipated to rise to more than 75 billion by 2025 [5]. The increasing availability of affordable IoT devices, as well as the proliferation of IoT applications in new domains such as healthcare, transportation, and smart cities, is driving this rise.

Edge computing is also becoming more prevalent in IoT networks. The term “edge computing” is used to describe the practice of processing data at or near the point of data collection as opposed to storing it in a centralised facility [6]. Because of this, data may be processed more quickly and efficiently while also being protected from unauthorised access [7]. When it comes to the Internet of Things, edge computing shines when it comes to low-latency processing for applications like industrial automation, robotics, and autonomous cars. One major development in the Internet of Things is the growing interest in using artificial intelligence (AI) and machine learning (ML) to decipher the massive volumes of data produced by IoT gadgets [8,9]. As a result, we can make better, more informed decisions and develop cutting-edge services and software [10].

The integration of 5G networks for IoT devices is another direction that the industry is heading [11,12]. In order to improve the efficiency and dependability of communication between IoT devices, 5G delivers higher data rates and lower latency than previous generations of mobile networks [13]. This will open the door to novel applications like real-time analytics, driverless cars, and smart cities. Furthermore, there is an increasing number of people apprehensive about the safety and privacy of their IoT devices [14]. The threat of data breaches and cyber assaults increases as more gadgets gather and communicate data. This has prompted a greater effort to create confidential methods for IoT devices to communicate with one another [15,16].

The metaverse is a virtual realm in which individuals may communicate and share digital products in real time [17]. It is a cutting-edge innovation that might change the face of the digital future. Despite the fact that the metaverse is most commonly linked with gaming, it has several potential uses in fields like teaching, performing arts, and even commerce [18,19]. Virtual and augmented reality (VR and AR) technologies are becoming increasingly popular in the metaverse. Users are able to fully engage with digital worlds because of these advancements in technology. In the sphere of education, for instance, it is possible to establish virtual classrooms and virtual labs to provide students real-world experience in a supervised setting. Blockchain technology is becoming increasingly popular, which is another metaverse trend [20]. Transactions made using blockchain technology are both private and immutable since it is a distributed ledger system. Using this innovation, people may build economies in the metaverse where they can buy, sell, and exchange digital representations of real-world products and services.

Moreover, for growth, there is the integration of AI and ML into metaverse creations in an effort to make virtual worlds that seem more genuine and interesting to users [21]. The application of AI and ML allows for the development of more lifelike and interactive digital environments, as well as more convincing and lifelike avatars that can interact with people in more natural ways. Bringing together various types of social media is another growing movement in the metaverse. Facebook, Twitter, and TikTok are building their own metaverses, where users may communicate and share content with one another and with virtual things in real time [22]. It is becoming increasingly possible on these systems for users to build and share their own virtual environments. Last but not least, privacy and security are becoming increasingly pressing issues in the virtual world [23]. The potential for cyber assaults and data breaches increases as more people use these platforms to exchange sensitive information. The need for safe and confidential methods of transmitting data in the metaverse has, therefore, become more important.

The convergence of IoT and the metaverse presents an opportunity to design more realistic and interactive virtual worlds [18,24,25]. Incorporating IoT devices into the metaverse allows for more dynamic responses to events in the physical world, as depicted in Figure 1. The integration of components in an IoT network with the metaverse involves various elements working together seamlessly. IoT devices, such as sensors and actuators, are connected to the network and collect data from the physical world. These data are then transmitted to edge gateways, which serve as intermediate points for processing and filtering the information before sending it to the metaverse platforms. Metaverse platforms, powered by advanced technologies like virtual reality and artificial intelligence, create a virtual world where users can interact. The data collected from IoT devices are utilised by these platforms to provide real-time information and enable virtual spaces to interact with the real world [18]. This integration allows users to have a realistic and immersive experience in the metaverse, where they can interact, work, and play. IoT devices and edge gateways play a crucial role in capturing and transmitting data, while metaverse platforms utilise these data to create a dynamic and interactive virtual environment. Overall, the integration of these components enhances the capabilities of the metaverse and enables a seamless interaction between virtual and physical worlds.

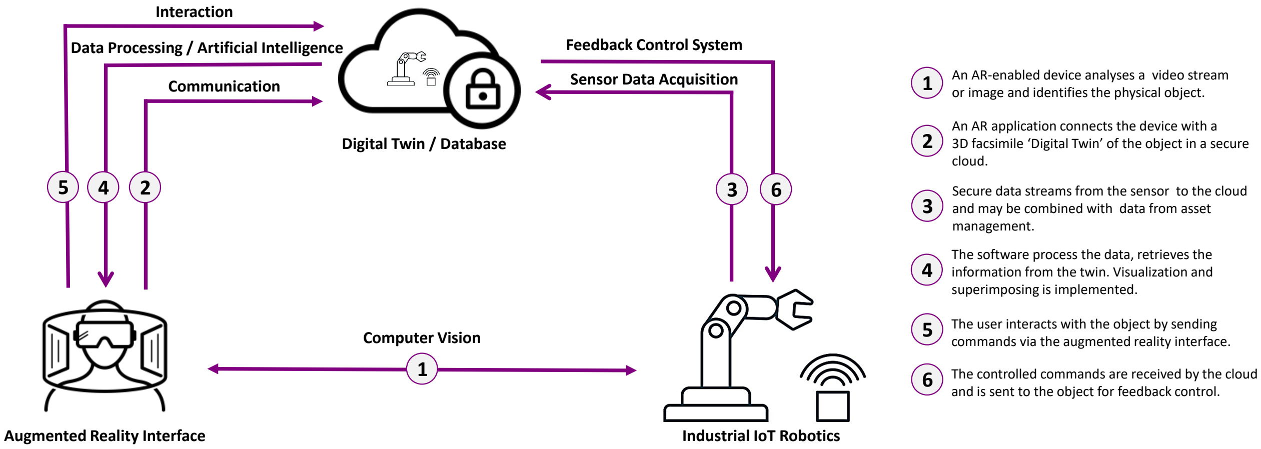
Interaction
Data Processing / Artificial Intelligence
Communication
Digital Twin / Database
Feedback Control System
Sensor Data Acquisition
5
4
2
3
6
Computer Vision
1
Augmented Reality Interface
Industrial IoT Robotics
1 An AR-enabled device analyses a video stream or image and identifies the physical object.
2 An AR application connects the device with a 3D facsimile 'Digital Twin' of the object in a secure cloud.
3 Secure data streams from the sensor to the cloud and may be combined with data from asset management.
4 The software process the data, retrieves the information from the twin. Visualization and superimposing is implemented.
5 The user interacts with the object by sending commands via the augmented reality interface.
6 The controlled commands are received by the cloud and is sent to the object for feedback control.

**Figure 1.** Basic workflow of augmented reality (AR) devices including communication links, data analytics, and cloud computing.

Developing novel use cases and applications for IoT devices across sectors, including healthcare, education, and entertainment, is another promising area of exploration [26]. The IoT might be used to construct virtual classrooms where students can interact with each other and digital items in real time, or virtual medical clinics where patients can receive treatment and consultation remotely. Furthermore, new kinds of digital trade may emerge as a result of the merging of the IoT and metaverse. Incorporating blockchain technology would enable the development of virtual economies within the metaverse, wherein users would be able to engage in the buying, selling, and trading of virtual products and services [27,28].

Despite these benefits, the merging of these technologies also presents some new difficulties. As people become more comfortable sharing details about their lives online, privacy and security have become pressing issues. Using IoT devices in the metaverse raises ethical considerations as it threatens to dissolve the boundaries between the real and the virtual [29].

In recent years, the integration of the Internet of Things (IoT) with the metaverse has attracted substantial attention, with global surveys suggesting a growing interest in this technology's potential applications. Through IoT, the integration of physical objects with virtual environments has the potential to produce novel and inventive user experiences in the metaverse. Moreover, AI may play a vital role in enriching these experiences and making them more engaging and personalised, as detailed in [18,25]. However, the integration of IoT with the metaverse also raises worries over the possibility of cyber-attacks, as this technology presents a new target for cybercriminals. Organisations must employ stringent security measures to safeguard user data and reduce the likelihood of cyber assaults. This article, in the following sections, intends to offer a complete overview of the integration of IoT and the metaverse, covering the present state of worldwide surveys, the integration of AI, user applications, and real-world metaverse platforms. We have comprehensively discussed the tools that can be used based on an as-a-service model to create digital twins for IoT and metaverse, while the main focus will be on potential cyber security threats and challenges.

## 2. Global Adoption Surveys

Several significant survey reports on the subject of IoT and the metaverse have been published, which include information such as market size, growth rate, and market segmentation using several parameters, including component, application, organisation size, vertical, and region [30,31]. These papers also provide information on regional growth and industry trends.

A survey conducted by the International Data Corporation (IDC) in 2020 found that the global market for IoT is expected to grow from GBP 190 billion in 2020 to GBP 1.1 trillion in 2027 (https://www.idc.com/getdoc.jsp?containerId=US48087621 accessed on

16 January 2023). The study also found that the manufacturing, transportation and logistics, and healthcare industries are expected to be the top adopters of IoT technology. Another survey conducted by the research firm Gartner in 2020 found that worldwide spending on IoT is expected to reach GBP 1.3 trillion in 2022, up from GBP 745 billion in 2019 (https://www.gartner.com/en/information-technology/insights/internet-of-things accessed on 16 January 2023). The study also found that the transportation and logistics, manufacturing, and healthcare industries are the top adopters of IoT technology. A study by the research firm MarketsandMarkets, in 2020, found that the global metaverse market is expected to grow from GBP 1.7 billion in 2020 to GBP 11.9 billion by 2026, at a CAGR of 50.3% during the forecast period. The study also found that the gaming and entertainment industry is expected to be the largest contributor to the metaverse market during the forecast period (https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html accessed on 16 January 2023).

There are a number of survey studies on the adoption of the metaverse that contain information on age and geographic location. These studies give information on the metaverse's popularity by location and the age group most likely to embrace it. These data are important for businesses and developers intending to target certain audiences with their metaverse-related products and services, as depicted in Figure 2. One such report is the "Global Metaverse Market Survey and Trend Research 2018" published by ReportsWeb. This report provides a detailed analysis of the global metaverse market, including market size, growth rate, and market segmentation by component, application, and region. The report also includes survey data on the adoption of the metaverse by geographical region and age, including information such as the following:

- The metaverse is most popular among young adults aged 25–34, followed by those aged 16–24.

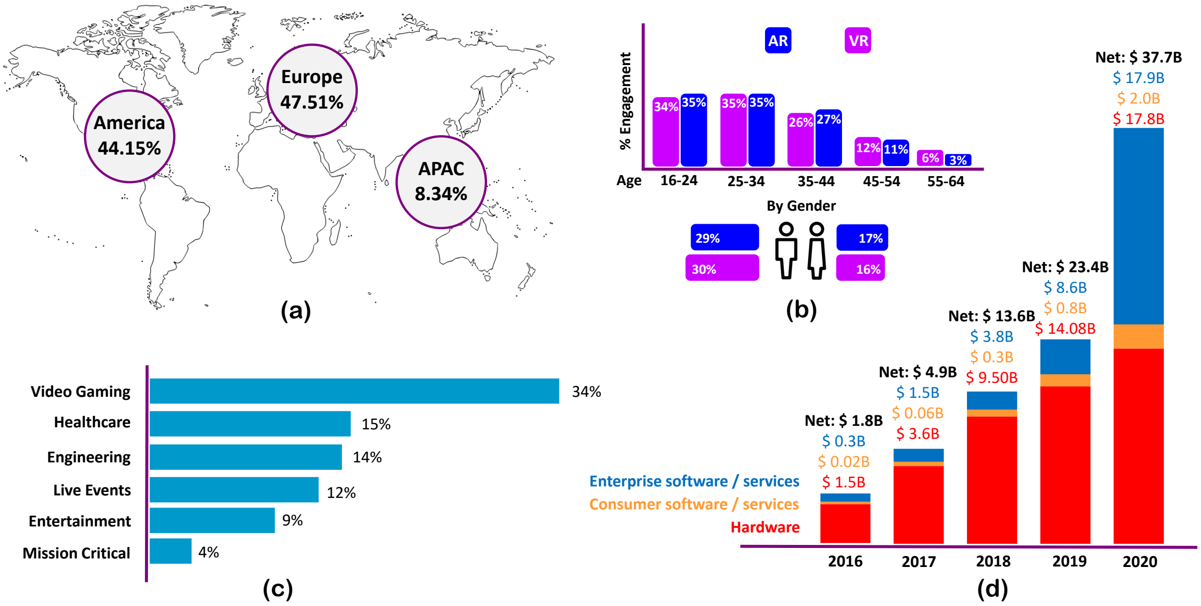

**Figure 2.** Global augmented reality (AR) sales and marketing revenue, including geographical sales distribution and end-user applications. (**a**) Technology adoption as per the geographical location, (**b**) age and gender distribution, (**c**) sectors incorporating IoT and metaverse, and (**d**) market capitalisation on software, hardware, and consumer service.

Another report is the "Metaverse Market: Global Forecast 2022" published by MarketsandMarkets. This report provides a detailed analysis of the global metaverse market, including market size, growth rate, and market segmentation by component, application, and region. The report also includes survey data on the adoption of the metaverse by geographical region, including information such as the following:

- Europe is the largest market for the metaverse, followed by North America and Asia Pacific.
- The Asia Pacific region is expected to be the fastest-growing market for the metaverse due to the increasing adoption of virtual and augmented reality technology in the region.

Most of the end-user applications of IoT devices and metaverse are in the gaming industry, and it is expected to reach GBP 196.0 billion by 2025, growing at a CAGR of 9.3% during the forecast period. There are several other potential applications for the metaverse beyond gaming and entertainment. One such application is in the field of education and training. The metaverse can be used to create immersive learning experiences for students and employees. With the ability to simulate real-world scenarios, the metaverse can provide hands-on training and allow for more interactive and engaging learning. We will discuss the use cases in detail in a later section.

## 3. System Architecture and Integration

System design would include the integration of several diverse technologies and components to provide users with a smooth and secure experience, as depicted in Figure 3. These include IoT devices, cloud computing, data processing via AI algorithms, virtual reality software or hardware, etc. [32]. Data would be collected by IoT devices and sent to edge gateways, which would subsequently transfer it to cloud platforms for storage, analysis, and processing [33,34]. This information would then be utilised to develop and update virtual worlds in the metaverse, with which users may engage via VR and AR technologies [35]. Blockchain networks would be utilised to build virtual economies inside the metaverse, while AI and ML models would be employed to make virtual settings more realistic and engaging [36,37].

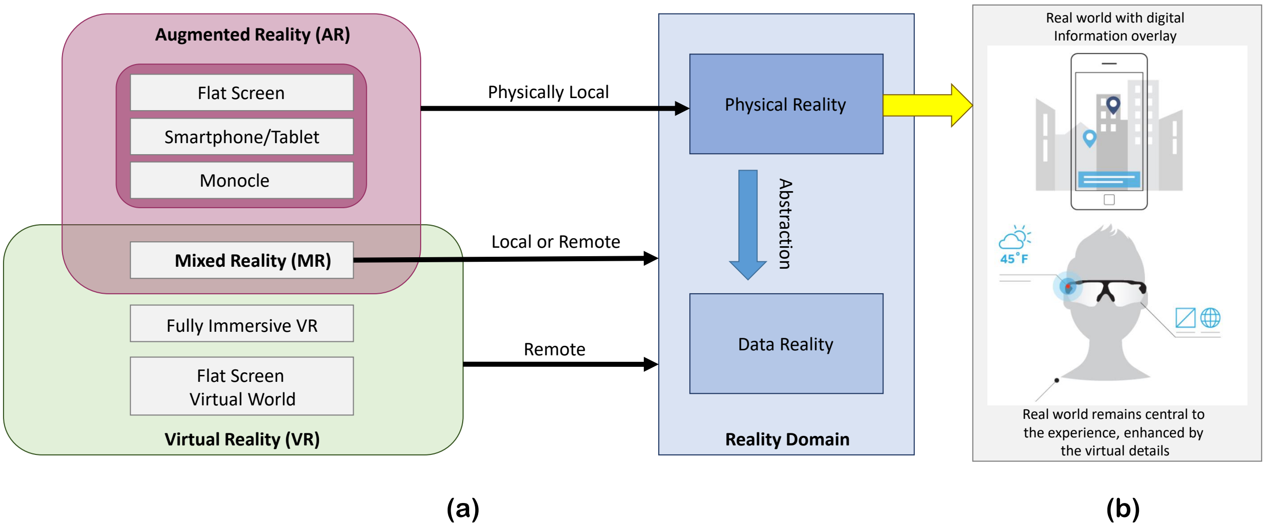

**Figure 3.** (**a**) A system architecture view of augmented, virtual, and mixed reality and (**b**) user experience vectors in case of augmented reality.

Several essential parts would make up the system architecture of an IoT-embedded metaverse. Among them are the following:

- **IoT Devices:** These are the physical devices that are connected to the internet and capable of collecting and transmitting data. They may include sensors, actuators, and communication capabilities. Examples include smart thermostats, cameras, and wearable devices.
- **Edge Gateways:** These are devices that act as intermediaries between IoT devices and the cloud. They are responsible for collecting and processing data from IoT devices and transmitting them to the cloud. Edge gateways are important for edge computing, which enables low-latency processing of data.

- **Cloud Platforms:** These are servers and software that are responsible for storing, analysing, and processing data from IoT devices. They may include platforms such as Amazon Web Services or Microsoft Azure.
- **Metaverse Platforms:** These are the virtual worlds wherein users can interact with each other and digital objects in real time. They may include platforms such as Second Life or VRChat.
- **Blockchain Networks:** These are decentralised and distributed ledger technologies that are responsible for secure and transparent transactions within the metaverse. They may include platforms such as Ethereum or EOS.
- **AI and ML Models:** These are used to analyse and make sense of the vast amounts of data generated by IoT devices and to create more realistic and engaging virtual environments.
- **Data Security and Privacy:** This component is necessary to ensure that data transmitted and stored are protected against unauthorised access and breaches. This is essential for keeping user data private and safe.

Network connectivity is essential for analysing information from the metaverse in an IoT system. To transport data from the metaverse to the cloud or edge gateways, IoT devices must be able to connect to a network [38]. There are several sorts of network connectivity options available:

1. Wi-Fi: Wi-Fi is a popular choice for network connectivity as it is widely available and can provide high-speed and reliable connectivity. IoT devices can connect to a Wi-Fi network using a built-in wireless module or an external adapter.
2. Cellular: Cellular networks, such as 3G, 4G, and 5G, can provide IoT devices with a reliable and secure connection, even in remote or hard-to-reach areas. This option is particularly useful for IoT devices that are located in areas where Wi-Fi is not available.
3. Low-power wide-area networks (LPWANs): LPWANs, such as LoRaWAN, Sigfox, and NB-IoT, are designed specifically for low-power IoT devices and can provide long-range connectivity. They are particularly useful for IoT devices that are located in remote areas or require low power consumption.
4. Satellite: Satellite networks can provide IoT devices with connectivity in remote or hard-to-reach areas where other types of networks are not available. This option is particularly useful for IoT devices that are located in areas with no cellular or Wi-Fi coverage.
5. Mesh networks: Mesh networks are a type of network that allows IoT devices to communicate with each other directly, without the need for a central hub. This type of network is particularly useful for IoT devices that are located in remote or hard-to-reach areas, as it allows for increased reliability and scalability.

The key characteristics and performance parameters of these communication networks are summarised in Table 1. It is worth mentioning that the selection of communication medium depends on the end-use application [39]. If high-bandwidth data transmission is required, we are only limited to WiFi and cellular transmission. Most of the metaverse content is high-definition in nature, and careful consideration should be made to collect the system requirements, such as latency, frequency, bandwidth, etc.

**Table 1.** Network connectivity options available for metaverse.

| Connectivity | Data Rates | Frequency | Latency | Coverage | Cost |
|---|---|---|---|---|---|
| **WiFi** | 100–300 Mbps | 2.4/5 GHz | 150 ms | Indoors | Economical |
| **Cellular 5G** | 1 Gbps | 26/66 GHz | 20–50 ms | Outdoors/indoors | Expensive |
| **LPWAN** | 10–50 Kbps | 433 MHz | 300 ms | Indoors | Economical |
| **Satellite** | 10–50 Mbps | 10-/2 GHz | 550 ms | Outdoors | Expensive |
| **NB-IoT** | 60 Kbps | 900 MHz | 1.5 s | Outdoors/indoors | Economical |

A more secure and dependable link between devices and the metaverse is provided by Software-Defined Wide Area Networking (SD-WAN), which might benefit both the IoT and the metaverse [40,41] as shown in Figure 4. With SD-WAN, network traffic can be better managed and optimised, which is especially important for data-intensive applications like those found in the Internet of Things and the metaverse [42,43]. IoT and metaverse communications benefit greatly from SD-ability WANs to lower their latency, as this is a crucial factor in real-time interactions. With its VPN and strong encryption features, SD-WAN may also make IoT and metaverse connections safer [44]. The security of personal information and the prevention of cyber-attacks are both aided by this measure. IoT and metaverse implementations can benefit greatly from SD-WAN because of the increased flexibility and scalability it offers. In order to accommodate the ever-increasing number of devices and users in the IoT and metaverse, SD-WAN can enable dynamic adjustments to network configurations, depending on changing network circumstances [45].

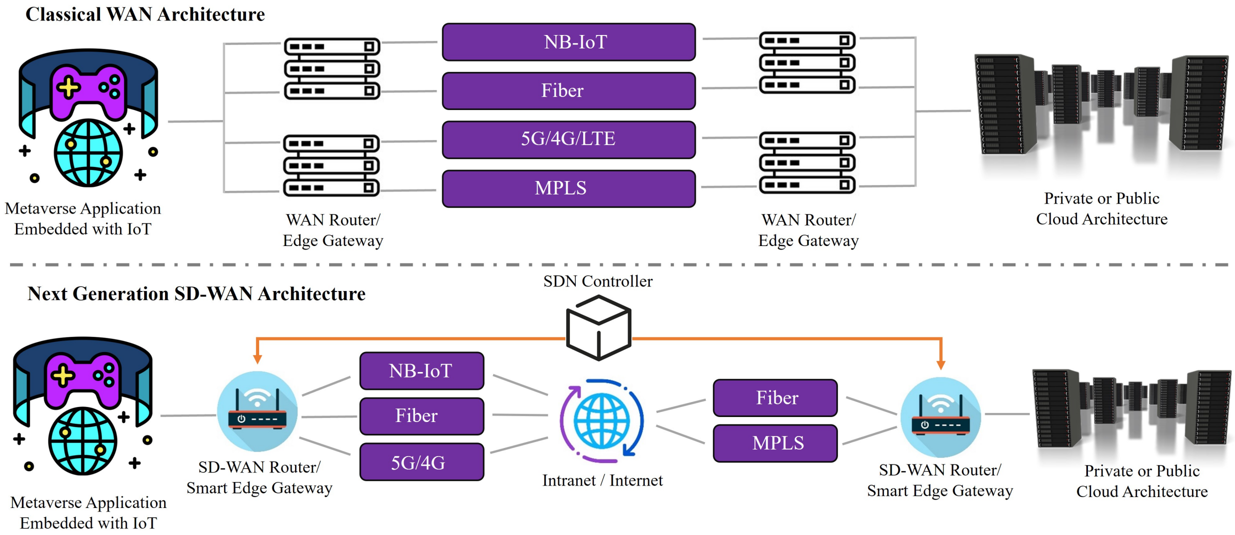
Classical WAN Architecture
Metaverse Application Embedded with IoT
WAN Router/ Edge Gateway
NB-IoT
Fiber
5G/4G/LTE
MPLS
WAN Router/ Edge Gateway
Private or Public Cloud Architecture
Next Generation SD-WAN Architecture
SDN Controller
Metaverse Application Embedded with IoT
SD-WAN Router/ Smart Edge Gateway
NB-IoT
Fiber
5G/4G
Intranet / Internet
Fiber
MPLS
SD-WAN Router/ Smart Edge Gateway
Private or Public Cloud Architecture

**Figure 4.** SD-WAN architecture, a potential candidate to provide communication resources to metaverse applications.

Over the last few years, several standards and frameworks have been created to allow IoT and metaverse integration, including Open Metaverse Interoperability (OMI), Virtual World Framework (VWF), and OpenXR [46,47]. These standards intend to provide a standardised set of tools and technologies for creating metaverse settings and connecting IoT devices to them, making it easier for developers to construct and integrate IoT devices into these environments [48]. Some of them are summarised in this section:

- IEEE P2413: This is a standard developed by the Institute of Electrical and Electronics Engineers (IEEE) that defines a reference architecture for the metaverse [47,49]. It provides a framework for the integration of virtual and physical worlds and covers areas such as security, identity, and data management.
- Open Metaverse Interface (OMI): This is a framework that provides a common set of APIs and protocols for different virtual worlds and metaverse platforms. It allows for the interoperability of different virtual worlds and makes it easier for developers to create applications that can be used across multiple platforms [46].
- Web3D Consortium: This is an international industry consortium that develops and maintains standards for 3D web technologies. The main goal of the consortium is to make it possible to create and share interactive 3D content on the web [50,51].
- Virtual Reality Modelling Language (VRML): This is a standard for representing 3D interactive vector graphics, designed particularly for the World Wide Web. VRML is being succeeded by X3D, which is an ISO standard for 3D graphics, and is also compatible with VRML [52].

- OpenXR: This is an open standard for virtual and augmented reality that aims to provide a common API for different VR and AR hardware and software platforms. This makes it easier for developers to create VR and AR applications that can be used across different hardware and software platforms [53].
- ISO/IEC 30141: This is an ISO/IEC standard that describes the requirements and characteristics of an IoT system. It covers various aspects, including security, data management, device management, and communication protocols, which can be applied to IoT systems that collect data from the metaverse [54].

## 4. Metaverse Platforms and Digital Twins

The phrase "metaverse" refers to a virtual reality realm that is interconnected and available to a large number of users, comparable to the notion of the internet but in a 3D, immersive environment [18,37,46]. These platforms are intended to let users engage with one another and with digital items in a shared area and may include elements like social networking, gaming, and commerce [55]. There are a number of different metaverse platforms that are currently available or in development. Some examples include:

- **Second Life:** One of the oldest and most well-established metaverse platforms, Second Life has been in operation since 2003. It allows users to create and customise their own avatars and virtual spaces and has a strong focus on user-generated content and community building [19,56].
- **VRChat:** A social platform for virtual reality users, VRChat allows users to interact with each other in a variety of virtual environments. It has a large and active community and is particularly popular among gamers and VR enthusiasts [57,58].
- **Decentraland:** A decentralised, blockchain-based metaverse platform that allows users to create, experience, and monetise content and applications. Users can purchase virtual land and create their own experiences, and the platform is also home to a variety of games and social spaces [59,60].
- **Somnium Space:** A decentralised and blockchain-based metaverse platform that allows users to buy, rent, and monetise virtual land. Somnium Space is focused on creating a seamless and realistic VR experience, allowing users to interact with each other and the virtual world in real time [61].
- **VR Gaming Platforms:** Some popular VR gaming platforms, such as Oculus Quest, also offer social and multiplayer features that allow users to interact with each other in a virtual environment [62,63].
- **Blue Marble:** A metaverse platform that uses blockchain technology to create a decentralised and community-driven virtual world (https://thebluemarble.io/ accessed on 16 January 2023). It allows users to create and share content, as well as engage in commerce and social activities.

The metaverse is currently in its early phases of development, with numerous platforms still under construction [64]. The technology and infrastructure needed to enable fully realised metaverse platforms are still growing, but it is apparent that these platforms will play an important part in the future of the internet and human connection [65].

Metaverse platforms often use their own native cryptocurrency to facilitate transactions within the virtual world [66]. These cryptocurrencies are designed to be used as a form of payment for virtual goods and services, such as buying virtual land, in-game items, or other digital assets. They can also be used to incentivise users to participate in the ecosystem, such as through staking or governance mechanisms. Some examples of metaverse cryptocurrencies include SAND, the native cryptocurrency of the Decentraland metaverse platform, and AXIOM—the native cryptocurrency of the AxiomVerse metaverse platform [67,68]. Additionally, some existing cryptocurrencies, like Bitcoin and Ethereum, can also be used in metaverse platforms as a form of payment. These metaverse cryptocurrencies are still in their early stages of development, but they have the potential to play a significant role in the economy of the metaverse and in the future of digital currencies.

Digital twin technology enables the establishment of a seamless and interconnected virtual and physical environment by integrating metaverse platforms with the Internet of Things (IoT) [69,70]. The production of a virtual counterpart of a physical thing, such as a building or a machine, that can be used to remotely monitor and operate the real-world object is referred to as digital twin technology [71,72]. It is feasible to construct a virtual representation of the physical world that is continually updated with real-world data by merging metaverse platforms with IoT via digital twin technologies. This allows users in the metaverse to interact with the physical world in novel ways, such as remotely manipulating objects and machinery or seeing the physical world in a virtual manner [73,74]. There are tools available that can help to integrate the IoT and metaverse platforms; these are summarised in Table 2.

**Table 2.** Summary of the platforms available for integrating IoT with metaverse via digital twin.

| Tools | Description | References |
|---|---|---|
| **Unity** | Unity is a popular game engine and development platform that can be used to create virtual environments and digital twins. It has built-in support for IoT devices, making it easy to integrate real-world data into virtual environments. | [75] |
| **Unreal Engine** | Similar to Unity, Unreal Engine is another popular game engine and development platform that can be used to create digital twins. It also has built-in support for IoT devices and can be used to create highly detailed and realistic virtual environments. | [76] |
| **ThingWorx** | ThingWorx is an IoT platform that can be used to connect and manage IoT devices, as well as to create and implement digital twin models. It offers a wide range of features and tools for integrating real-world data into virtual environments, such as data visualisation, analytics, and machine learning. | [77,78] |
| **AWS IoT** | AWS IoT is a cloud-based platform that can be used to connect and manage IoT devices, as well as to create and implement digital twin models. It offers a wide range of tools and services to support the integration of IoT and metaverse, such as AWS IoT SiteWise, AWS IoT Things Graph, and AWS IoT Analytics. | [79] |
| **Bosch IoT** | Bosch IoT Suite is an IoT platform that provides a set of tools and services for connecting, managing, and analysing IoT devices. The platform also includes a digital twin capability that allows customers to create virtual models of physical assets, enabling them to make better-informed decisions based on real-time data. | [80] |

## 5. Artificial Intelligence and Data Processing

AI plays an important role in the IoT embedded metaverse because it allows intelligent decision making and autonomous behaviour in IoT devices and systems. As the number of connected devices grows, so does the volume of data created by these devices [81]. AI may be used to evaluate and interpret this data, hence improving the overall performance and efficiency of IoT systems. Machine learning is a significant area where AI may play a role in IoT-embedded metaverse [82]. Machine learning algorithms could be employed to study and learn from data from IoT devices, which can then be used to anticipate future behaviour. Machine learning algorithms, for example, may be used in a smart home environment to learn the normal usage patterns of household equipment and then utilise this knowledge to optimise energy consumption and save expenses. Natural language processing (NLP) is another area where AI may well be employed in IoT-embedded metaverse [81,83]. NLP algorithms may be utilised to improve the user experience by providing more intuitive and tailored interactions with IoT devices.

Another area where AI may be used in an IoT-embedded metaverse is computer vision. Computer vision algorithms may be used to analyse and understand visual input, allowing IoT devices to perform and operate better [64,84]. A security camera with computer vision capabilities, for example, might be used to identify and track persons or objects in real time, alerting the user if something is wrong. AI can also assist in improving the security and dependability of IoT devices. As the number of connected devices grows, so does the potential for security breaches and assaults. AI may be used, in real time, to detect and respond to possible threats and abnormalities, which can aid in the security of IoT systems and the data they create [85]. Furthermore, AI can play a significant role in the metaverse. It is capable of creating lifelike and interactive digital avatars, making the metaverse experience more realistic and engaging. AI may also be utilised to provide consumers with tailored experiences, such as proposing virtual settings or activities that are relevant to their interests [86]. Furthermore, AI may aid in the creation of more dynamic and responsive virtual worlds, such as one in which the weather changes based on real-world data. There are several specific algorithms that can be used in the context of IoT-embedded metaverse and AI. Some examples include the following:

- **Machine Learning Algorithms:** These algorithms can be used to learn from data generated by IoT devices and make predictions about future behaviour [87,88]. Examples include supervised learning algorithms like linear regression and decision trees, unsupervised learning algorithms like k-means and hierarchical clustering, and deep learning algorithms like convolutional neural networks and recurrent neural networks [81].
- **Natural Language Processing (NLP) Algorithms:** These algorithms can be used to process and understand natural language input, which can be used to improve the user experience by enabling more intuitive and personalised interactions with IoT devices [89]. Examples include part-of-speech tagging, syntactic parsing, and sentiment analysis [90].
- **Computer Vision Algorithms:** These algorithms can be used to process and understand visual data, which can be used to improve the performance and functionality of IoT devices. Examples include object detection, image segmentation, and facial recognition [91,92].
- **Anomaly Detection Algorithms:** These algorithms can be used to detect unusual or abnormal behaviour in IoT data, which can help to identify potential security threats and improve the overall reliability of IoT systems. Examples include statistical methods like Mahalanobis distance and density-based methods like local outlier factor [93,94].
- **Reinforcement Learning Algorithms:** These algorithms can be used to train IoT devices to make decisions based on rewards or penalties [95,96]. This can be used to optimise the performance of IoT systems [97].
- **Generative Algorithms:** These algorithms can be used to generate new data that can be used to create new experiences in the metaverse, for example, creating new virtual environments, digital avatars, or digital characters [98].

To summarise, the role of AI in an IoT-embedded metaverse is to enable intelligent decision making and autonomous behaviour in IoT devices and systems. It can improve the overall user experience by providing personalised and intuitive interactions with IoT devices and systems [99]. Furthermore, it can also help to improve the security and reliability of IoT systems by detecting and responding to potential threats and anomalies in real time [100,101]. Additionally, AI can also play an important role in the metaverse by creating believable and interactive digital avatars, personalised experiences, and more dynamic and responsive virtual environments. As the IoT and metaverse continue to evolve, the integration of AI will become even more important to improve the overall performance and functionality of these systems.

## 6. Security and Privacy

The interconnected architecture of these systems increases the risk of security breaches and cyber-attacks, making security and privacy paramount considerations in the IoT-embedded metaverse [100]. The absence of security in IoT devices is a major cause for worry. Insufficient thought that was given to the security of many IoT devices during their development phase leaves them vulnerable to malware and hacking. Many IoT devices also have weak or readily guessed passwords, increasing their susceptibility to attack [101]. The insufficient safety of the networks used to link IoT devices is also a cause for worry. It is common for IoT devices to rely on wireless communication methods, which are inherently less secure than their wired counterparts. There is also the fact that the massive amounts of data produced by IoT devices might make it hard to keep their interconnected communication networks safe [18].

Moreover, data privacy issues have been raised in relation to IoT devices. Location data, health data, and financial data are just a few examples of the kinds of sensitive information that IoT devices frequently gather and broadcast [102]. Without appropriate safeguards, sensitive information is vulnerable to interception and misuse. Worries about users' digital identities and private data being kept safe and secure are another issue in the metaverse. Users' digital identities are at risk in the metaverse because their avatars and their interactions with other users generate a trail of data that may be stolen in a data breach or used to steal their identities [103].

Strong security mechanisms must be included at all levels in IoT-embedded metaverse systems, from the devices themselves to the communication networks that connect them, in order to solve these concerns [104,105]. Methods for achieving this goal include encrypting data at rest and in transit, utilising strong authentication and access restrictions, and using secure communication protocols [106]. Data created by IoT devices must be protected by taking steps like anonymizing it and reducing the quantity of data that is gathered and retained. It is crucial to take measures in the metaverse to preserve the security and privacy of users' digital personas and data [107]. By allowing users to manage their own privacy and security settings and enforcing features like encryption and authentication, virtual environments may be made safer.

There have not been many reported cyber-attacks specifically targeting the metaverse as it is a relatively new and emerging technology. However, there have been some notable cyber-attacks that have targeted virtual worlds and online gaming platforms, as given in Table 3, which can provide insight into the types of threats that the metaverse may face in the future.

**Table 3.** Notable cyber-attacks specifically targeting the metaverse.

| Platform | Explanation of Cyber Incident | Year |
|---|---|---|
| **Second Life** | A group of hackers known as the "Griefers" launched a series of attacks on the virtual world Second Life. They used a variety of tactics, such as creating fake avatars to flood the virtual world with unwanted objects and stealing virtual currency from other users. The attacks caused widespread disruption and damage to the virtual world and its economy. | 2007 |
| **World of Warcraft** | Hackers launched a distributed denial of service (DDoS) attack on the popular online game World of Warcraft. The attack caused the game's servers to become overloaded and caused widespread disruption to the game's player base. | 2010 |
| **Pokemon Go** | The popular mobile game Pokemon Go was targeted by a DDoS attack. The attack caused the game's servers to become overloaded, making it difficult for players to access the game. | 2016 |
| **Roblox** | A massively multiplayer online game platform was targeted by a cyber-attack that resulted in unauthorised access to user data, specifically user's information like email addresses and hashed passwords. | 2021 |

These incidents are indicative of the potential dangers that the metaverse could face in the future, such as distributed denial of service assaults, hacking, and the theft of virtual money. The necessity of being aware of and equipped for these vulnerabilities increases as the metaverse expands and becomes increasingly integrated into our daily lives.

## 7. End-User Applications

Smart cities are one of the most common applications of IoT and metaverse technologies. IoT technology may be used to link and manage a city's different systems, such as traffic lights, public transit, and energy systems. These data may be collected and evaluated in real time, allowing municipal planners to make informed decisions on how to enhance city operations [86,108]. These data might be seen and interacted with in a virtual environment in a metaverse, allowing city planners and people to readily access and interpret this information. A metaverse, for example, might be used by city planners to model the consequences of alternative traffic flow patterns or by people to plan the most efficient route to work [109].

Another possible application of IoT and metaverse technologies is in retail. Retailers might employ IoT technology to collect data on customer preferences and behaviour, which they could then use to create individualised virtual shopping experiences in the metaverse [106]. Customers may explore merchandise, try on garments, and even make purchases all from the comfort of their own homes. This might improve customers' shopping experiences while also increasing revenue for merchants. Another area where IoT and metaverse technologies may be utilised to increase efficiency and productivity is remote collaboration [110]. IoT technology might be used to connect workers in different places, allowing them to work on projects in real time inside a metaverse [111]. Workers may be able to share information and collaborate as if they were in the same physical area, even if they are in different regions of the world, if this technology is implemented.

One area where IoT and metaverse technologies can have a huge influence is healthcare. Wearable and medical gadgets that are IoT-enabled can be used to monitor patient's health in real time. These data might be incorporated into a metaverse, making it easier for healthcare practitioners to access and evaluate them [112]. This might enhance patient outcomes by allowing healthcare practitioners to identify and address possible health risks more immediately [64]. Furthermore, virtual reality and augmented reality technologies, which are part of the metaverse, can be leveraged to deliver more immersive medical instruction and treatment. An intriguing application of IoT and metaverse technologies is virtual tourism [113,114]. IoT technology may be used to link and regulate numerous systems in tourist locations, such as lighting and temperature, as well as to gather data on visitor behaviour using cameras and other sensors [115]. These data may be utilised to construct individualised virtual tours of tourist places in a metaverse, giving tourists a new and fascinating way to experience these destinations.

## 8. Future Challenges and Open Issues

The future integration of the IoT and the metaverse is anticipated to present a variety of opportunities and difficulties. With increased connectivity and data exchange between IoT devices and the metaverse, security and privacy concerns become even more vital. The interconnectivity of devices and virtual environments introduces new vulnerabilities, making it imperative to implement stringent security measures to safeguard sensitive data and prevent unauthorised access [116]. The fusion of IoT and the metaverse will generate a massive quantity of data. Managing and analysing this enormous volume of data in real time presents a formidable challenge. Effective techniques for data storage, processing, and analysis will be required to derive actionable insights and optimise system performance [117].

Moreover, interoperability and standardised protocols are required for the seamless integration of various IoT devices and platforms within the metaverse. Without consistent standards, compatibility issues may arise between various devices and platforms, hindering their ability to interact and collaborate effectively. As the metaverse becomes an integral part of people's existence, ethical considerations become of the utmost importance. To ensure the responsible and ethical use of IoT technologies in the metaverse, issues such as data ownership, consent, digital rights, and the possibility of surveillance must be addressed. Furthermore, infrastructure and connectivity are essential to the successful integration of IoT and the metaverse. Extending network coverage, enhancing network bandwidth, and decreasing latency will be essential for delivering seamless experiences and supporting the expanding number of connected devices [118].

To address these challenges, technology providers, policymakers, industry stakeholders, and researchers will need to collaborate. By proactively addressing these issues, the integration of IoT and the metaverse can unlock immense potential and provide future experiences that are transformative.

## 9. Conclusions

In this paper, we discussed the integration of IoT and metaverse technologies that have the potential to alter the way we live and work by enabling the development of novel and fascinating use cases. The capacity of IoT technology to collect data, combined with the ability of metaverse technology to see and interact with these data in a virtual environment, can give useful insights and enhance decision-making processes via AI. However, it is critical to remember that for this integration to be successful, there must be a focus on security, systems, and frameworks. It is critical from a security standpoint to guarantee that data generated from IoT devices are kept safe and that a user‘s personal information is secured. This may be accomplished by creating stringent security rules and regularly auditing systems. This integration of IoT and metaverse technologies necessitates a solid and dependable infrastructure. This involves ensuring that systems can manage the massive volumes of data created by IoT devices, as well as the high levels of traffic and user interactions that are envisioned in a metaverse.

**Author Contributions:** Conceptualisation, R.A. and S.R.H.; resources, R.A. and S.R.H.; data curation, R.A.; writing—original draft preparation, R.A.; writing—review and editing, R.A. and S.R.H.; supervision, R.A.; project administration, R.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Not applicable.

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

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| AI | Artificial Intelligence |
| AR | Augmented Reality |
| CS | Cybersecurity |
| DApps | Decentralised Applications |
| DDOS | Distributed Denial of Service |
| DLT | Distributed Ledger Technology |
| GDPR | General Data Protection Regulation |
| IDC | International Data Corporation |
| IoT | Internet of Things |
| IIoT | Industrial Internet of Things |
| LPWAN | Low-Power Wide-Area Networks |
| ML | Machine Learning |
| MR | Mixed Reality |
| NB-IOT | Narrow Band IoT |
| NLP | Natural Language Processing |
| OMI | Open Metaverse Interface |
| SD-WAN | Software-Defined Wide-Area Networking |
| VR | Virtual Reality |
| VRML | Virtual Reality Modelling Language |
| VWF | Virtual World Framework |

## References

1. Asghari, P.; Rahmani, A.M.; Javadi, H.H.S. Internet of Things applications: A systematic review. *Comput. Netw.* **2019**, *148*, 241–261. [CrossRef]
2. Xu, L.D.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]

3. Lohiya, R.; Thakkar, A. Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review. *IEEE Internet Things J.* **2021**, *8*, 8774–8798. [CrossRef]
4. Ding, J.; Nemati, M.; Ranaweera, C.; Choi, J. IoT Connectivity Technologies and Applications: A Survey. *IEEE Access* **2020**, *8*, 67646–67673. [CrossRef]
5. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
6. Goudarzi, M.; Wu, H.; Palaniswami, M.; Buyya, R. An Application Placement Technique for Concurrent IoT Applications in Edge and Fog Computing Environments. *IEEE Trans. Mob. Comput.* **2021**, *20*, 1298–1311. [CrossRef]
7. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
8. Alshehri, F.; Muhammad, G. A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. *IEEE Access* **2021**, *9*, 3660–3678. [CrossRef]
9. Sandner, P.; Gross, J.; Richter, R. Convergence of Blockchain, IoT, and AI. *Front. Blockchain* **2020**, *3*, 522600. [CrossRef]
10. Sutjarittham, T.; Habibi Gharakheili, H.; Kanhere, S.S.; Sivaraman, V. Experiences with IoT and AI in a Smart Campus for Optimizing Classroom Usage. *IEEE Internet Things J.* **2019**, *6*, 7595–7607. [CrossRef]
11. Wang, D.; Chen, D.; Song, B.; Guizani, N.; Yu, X.; Du, X. From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies. *IEEE Commun. Mag.* **2018**, *56*, 114–120. [CrossRef]
12. Liu, X.; Zhang, X. Rate and Energy Efficiency Improvements for 5G-Based IoT with Simultaneous Transfer. *IEEE Internet Things J.* **2019**, *6*, 5971–5980. [CrossRef]
13. Agiwal, M.; Saxena, N.; Roy, A. Towards Connected Living: 5G Enabled Internet of Things (IoT). *IETE Tech. Rev.* **2019**, *36*, 190–202. [CrossRef]
14. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
15. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
16. Attkan, A.; Ranga, V. Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex Intell. Syst.* **2022**, *8*, 3559–3591. [CrossRef]
17. Mystakidis, S. Metaverse. *Encyclopedia* **2022**, *2*, 486–497. [CrossRef]
18. Wang, Y.; Su, Z.; Zhang, N.; Xing, R.; Liu, D.; Luan, T.H.; Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Commun. Surv. Tutor.* **2022**, *25*, 319–352. [CrossRef]
19. Sparkes, M. What is a metaverse. *New Sci.* **2021**, *251*, 18. . [CrossRef]
20. Yang, Q.; Zhao, Y.; Huang, H.; Xiong, Z.; Kang, J.; Zheng, Z. Fusing Blockchain and AI with Metaverse: A Survey. *IEEE Open J. Comput. Soc.* **2022**, *3*, 122–136. [CrossRef]
21. Hollensen, S.; Kotler, P.; Opresnik, M.O. Metaverse—The new marketing universe. *J. Bus. Strategy* **2022**, *44*, 119–125. [CrossRef]
22. Pasquini, C.; Amerini, I.; Boato, G. Media forensics on social media platforms: A survey. *EURASIP J. Inf. Secur.* **2021**, *2021*. [CrossRef]
23. Kim, J. Advertising in the Metaverse: Research Agenda. *J. Interact. Advert.* **2021**, *21*, 141–144. [CrossRef]
24. Benedict, S. Serverless Blockchain-Enabled Architecture for IoT Societal Applications. *IEEE Trans. Comput. Soc. Syst.* **2020**, *7*, 1146–1158. [CrossRef]
25. Li, K.; Cui, Y.; Li, W.; Lv, T.; Yuan, X.; Li, S.; Ni, W.; Simsek, M.; Dressler, F. When Internet of Things Meets Metaverse: Convergence of Physical and Cyber Worlds. *IEEE Internet Things J.* **2023**, *10*, 4148–4173. [CrossRef]
26. 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. *IEEE Internet Things J.* **2021**, *10*, 14671–14688. [CrossRef]
27. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhao, P.; Liu, S. A Survey of Blockchain and Intelligent Networking for the Metaverse. *IEEE Internet Things J.* **2022**, *10*, 3587–3610. [CrossRef]
28. Huang, H.; Zeng, X.; Zhao, L.; Qiu, C.; Wu, H.; Fan, L. Fusion of Building Information Modeling and Blockchain for Metaverse: A Survey. *IEEE Open J. Comput. Soc.* **2022**, *3*, 195–207. [CrossRef]
29. Fernandez, C.B.; Hui, P. Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse. In Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Bologna, Italy, 10 July 2022; pp. 272–277. [CrossRef]
30. Nalbant, K.G.; Aydın, S. Development and Transformation in Digital Marketing and Branding with Artificial Intelligence and Digital Technologies Dynamics in the Metaverse Universe. *J. Metaverse* **2023**, *3*, 9–18. [CrossRef]
31. Zhang, H.; Lee, S.; Lu, Y.; Yu, X.; Lu, H. A Survey on Big Data Technologies and Their Applications to the Metaverse: Past, Current and Future. *Mathematics* **2023**, *11*, 96. [CrossRef]
32. Han, Y.; Niyato, D.; Leung, C.; Kim, D.I.; Zhu, K.; Feng, S.; Shen, X.; Miao, C. A Dynamic Hierarchical Framework for IoT-Assisted Digital Twin Synchronization in the Metaverse. *IEEE Internet Things J.* **2023**, *10*, 268–284. [CrossRef]

33. Wang, Y.; Zhao, J. A Survey of Mobile Edge Computing for the Metaverse: Architectures, Applications, and Challenges. In Proceedings of the 2022 IEEE 8th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 14–16 December 2022. [CrossRef]
34. Chang, L.; Zhang, Z.; Li, P.; Xi, S.; Guo, W.; Shen, Y.; Xiong, Z.; Kang, J.; Niyato, D.; Qiao, X.; et al. 6G-Enabled Edge AI for Metaverse: Challenges, Methods, and Future Research Directions. *J. Commun. Inf. Netw.* **2022**, *7*, 107–121. [CrossRef]
35. Chang, C.; Bang, K.; Wetzstein, G.; Lee, B.; Gao, L. Toward the next-generation VR/AR optics: A review of holographic near-eye displays from a human-centric perspective. *Optica* **2020**, *7*, 1563–1578. [CrossRef]
36. Kim, J.C.; Laine, T.H.; Åhlund, C. Multimodal Interaction Systems Based on Internet of Things and Augmented Reality: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 1738. [CrossRef]
37. Maksymyuk, T.; Gazda, J.; Bugár, G.; Gazda, V.; Liyanage, M.; Dohler, M. Blockchain-Empowered Service Management for the Decentralized Metaverse of Things. *IEEE Access* **2022**, *10*, 99025–99037. [CrossRef]
38. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. A Survey on Mobile Augmented Reality with 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1160–1192. [CrossRef]
39. Wang, Y.; Zhao, J. Mobile Edge Computing, Metaverse, 6G Wireless Communications, Artificial Intelligence, and Blockchain: Survey and Their Convergence. In Proceedings of the 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 26 October–11 November 2022. [CrossRef]
40. Hu, P.; Ning, H.; Chen, L.; Daneshmand, M. An Open Internet of Things System Architecture Based on Software-Defined Device. *IEEE Internet Things J.* **2019**, *6*, 2583–2592. [CrossRef]
41. Troia, S.; Sapienza, F.; Varé, L.; Maier, G. On Deep Reinforcement Learning for Traffic Engineering in SD-WAN. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2198–2212. [CrossRef]
42. Wood, M. How to make SD-WAN secure. *Netw. Secur.* **2017**, *2017*, 12–14. [CrossRef]
43. Duliński, Z.; Stankiewicz, R.; Rzym, G.; Wydrych, P. Dynamic Traffic Management for SD-WAN Inter-Cloud Communication. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1335–1351. [CrossRef]
44. Pamplin, S. SD-WAN revolutionises IoT and edge security. *Netw. Secur.* **2021**, *2021*, 14–15. [CrossRef]
45. Rajagopalan, S. A Study on MPLS Vs SD-WAN. In *Computer Networks, Big Data and IoT*; Pandian, A., Fernando, X., Islam, S.M.S., Eds.; Spriger: Singapore, 2021; pp. 297–304.
46. Shi, F.; Ning, H.; Zhang, X.; Li, R.; Tian, Q.; Zhang, S.; Zheng, Y.; Guo, Y.; Daneshmand, M. A new technology perspective of the Metaverse: Its essence, framework and challenges. *Digit. Commun. Netw.* **2022**. [CrossRef]
47. Trivedi, Y. Innovation & competition: Succeeding through global standards: A new massive open online course delivered on IEEE X.org. *IEEE Commun. Mag.* **2016**, *54*, 7–9. [CrossRef]
48. Takahashi, K.; Ogata, Y.; Nonaka, Y. A proposal of unified reference model for smart manufacturing. In Proceedings of the 2017 13th IEEE Conference on Automation Science and Engineering (CASE), Xi'an, China, 20–23 August 2017; pp. 964–969. [CrossRef]
49. Park, H.; Kim, H.; Joo, H.; Song, J. Recent advancements in the Internet-of-Things related standards: A oneM2M perspective. *ICT Express* **2016**, *2*, 126–129. [CrossRef]
50. Daly, L.; Brutzman, D. X3D: Extensible 3D Graphics Standard [Standards in a Nutshell]. *IEEE Signal Process. Mag.* **2007**, *24*, 130–135. [CrossRef]
51. Polys, N.F.; Brutzman, D.; Steed, A.; Behr, J. Future Standards for Immersive VR: Report on the IEEE Virtual Reality 2007 Workshop. *IEEE Comput. Graph. Appl.* **2008**, *28*, 94–99. [CrossRef] [PubMed]
52. Brutzman, D. The Virtual Reality Modeling Language and Java. *Commun. ACM* **1998**, *41*, 57–64. [CrossRef]
53. Spiess, F.; Gasser, R.; Heller, S.; Rossetto, L.; Sauter, L.; van Zanten, M.; Schuldt, H. Exploring Intuitive Lifelog Retrieval and Interaction Modes in Virtual Reality with Vitrivr-VR. In Proceedings of the 4th Annual on Lifelog Search Challenge, New York, NY, USA, 21 August 2021; pp. 17–22. [CrossRef]
54. Di Martino, B.; Rak, M.; Ficco, M.; Esposito, A.; Maisto, S.; Nacchia, S. Internet of things reference architectures, security and interoperability: A survey. *Internet Things* **2018**, *1–2*, 99–112. [CrossRef]
55. Aburbeian, A.M.; Owda, A.Y.; Owda, M. A Technology Acceptance Model Survey of the Metaverse Prospects. *AI* **2022**, *3*, 285–302. [CrossRef]
56. Sanchez, J. Second Life: An Interactive Qualitative Analysis. In Proceedings of the Society for Information Technology & Teacher Education International Conference 2007, San Antonio, TX, USA, 26 March 2007; Carlsen, R., McFerrin, K., Price, J., Weber, R., Willis, D.A., Eds.; Association for the Advancement of Computing in Education (AACE): Waynesville, NC, USA pp. 1240–1243.
57. Reis, A.B.; Ashmore, M. From video streaming to virtual reality worlds: An academic, reflective, and creative study on live theatre and performance in the metaverse. *Int. J. Perform. Arts Digit. Media* **2022**, *18*, 7–28. [CrossRef]
58. Jeon, Y.A. Reading Social Media Marketing Messages as Simulated Self Within a Metaverse: An Analysis of Gaze and Social Media Engagement Behaviors within a Metaverse Platform. In Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Virtual, 12–16 March 2022; pp. 301–303. [CrossRef]
59. Guidi, B.; Michienzi, A. Social games and Blockchain: Exploring the Metaverse of Decentraland. In Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Bologna, Italy, 10 July 2022; pp. 199–204. [CrossRef]
60. Dowling, M. Is non-fungible token pricing driven by cryptocurrencies? *Financ. Res. Lett.* **2022**, *44*, 102097. [CrossRef]

61. Ante, L. Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations. *Econ. Innov. New Technol.* **2022**, 1–19. [CrossRef]
62. Yildirim, C.; Carroll, M.; Hufnal, D.; Johnson, T.; Pericles, S. Video Game User Experience: To VR, or Not to VR? In Proceedings of the 2018 IEEE Games, Entertainment, Media Conference (GEM), Galway, Ireland, 15–17 August 2018; pp. 1–9. [CrossRef]
63. Izountar, Y.; Benbelkacem, S.; Otmane, S.; Khababa, A.; Masmoudi, M.; Zenati, N. VR-PEER: A Personalized Exer-Game Platform Based on Emotion Recognition. *Electronics* **2022**, *11*, 455. [CrossRef]
64. Mozumder, M.A.I.; Sheeraz, M.M.; Athar, A.; Aich, S.; Kim, H.C. Overview: Technology Roadmap of the Future Trend of Metaverse based on IoT, Blockchain, AI Technique, and Medical Domain Metaverse Activity. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 13–16 February 2022; pp. 256–261. [CrossRef]
65. Dionisio, J.D.N.; Burns, W.G., III; Gilbert, R. 3D Virtual Worlds and the Metaverse: Current Status and Future Possibilities. *ACM Comput. Surv.* **2013**, *45*, 1–38. [CrossRef]
66. Akkus, H.T.; Gursoy, S.; Dogan, M.; Demir, A.B. Metaverse and Metaverse Cryptocurrencies (Meta Coins): Bubbles or Future? *J. Econ. Financ. Account.* **2022**, *9*, 22–29. [CrossRef]
67. Vidal-Tomás, D. The new crypto niche: NFTs, play-to-earn, and metaverse tokens. *Financ. Res. Lett.* **2022**, *47*, 102742. [CrossRef]
68. Kshetri, N. Policy, Ethical, Social, and Environmental Considerations of Web3 and the Metaverse. *IT Prof.* **2022**, *24*, 4–8. [CrossRef]
69. Banaeian Far, S.; Imani Rad, A. Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges. *J. Metaverse* **2022**, *2*, 8–15.
70. 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]
71. Zhang, J.; Zong, M.; Li, W. A Truthful Mechanism for Multibase Station Resource Allocation in Metaverse Digital Twin Framework. *Processes* **2022**, *10*, 2601. [CrossRef]
72. Lin, Y.; Chen, L.; Ali, A.; Nugent, C.; Ian, C.; Li, R.; Gao, D.; Wang, H.; Wang, Y.; Ning, H. Human Digital Twin: A Survey. *arXiv* **2022**, arXiv:2212.05937.
73. Lv, Z.; Shang, W.L.; Guizani, M. Impact of Digital Twins and Metaverse on Cities: History, Current Situation, and Application Perspectives. *Appl. Sci.* **2022**, *12*, 1208. [CrossRef]
74. Hashash, O.; Chaccour, C.; Saad, W.; Sakaguchi, K.; Yu, T. Towards a Decentralized Metaverse: Synchronized Orchestration of Digital Twins and Sub-Metaverses. *arXiv* **2022**, arXiv:2211.14686.
75. Messaoudi, F.; Simon, G.; Ksentini, A. Dissecting games engines: The case of Unity3D. In Proceedings of the 2015 International Workshop on Network and Systems Support for Games (NetGames), Zagreb, Croatia, 3–4 December 2015; pp. 1–6. [CrossRef]
76. Lee, H.; Ryoo, S.; Seo, S. A Comparative Study on the Structure and Implementation of Unity and Unreal Engine 4. *J. Korea Comput. Graph. Soc.* **2019**, *25*, 17–24. [CrossRef]
77. Heo, Y.J.; Oh, S.M.; Chin, W.S.; Jang, J.W. A Lightweight Platform Implementation for Internet of Things. In Proceedings of the 2015 3rd International Conference on Future Internet of Things and Cloud, Rome, Italy, 24–26 August 2015; pp. 526–531. [CrossRef]
78. Vanin, P.; Nesterov, A.; Kholodilin, I. Integration of IIoT and AR Technologies to Educational Process Through Laboratory Complex. In Proceedings of the 2018 Global Smart Industry Conference (GloSIC), Chelyabinsk, Russia, 13–15 November 2018; pp. 1–6. [CrossRef]
79. Bhatt, S.; Pham, T.K.; Gupta, M.; Benson, J.; Park, J.; Sandhu, R. Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future. *IEEE Access* **2021**, *9*, 107200–107223. [CrossRef]
80. Bröring, A.; Schmid, S.; Schindhelm, C.K.; Khelil, A.; Käbisch, S.; Kramer, D.; Le Phuoc, D.; Mitic, J.; Anicic, D.; Teniente, E. Enabling IoT Ecosystems through Platform Interoperability. *IEEE Softw.* **2017**, *34*, 54–61. [CrossRef]
81. Huynh, T.; Pham, Q.V.; Pham, X.Q.; Nguyen, T.T.; Han, Z.; Kim, D.S. Artificial intelligence for the metaverse: A survey. *Eng. Appl. Artif. Intell.* **2023**, *117*, 105581. [CrossRef]
82. Cao, L. Decentralized AI: Edge Intelligence and Smart Blockchain, Metaverse, Web3, and DeSci. *IEEE Intell. Syst.* **2022**, *37*, 6–19. [CrossRef]
83. Polas, M.R.H.; Afshar Jahanshahi, A.; Kabir, A.I.; Sohel-Uz-Zaman, A.S.M.; Osman, A.R.; Karim, R. Artificial Intelligence, Blockchain Technology, and Risk-Taking Behavior in the 4.0IR Metaverse Era: Evidence from Bangladesh-Based SMEs. *J. Open Innov. Technol. Mark. Complex.* **2022**, *8*, 168. [CrossRef]
84. Lim, W.Y.B.; Xiong, Z.; Niyato, D.; Cao, X.; Miao, C.; Sun, S.; Yang, Q. Realizing the Metaverse with Edge Intelligence: A Match Made in Heaven. *IEEE Wirel. Commun.* **2022**, 1–9. [CrossRef]
85. Almarzouqi, A.; Aburayya, A.; Salloum, S.A. Prediction of User′s Intention to Use Metaverse System in Medical Education: A Hybrid SEM-ML Learning Approach. *IEEE Access* **2022**, *10*, 43421–43434. [CrossRef]
86. Veeraiah, V.; Gangavathi, P.; Ahamad, S.; Talukdar, S.B.; Gupta, A.; Talukdar, V. Enhancement of Meta Verse Capabilities by IoT Integration. In Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022; pp. 1493–1498. [CrossRef]
87. Diro, A.; Chilamkurti, N.; Nguyen, V.D.; Heyne, W. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. *Sensors* **2021**, *21*, 8320. [CrossRef] [PubMed]

88. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]
89. Xie, Q.; Zhou, X.; Wang, J.; Gao, X.; Chen, X.; Liu, C. Matching Real-World Facilities to Building Information Modeling Data Using Natural Language Processing. *IEEE Access* **2019**, *7*, 119465–119475. [CrossRef]
90. Xu, M.; Ng, W.C.; Lim, W.Y.B.; Kang, J.; Xiong, Z.; Niyato, D.; Yang, Q.; Shen, X.S.; Miao, C. A Full Dive into Realizing the Edge-enabled Metaverse: Visions, Enabling Technologies, and Challenges. *IEEE Commun. Surv. Tutor.* **2022**, *25*, 656–700. [CrossRef]
91. Arshad, B.; Ogie, R.; Barthelemy, J.; Pradhan, B.; Verstaevel, N.; Perez, P. Computer Vision and IoT-Based Sensors in Flood Monitoring and Mapping: A Systematic Review. *Sensors* **2019**, *19*, 5012. [CrossRef]
92. Feng, X.; Jiang, Y.; Yang, X.; Du, M.; Li, X. Computer vision algorithms and hardware implementations: A survey. *Integration* **2019**, *69*, 309–320. [CrossRef]
93. Ahmed, M.; Naser Mahmood, A.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
94. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly Detection: A Survey. *ACM Comput. Surv.* **2009**, *41*, 1–58. [CrossRef]
95. Chen, W.; Qiu, X.; Cai, T.; Dai, H.N.; Zheng, Z.; Zhang, Y. Deep Reinforcement Learning for Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1659–1692. [CrossRef]
96. Uprety, A.; Rawat, D.B. Reinforcement Learning for IoT Security: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 8693–8706. [CrossRef]
97. Arulkumaran, K.; Deisenroth, M.P.; Brundage, M.; Bharath, A.A. Deep Reinforcement Learning: A Brief Survey. *IEEE Signal Process. Mag.* **2017**, *34*, 26–38. [CrossRef]
98. Xu, M.; Niyato, D.; Zhang, H.; Kang, J.; Xiong, Z.; Mao, S.; Han, Z. Generative AI-empowered Effective Physical-Virtual Synchronization in the Vehicular Metaverse. *arXiv* **2023**, arXiv:2301.07636.
99. Zhou, M. Editorial: Evolution from AI, IoT and Big Data Analytics to Metaverse. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 2041–2042. [CrossRef]
100. Ali, S.; Abdullah; Armand, T.P.T.; Athar, A.; Hussain, A.; Ali, M.; Yaseen, M.; Joo, M.I.; Kim, H.C. Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. *Sensors* **2023**, *23* 565. [CrossRef] [PubMed]
101. Bouachir, O.; Aloqaily, M.; Karray, F.; Elsaddik, A. AI-based Blockchain for the Metaverse: Approaches and Challenges. In Proceedings of the 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), San Antonio, TX, USA, 5–7 September 2022; pp. 231–236. [CrossRef]
102. Falchuk, B.; Loeb, S.; Neff, R. The Social Metaverse: Battle for Privacy. *IEEE Technol. Soc. Mag.* **2018**, *37*, 52–61. [CrossRef]
103. Chen, Z.; Wu, J.; Gan, W.; Qi, Z. Metaverse Security and Privacy: An Overview. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022. [CrossRef]
104. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [CrossRef]
105. Amiri-Zarandi, M.; Dara, R.A.; Duncan, E.; Fraser, E.D.G. Big Data Privacy in Smart Farming: A Review. *Sustainability* **2022**, *14*, 9120. [CrossRef]
106. Huang, Y.; Li, Y.J.; Cai, Z. Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Min. Anal.* **2023**, *6*, 234–247. [CrossRef]
107. Adil, M.; Attique, M.; Jadoon, M.M.; Ali, J.; Farouk, A.; Song, H. HOPCTP: A Robust Channel Categorization Data Preservation Scheme for Industrial Healthcare Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7151–7161. [CrossRef]
108. Guan, J.; Irizawa, J.; Morris, A. Extended Reality and Internet of Things for Hyper-Connected Metaverse Environments. In Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Christchurch, New Zealand, 12–16 March 2022; pp. 163–168. [CrossRef]
109. Sun, J.; Gan, W.; Chao, H.C.; Yu, P.S. Metaverse: Survey, Applications, Security, and Opportunities. *arXiv* **2022**, arXiv:2210.07990. https://doi.org/10.48550/ARXIV.2210.07990.
110. Anagnostakis, A.G.; Naxakis, C.; Giannakeas, N.; Tsipouras, M.G.; Tzallas, A.T.; Glavas, E. Scalable Consensus over Finite Capacities in Multiagent IoT Ecosystems. *IEEE Internet Things J.* **2022**, *10*, 6673–6688. [CrossRef]
111. Dohler, M.; Haque, I.; Misra, P.; Fortes, S.; Maksymyuk, T. Series Editorial: Internet of Things. *IEEE Commun. Mag.* **2022**, *60*, 18–19. [CrossRef]
112. Musamih, A.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Omar, M.; Ellahham, S. Metaverse in Healthcare:Applications, Challenges,and Future Directions. *IEEE Consum. Electron. Mag.* **2022**, *12*, 33–46. [CrossRef]
113. Al-Ghaili, A.M.; Kasim, H.; Al-Hada, N.M.; Hassan, Z.B.; Othman, M.; Tharik, J.H.; Kasmani, R.M.; Shayea, I. A Review of Metaverse's Definitions, Architecture, Applications, Challenges, Issues, Solutions, and Future Trends. *IEEE Access* **2022**, *10*, 125835–125866. [CrossRef]
114. Peng, H.; Chen, P.C.; Chen, P.H.; Yang, Y.S.; Hsia, C.C.; Wang, L.C. 6G toward Metaverse: Technologies, Applications, and Challenges. In Proceedings of the 2022 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Seoul, Republic of Korea, 24–26 August 2022; pp. 6–10. [CrossRef]

115. Suanpang, P.; Niamsorn, C.; Pothipassa, P.; Chunhapataragul, T.; Netwong, T.; Jermsittiparsert, K. Extensible Metaverse Implication for a Smart Tourism City. *Sustainability* **2022**, *14*, 14027. [CrossRef]

116. Chengoden, R.; Victor, N.; Huynh-The, T.; Yenduri, G.; Jhaveri, R.H.; Alazab, M.; Bhattacharya, S.; Hegde, P.; Maddikunta, P.K.R.; Gadekallu, T.R. Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions. *IEEE Access* **2023**, *11*, 12765–12795. [CrossRef]

117. Asif, R.; Hassan, S.R.; Parr, G. Integrating a Blockchain-Based Governance Framework for Responsible AI. *Future Internet* **2023**, *15*, 97. [CrossRef]

118. Banaeian Far, S.; Imani Rad, A.; Hosseini Bamakan, S.M.; Rajabzadeh Asaar, M. Toward Metaverse of everything: Opportunities, challenges, and future directions of the next generation of visual/virtual communications. *J. Netw. Comput. Appl.* **2023**, *217*, 103675. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.