Metaverse Meets Distributed Machine Learning: A Contemporary Review on the Development with Privacy-Preserving Concerns

Samuel Harry Gardner[a], Trong-Minh Hoang[b], Woongsoo Na[c], Nhu-Ngoc Dao[a,*], Sungrae Cho[d,*]

[a]*Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea*
[b]*Intelligently Connected Networks Lab, Posts and Telecommunications Institute of Technology, Hanoi 100000, Viet Nam*
[c]*Division of Computer Science and Engineering, Kongju National University, Cheonan 31080, South Korea*
[d]*School of Computer Science and Engineering, Chung-Ang University, Seoul 05006, South Korea*

Abstract

Distributed machine learning utilization in the metaverse exposes many potential benefits. However, the combination of these advanced technologies raises significant privacy concerns due to the potential exploitation of sensitive user and system data. This paper provides a systematic investigation of over 100 recent studies across key academic databases obtained by initial keyword-filter screening followed by a thorough full-text review. Particularly, metaverse evolution and enabling infrastructure technologies are briefly summarized. Subsequently, the distributed learning architectures and their features are analyzed as well as possibly associated vulnerability discussions. Then, envisioned metaverse applications and future research challenges are highlighted before concluding remarks.

Keywords: mobile metaverse, privacy preservation, distributed machine learning, virtual reality

1. Introduction

In recent years, mobile networks have witnessed a rapid evolution facilitating various services and applications with Internet access through efficient wireless communication infrastructures. In particular, the emergence of fifth-generation (5G) technology has prompted extensive research and development of mobile ecosystems, especially with the remarkable emergence of the metaverse [1, 2]. The mobility and ultimate networking performances such as mobile broadband, ultra low latency, high reliability, and offloading computation capabilities in 5G networks and beyond have shown great promise in advancing metaverse ideas. In this paradigm, vast volumes of user data and metaverse content can be exchanged over mobile networks to meet urgent, time-sensitive demands [3]. Meanwhile, artificial intelligence (AI) techniques may be involved in multiple operations of the metaverse services including data processing and generation as well as control decision-making [4, 5]. AI is increasingly being used in metaverse-driven smart city applications, enabling data-driven urban services through machine learning, deep learning, and generative AI [6]. Moreover, the advent of the sixth-generation (6G) technology, promising extremely lower latency, ultra-higher reliability, and extensive spectrum resources support, is expected to further enhance metaverse experiences, especially those involving shared real-world integration [7, 8].

The metaverse concept has been the subject of extensive recent debates, in which each manifestation of the metaverse strives to create a unique environment defined by distinct characteristics [9]. Scholars have since observed that the metaverse is moving from a science-fiction-inspired concept to a digital reality with widespread applications across various domains such as gaming, education, healthcare, and entertainment [10]. These concepts are typically tailored to align with the vision of the companies or organizations that develop them [11]. Nevertheless, the standard theme throughout metaverse concepts can be represented as an emulation of society in a digital form. Through such an emulation, companies aim to create shared experiences that seamlessly integrate with the real world, providing users with a more efficient and engaging way to experience reality and fostering various social benefits [12]. This integration can take various forms, including connections with digital asset systems that leverage blockchain technology and cryptocurrencies [13]. The advantages of this integration are multifaceted. For example, the metaverse can offer greater freedom to patients who have difficulty socializing outdoors due to physical or mental health challenges by enabling remote healthcare services[14]. The data derived from these sources is valuable contributing to further research in healthcare and social environments [15].

1.1. Motivations

Despite diverse potentials, the metaverse has been facing various challenges, particularly concerning data security and privacy issues due to the vast amounts of sensitive user data involved [19]. A recent sentiment analysis study on public perceptions of the metaverse revealed that while 59% of users had

*Corresponding authors
Email addresses: 20012868@sju.ac.kr (Samuel Harry Gardner), hoangtrongminh@ptit.edu.vn (Trong-Minh Hoang), wsna@kongju.ac.kr (Woongsoo Na), nndao@sejong.ac.kr (Nhu-Ngoc Dao), srcho@cau.ac.kr (Sungrae Cho)

Table 1: Summary of recent surveys and reviews of existing metaverse studies.

Year	Ref	Research Topic	Research Type	Findings	Limitations
2022	[15]	Big Data Meets Metaverse: A Survey	Survey	Investigates big data's role in metaverse applications, highlighting data processing, privacy concerns, and opportunities for growth.	Lacks empirical validation and real-world case studies. Limited discussion on regulatory frameworks for big data governance.
2022	[5]	Mobile Edge Computing, Metaverse, 6G Wireless Communications, Artificial Intelligence, and Blockchain: Survey and Their Convergence	Survey	Discusses how emerging technologies like AI, blockchain, and MEC converge to enhance metaverse capabilities.	Does not address real-world integration challenges. Limited scalability analysis of MEC and blockchain in large-scale metaverse applications.
2023	[14]	Metaverse for Healthcare: A Survey on Potential Applications, Challenges, and Future Directions	Survey	Metaverse applications in healthcare, including VR-based surgeries, AI-assisted diagnostics, and immersive patient experiences.	High infrastructure demands are not addressed. Lacks real-world implementation analysis and discussion on legal and ethical implications.
2023	[16]	Blockchain for the Metaverse: A Review	Review	Examines blockchain's role in securing digital content, data interoperability, and smart contracts in metaverse applications.	Overemphasizes public blockchains while neglecting permission-ed alternatives. Does not explore energy consumption concerns.
2023	[17]	Federated Learning for Metaverse: A Survey	Survey	Explores federated learning's role in preserving data privacy and improving AI training efficiency in metaverse environments.	Limited discussion on communication overhead and security risks. No real-world case studies to validate federated learning applications.
2024	[18]	Navigating the Metaverse: Unraveling the Impact of Artificial Intelligence—A Comprehensive Review and Gap Analysis	Review	Analyzes AI's influence on metaverse applications, focusing on user engagement, ethical concerns, and future developments.	Focuses heavily on ethical concerns while neglecting performance optimization. Lacks comparative analysis of AI techniques for metaverse applications.
2024	[6]	Artificial Intelligence-Enabled Metaverse for Sustainable Smart Cities: Technologies, Applications, Challenges, and Future Directions	Review	Examines how AI enhances smart cities via the metaverse, focusing on urban planning, governance, and sustainability.	No cost-benefit analysis of AI in smart cities. Lacks discussion on cyber security threats related to metaverse-based urban systems.
2025	Ours	Metaverse Meets Distributed Machine Learning: A Contemporary Review on the Development with Privacy-Preserving Concerns	Review	Investigates the role of distributed machine learning in metaverse applications, focusing on privacy-preserving techniques such as federated learning and split learning. Highlights vulnerabilities, potential threats, and the need for enhanced security frameworks.	No in-depth performance benchmarks comparing different privacy-preserving methods.

a positive outlook on security and 66% on privacy, concerns regarding legal and ethical uncertainties persisted, particularly in relation to identity protection and personal data security [20]. The lack of universally accepted security frameworks and data protection mechanisms poses a significant barrier to metaverse adoption [10]. Recent research highlights concerns over how user data is stored, accessed, and leveraged within the metaverse ecosystem, further emphasizing the need for comprehensive privacy-preserving solutions. Distributed machine learning approaches such as federated and split learning, which are considered efficient tools to optimize metaverse operations, exhibit vulnerabilities during data processing and mining, particularly information leakage and integrity [21]. One potential solution to mitigate these risks is the integration of blockchain technology, which ensures that all transactions and model updates are immutably recorded and verified through decentralized consensus mechanisms [22]. Despite these possible mitigations, these vulnerabilities could limit the potential of the framework implementation and necessitate further research to protect user data from illegal interception and exploitation. Furthermore, users have expressed hesitancy towards fully engaging with metaverse platforms due to the absence of security guarantees, with some tweets highlighting fears of personal identity exposure and digital footprint misuse [20]. Additionally, learning model manipulation by attackers may have unintended negative consequences on the metaverse operations and user assets. Furthermore, threats to identity authentication and access control in the metaverse remain critical, as attackers can impersonate users to steal digital assets and manipulate social interactions [23]. As the metaverse expands, research into preserving privacy is crucial to ensure its future success[24].

1.2. Related Works

Multiple aspects and versions of potential metaverse evolution have been investigated recently. Contemporary surveys have focused on critical aspects of its evolution, including healthcare ecosystem development [14], blockchain integration [16], and multi-access edge computing utilization [5]. Particularly, Chen et al. [17] highlighted the application of AI to promote the metaverse evolution in both service features and management domains. Although AI technologies have been widely acknowledged as one of the foundational tools for the development of the metaverse [18]. The social and privacy implications of user and system big-data exploitation remain crucial concerns [15]. In particular, AI-driven metaverse platforms raise challenges related to data privacy, security, and ethical concerns in smart city implementations, necessitating robust governance frameworks [6]. Furthermore, the overwhelming majority of existing surveys have not yet been focused on exposing in detail the privacy preservation within distributed machine learning applications utilized for the metaverse ecosystems. However, in recent years, authors in [25] and [26] have offered a particularly insightful perspective into the privacy issues that come with the integration of AI technologies into existing metaverse ideas.

When comparing existing surveys, it is evident that most focus on specifics such as edge computing [5]) or broad overviews [15]. Rather than detailing how distributed ML creates unique risks and opportunities for metaverse operators when it comes to privacy. We further respond to the need for clear and practical implementations of privacy techniques in distributed deep

Table 2: Nomenclature

Abbreviation	Description
6G	Sixth-Generation Technology
AI	Artificial Intelligence
AR	Augmented Reality
DCOR	Distance Correlation
DNN	Deep Neural Network
DL	Deep Learning
DQN	Deep Q Networks
DRL	Deep Reinforcement Learning
DT	Digital Twin
FL	Federated Learning
FSS	Function Secret Sharing
FSHA	Feature Space Hijacking Attack
HFL	Horizontal Federated Learning
HMD	Head-Mounted Display
IEEE	Institute of Electrical and Electronics Engineers
IoMT	Internet of Medical Things
IoT	Internet of Things
LocFedMix-SL	Local Federated Mixed Split Learning
LocSplitFed	Local Split Federated Learning
MAR	Mobile Augmented Reality
MEC	Mobile Edge Computing
MISP	Metaverse Infrastructure Service Provider
MR	Mixed Reality
MSP	Metaverse Service Providers
PGSL	Proximal Gradient Split Learning
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SAC-GCN	Soft Actor-Critic Convolutional Network
SAGIN	Space-Air-Ground Integrated Network
SL	Split Learning
SVRP	Structure To Vector
URLLC	Ultra-Reliable and low latency communications
VFL	Vertical Federated Learning
VR	Virtual Reality
VRTP	Virtual Reality Transfer Protocol
VRITIP	Virtual Reality IoT Platform
WSN	Wireless Sensor Networks

learning by detailing the practical need for robust threat taxonomies and realistic defense strategies. Operators can leverage the resulting findings to fortify security through reduced susceptibility to adversarial manipulations, without the penalty of worst performance. Therefore from a theoretical standpoint, we create a clearer map of the technical and algorithmic pitfalls of their resulting implementations. Overall, the metaverse's rapidly expanding user base and extreme real-time data processing demands underscore why a focused study on privacy-aware distributed ML is essential. Table 1 summarizes recent surveys and reviews of existing metaverse studies.

1.3. Our Contributions

Although prior research has focused on aspects such as blockchain-assisted infrastructure [16] and healthcare-oriented metaverse solutions [14], very few articles have comprehensively examined the privacy vulnerabilities that arise when advanced distributed deep learning frameworks intersect with virtual environments in metaverse infrastructure. We aim to address this by exploring the possible implementations of privacy-preserving distributed ML in the metaverse following the key research questions:

- Which distributed learning architectures potential to be securely integrated into metaverse ecosystems?
- What common attack vectors pose high-impact threats to certain deployment environments?
- How do recent privacy-preserving techniques improve user trust while upholding moral and legal privacy requirements?

A systematic approach has been employed to synthesize the current research in literature. The methodology is constituted by four key stages: literature search, study selection, data extraction, and synthesis. A comprehensive search was performed across key academic databases, including IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink as well as Arxiv during the past 5 years. Search terms were formulated based on central themes such as "Metaverse Applications and Security," "Federated Learning in AI," and "6G Wireless Networks for the Metaverse." Initially, articles were screened by titles and abstracts to eliminate duplicates and irrelevant entries. Full texts were then evaluated against predefined inclusion criteria: (i) studies addressing the intersection or creation of immersive metaverse technologies with or without distributed machine learning; (ii) papers discussing privacy and security aspects with or without this integration; and (iii) works focusing on technical innovations, practical applications, or future directions in metaverse-related distributed learning and privacy preservation. Data was systematically extracted using a structured template to capture details such as publication type, research focus (e.g., applications, privacy attacks, defense mechanisms), and the specific distributed machine learning techniques (e.g., Federated Learning, Split Learning) as well as metaverse technologies (e.g., VR, AR, MR). A narrative synthesis method was employed to categorize the extracted data into major themes, research gaps, and emerging trends. The categorization was guided by the technological underpinnings presented in [7] and the metaverse taxonomies discussed in [2].

In summary, our main contributions in this paper include: (i) cataloging the primary distributed ML strategies suitable for a metaverse environment, (ii) classifying known and emerging privacy and security issues specific to large-scale virtual environments with distributed ML aspects, (iii) evaluating the relative merits of privacy-preserving technologies in realistic deployment scenarios, and (iv) suggesting future research directions that balance user privacy protections with increasing computational demands.

The following review methodology workflow is used to organize the paper from this point forward:

- Section 2 focuses on metaverse evolution by discussing the advancement of virtual reality, augmented reality, mixed reality, and the metaverse concept.
- Section 3 examines potential infrastructure-enabled technologies, that support the metaverse developments and operations.
- We explore various distributed deep learning models that support the metaverse ecosystems in Section 4.

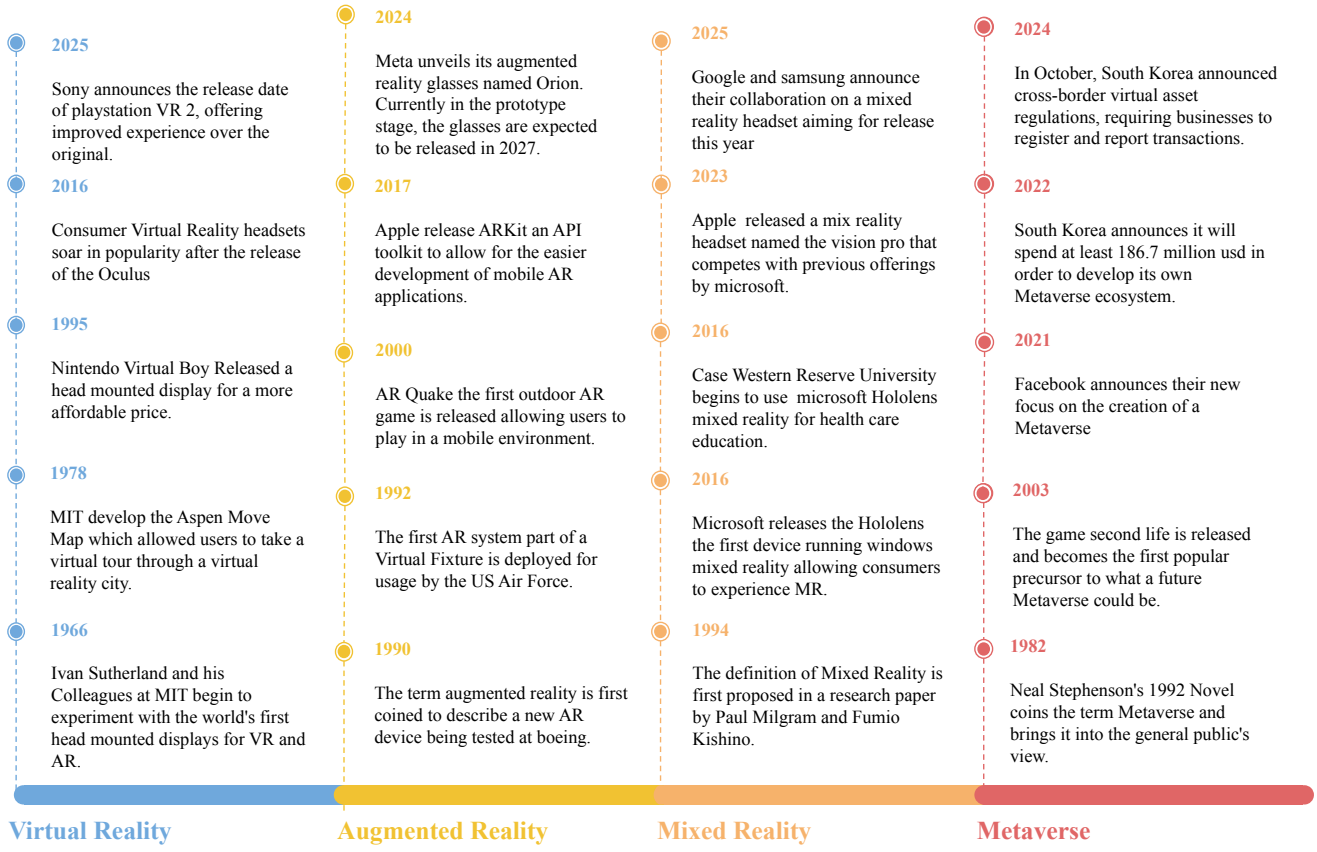

Figure 1: Milestones of technological development in metaverse evolution.

- Section 5 discusses potential vulnerabilities associated with distributed and private machine learning for the metaverse.
- Section 6 describes applications and utilization of metaverse concepts concerning privacy preservation as well as their implementations.
- Section 7 describes privacy challenges in the research field, the future research trajectory, and potential limitations around metaverse research studies.
- Finally, we concluded the paper with several key remarks in Section 8.

To facilitate interested readers, key abbreviations used in this paper are summarized in Table 2.

2. Metaverse Evolution

AR, MR, and VR are foundational technologies within the broader metaverse ecosystem, each offering distinct levels of immersion and interaction—from augmenting real-world environments to fully immersive virtual experiences—thereby shaping the evolution of digital connectivity and user engagement.

2.1. Virtual Reality

Originally emerging from science fiction media, virtual reality (VR) captured imaginations as a futuristic concept. In the 1970s, researchers such as Myron Krueger even used the term ”artificial reality” to describe early VR efforts [27]. Over time, VR evolved into a major research field and laid the groundwork for the metaverse. It offers immersive experiences and alternative forms of human-computer interaction by integrating advances in simulation, interaction, multimedia, sensors, and communications to create digital environments [28]. Moreover, ongoing developments in tactile sensors and display technologies have significantly enhanced both realism and practical applications [29]. Furthermore, companies such as Facebook and HTC have further boosted VR development by investing in high-quality media content [30].

As human perception is largely visual, VR development has prioritized enhancing headsets—particularly in terms of portability. With these headsets, users can interface with a workstation or integrated computer to access virtual spaces either locally or over the Internet [29]. This capability for shared virtual spaces is key to the metaverse concept, though it brings challenges regarding the data demands on traditional transfer protocols. To overcome this, Brutzman *et al.* [31] introduced the Virtual Reality Transfer Protocol (VRTP), designed to optimize the sharing of 3D virtual worlds.

VRTP employs a combination of client, server, peer-to-peer,

and monitoring components. In this system, the client integrates with a browser to support multi-user VR environments, while the server ensures data persistence. Additionally, peer-to-peer streaming improves scalability, and network monitoring is used to optimize performance.

Recent advances in VR networking now incorporate cloud computing, mobile infrastructures, and IoT [28]. Next-generation networks such as 5G and 6G support VR's expansion into social networking by offering higher bandwidth and enabling resource virtualization [32]. Furthermore, the IoT-based VR platform (VRITIP) delivers low-latency VR services through the connection of IoT devices via smart gateways [33]. The use of light fields—a technique for realistic 3D representation—further enhances VR environments by simulating stereo parallax and volumetric effects [34].

VR has been applied extensively in healthcare, entertainment, education, military training, architecture, and marketing [35, 36]. For example, virtual meetings saw a surge in popularity during the COVID-19 pandemic, and social VR spaces have provided a safe alternative to face-to-face interactions. Nevertheless, security risks remain, including potential attacks on VR tracking systems that can alter user perception [37].

2.2. Augmented Reality

Augmented reality (AR) differs from VR by overlaying digital elements onto the real environment instead of replacing it. AR improves real-world analysis and boosts productivity, remote assistance, and healthcare applications [4]. The concept emerged in the 1960s, when Ian Sutherland's experiments with a see-through head-mounted display (HMD) first demonstrated the overlay of 3D graphics [38]. By the 1990s, AR had developed into an established research field [39].

AR devices range from smart glasses and projected displays to smartphones, with Mobile AR (MAR) on smartphones being the most common. MAR leverages 5G's low latency and high data rates [4]. In addition, Web AR seeks to eliminate the need for app downloads by integrating AR directly within web browsers [40]. Furthermore, AR has been applied in civil engineering to enhance visualization [41].

AR finds applications across diverse fields such as education, healthcare, military, art, tourism, broadcasting, and retail [42]. Consumer examples include devices like the Xbox Kinect and Google Glass, although the latter struggled with public acceptance despite its technological promise [43]. Moreover, AR has been increasingly integrated into mobile applications and high-end vehicles, projecting essential information directly into drivers' fields of view.

Unlike VR, AR offers broader usability by integrating with existing environments instead of creating entirely new ones. Although AR shares many underlying technologies with VR, it requires higher precision in tracking and calibration. Its core components include input sensors, data processing, and output stages. The processing stage involves tasks such as registration, rendering, calibration, and tracking, which may utilize sensor-based, vision-based, or hybrid tracking methods [4].

2.3. Mixed Reality

A widely accepted definition of mixed reality (MR) was provided by Milgram and Kishino in 1994. MR combines real and virtual elements and differs from AR by enabling real-time interaction between digital and physical objects [44]. Recent studies have focused on leveraging cloud-edge computing to address MR's high processing and power demands. Offloading these requirements to cloud infrastructures can improve portability, which is particularly beneficial for applications like navigation assistance for the visually impaired [45].

The essential components of MR include tracking and registration, virtual environment modeling, and interaction interfaces. Accurate tracking is vital to maintain a convincing sense of presence. To achieve seamless registration of virtual and real-world objects, a variety of methods—using sensors and cameras—are employed. Moreover, environment modeling remains a key focus of ongoing research [46], with experts emphasizing the importance of spatial audio and haptics for enhancing immersion [47].

Compared to VR and AR, MR simplifies design by directly integrating real-world elements. Despite its significant potential, security and privacy issues remain a concern [48]. Protecting input data is necessary to prevent malicious alterations, while robust data security measures help safeguard user privacy—issues that are especially critical in healthcare, where MR devices might expose sensitive information. Additionally, hardware protection is essential to ensure safe user interactions. Recent developments in devices such as the Microsoft HoloLens and Google Glass have further advanced MR, particularly in healthcare and architecture [49].

2.4. Metaverse

The first mention of a metaverse concept comes from a novel named Snow Crash by Neil Stevensons in 1992. The word meta describes being beyond reality and verse refers to the universe. Over time the term has carried multiple different definitions that have been constantly adapted [50]. Recently promoted by large companies such as Facebook and Microsoft, the metaverse was redefined as the next Internet revolution to describe a global virtual social network platform. The metaverse offers the user the ability to place themselves into an immersive experience with comprehensive interactions [2]. There should be no interruptions when a user switches between the metaverse and the real world. Recently promoted by major companies such as Facebook and Microsoft, the metaverse has been redefined as the next Internet revolution—a global virtual social network platform. It enables users to immerse themselves in a fully interactive experience, with seamless transitions between the metaverse and the real world. [2]. The expected features and characteristics of a metaverse are very diverse and vary between each company's implementation. However, the general trend that is accepted dictates, persistence regardless of user interaction with the space, synchronization between users in real-time in comparison to the real world, availability from wherever a mobile network is able to reach and support players without a cap or server segregation, a separate economy supported by

Table 3: Comparison of different generations in the metaverse evolution.

Characteristic	VR	AR	MR	Metaverse
Environment	Virtual world	Real world	Real world	Virtual world
User device	Headsets	Accessories	Accessories	Headsets
Objects	Virtual	Virtual	Physical and virtual	Virtual
Interactivity	Low	High	High	Very high
System model	Local and centralised	Local and centralised	Local and centralised	Centralised
Data rate	High	Low	Medium	Very high
Complexity	Low	Medium	High	Very high
Synchronisation	Low	Medium	High	Very high
Privacy concern	Medium	High	High	Very high
Applications	Collaboration in planning and design management, Project Communication, Healthcare, Entertainment, Automotive, Military, Educational Instruction, Sciences, Tourism	Industry 4.0, Civil Engineering, Military, Training, Automotive Design, and Development, planning and design management, Healthcare	Healthcare, Entertainment, Education, Engineering, Planning and Design, Simulation of advanced infrastructure, prototyping, automotive, Military, Science, Automotive Design	Finance, Agriculture, Human involved simulation on a massive scale, Marketing, Entertainment, Education Instruction, Military, Science, Tourism, Healthcare, Design, Simulation with humans in the loop on a massive scale, Virtual real estate, Civil Engineering, prototyping, automotive industry, planning

many aspects shared in the real world such as trade and interoperability to have users move their virtual assets between competing metaverse. Expected features include virtual currency trading, avatars, teleportation or varied movement mechanics, social spaces, gaming, entertainment, and more. These features take advantage of the previously mentioned characteristics to allow for the creation of what can be imagined as an entire virtual world separate from the physical. The goal of metaverse development is to enable access to this virtual space in the most immersive way possible [2]. Because the basics of a society are often intended to be simulated in a metaverse means that the concept is also vulnerable to similar issues plaguing our current world. For example, If many users were to suddenly leave one metaverse in favor of a competing product, it could potentially crash its virtual economy and trigger an overall collapse [51].

The differences between AR, MR, and VR in the metaverse can be difficult to ascertain. It is important to remember that VR, AR, and MR are simply technologies that offer digital experiences; unlike the metaverse, they do not encompass all components—such as social networking that form a comprehensive metaverse product. The metaverse is the most complex virtual system, which contains the most privacy and security concerns. These security and privacy concerns are a natural development of the project that is so complex and are exacerbated by the large degree of Centralization making a single attack point vector for potential bad actors. In addition to this, the metaverse inherits the security concerns of all the devices being used to access or interact with it. The vulnerabilities involved can therefore range widely with the most apparent being the inherent network aspects of the projects. This will likely lead bad actors to target not only the users' digital assets but anything from sensitive information to identity theft in virtual spaces.

3. Infrastructure-Enabled Technologies

In this section, we describe the utilization of potential technologies in the development of metaverse infrastructure with specific attention paid to privacy and distributed deep learning. In combination with the continuous evolution of the metaverse, various technologies have grown alongside it, allowing for the integration of many cutting-edge networking technologies. These transformative technologies, if implemented, often need to account for potential privacy issues in their design. By further explaining possible infrastructure-enabled technologies, we hope to shed light on the potential issues that may arise from their integration into the metaverse concept, particularly focusing on how a complex combination of both physical and digital infrastructure is essential for seamless operation of such a concept.

3.1. Mobile Edge Computing for Metaverse Operations

Mobile Edge Computing (MEC), with regard to the metaverse, provides significant benefits over a simpler networking infrastructure. By bringing computational power closer to the network's edge, latency can be reduced creating an enhanced user experience. In an IoT scenario, MEC is the vital bridge connecting IoT devices and cloud services. The ability to locally process data at the edge of the overall data transfer to the cloud services can be reduced, lowering bandwidth requirements, improving real time analytics, and allowing for faster responses in time-sensitive applications [52]. As the metaverse envisions a space blending physical and virtual worlds into a seamless reality, MEC can optimize the distribution of processing resources for this application. Additionally, privacy-enhancing techniques, including secure multi-party computation (SMPC) and trusted execution environments (TEE), have been proposed as solutions to protect sensitive user data in edge

computing-based metaverse services [23]. This integration of MEC with IoT and the metaverse represents a dynamic evolution of networking to support futuristic, data-driven experiences [53]. Potential services to run on the network edge which would benefit from reduced latency times are time-sensitive AI applications. To address the security risks of deploying AI models that process sensitive data at the edge in a metaverse, mechanisms are being developed to protect against adversarial attacks targeting these deployments [54]. Furthermore, techniques for adaptive edge network resource allocation have been proposed for use in a large user environment such as the metaverse. Specifically, a method based on Soft actor-critic convolutional networks (SAC-GCN) has recently been shown to outperform multiple other methods based on ISAC (Independent SAC), DQN (Deep Q Networks), GCC-G (GCC With Greedy) and BBR-G (BBR With Greedy) [55].

3.2. Network Slicing for Metaverse Services

Networking Slicing is a concept often discussed in tandem with 5G networks. It involves partitioning physical network resources to meet the demands of a network at any given time. This adaptability allows for several benefits, such as adaptability, improved performance, and cost-effectiveness [56]. With the expectations of 6G becoming more defined, the proposed networks are expected to incorporate many unique features. This presents a challenge as the implementation of network slicing will now need to account for space, air, and ground networks amongst a variety of new services. To account for this, AI integrations into the network slicing architecture have been announced to reduce the overall network management complexity [57]. Additionally, it has been demonstrated that AI could be a key component in reducing the energy requirements of network slicing in a 6G environment [58]. In the metaverse, MetaSlicing is proposed to perform the function of separating network resources and allocating them effectively. To accomplish this, the framework proposes Metainstances. These instances are clusters of applications with common functions, which users of the metaverse can tap into to reduce the overall demand. This clustering and subsequent intelligent allocation of resources reduces resource demand enabling savings such as the rendering of a digital map in a single instance instead of servicing every user individually. The Metaverse Infrastructure Providers (MISPs) can take advantage of these resource savings to create richer and more diverse experiences than would otherwise be possible [59].

3.3. Blockchain Integration for Secure Transactions

Integrating blockchain into the metaverse creates the opportunity for a more complex virtual economy and supports the development of a decentralized system that enables users to shape the virtual economy according to their preferences. Furthermore, blockchain integration could be used to create individual user identities, provide additional security, and ensure the integrity of data [60]. The adoption of blockchain-based privacy-preserving authentication mechanisms can enhance security in decentralized metaverse applications. A hybrid blockchain model integrating consortium and private chains has been proposed to maintain decentralization while improving efficiency and privacy in transactions [61]. Before the blockchain can be used to process transactions through the metaverse network, it is important to take several other factors into account. While resource constraints on wearable IoT devices such as those in a metaverse may prevent them from utilizing a blockchain service efficiently, a solution to this has been developed in the form of a Multi-WSN network. This architecture allows for a hierarchy of devices to be created based on their power. The most powerful device available, which ideally is not a wearable, will then connect to the blockchain and distribute this to the wearable devices in the network [62]. Furthermore, when it comes to security the large number of devices utilizing the metaverse for activities that may have tangible economic benefits in the future requires that security is at the forefront of its design. To account for the vulnerabilities in the semantic communications taking place between edge devices and virtual service providers, a proposal for the inclusion of a blockchain-aided semantic communication framework has been created [63]. Moreover, to address the difficulty of implementing and taking advantage of a blockchain in a massively resource demanding service such as the metaverse, a proposal for a novel blockchain based framework was created. Known as MetaChain, the framework utilizes smart contracts to handle the complex interactions between MSPs and metaverse users, as well as improving upon potential future scalability issues in order by increasing resource management efficiency [64]. Lastly, to better understand the complex structure of a blockchain transaction network that would take place in a metaverse concept, a novel representation learning method known as structure-to-vector (SVRP) was proposed. The method allows for a deeper and more accurate insight into the latent representation and structural identity of blockchain transaction networks. Thus allowing for potential fraud detection, increased network security, and possible regulatory compliance [65].

3.4. 5G Access and Beyond for Communications

The integration of 5G and 6G technologies into the metaverse allows for far more potential in the concept. Ultra-reliable and low latency interactions from 5G and even more so 6G allow the metaverse to utilize technologies and frameworks, which in many cases would have been entirely impossible before. Creating the environment where the massive virtual universe can be fully realized [66]. A demonstrable application of 5G proposed for the metaverse is Remote collaboration. To help break geographic restrictions involved in collaboration, evaluations have been made on the characteristics of Remote Collaboration employing 5G, to gain a wider understanding of its limitations and potential optimizations. The possibilities of collaboration in this way on a global scale create a new paradigm for people to work, share, and communicate [67]. Furthermore, the advancements proposed in 6G could enable enhanced interactivity and integration between physical and virtual worlds, specifically in the form of digital twin (DT) technologies. This is enabled via large amounts of data transfer between the physical and virtual plane, making 6G the ideal candidate to support these interactions [68]. 6G additionally offers a promising

paradigm in the form of Space-Air-Ground Integrated Network (SAGIN), which when combined with metaverse to enhance network performance is known as (ME-SAGIN) the Metaverse-Inspired cybertwin-based SAGIN architecture. This paradigm aims to increase the functionality of SAGIN through the creation of a parallel cyberspace to the physical SAGIN [69]. To deal with the massive amounts of data without sacrificing communication efficiency while utilizing 6G in the metaverse, the application of deep learning techniques for service scheduling and network resource allocation has been proposed. These include: An ML-based framework for threat detection and prevention, A DL-based method to improve energy efficiency through the optimization of wireless resource allocation in RIS-assisted 6G systems, Deep reinforcement Learning (DRL) for non-convex problem optimization, and the integration of federated learning to improve security of mobile communication systems [8]. The amalgamation of these current and future technologies into the metaverse promises to elevate the overall experience of human interaction with virtual worlds far greater than what has been previously seen.

3.5. Digital Twins for Real World Synchronization

DT technology is described as a duplication of a physical entity to a virtual entity and the bi-directional data connections between these. The virtual spaces hosting the virtual representations can consist of sub-spaces, allowing for operations such as testing, optimizations, and modeling [70]. A conceptualized framework of DT integration into a metaverse environment has been proposed to create the expected immersive experiences possible. To achieve this, it is proposed that DTs of all operations, concepts, and entities work together to create a comprehensive and accurate representation for analysis of the provided services. This could take the form of a connection between a wireless network DT and the metaverse service DT [71]. DTs of physical entities can be represented in different scales depending on the requirements of the application and sensor data available. Substances large enough to be seen by the naked eye are known as macroscopic, while substances that cannot be seen are known as microscopic. Research into and utilization of microscopic DTs can be more difficult than macroscopic owing to the increased costs of a nanoscale sensor and the number of them required [72]. Furthermore, it has been proposed to combine DTs with advanced AI algorithms. This combined architecture could then be used for tasks such as performing predictive maintenance. This is accomplished by employing the AI to analyze data related to a DT for prediction of maintenance before signs occur in the physical object, decreasing operational costs and promoting sustainability [73]. Likewise, when combined with MEC and Ultra-Reliable and low latency communications (URLLC) a new digital twin architecture is proposed. This architecture is proposed to combine the benefits of task offloading at the edge, in synergy with task caching techniques, and could guarantee stronger reliability [74]. Another method of improving the reliability of DTs that has been proposed is blockchain integration. The method, named BlockNet, uses the immutable characteristics of Blockchains to ensure the security of the digital mapping process of the IoTs. These improvements are accomplished through the increased confidence achieved by the blockchain's fundamental traceability, compliance, authenticity, and security qualities [75]. Lastly, an obvious use case of DTs can be seen in industrial metaverses. The industrial metaverse refers to the industrial applications of metaverse technologies. These applications include city management, industrial management, and traffic and energy modeling. DTs in this sector play a crucial role in the advancement of intelligent manufacturing [76].

4. Distributed Machine Learning Architectures

Distributed deep learning refers to a potential improvement over regular deep learning via the distribution of training tasks over multiple client devices. A central server is used for administration and possibly to combine these individual models into a single larger model using the clients' training data. The advantages of this are that a much larger model can be created with significantly fewer resources per agent while increasing user privacy by only sending data such as weighted parameters to the server. However, it is important to take into account client device resource restrictions such as processing power which could pose negative effects, especially in terms of latency. The advantage of increasing user privacy by preventing the transfer of sensitive data to a single server, allows deep learning training to comply with ever-increasing user privacy laws. Various distributed deep learning algorithms and frameworks have been proposed with the most popular currently being federated learning, split learning, and early exiting.

In the metaverse evolution, distributed deep learning can leverage the thousands of dedicated devices required to access the metaverse while gaining unique new insights through training data. This presents some significant privacy implications as users will potentially be exposing more data than ever before. To address these privacy implications, a lot of research has been conducted in this area. In this section, we have described various distributed deep learning frameworks and algorithms currently being developed.

4.1. Federated Learning

Federated learning is a method of distributed machine learning where clients collaborate by each training a model on their individual devices before sending this trained model to a central server. In turn, the central server aggregates client models to improve an overall shared model. For instance, it currently has widespread usage with Google using the method with its keyboard application to improve predictive text. Its benefits include smarter models, lower latency and less power consumption than traditional machine learning methods. The fact that the client trains its own model additionally allows for a more user-tailored experience for each client. To create a distributed machine learning model, an algorithm computes high-quality updates before transmitting the user-trained model to the central server. Additional methods and algorithms can be used to achieve better results such as reducing bandwidth transmission for client uploads. Security on the server can be maintained

with the implementation of a secure aggregation protocol which prevents decryption with a low number of client updates [77].

4.1.1. One-Shot Federated Learning

This method of federated learning allows each client to improve its trained model to completion. In a single round of communication, the server will then collect these models from every device and produce a shared model. The difference from standard federated learning is that it does not perform continuous updates. This method could allow for separate models to be created with specific specialties in a federated network of devices by picking specific devices to create a global mode. For example, all devices in a specific region and using accounts of a specified age [78].

4.1.2. Vertical and Horizontal Federated Learning

Also known as Heterogeneous Federated Learning, vertical federated learning (VFL) differs from Horizontal Federated Learning (HFL), also known as Homogenous Federated Learning, in that it is applicable to situations where two data sets have a shared sample ID but different feature spaces [77]. HFL would be applicable in situations where data sets share feature space but possess different sample IDs. This makes it good for situations using large collections of mobile devices to create a single model. VFL is more useful when multiple different businesses with close data relationships want to collaborate, in this method they are able to combine their data despite the differences in feature space. HFL is far more common due to the lower amount of implementation challenges when compared to VFL, despite this VFL does have real world implementations [79, 80].

4.2. Split Learning

Split learning is a technique developed by MIT Media labs Camera Culture Group. Similar to federated learning, it allows a machine Learning model to be trained without clients sharing raw data, reducing the burden of training [81]. The advantages compared to federated learning include stronger privacy, higher accuracy, computational resources efficiency, reduced communication cost, and seamless integration for edge devices with compression. However, its disadvantage is the speed due to relay-based training across clients. Recently, various solutions such as Split-Federated learning have been proposed to potentially solve this.

4.2.1. Two-Party Split Learning

The two parties in a basic or vanilla split learning configuration are the non-label part and the label party. During training the non-label part sends an intermediate layer known as the cut layer to the label party. This naturally creates some semblance of privacy preservation, although gradient-sharing schemes previously used in federated learning methods have shown possible vulnerabilities that may be applicable to split learning as well [82, 83].

One of the current focus areas of research in split learning is communication reduction. This often gets discussed in papers focusing on parallel split learning algorithms which have varying degrees of impact. Additionally, a method called AdaSplit, which adapts to varying resource constraints, has been proposed to reduce bandwidth consumption and improve the performance of clients. The goal of reducing the communication costs in split learning is to make it more comparable to the costs associated with federated learning, making split learning a viable alternative in resource-limited scenarios. It works by employing multiple different techniques such as eliminating client dependence on server gradients, intermittent server training, reducing payload size, reducing communication frequency, and constraining client updates [84].

4.2.2. Parallel Split Learning

Parallel Split Learning is the term used to describe the adaptation of split learning allowing the local data to be trained parallel. This can solve the issue of overfitting and high latency which could occur with sequential split learning [85]. Several variations of solutions to parallel split learning have been proposed in research, each with its advantages and disadvantages. The overall goal of its implementation is most often to take as many advantages as possible from split learning while overcoming its shortcomings. These shortcomings could be scalability issues or those previously mentioned such as overfitting [86].

SplitFed - Split Federated Learning. Split-Fed learning combines the Split learning technique with Federated learning to overcome the disadvantages of implementing Split Learning on its own while creating additional advantages. The additional advantages include privacy elements such as differential privacy and PixelDP. Although the method is not immune to privacy-related vulnerabilities, which have already been proposed in various papers. The combination of split and federated learning does now have much effect on communication efficiency or test accuracy. However, it shows a significant decrease in the computation time when compared to Split learning with multiple clients and does not affect the benefits of communication efficiency over federated learning [87].

LocFedMix-SL - Local Federated Mixed Split Learning. This method of localized, federated, and mixup augmentation techniques for split learning was developed to further address the problem of parallelism in split learning models. Methods for addressing this in an alternative way were proposed in the past. However, they came at the cost of speed and scalability. The LocFedMix-SL method solves these issues by the techniques that make up its name. When compared to previous methods. Simulations conducted with this parallel framework showed a greater improvement in speed, latency, and scalability in comparison to previously proposed algorithms, such as Split-Fed, and additionally improvements over the standard sequential split learning. The mixup augmentation technique, which differentiates it from previously proposed techniques, uses local regularization of lower model segments on clients and augmenting smashed data on the server. In combination this smashed data, mixup allows for improved convergence speed and accuracy without sacrificing split learning advantages [86].

4.3. Early Exiting

Early Exiting is a concept in deep learning neural networks that allows you to obtain predictions at intermediate points of the stack in a neural network by embedding exits earlier in the training architecture. This means that as soon as the desired confidence is achieved on an inputted sample, the execution will be terminated saving time. Whether or not an EE is relative, depends on the type of ML model used for training. To implement EE strategies, early classifiers are trained to provide a point of comparison. Methods for generating the early classifiers are split into Joint training and Separate Training. As the name suggests, joint training is the method of training all early classifiers at the same time and is the more popular option. Separate training, training the classifiers separately relies on two stages. The first stage trains a model, and the second stage then trains the classifiers after they have been introduced to a per-trained model, which then fixes the parameters [88].

5. Vulnerabilities

Regarding distributed and private machine learning, the privacy and vulnerability problems surrounding a metaverse are quite extensive in comparison to previous ventures, such as those faced in traditional social networking deployments. In this section, we have outlined some of the possible privacy issues, possible vulnerabilities that could be exploited to cope with those issues, and an adversary model to present a logical view of how those vulnerabilities could be exploited. It is worth noting that the specific vulnerabilities and privacy issues do not cover every event in any manner. They were chosen in the order of possible impact while taking into account the latest discovered attack vectors and vulnerabilities currently being explored.

5.1. Data Eavesdropping

Data eavesdropping, also known as a sniffing or snooping attack, is the act of intercepting, modifying, or deleting data traffic to create a beneficial outcome for the attacker. The network infrastructure required to operate a distributed deep learning network creates a large amount of possible attack vectors, due the complexity and sensitivity of the data involved. This means that security in all areas will be of paramount importance. Several attack vectors relating to these areas are described below along with examples of how to possibly mitigate them [89].

5.1.1. Preference Profiling Attacks

Objective. The objective of this attack is to profile user data by exploiting vulnerabilities in the federated learning model, which happens to be one of the most popular machine learning models currently in use. Very recently as of this paper's release date, it has been demonstrated that it is possible to achieve this, in a social media model, similar to how a metaverse may be deployed. Profiling user data with this model through machine learning on a massive scale could therefore lead to data leakage and present attackers with unauthorized access to it.

Initial Capabilities. For this attack to be carried out certain conditions must be met. For these conditions to be met, we have written assumptions outlined in the research paper recently written on this topic. Firstly, it is assumed that the server is aware of the type of training data set for the users. The server is also assumed to be able to collect small samples from each user's training data set in addition to collecting samples covering all possible categories from auxiliary data sets. It is then assumed that the server has a chosen subset of local models with the purpose of updating the global model by leveraging aggregation.

Attack Process. The attack process has 4 steps. These are local model training, Extracting the model's sensitivity, Profiling user preferences, and selective aggregation. The user local model training. The user local model training step consists of users creating diverse data sets, locally training them on their devices, and then uploading this information to the servers. Once uploaded, the attack process moves on to the next step of extracting the models' sensitivity. In this step, the server will use the sampled aggregated public data that was previously collected and use it to retrain the users uploaded and trained data set. This allows for the extraction of the model sensitivity on a per-class basis. Once this has been achieved the attack moves on to the next step of profiling user preferences. This step utilizes a meta-classifier to predict a user's preferred class. Lastly, the attack moves onto its final stage of selective aggregation. The goal of this step is to improve the attack accuracy for future use. This is performed by manipulating the global model and sending the aggregated model to the targeted users. For this step to be performed, however, the attacker must first train a meta-classifier offline.

Feasible Defense Strategy. Current defenses against these attacks on a federated learning model come with significant downsides. These range from negatively affecting model accuracy to increased computational costs. So far, two methods of defense against this type of attack have been proposed. The first is through the employment of Dropout and differential privacy techniques [90]. These reduce attack accuracy, although not always by a significant amount, and introduce a decrease in model utility and accuracy. The second method is leveraging cryptographic-based federated learning. This avoids the degradation of model utility and accuracy, but introduces higher computational requirements and increased communication overhead [91].

5.1.2. Membership Inference Attacks

Objective. An inference attack focuses on revealing secrets by supplying varying input data and monitoring the results. There are multiple types of inference attacks, each with fundamental differences. Unlike the attribute inference attack, which assumes the attacker already has some knowledge of a training record before trying to guess the missing attribute, membership inferences rebuild the records by running possible options through a machine learning model and monitoring the output to understand if it was present in the original model.

Table 4: Summary of vulnerabilities, their features, and countermeasures.

Vulnerability	Victim	Influence	Countermeasure
Preference profiling attacks	The local users' preferences obtained through profiling.	Through the obtaining of a local client's preferences, an attacker can go on to use the information for malicious purposes, such as social engineering attacks or supporting targeted identity theft.	A defense for this, which is currently available, is through leveraging cryptographic-based federated learning techniques.
Membership inference attacks	The victim of this attack is the local user client who could have their participation in the data set exposed.	The negative consequences of this are the potential release of private information. For example, a user's participation in a medical study or investment scheme is marketed towards highly vulnerable individuals.	A current defense for these attacks was traditionally differential privacy. However, an alternative approach would be the implementation of a digestive neural network independent from the network it is protecting.
Fault attacks	The victim in this attack is the deep learning model and by extension the model's creator, with the potential to also impact the model's clients.	The negative effects from this type of attack could be far-reaching as once misclassification is achieved, depending on the security methods being employed, the attacker could alter a significant classification. For example, a model created to scan medical images for cancerous cells could miss those cells when attached to a specific organ.	A defense against these attacks is to employ a collection of onsite security, hardware access protections, and hardware design protection, such as em shielding on chips and overcurrent protection circuits.
Model replacement attacks	Federated Learning Training Model data on a central server	If an attacker is able to create a subtask in the network, generating a model for their own use, it could constitute a serious privacy threat. Additionally, the attacker would be taking advantage of the free computing power required to train the model, causing the owner of the original model to pay higher costs.	Several strategies can be chosen to mitigate these potential attacks. Including FederatedReverse, a 4-stage system including detection and repair from an attack. As well as a framework for a robust federated learning model.
Model inversion attacks	Local users who generated model Inputs	The goal of the attack is to predict the inputs used to generate the model. This can also be applied to federated learning.	The attack can be mitigated by ensuring that the split neural network protocol is only used in secure environments.
Feature space hijacking attacks	User client's individual private data are used to train the model in a split learning network	In this attack the goal is to obtain a client's data by reconstructing the model inputs.	The countermeasures for this are potentially differential privacy, prevention through detection, and keeping information of related public data sets private.
Model data poisoning attacks	A trained federated learning model that is currently on a central server	The negative effects of model poisoning can cause an entire model to have significantly lower usability than expected. Additionally, an attacker may choose to poison specific parts of the model for their own gain.	A proposed defense is through the detection of malicious participants in the network by identifying unique characteristics in their submissions.

Initial Capabilities. To carry out this attack on a federated learning neural network, the attacker needs a reference of the records that could be contained in the model. If the attacker does not have access to the target's training data, entropy can be employed to variably shorten the total time for the attack to take place. For the attack to take place, the adversary must be either the centralized parameter server or a participant in the model [92].

Attack Process. To achieve its goal and obtain private records through the restoration of training data, the attack will vary based on the position of the adversary in the network. If the adversary is a participant or not. If the adversary is the centralized parameter server, it can be used to infer training data when receiving updates from each participant over time. Alternatively, if the adversary is a participant in the network, they can only observe the parameters over time in comparison to updates to gain information. Both of these methods have a downside that dependencies between parameters may not be captured over time, a solution for this was recently proposed [93].

Feasible Defense Strategy. Traditionally, differential privacy has been the potential defense against inference attacks on machine learning models. Unfortunately, this comes at a significant cost in model accuracy. A technique called adversarial training can improve these results slightly but is still not a perfect solution. Additionally, inference attacks can come in several different forms, such as input inference, attribute inference, parameter inference. Each of these has varying degrees of results when it comes to defense implementations. However, novel approaches to defense against these types of attacks are being proposed. For example, the approach of attaching an independent neural network to the federated learning model is called a digestive neural network [94]. The goal of this approach is to modify input

data, distort updates, and maximize the accuracy of the federated learning model while minimizing the accuracy of inference attacks [95].

5.2. Data Reconstruction

Data reconstruction attacks are used to reconstruct private information using private or public datasets that have been obtained by an attacker. In distributed deep learning networks these datasets could contain potentially sensitive data which could cause damage in many ways, for example, if an attacker was able to link the data to an individual who contributed it to the model. Despite the potential for attack, large data sets can be extremely valuable to companies and many have been facing the challenge of securing them for many years. The metaverse will face many of the same challenges that were previously tackled by businesses to prevent these types of attacks from occurring. It is also apparent that the large swaths of data involved and large complexity will make it a prime choice for attackers. In this section we have outlined some possible attacks that could be used and possible defenses [96].

5.2.1. Model Inversion Attacks

Objective. The objective of this attack is to determine the missing pieces of split learning training data by attacking the intermediate layers in a deep learning model that has already been trained. Feature maps are then used to recover the original data. This is done through the recovery of any input given to the network and the acquisition of a functionally similar clone of the network. This attack has been demonstrated against IoMT (Internet of Medical Things) deep learning models in the past and could be a common attack point for metaverse data in the future [97].

Initial Capabilities. For this attack to take place, it is assumed that the attacker knows the architecture of the model but does not have knowledge of the parameters. It is not required for the attacker to have knowledge or access to specific data and they do not need to query the client network. The attacker is attempting to search all possible input values and client network parameters. This becomes an optimization issue that has various solutions available for the attacker to take advantage of.

Attack Process. The process begins with the sever randomly initializing a deep learning model with an architecture that matches the client's model. Next two objective functions are defined, these are not related to the loss function used for training the model. Depending on the domain being worked on, variations measures can be implemented to improve the output data from the task at this point. Using the assumptions made from the model inversion attack and a possible stealing attack together can then lead to a possible label inference attack [98].

Feasible Defense Strategy. Multiple studies have tested possible defenses against model inversion attacks on split learning. However, it has been demonstrated that some traditional defense methods do not show a strong result when attackers are utilizing model inversion attacks. For example, the distance correlation defense using (DCOR) showed that recovered images were still of high quality despite the defense having some impact on the attack. Additionally, it showed zero impact on the potential of a model to be stolen. Although, the effectiveness of the model inversion attacks on split learning will decrease with the depth of the split layers, creating a performance-to-security trade-off for clients in the network [99].

Additionally, other methods such as proximal gradient split learning (PGSL) have shown effectiveness in defending against model inversion compared to techniques such as the addition of label perturbations and adding noise to data input levels. The PGSL technique works by reconstructing data into its original form once it has been transmitted to the server side of the split network.

5.2.2. Feature Space Hijacking Attacks

Objective. The goal of this attack is to re-construct a client's data used for training with the lowest error rate possible, even when the data was protected with DP. To do this the attacker will employ a Feature Space Hijacking Attack (FSHA). Once the attack has been completed. The reconstructed data should allow an attacker to view specific data or images inputted into a split learning model with minimal distortion or blurring.

Initial Capabilities. For an attack to take place using the FSHA method, the client part of the model must be able to successfully be trained. With the client model, the attacker can the private data that was entered into it can then be re-constructed. This will not work if the attacker does not have access to the server or another component of the network where the data is passing through, such as the client's own device. Additionally, an attack would not be able to obtain the data required to perform the attack if the server was enforcing a secure compute environment [100].

Attack Process. The attack process begins with the attacker targeting the client's trained data through a server or network component. If the attacker has chosen to target the server instead of the client's device, the attack would begin by the attacker deploying code to the server. This code will learn how to reconstruct the original data and then allow the attacker to re-construct the client's model [101]. Additionally, alternate attack methods to traditional approached that achieve similar results, such as Unsplit, have been proposed and are potentially even more harmful [98].

Feasible Defense Strategy. To mitigate the potential damage caused by this attack and improve the safety of the model, it is possible to implement differential privacy with dimensionality reduction techniques. However, this can have several downsides. Differential privacy on its own is not able to protect against this type of attack. The addition of dimensionality reduction can cause the produced model to be of low usability while potentially still giving the attacker sensitive data. Detection methods have also been proposed as a defense, such as SplitGuard but this is not bulletproof [102]. This means that the preferred defense was to simply ensure that the model is

running in a secure computing environment, checking for certified versions of models on the client and denying attackers any access to the model where possible. Though a new method of combining SL with Function Secret Sharing (FFS) shows promising results, through adding a random mask to the activation map before providing it to the central server. The server works with the FFS generated shares instead of accessing the original function data, effectively improving privacy without the downsides previously mentioned [103].

5.3. Model Modification

Model modification attacks are focused on modifying the resulting classifications achieved from a trained deep learning model or corrupting the final results. This can be a simple or small change such as modifying an image recognition model to misclassify an animal species or creating new classifications unintended by the creator in order for an attacker to use the model for their own personal gain. While most attacks of this nature are software-based, revolving around the server or distributed deep learning frameworks and architecture, alternative attacks such as those that are hardware-based have begun to be explored. In this section, we have outlined some of these exploits with a connection to how models could be manipulated or mishandled by an attacker.

5.3.1. Model Data Poisoning Attacks

Objective. Through this vulnerability, the attacker aims to poison the globally trained federated learning model, which was created from participating clients using their own per-trained data models. This is done through manipulating the data used to create a client's model on their own device, either through compromised devices or through the attacker's own clients. An attacker using this method will target specific classes in the model so that they can remain undetected for as long as possible. The outcome of this attack could potentially be that a model trained to recognize a car may misclassify it as a truck.

Initial Capabilities. For this attack to take place, the attacker must have access to clients that are being used to contribute towards to federated learning model. It is not required for the server combining the clients' models to be compromised. This makes the attack quite approachable for bad actors.

Attack Process. The attack makes use of label flipping in the client's data set. For the attack to be most effective the attacker must ensure that they begin the attack towards the relative beginning of the training. Once the attacker has gained enough compromised clients they can begin to perform the label-flipping attack by manipulating the raw data before it is trained on the users' devices. To increase the effectiveness of the attack, the attacker can increase the number of compromised clients they are using to attack the model in the late stages of the training [104].

Feasible Defense Strategy. This attack can be defended against using various techniques. One method is centered around the identification and reversal of damages by blocking future updates from bad actors. This method uses an automated strategy to identify "relevant parameter subsets" in a DNN and "study participant updates using dimensionality reduction" techniques. Additionally, a framework known as Sparsefed has been proposed which mitigates possible attacks through gradient specification. This is achieved through the monitoring of "the upper bound on the distance between poisoned and benign models" [105].

5.3.2. Model Replacement Attacks

Objective. The objective of this attack is to install a backdoor and run an additional subtask chosen by the attacker in addition to the model that was intended while maintaining a high accuracy, in a federated learning model utilizing a method called model replacement. This differs from the more well-known poisoning attack, as it will not recognizably change performance. A secondary objective of this attack is to maintain the backdoor for as many rounds as possible to allow the adversary to create more corruption in the network.

Initial Capabilities. To perform the attack, the attacker must first be a participant in a federated learning model. With this access, the attacker is able to begin the model flip by poisoning the data that is distributed into the network. For this to be successful on a federated learning model within a reasonable amount of time, the adversaries must take advantage of methods cited in the proposed paper, such as the employment of secure aggregation. This will attempt to prevent the malicious model detection.

Attack Process. The attack begins with the adversary choosing a malicious model that they wish to implement in the victim's network. Once determined, the attacker will become a participant in the network and begin poisoning the training data supplied to the server. The backdoor malicious model will only be trained when the attacker is selected, making it in the adversary's best interest to be selected as much as possible. This limitation is what ensures that the original model's training results will not be negatively affected to a significant degree [106].

Feasible Defense Strategy. Several papers have demonstrated the possibility of model replacement attacks in federated learning to gain backdoor access. Multiple defense strategies against this have been proposed in the form of protocols and algorithms utilizing residual-based reweighting. A framework for a certifiably robust federated learning model has also been proposed. This general framework works by exploiting clipping and smoothing model parameters. During training, the local agent updates their model parameters with the central server. The central server then "aggregates the data", "clips the norm of the aggregated model parameters", "add a random noise to the clipped model" and "send the new model parameters back to the agents". Using this technique the server can make a final prediction for the output by "smoothing the final global model

with randomized parameters". An alternative defense proposal is called FederatedReverse. This method can detect and defend against backdoor attacks with little impact on overall model accuracy. The implementation consists of 4 stages: reverse engineering, global reserve trigger generation, outlier detection, and finally model repairing. By carrying out these stages in sequence the proposal is able to obtain high rates of detection among backdoor attacks [107].

5.3.3. Fault Attacks

Objective. The objective of this attack is to create a fault in an integrated circuit running a distributed machine learning model to provoke it into an unintended state. In the notion of machine learning, this can allow the attacker to manipulate the model causing a misclassification in the neural network.

Initial Capabilities. This attack's initial requirements can vary. Typically, the requirements rely on four common activation functions that are ReLu, softmax, sigmoid, and tanh. To accomplish the task in the most precise manner, a diode pulse laser capable of fault injection must be available to the adversary as it can reliably flip single bits.

Attack Process. This attack begins by surrounding the activation functions with a separate layer and using a trigger signal in combination with a microcontroller, such as an Arduino, to measure the correct laser timing. Using the laser, the attacker can then target the skip/change instruction and inspect the outputs until producing the desired result.

Feasible Defense Strategy. As a hardware-focused attack, fault injection can be difficult to defend against. However, by employing a comprehensive collection of defense measures, the difficulty of the attack can be increased dramatically. The most obvious defense strategy is to make the hardware as difficult to access as possible for the attacker. However, if the attacker has gained access to the hardware and in the case of a chip, decapped and removed the passivation layer, other countermeasures must be employed. These include the implementation of EM shielding, implementing fault detection mechanisms such as an error detection circuit or code, and implementing redundancy. Unfortunately in the case of a laser-based attack, countermeasures such as EM shielding would not have a significant impact and many other methods can be overcome by a determined attacker [108].

5.4. Discussion Summary and Lessons Learned

Throughout the study of vulnerabilities related to distributed deep learning networks, we have been evaluating the potential impact and difficulties that may be faced through potential attacks in a metaverse. The recent development of federated and split learning networks has led to increased research focus in the area and presented several interesting challenges when it comes to protecting clients' data in the network. Several papers that have recently been released outlined the potential for data such as user preferences to be determined without consent. The main lessons learned from this are that the overall privacy implications derived from the implementation of a distributed learning networks application in the metaverse are wide-ranging. But despite the inherent risks the potential uses could greatly expand the overall user experience and give invaluable data to companies. The vulnerabilities can be classified in many different ways and these classifications should focus on different impacts to the contributors to the models. In this regard, we classify them as User profiling and pervasive data collection - Impersonation, miss-classification, and identity theft - Manipulation and mishandling of user data and storage. To ensure that users are not impacted by potential vulnerabilities in these areas, significant attention should be paid to ongoing research in the area to ensure that implementations of the model remain secure. Table 4 provides a summary of the mentioned attacks and corresponding countermeasures.

6. Metaverse Developments

6.1. Metaverse Applications

The applications of distributed and private machine learning when applied to the metaverse concept are wide-ranging. Research has identified the possibility for it to facilitate metaverse services through its applications in healthcare, manufacturing, and finance to name just a few. Furthermore, the scalability requirements of the metaverse make it an ideal candidate for distributed machine learning, as it is able to exploit the large amount of computing resources and data available [109]. In what can be described as a healthcare metaverse, the application of FL opens up massive opportunities to overcome challenges that usually come from working with health-related data. This is achieved due to the inherent benefits of FL integration such as security, data management, better interoperability, automation, scalability, and low latency support. When applied in the metaverse this could allow for medical diagnoses, in what could be considered the successor to telemedicine, patient monitoring, collaboration of research, effective pandemic management, and drug discovery [110]. It has also been suggested that the combination of FL with MAR capable devices in a metaverse could be used for object detection tasks. The implementation of FL into this scenario would create a more private a secure manner of conducting these tasks, with the overall goal being to allow object detection without revealing the users' data. For example, the user may look towards a building and see a description of it, without revealing to the metaverse provider their current location [111]. Another application of FL in the metaverse can be seen in a proposal for a novel wireless VR content delivery network. The proposal aimed to create a multi-view synthesizing framework that transmitted images to users of the metaverse with overlapping fields of view, reducing the massive content transmission requirements that would usually take place. FL was effectively used to train the multi-view synthesizing model applied in this framework [112].

6.2. Implementations

Table 5: Metaverse applications and their features.

Applications	Description	Network Requirements	User Interaction
Education and Training	Education and training can take place in the form of virtual classes and engaging environments, where hands-on learning can be conducted in a safe, efficient, and repeatable manner.	Although it does require a high-speed connection and large amounts of bandwidth, the requirements for virtual classes and training environments are not particularly large in comparison to other applications in the metaverse	In the education and training concept, user interaction can be complex, virtual reality, mixed reality, augmented reality and features such as haptic feedback.
Healthcare	Various types of healthcare settings can be created and utilized in a metaverse environment. This can take many different forms, such as helping patients with mental health issues, encouraging physical fitness, or allowing for virtual consultations with a medical professional.	Large amounts of bandwidth and high-speed connections in healthcare environments, for applications such as socializing and engagement with doctors while in remote areas, demand the implementation of several networking concepts. These include network slicing, 5G and 6G networking integration, and digital twin networking.	Interaction in healthcare environments could take place in several forms, for example: among virtual and physical objects, between users, or through direct streaming of live video feeds.
Entertainment	movies, games, experiences, and social interaction create the building blocks of entertainment settings in the metaverse. It offers a large and dynamic platform for participation and utilization within these virtual spaces catering to a wide audience of potential users.	Depending on the application and platform, networking considerations which may need to be made when creating an entertainment environment could include scalability, edge computing utilization, load balancing, low latency, and high bandwidth requirements.	An integral part of entertainment activities in the metaverse is the interaction between the user and the virtual environment. This interaction could be in relative terms simplistic, such as selecting an item on a user interface to watch a movie. Alternatively, in entertainment settings such as a video game, complex interactions could take place utilizing mixed reality, haptic feedback, and virtual interactions with items and other users.
Architecture and Design	The virtual environment offered in a metaverse allows for architectural and design decisions to be tested and observed extensively before transitioning them into a real-world space, saving costs and creating a unique opportunity for developments that otherwise may be considered outlandish.	In a metaverse environment, networking requirements are paramount for seamless user experiences. High-speed, low-latency connections are essential to support real-time interactions and data exchange between users and the virtual world. Scalable infrastructure, robust security measures, and global reach are crucial to accommodate the vast user base and ensure data privacy and integrity in this interconnected digital realm.	In a metaverse environment, user interaction centers on immersive experiences. Users navigate through virtual spaces using avatars, engaging in real-time communication, exploration, and collaboration with others. They can customize their surroundings, create content, and participate in dynamic, user-generated content, blurring the line between virtual and physical reality.
Tourism and Travel	Tourism and travel applications in the metaverse enable users to explore virtual replicas of real-world destinations. Travelers can virtually visit places, interact with historical or cultural simulations, and experience adventures without leaving their homes. These metaverse experiences offer accessibility, safety, and novel opportunities for tourism promotion and education.	Tourism and Travel networking requirements in the metaverse demand high bandwidth to support rich multimedia content and real-time interactions. Low latency is crucial for seamless exploration and communication. Scalable infrastructure is needed to accommodate a potentially large user base, while data security measures are essential to protect personal information and ensure safe online experiences for travelers.	In a metaverse environment, Tourism and Travel user interaction involves immersive exploration and engagement. Travelers use avatars to navigate virtual destinations, interact with simulations of real-world attractions, and communicate with fellow explorers. They can customize their experiences, share travel memories, and participate in collaborative virtual adventures, enhancing their travel experiences in novel and interactive ways.
Social Engagement	Social engagement in the metaverse involves creating virtual communities and connections. Users interact through avatars, engaging in real-time conversations, events, and shared activities. These applications facilitate social networking, virtual gatherings, and collaborative experiences, allowing individuals to connect, communicate, and socialize with others globally, transcending physical limitations.	Social engagement networking in the metaverse demands robust infrastructure with high bandwidth and low latency to support real-time interactions. Scalable servers are necessary to accommodate a vast user base. Strong security measures are crucial to protect user data and ensure safe social experiences, while seamless cross-platform compatibility enhances accessibility and user engagement.	Social engagement in the metaverse enhances user interaction by enabling immersive, virtual experiences. It's used for virtual meetings, conferences, social gatherings, and entertainment. Users can communicate through avatars, share content, attend events, and build communities, fostering connection and collaboration in this digital, interconnected world.
Virtual Commerce	Virtual commerce in the metaverse allows users to buy and sell virtual goods, services, and experiences. It's utilized for virtual real estate, digital fashion, NFT marketplaces, and virtual events. Brands can establish virtual storefronts, enhancing e-commerce and enabling new revenue streams in the immersive, digital realm.	Virtual commerce in the metaverse demands robust networking infrastructure. High-speed, low-latency connections are crucial for seamless transactions, secure payments, and real-time interactions. Scalable servers and decentralized blockchain networks support NFTs and virtual asset trading. Reliable networking is the backbone of a thriving metaverse economy.	Virtual commerce in the metaverse enhances user interaction through immersive shopping experiences. Users can explore virtual stores, interact with products, and engage with sellers via avatars or chatbots. Social elements like virtual showrooms and shared shopping with friends enrich the buying process, fostering a sense of community and connection.

6.2.1. Practical Implementations

Recent advances in mobile edge computing and digital twins highlight how metaverse platforms can and are being used streamlines industrial tasks, such as predictive maintenance and real-time monitoring of factory floors [74]. By incorporating virtual replicas of physical systems, operators can proactively prepare for potential future issues or detect anomalies without halting on-site operations, in turn reducing costs and downtime.

6.2.2. Theoretical Implementation Advancements

From a theoretical implementation standpoint, the inter connectivity between digital twins and deep learning model training suggests the need for sustainable design protocols that minimize energy consumption while maintaining accurate simulations [73]. Furthermore, emerging frameworks such as BlockNet [75] illustrate how blockchain-enabled architectures can ensure authenticated data exchanges across metaverse services, reinforcing trust and transparency at scale.

Table 5 continues by summarizing metaverse applications and their features.

7. Future Research Directions and Challenges

The potential privacy challenges of implementing distributed deep learning into a metaverse concept are wide-ranging. A specific example of one of these challenges can be seen in the implementation of a metaverse healthcare service, where a previous research paper has assumed that virtual clinics are trustworthy. When considering that these virtual clinics could potentially be less reliable for storing data than their physical counterparts, the difficulty in safeguarding the privacy of distributed deep learning algorithm applications becomes apparent. If an attacker were able to leverage the fact that these clinics are not trustworthy, they could possibly retrieve the private attributes from the medical dataset being used to train the distributed deep learning model. Which they could then use to target the initial contributor [113]. Furthermore, the large number of contributors to a distributed deep learning deployment, such as in the federated learning framework, increases the potential for a malicious attacker to be included in the model [114]. The consequence of this is that a privacy challenge is created for those who wish to employ FL and other distributed deep-learning frameworks in the metaverse. Another potential privacy-related challenge of FL integration in a metaverse healthcare service is meeting the laws or regulations related to sharing health data. Depending on the jurisdiction, there may also be no requirement for a company to delete information it has gathered from distributed deep learning, increasing the chance of potential future exposure if not well-managed [115]. Lastly, to ensure that privacy is respected in a distributed deep learning environment, the creator of the model must generate the dataset in an informed manner. The data collection for dataset generation involves several sources, such as sensors, databases, and the web. This data is then pre-processed for use in the final model [116]. It is important that the privacy of users generating the data is not impacted by the collection of irrelevant sensitive data in a metaverse environment.

The combination and integration of distributed deep learning with the metaverse create promising future opportunities with several unresolved challenges. Though federated and split learning have been used to enhance privacy. Issues related to data leakage, computational efficiency and data leakage remain largely unresolved [90, 92, 102]. Additionally, further study is needed when it comes to ensuring privacy in digital twin implementations [71] and decentralized identity authentication [60]. Another critical challenge to be addressed as the metaverse develops is the scalability of its underlying infrastructure, as metaverse applications collect diverse data from different devices with varying processing power [8, 15]. A portion of these scalability issues could potentially be addressed with advances in adaptive federated learning and hierarchical model aggregation. These techniques could potentially enhance performance while maintaining the positive aspects of model training [5, 18]. Moreover, ensuring that resource allocation in MEC is optimized will be essential for reducing latency within real time metaverse environments [53]. The security consequences of potential adversarial attacks, model inversion and backdoors also pose significant risks. Particularly, as blockchain based transactions grow in size and become more integrated into a digital economy [63, 65]. To mitigate these potential threats, lightweight cryptographic methods and privacy aware AI frameworks should be further explored [57]. Moving beyond the technical aspect, ethical and regulatory considerations when it comes to user data, AI biases and algorithmic accountability will also need to be addressed as the technology develops [12, 24]. Through the establishment of standardized privacy regulations and explainable AI models, crucial trust can be built in the metaverse ecosystems [94, 95]. Future research should therefor focus on enhancing security, improving efficiency, and ensuring ethical AI governance to support the sustainable growth of the metaverse as a scalable, privacy-preserving digital environment [64].

8. Concluding Remarks

This paper has reviewed metaverse developments with strict consideration of distributed machine learning association from a privacy preservation perspective. Our investigation of contemporary work reveals a high potential of distributed learning architectures to assist the metaverse system and operations even though several challenging privacy vulnerabilities exist. Obviously, privacy preservation is a critical concern and it deserves thorough studies to ensure the success of distributed learning utilization in the metaverse evolution. This paper wishes to provide a state-of-the-art reference and direction for interested researchers and engineers in the fields.

References

[1] D. G. Morín, P. Pérez, A. G. Armada, Toward the distributed implementation of immersive augmented reality architectures on 5G networks, IEEE Communications Magazine 60 (2) (2022) 46–52.

[2] S. M. Park, Y. G. Kim, A metaverse: Taxonomy, components, applications, and open challenges, IEEE Access 10 (2022) 4209–4251.

[3] M. Y. Akhlaqi, Z. B. M. Hanapi, Task offloading paradigm in mobile edge computing-current issues, adopted approaches, and future directions, Journal of Network and Computer Applications 212 (2023) 103568.

[4] Y. Siriwardhana, P. Porambage, M. Liyanage, M. Ylianttila, A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects, IEEE Communications Surveys & Tutorials 23 (2) (2021) 1160–1192.

[5] Y. Wang, J. Zhao, Mobile edge computing, metaverse, 6g wireless communications, artificial intelligence, and blockchain: Survey and their convergence, in: 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), 2022, pp. 1–8.

[6] Z. Lifelo, J. Ding, H. Ning, Qurat-Ul-Ain, S. Dhelim, Artificial intelligence-enabled metaverse for sustainable smart cities: Technologies, applications, challenges, and future directions, Electronics 13 (24) (2024). doi:10.3390/electronics13244874.
URL https://www.mdpi.com/2079-9292/13/24/4874

[7] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland, F. Tufvesson, 6G wireless systems: Vision, requirements, challenges, insights, and opportunities, Proceedings of the IEEE 109 (7) (2021) 1166–1199.

[8] H. Peng, P.-C. Chen, P.-H. Chen, Y.-S. Yang, C.-C. Hsia, L.-C. Wang, 6g toward metaverse: Technologies, applications, and challenges, in: 2022 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 2022, pp. 6–10. doi:10.1109/APWCS55727.2022.9906483.

[9] J. Sun, W. Gan, H.-C. Chao, P. S. Yu, Metaverse: Survey, applications, security, and opportunities (2022). arXiv:2210.07990.

[10] S. Dong, M. Liu, K. Abbas, The metaverse review: Exploring the boundless ream of digital reality, Computers, Materials and Continua 81 (3) (2024) 3451–3498. doi:https://doi.org/10.32604/cmc.2024.055575.
URL https://www.sciencedirect.com/science/article/pii/S1546221824008270

[11] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, M. Daneshmand, A survey on metaverse: the state-of-the-art, technologies, applications, and challenges (2021). arXiv:2111.09673.

[12] H. J. Oh, J. Kim, J. J. Chang, N. Park, S. Lee, Social benefits of living in the metaverse: The relationships among social presence, supportive interaction, social self-efficacy, and feelings of loneliness, Computers in Human Behavior 139 (2023) 107498.

[13] Y. Fu, C. Li, F. R. Yu, T. H. Luan, P. Zhao, S. Liu, A survey of blockchain and intelligent networking for the metaverse, IEEE Internet of Things Journal 10 (4) (2022) 3587–3610.

[14] R. Chengoden, N. Victor, T. Huynh-The, G. Yenduri, R. H. Jhaveri, M. Alazab, S. Bhattacharya, P. Hegde, P. K. R. Maddikunta, T. R. Gadekallu, Metaverse for healthcare: A survey on potential applications, challenges and future directions, IEEE Access 11 (2023) 12765–12795.

[15] J. Sun, W. Gan, Z. Chen, J. Li, P. S. Yu, Big data meets metaverse: A survey, ArXiv abs/2210.16282 (2022).

[16] T. Huynh-The, T. R. Gadekallu, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, M. Liyanage, Blockchain for the metaverse: A review, Future Generation Computer Systems 143 (2023) 401–419. doi:https://doi.org/10.1016/j.future.2023.02.008.
URL https://www.sciencedirect.com/science/article/pii/S0167739X23000493

[17] Y. Chen, S. Huang, W. Gan, G. Huang, Y. Wu, Federated learning for metaverse: A survey, WWW '23 Companion, Association for Computing Machinery, New York, NY, USA, 2023, p. 1151–1160.

[18] M. A. Fadhel, A. M. Duhaim, A. S. Albahri, Z. T. Al-Qaysi, M. A. Aktham, M. A. Chyad, W. Abd-Alaziz, O. S. Albahri, A. H. Alamoodi, L. Alzubaidi, A. Gupta, Y. Gu, Navigating the metaverse: unraveling the impact of artificial intelligence—a comprehensive review and gap analysis, Artificial Intelligence Review 57 (10) (2024) 264. doi:10.1007/s10462-024-10881-5.
URL https://doi.org/10.1007/s10462-024-10881-5

[19] G. Siwach, A. Haridas, D. Bunch, Inferencing big data with artificial intelligence & machine learning models in metaverse, in: 2022 International Conference on Smart Applications, Communications and Networking (SmartNets), 2022, pp. 01–06.

[20] M. Al-Kfairy, A. Al-Adaileh, M. Tubishat, O. Alfandi, M. BinAmro, A. Alomari, A sentiment analysis approach for identifying users' security and privacy perception of metaverse in twitter, in: 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), 2023, pp. 1–6. doi:10.1109/SmartNets58706.2023.10215677.

[21] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, Z. Lin, When machine learning meets privacy: A survey and outlook, ACM Comput. Surv. 54 (2) (mar 2021).

[22] S. Dong, K. Abbas, M. Li, J. Kamruzzaman, Blockchain technology and application: An overview, PeerJ Computer Science 9 (2023) e1705. doi:https://doi.org/10.7717/peerj-cs.1705.
URL https://doi.org/10.7717/peerj-cs.1705

[23] C. Chen, Y. Li, Z. Wu, C. Mai, Y. Liu, Y. Hu, J. Kang, Z. Zheng, Privacy computing meets metaverse: Necessity, taxonomy and challenges, Ad Hoc Networks 158 (2024) 103457. doi:https://doi.org/10.1016/j.adhoc.2024.103457.
URL https://www.sciencedirect.com/science/article/pii/S1570870524000684

[24] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, X. Shen, A survey on metaverse: Fundamentals, security, and privacy, IEEE Communications Surveys & Tutorials 25 (1) (2023) 319–352.

[25] M. Alkaeed, A. Qayyum, J. Qadir, Privacy preservation in artificial intelligence and extended reality (ai-xr) metaverses: A survey, J. Netw. Comput. Appl. 231 (C) (2024). doi:10.1016/j.jnca.2024.103989.
URL https://doi.org/10.1016/j.jnca.2024.103989

[26] M. Al-kfairy, A. Alomari, M. Al-Bashayreh, O. Alfandi, M. Altaee, M. Tubishat, A review of the factors influencing users' perception of metaverse security and trust, in: 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), 2023, pp. 1–6. doi:10.1109/SNAMS60348.2023.10375478.

[27] C. Machover, S. Tice, Virtual reality, IEEE Computer Graphics and Applications 14 (1) (1994) 15–16.

[28] Y. Ding, Y. Li, L. Cheng, Application of Internet of things and virtual reality technology in college physical education, IEEE Access 8 (2020) 96065–96074.

[29] A. Yarramreddy, P. Gromkowski, I. Baggili, Forensic analysis of immersive virtual reality social applications: A primary account, in: 2018 IEEE Security and Privacy Workshops (SPW), 2018, pp. 186–196.

[30] T. S. Perry, Virtual reality goes social, IEEE Spectrum 53 (1) (2016) 56–57.

[31] D. Brutzman, M. Zyda, K. Watsen, M. Macedonia, Virtual reality transfer protocol (vrtp) design rationale, in: Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997, pp. 179–186.

[32] E. Bastug, M. Bennis, M. Medard, M. Debbah, Toward interconnected virtual reality: Opportunities, challenges, and enablers, IEEE Communications Magazine 55 (6) (2017) 110–117. doi:10.1109/MCOM.2017.1601089.

[33] A. A. Simiscuka, T. M. Markande, G.-M. Muntean, Real-virtual world device synchronization in a cloud-enabled social virtual reality iot network, IEEE Access 7 (2019) 106588–106599.

[34] J. Yu, A light-field journey to virtual reality, IEEE MultiMedia 24 (2) (2017) 104–112.

[35] Z. Abrams, Enhancing mental health care with vr, IEEE Pulse 13 (5) (2022) 16–20. doi:10.1109/MPULS.2022.3208824.

[36] J. Jia, W. Chen, The ethical dilemmas of virtual reality application in entertainment, in: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Vol. 1, 2017, pp. 696–699. doi:10.1109/CSE-EUC.2017.134.

[37] M. U. Rafique, S.-c. S. Cheung, Tracking attacks on virtual reality systems, IEEE Consumer Electronics Magazine 9 (2) (2020) 41–46.

[38] P. Fraga-Lamas, T. M. FernáNdez-CaraméS, O. Blanco-Novoa, M. A. Vilar-Montesinos, A review on industrial augmented reality systems for the industry 4.0 shipyard, IEEE Access 6 (2018) 13358–13375.

[39] R. Azuma, Y. Baillot, R. Behringer, S. Feiner, S. Julier, B. MacIntyre, Recent advances in augmented reality, IEEE Computer Graphics and Applications 21 (6) (2001) 34–47.

[40] X. Qiao, P. Ren, S. Dustdar, L. Liu, H. Ma, J. Chen, Web ar: A promising future for mobile augmented reality—state of the art, challenges, and insights, Proceedings of the IEEE 107 (4) (2019) 651–666.

[41] S. Meža, Žiga Turk, M. Dolenc, Measuring the potential of augmented reality in civil engineering, Advances in Engineering Software 90 (2015) 1–10.

[42] R. Thilagavathy, T. Veeramani, B. Ramakrishna, Role of augmented reality and virtual reality in digital world, in: 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Vol. 1, 2019, pp. 179–186.

[43] D. Polap, K. Kesik, A. Winnicka, M. Woźniak, Strengthening the perception of the virtual worlds in a virtual reality environment, ISA Transactions 102 (2020) 397–406.

[44] P. Liu, L. Lu, S. Liu, M. Xie, J. Zhang, T. Huo, Y. Xie, H. Wang, Y. Duan, Y. Hu, Z. Ye, Mixed reality assists the fight against COVID-19, Intelligent Medicine 1 (1) (2021) 16–18. doi:https://doi.org/10.1016/j.imed.2021.05.002.

[45] A. Akter, A. Islam, S. Y. Shin, Mobile edge computing based mixed reality application for the assistance of blind and visually impaired people, in: 2019 7th International Conference on Information and Communication Technology (ICoICT), 2019, pp. 1–5.

[46] M. K. Bekele, R. Pierdicca, E. Frontoni, E. S. Malinverni, J. Gain, A survey of augmented, virtual, and mixed reality for cultural heritage, J. Comput. Cult. Herit. 11 (2) (2018).

[47] M. Speicher, B. D. Hall, M. Nebeling, What is mixed reality?, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19, Association for Computing Machinery, 2019, p. 1–15.

[48] J. A. De Guzman, K. Thilakarathna, A. Seneviratne, Security and privacy approaches in mixed reality: A literature survey, ACM Comput. Surv. 52 (6) (2019).

[49] L. Chen, T. W. Day, W. Tang, N. W. John, Recent developments and future challenges in medical mixed reality, in: 2017 IEEE International Symposium on Mixed and Augmented Reality (ISMAR), 2017, pp. 123–135.

[50] R. Zhao, Y. Zhang, Y. Zhu, R. Lan, Z. Hua, Metaverse: Security and privacy concerns (2022). doi:10.48550/ARXIV.2203.03854.

[51] C. Khansulivong, S. Wicha, P. Temdee, Adaptive of new technology for agriculture online learning by metaverse: A case study in faculty of agriculture, national university of laos, in: 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT NCON), 2022, pp. 428–432.

[52] N. Aung, S. Dhelim, L. Chen, H. Ning, L. Atzori, T. Kechadi, Edge-enabled metaverse: The convergence of metaverse and mobile edge computing, Tsinghua Science and Technology 29 (3) (2024) 795–805. doi:10.26599/TST.2023.9010052.

[53] S. Karunarathna, S. Wijethilaka, P. Ranaweera, K. T. Hemachandra, T. Samarasinghe, M. Liyanage, The role of network slicing and edge computing in the metaverse realization, IEEE Access 11 (2023) 25502–25530. doi:10.1109/ACCESS.2023.3255510.

[54] Z. Yi, Y. Qian, M. Chen, S. A. Alqahtani, M. S. Hossain, Defending edge computing based metaverse ai against adversarial attacks, Ad Hoc Networks 150 (2023) 103263. doi:https://doi.org/10.1016/j.adhoc.2023.103263.
URL https://www.sciencedirect.com/science/article/pii/S157087052300183X

[55] Z. Long, H. Dong, A. E. Saddik, Human-centric resource allocation for the metaverse with multiaccess edge computing, IEEE Internet of Things Journal 10 (22) (2023) 19993–20005. doi:10.1109/JIOT.2023.3283335.

[56] S. Zhang, An overview of network slicing for 5g, IEEE Wireless Communications 26 (3) (2019) 111–117. doi:10.1109/MWC.2019.1800234.

[57] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X. S. Shen, W. Zhuang, Ai-native network slicing for 6g networks, IEEE Wireless Communications 29 (1) (2022) 96–103. doi:10.1109/MWC.001.2100338.

[58] H. Chergui, L. Blanco, L. A. Garrido, K. Ramantas, S. Kukliński, A. Ksentini, C. Verikoukis, Zero-touch ai-driven distributed management for energy-efficient 6g massive network slicing, IEEE Network 35 (6) (2021) 43–49. doi:10.1109/MNET.111.2100322.

[59] N. H. Chu, D. T. Hoang, D. N. Nguyen, K. T. Phan, E. Dutkiewicz, D. Niyato, T. Shu, Metaslicing: A novel resource allocation framework for metaverse, IEEE Transactions on Mobile Computing (2023) 1–18doi:10.1109/TMC.2023.3288085.

[60] V. T. Truong, L. Le, D. Niyato, Blockchain meets metaverse and digital asset management: A comprehensive survey, IEEE Access 11 (2023) 26258–26288. doi:10.1109/ACCESS.2023.3257029.

[61] H. Su, S. Dong, T. Zhang, A hybrid blockchain-based privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 73 (11) (2024) 17059–17072. doi:10.1109/TVT.2024.3424786.

[62] Z. Cui, F. XUE, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A hybrid blockchain-based identity authentication scheme for multi-wsn, IEEE Transactions on Services Computing 13 (2) (2020) 241–251. doi:10.1109/TSC.2020.2964537.

[63] Y. Lin, H. Du, D. Niyato, J. Nie, J. Zhang, Y. Cheng, Z. Yang, Blockchain-aided secure semantic communication for ai-generated content in metaverse, IEEE Open Journal of the Computer Society 4 (2023) 72–83. doi:10.1109/OJCS.2023.3260732.

[64] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, Metachain: A novel blockchain-based framework for metaverse applications, in: 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), 2022, pp. 1–5. doi:10.1109/VTC2022-Spring54318.2022.9860983.

[65] B. Tao, H.-N. Dai, H. Xie, F. L. Wang, Structural identity representation learning of blockchain transaction network for metaverse, in: 2022 IEEE 24th International Workshop on Multimedia Signal Processing (MMSP), 2022, pp. 1–6. doi:10.1109/MMSP55362.2022.9949334.

[66] A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar, S. Zeadally, Metaverse for 6g and beyond: The next revolution and deployment challenges, IEEE Internet of Things Magazine 6 (1) (2023) 32–39. doi:10.1109/IOTM.001.2200248.

[67] X. Zhang, H. Zhao, J. Zhou, F. Yang, S. Liu, G. Xie, Remote collaborations in metaverse under 5g mobile networks, IEEE Communications Magazine 61 (9) (2023) 16–22. doi:10.1109/MCOM.003.2200624.

[68] F. Tang, X. Chen, M. Zhao, N. Kato, The roadmap of communication and networking in 6g for the metaverse, IEEE Wireless Communications 30 (4) (2023) 72–81. doi:10.1109/MWC.019.2100721.

[69] C. Wang, L. Zhao, C. Fan, K. Zhao, N. Kumar, J. Li, S. Wan, Metaverse-inspired cybertwin-based space-air-ground integrated networks, IEEE Network 37 (2) (2023) 294–300. doi:10.1109/MNET.003.2200519.

[70] D. Jones, C. Snider, A. Nassehi, J. Yon, B. Hicks, Characterising the digital twin: A systematic literature review, CIRP Journal of Manufacturing Science and Technology 29 (2020) 36–52. doi:https://doi.org/10.1016/j.cirpj.2020.02.002.
URL https://www.sciencedirect.com/science/article/pii/S1755581720300110

[71] M. Aloqaily, O. Bouachir, F. Karray, I. Al Ridhawi, A. E. Saddik, Integrating digital twin and advanced intelligent technologies to realize the metaverse, IEEE Consumer Electronics Magazine 12 (6) (2023) 47–55. doi:10.1109/MCE.2022.3212570.

[72] Z. Lv, S. Xie, Y. Li, M. S. Hossain, A. El Saddik, Building the metaverse using digital twins at all scales,states, and relations, Virtual Reality & Intelligent Hardware 4 (6) (2022) 459–470. doi:https://doi.org/10.1016/j.vrih.2022.06.005.
URL https://www.sciencedirect.com/science/article/pii/S2096579622000602

[73] M. Bordegoni, F. Ferrise, Exploring the Intersection of Metaverse, Digital Twins, and Artificial Intelligence in Training and Maintenance, Journal of Computing and Information Science in Engineering 23 (6) (2023) 060806. arXiv:https://asmedigitalcollection.asme.org/computingengineering/article-pdf/23/6/060806/7014963/jcise_23_6_060806.pdf, doi:10.1115/1.4062455.
URL https://doi.org/10.1115/1.4062455

[74] D. Van Huynh, S. R. Khosravirad, A. Masaracchia, O. A. Dobre, T. Q. Duong, Edge intelligence-based ultra-reliable and low-latency communications for digital twin-enabled metaverse, IEEE Wireless Communications Letters 11 (8) (2022) 1733–1737. doi:10.1109/LWC.2022.3179207.

[75] Z. Lv, L. Qiao, Y. Li, Y. Yuan, F.-Y. Wang, Blocknet: Beyond reliable spatial digital twins to parallel metaverse, Patterns 3 (5) (2022) 100468. doi:https://doi.org/10.1016/j.patter.2022.100468.
URL https://www.sciencedirect.com/science/article/

pii/S2666389922000484

[76] Z. Lyu, M. Fridenfalk, Digital twins for building industrial metaverse, Journal of Advanced Research (2023). doi:https://doi.org/10.1016/j.jare.2023.11.019.
URL https://www.sciencedirect.com/science/article/pii/S2090123223003594

[77] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. (2019).

[78] N. Guha, A. Talwalkar, V. Smith, One-shot federated learning (2019). arXiv:1902.11175.

[79] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, H. Yu, Vertical Federated Learning, pringer International Publishing, 2020, pp. 69–81.

[80] Y. Liu, Y. Kang, T. Zou, Y. Pu, Y. He, X. Ye, Y. Ouyang, Y.-Q. Zhang, Q. Yang, Vertical federated learning: Concepts, advances, and challenges, IEEE Transactions on Knowledge and Data Engineering 36 (7) (2024) 3615–3634. doi:10.1109/TKDE.2024.3352628.

[81] J. Ryu, D. Won, Y. Lee, A study of split learning model, in: 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), 2022, pp. 1–4. doi:10.1109/IMCOM53663.2022.9721798.

[82] O. Li, J. Sun, X. Yang, W. Gao, H. Zhang, J. Xie, V. Smith, C. Wang, Label leakage and protection in two-party split learning (2022). arXiv:2102.08504.

[83] X. Wan, J. Sun, S. Wang, L. Chen, Z. Zheng, F. Wu, G. Chen, Pslf: Defending against label leakage in split learning, in: Proceedings of the 32nd ACM International Conference on Information and Knowledge Management, CIKM '23, Association for Computing Machinery, 2023. doi:10.1145/3583780.3615019.

[84] A. Chopra, S. K. Sahu, A. Singh, A. Java, P. Vepakomma, V. Sharma, R. Raskar, Adasplit: Adaptive trade-offs for resource-constrained distributed deep learning (2021). arXiv:2112.01637.

[85] J. Jeon, J. Kim, Privacy-sensitive parallel split learning, in: 2020 International Conference on Information Networking (ICOIN), 2020, pp. 7–9.

[86] S. Oh, J. Park, P. Vepakomma, S. Baek, R. Raskar, M. Bennis, S.-L. Kim, Locfedmix-sl: Localize, federate, and mix for improved scalability, convergence, and latency in split learning, in: WWW 2022 - Proceedings of the ACM Web Conference 2022, Association for Computing Machinery, 2022, p. 3347–3357.

[87] C. Thapa, P. C. Mahawaga Arachchige, S. Camtepe, L. Sun, Splitfed: When federated learning meets split learning, Proceedings of the AAAI Conference on Artificial Intelligence 36 (8) (2022) 8485–8493.

[88] Y. Matsubara, M. Levorato, F. Restuccia, Split computing and early exiting for deep learning applications: Survey and research challenges, ACM Comput. Surv. (2022).

[89] O. Hasan, B. Habegger, L. Brunie, N. Bennani, E. Damiani, A discussion of privacy challenges in user profiling with big data techniques: The eexcess use case, in: 2013 IEEE International Congress on Big Data, 2013, pp. 25–30.

[90] Q. Zhou, Z. Han, J. Wu, Local difference-based federated learning against preference profiling attacks, in: Web Information Systems Engineering – WISE 2023: 24th International Conference, Melbourne, VIC, Australia, October 25–27, 2023, Proceedings, Springer-Verlag, 2023, pp. 275–288. doi:10.1007/978-981-99-7254-8_21.
URL https://doi.org/10.1007/978-981-99-7254-8_21

[91] C. Zhou, Y. Gao, A. Fu, K. Chen, Z. Dai, Z. Zhang, M. Xue, Y. Zhang, Ppa: Preference profiling attack against federated learning (2022).

[92] Y. Liu, P. Jiang, L. Zhu, Subject-level membership inference attack via data augmentation and model discrepancy, IEEE Transactions on Information Forensics and Security 18 (2023) 5848–5859. doi:10.1109/TIFS.2023.3318950.

[93] L. Zhang, L. Li, X. Li, B. Cai, Y. Gao, R. Dou, L. Chen, Efficient membership inference attacks against federated learning via bias differences, in: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, RAID '23, Association for Computing Machinery, 2023, pp. 222–235. doi:10.1145/3607199.3607204.
URL https://doi.org/10.1145/3607199.3607204

[94] H. Lee, J. Kim, S. Ahn, R. Hussain, S. Cho, J. Son, Digestive neural networks: A novel defense strategy against inference attacks in federated learning, Computers & Security 109 (2021) 102378.

[95] L. Bai, H. Hu, Q. Ye, H. Li, L. Wang, J. Xu, Membership inference attacks and defenses in federated learning: A survey, ACM Comput. Surv. (November 2024). doi:10.1145/3704633.
URL https://doi.org/10.1145/3704633

[96] yuntao wang, Z. Su, N. Zhang, rui xing, D. Liu, T. H. Luan, X. Shen, A Survey on Metaverse: Fundamentals, Security, and Privacy, IEEE Communications Surveys & Tutorials (10 2022).

[97] M. Fredrikson, S. Jha, T. Ristenpart, Model inversion attacks that exploit confidence information and basic countermeasures, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15, Association for Computing Machinery, New York, NY, USA, 2015, p. 1322–1333.

[98] E. Erdoğan, A. Küpçü, A. E. Çiçek, Unsplit: Data-oblivious model inversion, model stealing, and label inference attacks against split learning, in: Proceedings of the 21st Workshop on Privacy in the Electronic Society, WPES'22, Association for Computing Machinery, 2022, pp. 115–124. doi:10.1145/3559613.3563201.
URL https://doi.org/10.1145/3559613.3563201

[99] T. Titcombe, A. J. Hall, P. Papadopoulos, D. Romanini, Practical defences against model inversion attacks for split neural networks, CoRR abs/2104.05743 (2021). arXiv:2104.05743.

[100] D. Pasquini, G. Ateniese, M. Bernaschi, Unleashing the tiger: Inference attacks on split learning, in: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21, Association for Computing Machinery, 2021, pp. 2113–2129. doi:10.1145/3460120.3485259.
URL https://doi.org/10.1145/3460120.3485259

[101] G. Gawron, P. Stubbings, Feature space hijacking attacks against differentially private split learning, CoRR abs/2201.04018 (2022). arXiv:2201.04018.

[102] E. Erdogan, A. Küpçü, A. E. Çiçek, Splitguard: Detecting and mitigating training-hijacking attacks in split learning, in: Proceedings of the 21st Workshop on Privacy in the Electronic Society, WPES'22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 125–137. doi:10.1145/3559613.3563198.
URL https://doi.org/10.1145/3559613.3563198

[103] T. Khan, M. Budzys, A. Michalas, Make split, not hijack: Preventing feature-space hijacking attacks in split learning, in: Proceedings of the 29th ACM Symposium on Access Control Models and Technologies, SACMAT 2024, Association for Computing Machinery, New York, NY, USA, 2024, pp. 19–30. doi:10.1145/3649158.3657039.
URL https://doi.org/10.1145/3649158.3657039

[104] V. Tolpegin, S. Truex, M. E. Gursoy, L. Liu, Data poisoning attacks against federated learning systems, CoRR abs/2007.08432 (2020). arXiv:2007.08432.

[105] A. Panda, S. Mahloujifar, A. Nitin Bhagoji, S. Chakraborty, P. Mittal, Sparsefed: Mitigating model poisoning attacks in federated learning with sparsification, in: G. Camps-Valls, F. J. R. Ruiz, I. Valera (Eds.), Proceedings of The 25th International Conference on Artificial Intelligence and Statistics, Vol. 151 of Proceedings of Machine Learning Research, PMLR, 2022, pp. 7587–7624.

[106] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, V. Shmatikov, How to backdoor federated learning, in: S. Chiappa, R. Calandra (Eds.), Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics, Vol. 108 of Proceedings of Machine Learning Research, PMLR, 2020, pp. 2938–2948.

[107] C. Xie, M. Chen, P.-Y. Chen, B. Li, Crfl: Certifiably robust federated learning against backdoor attacks, in: M. Meila, T. Zhang (Eds.), Proceedings of the 38th International Conference on Machine Learning, Vol. 139 of Proceedings of Machine Learning Research, PMLR, 2021, pp. 11372–11382.

[108] J. Breier, X. Hou, D. Jap, L. Ma, S. Bhasin, Y. Liu, Practical fault attack on deep neural networks, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 2204–2206.

[109] M. Le, T. Huynh-The, T. Do-Duy, T.-H. Vu, W.-J. Hwang, Q.-V. Pham, Applications of distributed machine learning for the internet-of-things: A comprehensive survey (2023). arXiv:2310.10549.

[110] A. K. Bashir, N. Victor, S. Bhattacharya, T. Huynh-The, R. Chengoden, G. Yenduri, P. K. R. Maddikunta, Q.-V. Pham, T. R. Gadekallu, M. Liyanage, Federated learning for the healthcare metaverse: Con-

cepts, applications, challenges, and future directions, IEEE Internet of Things Journal 10 (24) (2023) 21873–21891. doi:10.1109/JIOT.2023.3304790.

[111] X. Zhou, C. Liu, J. Zhao, Resource allocation of federated learning for the metaverse with mobile augmented reality, IEEE Transactions on Wireless Communications (2023) 1–1doi:10.1109/TWC.2023.3326884.

[112] Y. Guo, Z. Qin, X. Tao, G. Y. Li, Federated multi-view synthesizing for metaverse, IEEE Journal on Selected Areas in Communications (2023) 1–1doi:10.1109/JSAC.2023.3345427.

[113] M. Letafati, S. Otoum, Global differential privacy for distributed metaverse healthcare systems, in: 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA), 2023, pp. 01–08. doi:10.1109/iMETA59369.2023.10294469.

[114] H. Moudoud, S. Cherkaoui, Multi-tasking federated learning meets blockchain to foster trust and security in the metaverse, Ad Hoc Networks 150 (2023) 103264. doi:https://doi.org/10.1016/j.adhoc.2023.103264.
URL https://www.sciencedirect.com/science/article/pii/S1570870523001841

[115] E. Antwi-Boasiako, S. Zhou, Y. Liao, Q. Liu, Y. Wang, K. Owusu-Agyemang, Privacy preservation in distributed deep learning: A survey on distributed deep learning, privacy preservation techniques used and interesting research directions, Journal of Information Security and Applications 61 (2021) 102949. doi:https://doi.org/10.1016/j.jisa.2021.102949.
URL https://www.sciencedirect.com/science/article/pii/S2214212621001630

[116] M. U. Afzal, A. A. Abdellatif, M. Zubair, M. Q. Mehmood, Y. Massoud, Privacy and security in distributed learning: A review of challenges, solutions, and open research issues, IEEE Access 11 (2023) 114562–114581. doi:10.1109/ACCESS.2023.3323932.