# Machine Learning in Metaverse Security: Current Solutions and Future Challenges

YAZAN OTOUM, University of Ottawa, Ottawa, Canada
NAVYA GOTTIMUKKALA, University of Ottawa, Ottawa, Canada
NEERAJ KUMAR, Thapar Institute of Engineering & Technology, Patiala, India and UEHS, Warsaw, Poland
AMIYA NAYAK, University of Ottawa, Ottawa, Canada

The Metaverse, positioned as the next frontier of the internet, has the ambition to forge a virtual shared realm characterized by immersion, hyper spatiotemporal dynamics, and self-sustainability. Recent technological strides in AI, Extended Reality (XR), 6G, and blockchain propel the Metaverse closer to realization, gradually transforming it from science fiction into an imminent reality. Nevertheless, the extensive deployment of the Metaverse faces substantial obstacles, primarily stemming from its potential to infringe on privacy and be susceptible to security breaches, whether inherent in its underlying technologies or arising from the evolving digital landscape. Metaverse security provisioning is poised to confront various foundational challenges owing to its distinctive attributes, encompassing immersive realism, hyper spatiotemporally, sustainability, and heterogeneity. This paper undertakes a comprehensive study of the security and privacy challenges facing the Metaverse, leveraging Machine Learning (ML) models for this purpose. In particular, our focus centers on an innovative distributed Metaverse architecture characterized by interactions across 3D worlds. Subsequently, we conduct a thorough review of the existing cutting-edge measures designed for Metaverse systems while also delving into the discourse surrounding security and privacy threats. As we contemplate the future of Metaverse systems, we outline directions for open research pursuits in this evolving landscape.

Additional Key Words and Phrases: Machine Learning in Metaverse Security: Current Solutions and Future Challenges

## 1 INTRODUCTION

The Metaverse is a shared virtual space where individuals can connect, engage, and shop. This can also be envisioned as the logical next step of growth and would ideally be accessed through a single gateway, essentially a 3D version of the internet. However, the future of entertainment, gaming, fashion, education, and even parties is already being predicted for the Metaverse. Due to its high-value projection, experts claim it is praised as a crucial element in growing the digital economy. Now, the key topic of discussion on Metaverse is whether it can provide a responsible, safe and secure immersive environment for users and businesses. While Virtual Reality (VR) and Augmented Reality (AR) are two primary forms of the Metaverse, most of the cybersecurity risks that exist are related to privacy, which involves all that relates to data integrity, data protection, and security, involving AAA (Authentication, Authorization, and Accounting) in both of the forms [1]. Due to the constant surveillance of VR, there will be much information collected from all the devices without user knowledge and end up in an abundance of endpoints with the storage of this data. Here, the data could be an avatar used by any registered

Authors' addresses: Yazan Otoum, yazan.otoum@uottawa.ca, University of Ottawa, 75 Laurier Ave. E, Ottawa, ON, Canada, K1N 6N5; Navya Gottimukkala, ngott046@uottawa.ca, University of Ottawa, 75 Laurier Ave. E, Ottawa, ON, Canada, K1N 6N5; Neeraj Kumar, neeraj.kumar@thapar.edu, nehra04@gmail.com, Thapar Institute of Engineering & Technology, Patiala, India and UEHS, Warsaw, Poland; Amiya Nayak, amiya.nayak@uottawa.ca, University of Ottawa, 75 Laurier Ave. E, Ottawa, ON, Canada, K1N 6N5.

ACM 0360-0300/2024/3-ART
https://doi.org/10.1145/3654663

individual or some biometric data that allows the same individual to access the platform, leading to the sharp rise in phishing activities, biometric hacking, and cryptocurrency thefts, which can lead to the downfall of the digital economy. Also, there will be a vague way to recognize cybercriminals in the Metaverse because it will function through avatars, as the dark web proves that anyone can manipulate the digital environment. Although the Metaverse is a truly fantastic idea that has the potential to benefit the world in many ways, it is essential to understand that if the cybersecurity issue is disregarded, it might all fail. Therefore, taking all these possible vulnerable data breaches into account, it is crucial to have some security systems that are safe, secure, and able to devoid of any flaws that could seriously harm not only the businesses' reputation and revenue but also the users. This leads our motivation to consider the possible security risks and challenges in the Metaverse and build a few detection mechanisms for the system which are prone to the type of attack. We can also detect anomalous behaviour in the user's profile through these mechanisms using ML models, which are defined as programs that use a previously unexplored dataset to detect patterns or make choices and are known as an ML model.

## 1.1 State-of-the-art

This section indicates some of the significant historical events from the 1830s to 2020s depicted in Fig: 1 that have led to our current position as we develop cutting-edge Web 3.0 technology mentioned by Bernard Marr [2], who is a world-renowned futurist, influencer, and thought leader in the fields of business and technology, with a strong desire to use technology for the greater good.

It all began in 1838 when scientist Sir Charles Wheatstone proposed the concept of "binocular vision," in which two images — one for each eye — are combined to create a single 3D image. This is the same idea that inspired the development of stereoscopes, the same idea that is used in modern VR headsets. Pygmalion's Spectacles was published in 1935 by American science fiction writer Stanley Weinbaum, in which the main character travels through a fictional world while wearing goggles that provide touch, sound, sight, and smell. The Sensoraman machine is the first VR machine created by Morton Heilig in 1956. It combines 3D video with scents, audio, and a vibrating chair to simulate the experience of riding a motorcycle in Brooklyn. MIT developed the Aspen Movie Map in the 1970s, allowing users to take a computer-generated tour. This was the first time we could transport users to another location using VR. The term" metaverse" was first used in Neil Stevenson's 1982 novel Snow Crash to describe a virtual world where characters could escape a bleak, totalitarian reality.

The 1990s to the early 2000s were the sports era when VR arcade machines were invented by Sega, and Sports Vision broadcasted the first live NFL game, which indicates the concept of superimposing graphics on real-world views. In 2011, Ernest Cline published Ready Player One, which gave us another look inside a fully immersive world into which we could escape reality. 2014 was a great year for technology, with companies like Facebook, Oculus, Sony, Samsung, and Google working on developing more games by releasing VR headsets and AR glasses that can be integrated with smartphones. HoloLens headsets were released in 2016 by Microsoft, which can create a holographic image in front of us by introducing Mixed Reality (MR) (AR & VR) for the first time to place it in the real world and manipulate it with AR. In 2017, IKEA entered the Metaverse with its innovative Place app, which allows users to choose an item of furniture and see how it will look in their home or office. Apple added a Light Detection and Ranging mechanism to iPads and iPhones in 2020, which improves the quality of photos in AR viewers and also helps for MR in the future. It is currently working on the development of headsets that could eventually replace our smartphone's interface with the future Metaverse. In 2021, Facebook changed its name to Meta to reflect its focus on shaping the future of the Metaverse. Along with it, HTC and Rayban introduced smart glasses and highly portable VR headsets that resemble sunglasses.

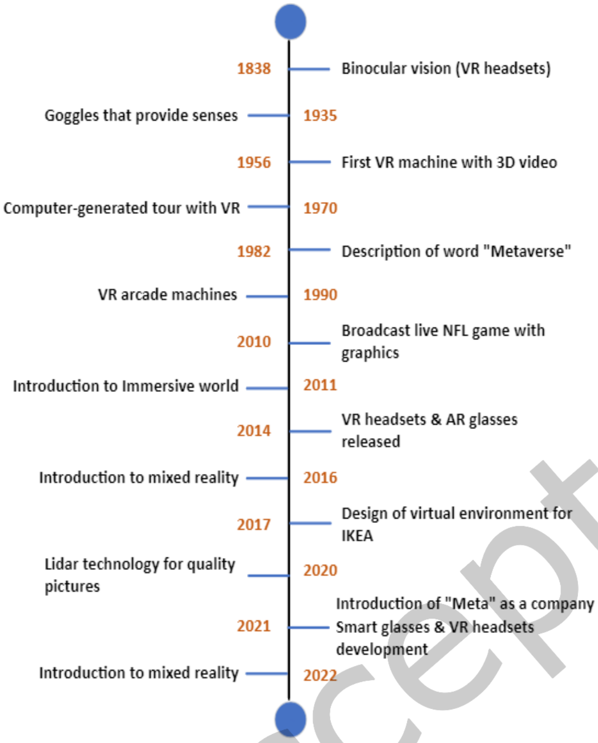
1838
Binocular vision (VR headsets)
Goggles that provide senses
1935
1956
First VR machine with 3D video
Computer-generated tour with VR
1970
1982
Description of word "Metaverse"
VR arcade machines
1990
2010
Broadcast live NFL game with graphics
Introduction to Immersive world
2011
2014
VR headsets & AR glasses released
Introduction to mixed reality
2016
2017
Design of virtual environment for IKEA
Lidar technology for quality pictures
2020
2021
Introduction of "Meta" as a company
Smart glasses & VR headsets development
Introduction to mixed reality
2022

Fig. 1. History of Metaverse

### 1.2 Scope of This Survey and Contributions

While the virtual platform promises to provide numerous possibilities for companies to transform their operations, we cannot discuss the Metaverse without mentioning or including cybersecurity issues. Many technological challenges remain to be overcome as the Metaverse is implemented, implying ever-increasing amounts of connected technology. Metaverse implementations will necessitate massive amounts of motion and environmental sensor data, similar to IoT devices. Responsive wireless devices will be connected to Metaverse control systems, which will undoubtedly be based in the cloud to track human participants. These cloud connections represent a massive potential attack surface for a bad actor to exploit vulnerabilities and gain control of the Metaverse. If a group of Metaverse actuators and sensors were compromised, the implications would be far worse, potentially fatal. However, the fundamental cybersecurity challenges that lie ahead are clear. Now, we must address them immediately for the Metaverse to thrive. Also, because the Metaverse incorporates a variety of cutting-edge technologies and systems built on them as its foundation, the Metaverse may inherit its vulnerabilities and inherent flaws. Therefore, it is also crucial to address the security challenges faced by each technology and study the potential countermeasures to each vulnerability. For all these reasons, we presented the study for a few ML models that solve our security issues of the Metaverse. The main contributions of this paper are as follows:

- Detailed exploration of Metaverse characteristics impacting security, emphasizing the role of immersion, hyper-spatiotemporality, and self-sustainability.

- Critical examination of technological advancements such as AI, XR, 6G, and blockchain and their influence on Metaverse security.
- In-depth discussion of potential hindrances to Metaverse deployment, focusing on privacy invasions and security breaches.
- Analysis of fundamental Metaverse challenges, including immersive realism and sustainability, and their security implications.
- Innovative methodologies using ML for comprehensive security and privacy analysis in the Metaverse.
- Proposal of a novel distributed architecture for enhanced security in Metaverse interactions.
- Comprehensive review and critical analysis of current state-of-the-art security countermeasures in the Metaverse.
- Identification of open research directions for future security enhancements in Metaverse systems.
- Detailed focus on cybersecurity challenges in cloud-based Metaverse control systems.

The rest of the article is organized as follows. Section 2 includes the background and technical aspects of the model architecture and relevant technologies, which include User Interactivity (UI), which is a point of interaction between human and computer in a device; XR, which is used to describe the interaction between real-world and virtual (computer-generated) worlds [3]; Computer Vision (CV) is the technology that empowers computers and systems to extract insights and data from digital images, videos, and similar visual inputs. It further enables these systems to take actions or provide recommendations based on the extracted information, AI which is termed as the ability of a computer that can mimic the tasks done by humans; Digital Twin (DT) in the Metaverse refers to a 3D representation of any real thing or setting, including its physical characteristics and behaviour, Blockchain is the most well-known for maintaining a safe and decentralized record of transactions in cryptocurrency systems like Bitcoin; Networking (5G/6G) referring to a cellular network, which operates in radio frequencies and using the latest technologies such as AI to connect with everyone all across the world; The term "Internet of Things" (IoT) denotes an interconnected system of tangible entities, often referred to as "things," which are equipped with sensors, software, and additional technologies to enable their connection to the internet and facilitate the exchange of data with other systems and devices. According to [4]; Edge/Cloud bundles the storage and computing capacity and can be interconnected by a scalable network that can adapt to changing requirements in real-time. Section 5 presents the role of ML in Metaverse security dealing with its applications, algorithms, and challenges, while Section 5 also covers several ML-based techniques that work for security challenges in Metaverse. Challenges and future research directions are entailed in Section 6 and Section 7 concludes the survey. Finally, this survey's organizational structure as a whole is depicted in Fig:3.

## 2 BACKGROUND

### 2.1 Metaverse Models Architecture

The Metaverse architecture, as illustrated in Fig.2, has been extensively discussed in various works, including [5] and [6]. In this paper, we classify it into two main categories: technology and ecosystem. These categories encompass several entities discussed, and we explore the data flow within each category. Specifically, we focus on the sub-categories 'Metaverse Engine' within the Technology category and 'Digital and Virtual World' within the Ecosystem category. This section provides an in-depth exploration of these sub-categories, with Fig. 4 illustrating the central role of Metaverse as a whole in serving as a massive application.

*2.1.1 Technology.* The technological aspect is further divided into eight main pillars, where each of the topics is discussed below.

(1) **User Interactivity:** For the Metaverse to become more immersive, there must be natural interaction. It can mimic friends' and celebrities' faces to facilitate natural interactions and give users the impression that

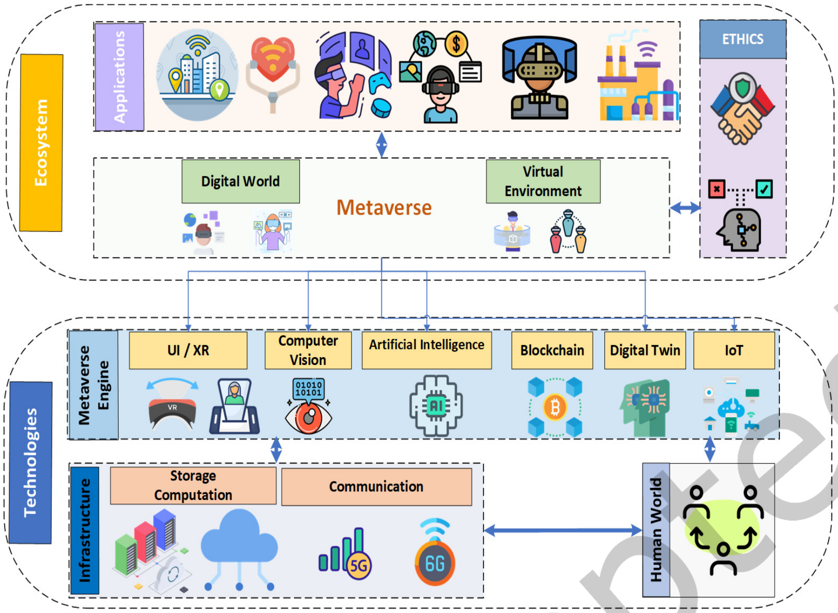

Fig. 2. Metaverse Architecture

they are in well-known and familiar locations. Hands are a key interaction component because people are the primary target audience. According to Sang-Min Park et al. [7], user interaction is divided into four main subsections: Language Interaction, which is a simple method of delivering user intent through voice recognition in the conversation; Multi-modal Interaction, described as an approach of communicating with gestures, facial expressions, tone of voice and other modalities leveraging human skills which outputs more advanced pattern detection and classification approaches to human-computer interaction; Multi-Task Interaction seen as a model that manages numerous tasks simultaneously is helpful from a complexity perspective; and Embodied Interaction termed as communication using motion and speech.

(2) **Extended Reality:**
According to Lee et al., [8], the Metaverse is a virtual setting created by the Internet, Web technologies, and XR to combine physical and virtual space. The word "Virtual" means computer-generated environment, which also references a particular realistic simulation style [9], "Augmented" is the combination of real-world elements and computer-generated elements, and "Mixed" is the same as Augmented where there is a possible interaction between real-world and computer-generated elements. At last, "Reality" is how the simulated environment makes the users feel immersed. XR can be integrated into the Metaverse to create immersive and interactive experiences. By combining VR, AR, and Mixed Reality (MR), XR allows users to transition between virtual and physical environments seamlessly. XR enhances Metaverse interactions through lifelike avatars, real-world object recognition, and spatial awareness, creating a more engaging and dynamic virtual world. This integration opens up possibilities for various applications, from entertainment and education to remote collaboration and training.
To enhance our experience, the layers mentioned above could include sensory, aural, and visual data. In order to market their goods, gather important data, and start marketing campaigns, businesses use AR tactics. Participants can use the Metaverse, a digital environment, to create their virtual worlds. The

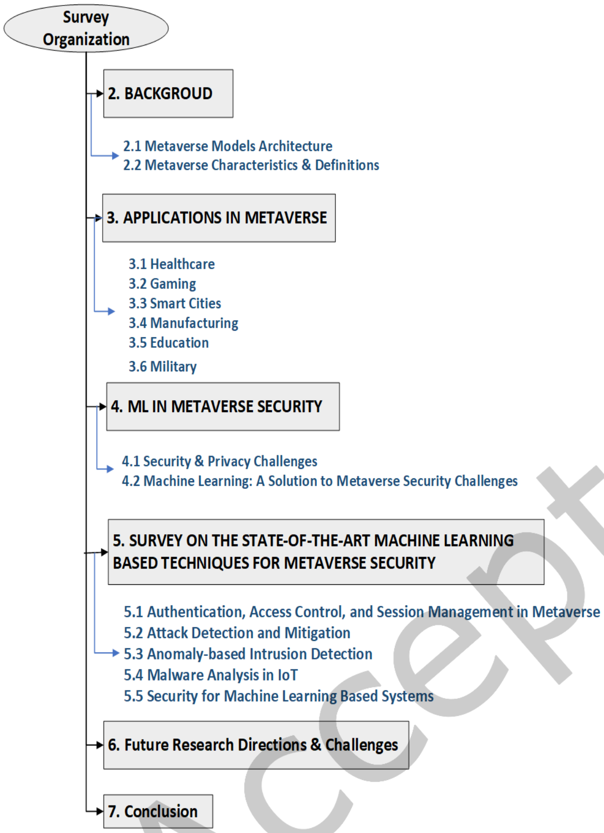
Survey Organization
2. BACKGROUD
2.1 Metaverse Models Architecture
2.2 Metaverse Characteristics & Definitions
3. APPLICATIONS IN METAVERSE
3.1 Healthcare
3.2 Gaming
3.3 Smart Cities
3.4 Manufacturing
3.5 Education
3.6 Military
4. ML IN METAVERSE SECURITY
4.1 Security & Privacy Challenges
4.2 Machine Learning: A Solution to Metaverse Security Challenges
5. SURVEY ON THE STATE-OF-THE-ART MACHINE LEARNING BASED TECHNIQUES FOR METAVERSE SECURITY
5.1 Authentication, Access Control, and Session Management in Metaverse
5.2 Attack Detection and Mitigation
5.3 Anomaly-based Intrusion Detection
5.4 Malware Analysis in IoT
5.5 Security for Machine Learning Based Systems
6. Future Research Directions & Challenges
7. Conclusion

Fig. 3. Metaverse Architecture with Focused Areas

AR approach has some persuasive power; it might make our brains believe that the elements are in our environment. Moreover, at that point, the world around us becomes much more intriguing. [10]

(3) **Computer Vision:** AI has a sub-field called CV. Both AI and CV enable machines to see, hear, and comprehend. The development of humans' ability to experience the virtual environment in the Metaverse universe depends heavily on CV.
CV can seamlessly integrate into the Metaverse to enhance user experiences and interactions. It enables realistic avatars that mimic real-world gestures, recognize physical objects for interaction, and adapt virtual environments to real-world surroundings. Moreover, CV enhances security, content moderation, and accessibility while allowing the Metaverse to bridge the gap between the digital and physical worlds. The author in the paper [11] stated that digital avatars provide a VR mimic of the experiences of real-life presence and interaction. Although XR goods can transport us to this virtual world, XR is built on the CV. To enhance the accuracy and reliability of virtual and augmented worlds, CV plays a crucial role in XR by enabling devices to recognize and interpret visual data related to users' actions and their real-world environment. While metadata transmission is an option, CV offers an alternative approach for extracting relevant information from visuals, contributing to a more seamless XR experience.

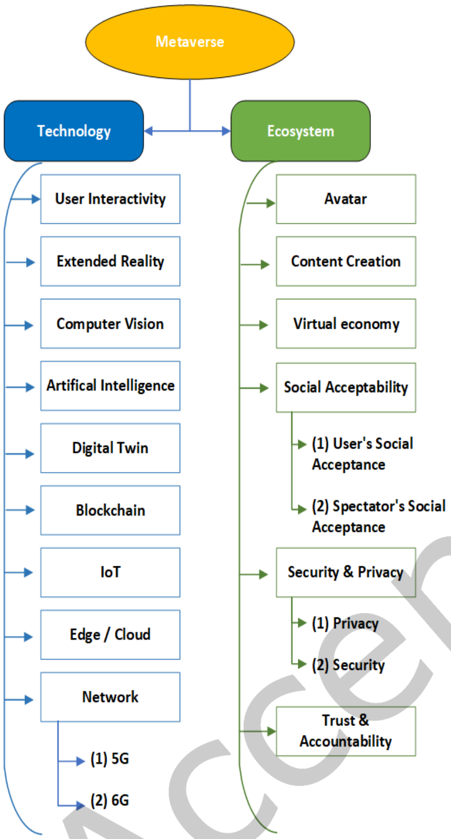

Fig. 4. Metaverse Architecture with Focused Areas

(4) **AI:** AI refers to enabling computers to make autonomous decisions, with ML being a prevalent approach. ML allows computers to learn from data without explicit programming, using trial and error to identify data patterns. DL, a more advanced ML method, employs artificial neural networks inspired by the human brain, enabling complex tasks like image recognition and natural language processing [12]. AI can be integrated into the Metaverse to enhance user experiences and security. Natural Language Processing (NLP) and CV AI enable realistic interactions and communication within the virtual world. ML algorithms can personalize content, improve user recommendations, and detect anomalies or security threats in real-time, ensuring a safer and more engaging environment. AI-powered chatbots and virtual assistants provide technical support and enhance user engagement within the Metaverse.
In accordance with the findings of Qinglin Yang et al. [13], contemporary AI research is significantly enhancing CV, decision-making, and NLP. This research primarily focuses on ML, DL, and reinforcement learning (RL), enabling computers to comprehend, manipulate, and interpret human language. Consequently, these advancements are driving individuals' enthusiasm to bring the Metaverse into reality. ML offers extensive technical support to all components within the Metaverse, with the potential to surpass human-level learning capabilities. This capacity has the power to enhance the intelligence and operational efficiency of the Metaverse significantly. Notably, advancements in AI technology, especially DL, open the door to

more advanced automated processes and content creation within the Metaverse, surpassing conventional methods, as detailed in the findings of Huynh et al.'s research [14]. Additionally, intelligent voice services are essential for Metaverse users, providing critical technical assistance in areas like voice recognition and communication.

(5) **Digital Twin:** In the Metaverse, DT plays a pivotal role within its environment. Two primary types of DTs exist: the Digital Twin Prototype (DTP) and the Digital Twin Instance (DTI). DTIs represent a specific manifestation of DTs within the Metaverse. The linkage between the digital and physical counterparts of DTs is seamlessly maintained across their complete lifecycle. Contemporary domains such as healthcare systems, Smart cars, Industry 4.0, and the IoT are significantly enhanced by the capabilities of DTs. These capabilities enable the anticipation of processes and the reduction of risks in the physical realm through informed data input.
Moreover, DTs find wide-ranging applications in the domains of science and technology, expediting manufacturing timelines, assisting in the creation of refined products, simulating the retail industry, and even forecasting weather patterns. The comprehension and application of DTs in wireless communication channels are inherently tied to specific objects, applications, and requisites. While established DTs may not necessitate the embodiment of all theoretical ideals throughout their deployment, they can be tailored to address the distinct demands of users. From an application-centric perspective that prioritizes actual requirements, established DTs hold the potential to offer multiple advantages in fulfilling the specific needs of users [15].

(6) **Blockchain:** A blockchain functions as a digital database for the storage of data. A decentralized, distributed ledger with records called 'blocks' containing immutable, encrypted data related to digital assets (cryptocurrency) stored in a chain together, establishing a time-based single source of truth for the data. A blockchain's novelty is that by guaranteeing the accuracy and security of a data record, it promotes confidence without the need for a trustworthy third party [16]. According to the author in paper [13], the blockchain and AI in the Metaverse are integrated to explore their close interactions, which are called blockchain intelligence (blockchain for AI) and intelligent blockchain (AI for blockchain). Blockchain is driving unprecedented levels of innovation and adoption in AI within the Metaverse. By facilitating decentralized market transactions, blockchain technology enables the exchange of various AI-related elements, including datasets, algorithms, and computational resources. The significance of combining AI tools with blockchain technology is to address the Internet's security problems. During the creation of a blockchain, developers face the task of fine-tuning a multitude of parameters and balancing considerations like incentive mechanisms, consensus protocols, security measures, and various other factors. One potential solution is harnessing AI technology to tackle these challenges, enhancing the overall performance of blockchain systems. Additionally, progress in ML could pave the way for automated threat identification and the activation of vital protection measures within a blockchain governed by an ML-driven algorithm. From the article [17], it is mentioned that the fusion of blockchain and ML could yield novel and trustworthy remedies. To illustrate, blockchain technology has the potential to create an unalterable ledger of transactions, while ML algorithms can be trained to recognize suspicious patterns within financial dealings. Furthermore, blockchain might function as a safe storage for data related to network activities, wherein ML algorithms assume the task of immediate protectors, precisely detecting and preventing cyber assaults.

(7) **IoT:** Authors in the paper [18] have explained that they have explored the case where the Metaverse platform uses a set of IoT devices to gather data on behalf of Virtual Service Providers (VSP). The main contributions stated in the above-mentioned paper are:

(a) The Metaverse platform employs IoT devices within a specific real-world area to enhance its hosted VSPs, promoting a more efficient and collaborative environment for producing virtual content. However, this gives rise to a resource management challenge when it comes to selecting and synchronizing virtual services due to the complexities of managing these resources effectively.
(b) The equilibrium knowledge (complete rationale) is hardly possible given the enormous number of independent IoT device owners at the edge and their self-interested character. The authors suggested a dynamic strategy based on evolutionary game theory, in which the owners of bounded-rational devices can gradually modify their tactics toward the equilibrium state.

(8) **Edge/ Cloud:** By bringing the computationally intensive work close to the end user and distributing it among edge devices, Mobile Edge Computing (MEC)[19], and Fog Computing [20] have been shown to be effective at addressing the problems that cloud-based systems face. This approach can significantly lower latency and improve system performance. In the study [21], authors presented a hybrid Fog-Edge computing architecture for Metaverse applications, which uses edge devices to fulfill the necessary computational power for demanding tasks like collision detection in virtual worlds and computation of 3D physics.

(9) **Network:** To achieve a seamless and immersive experience within the Metaverse, the role of computer networks is pivotal. These networks serve as the foundation for global sensing and communication, which are essential for providing users with a unified and interconnected environment. In this context, the utilization of DT combined with ML, data analytics, and multi-physics simulation plays a critical role. These technologies enable a deep understanding of network dynamics, enhancing network efficiency and adaptability to support the intricate demands of the Metaverse better.
Moreover, computer networks facilitate the integration of accurate DT models with real-world data. This involves capturing the intricate details of the physical world, from geometric configurations to environmental attributes and behaviours. By deploying intelligent sensing technologies, such as strategically placed sensors and wireless signal utilization [22–24], computer networks continuously gather real-time data from the physical environment. This data is then transmitted from the physical plane to the virtual plane, bridging the gap between reality and the virtual realm.
In this dynamic interaction between the physical and virtual planes, computer networks serve as the conduit for synchronized data exchange—the virtual plane benefits from the accurate replication of the real world facilitated by DTs. The precise representation of real-world characteristics within the virtual environment enables seamless interaction, dynamic evolution, and immersive experiences. Ultimately, the role of computer networks is integral to creating a coherent and interconnected Metaverse where users can engage, explore, and interact seamlessly.

(10) **5G:** 5G has outperformed 4G, offering faster speeds and lower latency, marking a significant advancement in wireless technology [25]. Also, it outperforms 4G by employing microwave and mm-Wave technology to increase speed to 900 Mbps or higher. Faster speeds and capacity are comparable to those offered by commercial broadband providers, allowing for more applications other than streaming media. In the study conducted by IEEE [26], it is mentioned that 5G will have an impact on automation in several domains, such as remote learning and education, entertainment, sports, live event streaming, personal and professional day-to-day communications, etc. in 2023, according to 97% of survey respondents which is an important thing to consider for the Metaverse.
In [25], the author also emphasizes the rapid emergence of diverse Internet of Everything applications, including MR, telemedicine, haptics, flying vehicles, brain-computer interfaces, and connected autonomous systems. These applications demand a network capable of providing high reliability, low latency, and high data rates simultaneously. The paper advocates the necessity of 6G as a new wireless technology to address

these challenges and propel technological advancements effectively. This acknowledgment sets the stage for the necessity of 6G wireless technology to address these pressing challenges and pave the way for the next frontier in connectivity.

(11) **6G:** Within the next decade, 6G (6th-generation) cellular technology is expected to be an exponentially more powerful successor to 5G cellular technology. It will operate at much higher frequencies than 5G networks and is expected to provide significantly higher capacity and extremely low latency [27]. One of the primary goals of the 6G internet is to support a microsecond latency, a breakthrough that significantly enhances real-time communication and interaction. This ultra-low latency is instrumental in enabling seamless connectivity between the internet and everyday life, ensuring a smooth and instant user experience across various applications and services.
As per the research presented in the paper by Tang et al. [28], the conventional approach of deploying fixed-ground communication infrastructure for on-demand applications within the Metaverse lacks flexibility. Instead, they propose the SAGSIN multi-dimensional networks, which involve deep integration across various domains such as space (e.g., satellites), air (e.g., balloons, drones, Unmanned Aerial Vehicles (UAVs), etc.), ground (cellular/Wi-Fi/wired) networks, and sea layers. This integration aims to establish seamless global connectivity to achieve extreme levels of intelligent sensing and communication in the Metaverse, particularly in the context of 6G technology.
Muhammad Zawish et al., in the paper [29], mentioned that 6G networks are expected to be faster, more capable, and have lower latency. In 5G, they expect the telecommunications industry to employ dynamic, distributed marketing techniques with local bandwidth licensing/sharing and development. Also, 5G serves as a foundational technology that enables integration with various web-based applications, resulting in a notable enhancement of the performance of existing applications. On the other hand, 6G takes a significant leap forward by seamlessly integrating with web-based systems, facilitating swift and intricate interactions among users, devices, vehicles, and the environment [30]. This elevated level of integration positions 6G as a technology surpassing the capabilities of 5G, offering a more comprehensive and seamless experience for users across multiple domains. As a result, we can forecast when we will transition from the IoT to the Internet of Everything, which 6G could feasibly provide. Some of the applications of 6G in the Metaverse are that it has AI-assisted intelligent connectivity, makes holographic connectivity simpler for the use of AR/VR to provide continuous coverage anywhere, and a ubiquitous link that encompasses air, land, space, and sea [31].

#### 2.1.2 *Ecosystem.* The ecosystem is further divided into six main pillars, and each topic is discussed below.

(1) **Avatar:** For usage in digital settings, an avatar is a visual depiction of a person. Typically, a bitmoji or other computer-generated picture is used. The term "avatar" on social media also refers to your profile picture, the image that serves as your online persona. The majority of unique users select a photo as their social media avatar, occasionally with the addition of a digital frame or filter. The greatest avatar option for brands is typically the business logo [32]. The Metaverse avatar is the virtual representation of a user in this digital environment. It offers users the flexibility to choose from various visual representations, ranging from lifelike depictions to more abstract forms. The diversity in avatar design stems from how different businesses and platforms implement them. Some opt for minimalist avatars, while others prioritize photorealistic or expressive options. These avatars can take various forms, including 2D, 3D, VR, Leg-less VR, and Full Body avatars [33].

(2) **Content Creation:** Because of advancements in VR and AR, the Metaverse is expected to aid creators in producing more interactive and immersive content intelligently. This can be done with the help of AI. For this, creators will collaborate using AI-assisted tools to turn a high-level vision into content ready

for consumption if the Metaverse reaches its full potential. This might entail AI-powered animation, AI-powered video editing, or even AI-powered music composition. Since content creators will be required to provide more immersive and interactive material than ever, the stakes will be higher [34]. In the paper [35], the author has also mentioned that one of the major obstacles is the efficient generation and creation of 3D immersive content and the efficient transmission of multimedia content. For this, one of the solutions given by [36] for procedural content generation is by introducing Neural Radiance Fields (NeRFs). Based on a predetermined set of input photos, NeRFs enable novel-view synthesis. Numerous variations available enable quick training, compression for low-latency viewing, and lack of dependence on camera specifications.

(3) **Virtual Economy:** The economy in the Metaverse, which is stated as a virtual economy, depends on the identification of digital assets such as personal belongings and property, allowing for a diverse range of virtual possessions. It also needs the freedom to move around and conduct business between realms that might have various laws and regulations to prosper. Non-Fungible Tokens (NFTs) [37] records of digital ownership stored in the blockchain will serve as the foundation of the Metaverse economy by enabling the authentication of things, property, and even identity. Each NFT is fortified by an advanced cryptographic key, setting a high standard of security that extends far beyond the fundamental aspects of NFT trading. This formidable security measure ensures that altering, copying, or destroying the NFT becomes an immensely challenging task. This level of security plays a pivotal role in enabling a decentralized federation, allowing for the robust verification of one's digital assets and virtual identity. It forms a backbone for Metaverse communities, facilitating secure and reliable communication and interactions between them.

(4) **Social Acceptability:** Calkin S. Montero et al. [38] termed the user's social acceptance and the spectator's social acceptance, making up an overall measure of social acceptance.
(a) User's social acceptance: A user will have an impression of each activity they complete: did they feel at ease or uneasy, awkward or natural, calm or embarrassed? This will result in a generally favourable or negative opinion of the activity or technology.
(b) Spectator's social acceptance: User activities occur in various public and private contexts or scenarios. The spectator's perceptions of these activities serve as an indicator of their societal acceptance. Is the user's action clear to the audience? Do they consider the behaviour "strange" or "normal"? A spectator's opinion of the user's behaviour can be formed rapidly, either favourably or unfavourably.

(5) **Security & Privacy:** An increase in the quantity and quality of threats related to the existing technology will be used to actualize the Metaverse [39], [40]. These dangers are particularly relevant to users' security and privacy in the Metaverse, which we cover in the following section.
**Privacy:** The Metaverse will increasingly attract a growing number of users, content creators, business proprietors, and entrepreneurs. In simpler terms, it will function as a unified meta-platform for users, regardless of their specific interests or preferred applications (such as reading, gaming, learning, etc.), and for the companies responsible for developing and sustaining these applications. Three topics are critical in terms of privacy for all of these users in the Metaverse: (i) personal information, which is any data or details that can identify an individual in the Metaverse, such as their real name, location, biometrics, etc.; (ii) conduct of users within the Metaverse, including issues like harassment, discrimination, and inappropriate behaviour, designed to ensure a safe and respectful virtual environment, and (iii) communications Involves the exchange of messages, voice, or video within the Metaverse, emphasizing privacy in terms of secure and confidential conversations, protecting users from eavesdropping or unsolicited contact [41]. Each of these sectors will provide the platforms with significantly more data than they presently have, with new and heightened dangers resulting from our earlier concerns. Notably, private and delicate information gathered

from social networking sites is already being used for "doxing," which is the act of disclosing confidential information [42]. Information that leaks through the Metaverse will include a wealth of real-world data about user habits and their physiological characteristics.

**Security:** Beyond the overarching privacy concerns discussed earlier, the Metaverse's seamless integration of multiple cutting-edge technologies presents specific security challenges that demand proactive solutions. With the prevalence of synthetic content and the proliferation of automated and unreliable user profiles, including both bots and human-operated personas engaging in disruptive behaviour, the Metaverse will encounter an escalating frequency of human-machine interactions. To address these emerging security risks effectively, it is imperative that multidisciplinary efforts from research communities specializing in AI, ML, cybersecurity, ethics, and related fields collaboratively tackle these pressing issues. Our collective efforts are vital in identifying, analyzing, and devising concrete countermeasures to safeguard the integrity and safety of the Metaverse environment.

(6) **Trust & Acceptability:** Establishing trust in the Metaverse is a multifaceted challenge that goes beyond the simple application of blockchain technology. As Jiliang Tang [43] noted in the context of social media, trust serves as a critical factor in determining whom we can rely on for sharing and accepting information without additional verification. Tiffany Wang [44] also highlights the erosion of trust due to safety, privacy, and inclusion concerns prevalent today. However, in the Metaverse, the question of how to define trust becomes particularly nuanced. While blockchain technology [45] can play a pivotal role in fostering trust, it is essential to recognize that blockchains primarily ensure data integrity rather than the authenticity of social identities. To truly establish trust in social interactions within the Metaverse, additional infrastructure and mechanisms are needed to verify the authenticity of key holders and their associated social identities. Blockchains offer undeniable benefits, such as providing evidence of originality, ownership, and legitimacy, making them a foundational component of trust. For instance, in the context of rare VR artwork transactions, blockchain technology can confirm the authenticity of digital assets. However, it is crucial to understand that trust in the Metaverse extends beyond blockchain's scope and necessitates a comprehensive approach incorporating identity verification, reputation systems, and social protocols. In pursuing social acceptability within the Metaverse, trust in the sincerity of counterparties remains paramount, impacting various facets of life, including business dealings and personal relationships. Therefore, a holistic understanding of trust, encompassing both the capabilities of blockchain and additional layers of identity authentication, is essential to ensure a secure and trustworthy Metaverse environment [46].

## 2.2 Metaverse Characteristics & Definitions

The definitions, traits, and difficulties of the Metaverse have been discussed in Table 1 for each study. We have meticulously reviewed the most recent papers to gather comprehensive insights and challenges authors encountered while implementing their ideas in practice. Our selection of these papers was deliberate, considering they discussed the latest advancements in the field of the Metaverse. By doing so, we aim to anticipate future challenges and identify the scope within the Metaverse domain while concurrently deepening our understanding of its definitions and traits.

# 3 APPLICATIONS IN METAVERSE:

The existing works are presented in this section from the perspectives of four major industries: manufacturing, smart cities, healthcare, and gaming in Fig:5. These industries are likely viewed as providing specialized services in the Metaverse [58], [59], [60].

Table 1. Comparison of previous works

| AUTHOR | DEFINITION | CHARACTERISTICS | CHALLENGES |
|---|---|---|---|
| Huansheng Ning et al. [47] | A new type of Internet application and social form that integrates a variety of new technologies. | Multi-technology, sociality, and hyper spatiotemporality. | Interaction problem, communication, ethical, privacy issues, cyber-syndrome, standards, and compatibility. |
| Thien Huynh-The et al. [48] | A new term, formed by merging "meta" and "universe," has been introduced to describe a collectively experienced virtual world powered by a range of emerging technologies, including fifth-generation networks and beyond, VR, and AI. | Virtual environment, continuity, expandability, constant availability with synchronization, budgetary allocation, decentralization, safety, and compatibility. | The substantial costs associated with frequent system reconfigurations and upgrades, particularly in the case of ML systems that require significant time and computational resources for tasks like new data collection, preprocessing, and model learning. |
| Yuntao Wang et al. [49] | The emerging paradigm of the next-generation Internet seeks to create a completely immersive, highly dynamic, and self-sustaining virtual communal realm where people can engage in leisure, professional activities, and social interactions. | Immersive realism, hyper spatiotemporality, sustainability, heterogeneity | Scalability, and interpretability fast service authorization, compliance auditing, and accountability enforcement in seamless service mitigation and multi-source data fusion. |
| Qinglin Yang et al. [13] | Seamlessly integrate the real-world with the virtual world and allow avatars to carry out rich activities, including creation, display, entertainment, social networking, and trading. | Key Characteristics: Identity, friends, immersive experience, low friction, civility, economy, anywhere, variety. Other characteristics: open space, decentralization, human-computer interaction experience, digital assets, and digital economy | High burden for resource-constrained mobile devices to deploy learning-based applications. Poor robustness and poor interpretability. |
| Lik-Hang Lee et al. [8] | The term has been coined to further facilitate digital transformation in every aspect of our physical lives. At the core of the Metaverse stands the vision of an immersive Internet as a gigantic, unified, persistent, and shared realm. | Distinct distribution and heterogeneity. | AI models are usually very deep and require massive computation capabilities, which is unfriendly for resource-constrained mobile devices. |
| Mark Wright et al. [50] | It is an extensive 3D networked virtual world capable of supporting a large number of people simultaneously for social interaction | Social interaction and collaboration, which implies the interaction of real people with the virtual environments and agents, including avatars with increasing levels of immersion and presence. | A key implementation issue is that we have created all of these interactions without altering the second life client. Using the standard client was seen as more of an interesting software challenge rather than a justified design decision, as it limits choices and adds to the complexity. |
| Eliane Schlemmer [51] | It is a lifelike private and public utility because it is an extension of the physical world's real space within a virtual Internet space. It is also known as the technological incarnation of the old daydream of creating a parallel world, a collective memory, imagery, myths, and symbols pursuing man since ancestral times. | Experience immersion through telepresence by interacting and creating several 3D spaces for living and living together, thus allowing parallel worlds to emerge. | Demands new methodologies, teaching practices, and mediating processes that are in tune with the potential 3D-Digital Virtual World offers. |
| C. Jaynes et.al [52] | Objective is to provide users with an open, untethered, immersive environment that fools their visual senses into believing that the traditional barriers of time and space have been removed. | Self-organizing and monitoring, visually immersive, collaborative capabilities. | The cost of purchasing, installing, and maintaining immersive systems must be reduced to the point where they become affordable (e.g., as a replacement for the user's office computing environment). |
| Cory Ondrejka [53] | An online environment that was a real place to its users, one where they interacted using the real-world as a metaphor and socialized, conducted business, and were entertained. | It has the potential to open dramatically larger markets by giving its users the vibrant complexity and dynamics of real-world cities. | Limits on flexibility and variety. |
| Dawn Owens et al. [54] | It is an immersive three-dimensional virtual world where people interact with each other and their environment, using the metaphor of the real-world but without its physical limitations. | Explores an immersive three-dimensional virtual world that enables interaction among users and the environment, employing real-world metaphors without physical constraints. | Inability to verify the cultural identity of the participants. |
| Haihan Duan et al. [55] | A combination of "meta" (meaning beyond) and the stem "verse" from "universe," denoting the next-generation Internet in which the users, as avatars, can interact with each other and software applications in a 3D virtual space. | Realism, ubiquity, interoperability, and scalability. | Restricted to physical limitations (such as geography, language, etc.), the real-world cannot integrate various elements in one place to satisfy the requirements of different people. |
| Amina Almarzouq et al. [56] | It is a digital universe accessible through a virtual environment, which is through the merging of virtually improved physical and digital reality | Interactivity characteristics: ensures real-time, interoperable, and synchronous learning personal and technology-based characteristics: influenced respondents' perception of Metaverse. | Need for new leadership and management models. Need to examine how educational contexts' behaviors differ from the real settings. |
| Chen, Shu-Ching et al.[35] | It aims to build an immersive virtual world that allows the users to interact with the digital environment and other users in real-time. | Procedural content-creation in multimedia. | Hurdles toward the creation of a full-fledged Metaverse, including efficient creation and generation of 3D immersive content and efficient multimedia content transmission. |
| R. Di Pietro et al. [57] | It is a combination of persistent, multi-user, shared, 3D virtual spaces that are intertwined with the physical world and merged together to create a unified and perpetual virtual universe. | The concept of singularity, which can be described as a point in time at which technological growth becomes uncontrollable and irreversible, resulting in unforeseeable changes to human civilization. | Preventing fair outcomes, lack of transparency, and vulnerability to attacks and manipulations are some of the open scientific challenges that need to be conquered and resolved by several collaborative efforts from various scientific groups (such as AI and ML, security, ethics, and more). |

### 3.1 Healthcare:

In order to improve patient experience and increase the accessibility of medical care, the healthcare sector is investigating how to integrate the characteristics of the Metaverse into the specialties and practices of medical professionals [61]. This area includes various elements, including encrypted communication and work areas, AR, and VR. These days, AI approaches are used in various specialized medical fields, including cardiology and neurology. It has given specialty services access to cutting-edge algorithms that can evaluate vast amounts of data. Large-scale data production and high-calibre intelligence can be produced using AI. The work [62] lacks concrete implementation examples and real-world case studies to validate the proposed architecture's effectiveness in healthcare. However, its innovative integration of the Metaverse, AI, and blockchain enhances healthcare experiences, emphasizing data security. In order to ensure that the new research can be applied in real healthcare settings, further research needs to be conducted on practical implementations and comprehensive ethical assessments.

### 3.2 Gaming:

As ML, DL is reinventing and transforming the Metaverse, gaming has always been a key application. These domains are redefining the video game market on several platforms, including console to computer and mobile platforms [63].

### 3.3 Smart cities:

Smart Cities gather useful data via the Internet of Things, video cameras, social media, also from other sources. Based on data gathered from users, city governments must make decisions regarding which services to add, drop, and improve. With the aid of more cutting-edge technologies, digital tools, and smart cities will offer people over the Internet more intelligent interactive services in the Metaverse platform, as stated by Shahab S.Band et al. [64]. In another work, [65], the authors explore the intersection of Brain-Computer Interfaces (BCIs) and XR, highlighting their potential to address diverse applications in smart cities, from rehabilitation to robotics. However, the work lacks specific case studies or concrete examples to illustrate the practical implementation and real-world impact of the discussed BCI and XR technologies in smart cities. Ethical, privacy, and security aspects should be comprehensively addressed to ensure responsible and secure integration of these technologies in urban environments, ensuring their broader acceptance and impact.

### 3.4 Manufacturing:

Using digital connections between machines and systems, manufacturing has undergone a digital transformation as part of the present industrial revolution in order to comprehend better and analyze physical objects. In contrast to digital transformation, which improves the physical world through digital operations, the Metaverse builds a virtual environment that is transposed onto the actual world based on real interaction and persistence. The Metaverse for manufacturing may considerably update digital operations in the current digital revolution by jointly using cutting-edge technologies like AI and DT. Some of the applications for manufacturing in the line of Metaverse are companies that produce items on demand, monitor machine conditions, detect and diagnose product faults, increase the scalability and compatibility in manufacturing and create virtual entities for operating transparency. Innovative information and communication technologies, particularly AI ones, are the foundation of smart manufacturing. AI systems are becoming increasingly crucial due to the increased amount of information processing in today's society [66], [67]. The work [68] contributes by addressing the need for the application of the Metaverse in manufacturing, proposing a blockchain-based governance system and establishing a value-oriented Metaverse trusted manufacturing framework, providing a theoretical foundation for practical implementation.

The paper mentions the proposal of a blockchain-based trusted collaborative governance system but lacks detailed implementation examples or validation of this system in real-world manufacturing scenarios. Future research could enhance the paper by including practical case studies and real-world examples to demonstrate the tangible benefits and effectiveness of Metaverse applications in traditional manufacturing.

## 3.5 Education:

Education in Metaverse or Learning in Edu-Metaverse are recently in trend, and its impact on education is being investigated by scholars all over the world [69], and thus more intelligence, digitalization, and virtualization will shape education in the future. Regarding education, the Edu-Metaverse will undoubtedly promote massive changes in the education system, such as hosting ceremonies online and building automation that studies students' behaviour in real-life versus virtual world scenarios. Therefore, as mentioned in [70], the future of education consists of three main characteristics, which are teaching models, teaching evaluation, and teaching environment involving technologies such as AI, blockchain, interaction, IoT, Learning Analytics, which help in increasing student academic performance and engagement in activities. All these perspectives can empower future education with value-driven development. According to [71], VR can be used in classroom interaction. Metaverse is a virtual networking experience where students can interact in a lifelike digital realm via an internet connection and the teaching environment to engage college students. The authors in [72] contribute by highlighting the potential of ML and Metaverse technologies in transforming preschool education, particularly in creating personalized and interactive learning experiences, and it emphasizes the importance of cybersecurity within the Metaverse and suggests the implementation of encryption, multi-factor authentication, and access controls to protect user data and privacy. However, the paper can benefit from discussing the potential challenges and limitations of implementing robust cybersecurity measures within the Metaverse, including technical and practical hurdles, to ensure a secure learning environment for children.

## 3.6 Military:

The buzzword Metaverse is now into defence services as well. Adhering to the fact that the fundamental technologies of Metaverse, like AR, VR, and AI-powered virtual environments with 3D simulations covering air, land, sea, and space, are recently being used in the defence industry, the Metaverse concept for the military is not new. The military has a lot to gain by shaking hands with the Metaverse. Some of the reasons which are mentioned in [73] are Attracting and Retaining Talent, Military VR Training, Live AR Tools for Maintenance, and the Right Decision at the Right Time. These benefits for the military Metaverse may aid in keeping soldiers out of potentially lethal situations. However, these integrations also have a few limitations, such as simulating a crowded metropolitan environment is challenging as it is time-consuming and expensive. It is also difficult to create a perfectly correlated landscape because each simulation utilizes a different format for its terrain data [74].

# 4 ML IN METAVERSE SECURITY

This section examines the most advanced AI-based methodologies in six technical areas, including natural language processing, machine vision, blockchain, networking, DTs, and neural interface, which have the ability to create the Metaverse [75]. Connecting the virtual and physical worlds in the Metaverse has the potential to make the user experience better, and ongoing experiments are being conducted to measure these improvements. AI encompasses a computer's or robot's ability, controlled by a computer, to perform tasks that traditionally require human intelligence. These tasks are typically carried out by humans. The Metaverse delves into various AI-related fields such as content analysis, supervised speech processing, CV, and more. ML, DL, and RL are employed in the Metaverse to empower its systems, ensuring they possess the technical capabilities to match or surpass human intelligence levels. It is important to note that ML is a subset of AI, and AI encompasses a broader spectrum of capabilities and technologies [13].

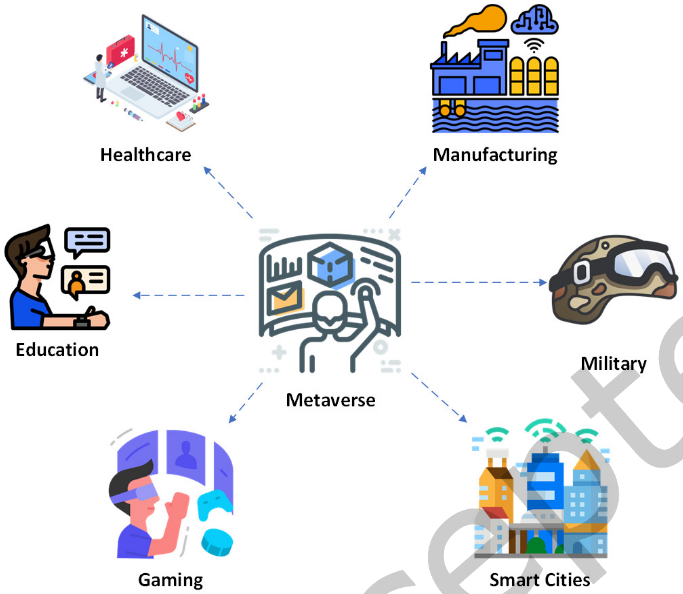

Fig. 5. Applications of Metaverse

For law enforcement authorities, criminal conduct in virtual worlds is more problematic. It is becoming more and more desirable for forensic investigators to be able to precisely and automatically follow individuals in online forums. Roman V. Yampolskiy et al. [76] described algorithms capable of recognizing and verifying avatar faces with high accuracy. The proposed framework of a standard face recognition system consists of face detection & image normalization, face representation, and matching. They have used packages in OpenCV for detection and geometric normalization involving rotations, scaling, and translations for image normalization. This normalized face image is further divided and extracted as feature vectors to find salient descriptions. After some pre-processing, such as image smoothing and colour variation, face matching is performed with a Chi-square similarity test by setting some threshold values.

According to Aitor Rovira et al., [77], a subfield of ML known as RL involves an active entity known as an agent interacting with its surroundings and learning how to respond in order to accomplish a predetermined objective. To direct a person to a specified area in a virtual environment using immersive VR. The computer graphics sector faces a difficult challenge when it comes to controlling character animation. One of the challenges is finding a way to balance animation's realism and accuracy. Iason Kastanis et al. [78] gave an example of how RL can be used to help human participants in immersive virtual environments accomplish certain goals by interacting with an avatar that is under the direction of an RL agent. Therefore, RL is used here not to make the avatar's behaviour more realistic but to teach the avatar how to cause a specific behaviour in the participant. The eyes are the primary human sensors for gathering information about the outside world. Imaging systems, such as video cameras, are required to capture the visual characteristics of the real environment. Acquiring higher image quality in the Metaverse poses challenges due to the need for real-time rendering, vast data transmission, and limited bandwidth resources. Balancing immersive experiences with image fidelity remains a technical hurdle in this dynamic virtual environment. Thus, AR/VR glasses should integrate high-speed imaging and record the depth or spectral information of the scene, among other things. To solve this problem, DL algorithms effectively decode the coded measurement. This has a number of benefits, such as an increased signal-to-noise ratio, fewer artifacts, faster calculation times, lower computation costs, and increased adaptability and flexibility of the imaging system.

Snapshot Compressive Imaging (SCI), which proposes a sequence of Convolutional Neural Networks (CNN) to rebuild several connected images or videos from a single coded image, is one approach to solving this problem. The use of new network models such as recurrent neural networks, untrained neural networks, memory-efficient networks, and meta-learning allows DL-based reconstruction to be improved in terms of speed, calculation costs, and richer functionality.

All operations will be autonomously driven by DL-based software, with chatbots and other NLP systems controlling interactions. Regardless of the user's language, AI will be expected to comprehend words, photos, videos, and texts and reply appropriately. All of this necessitates an enormous quantity of training data and modelling [79]. Coming to gaming, AI-driven non-player characters have a significant impact on the issue of the underpopulated Metaverse. Becoming one of the first few users in a new universe may feel thrilling initially, but it will quickly get boring if there are no other users to interact with or fascinating activities being done [80]. A metatarsal 'ghost town,' referring to a previously inactive or underutilized virtual space, can undergo a vibrant transformation when a community of AI characters engages in activities such as creating, interacting, making music, producing art, conducting commerce, and more.

Till now, we have discussed how AI will help in the recognition and verification of Avatar faces, their behaviour, and in other domains. An intuitive interface is one that operates exactly as the user expects, where every click holds paramount importance in conveying actions and functions seamlessly. It ensures users can effortlessly navigate and interact based on their familiar understanding of the system, enhancing overall usability and user satisfaction. Contemporary human-computer interactions are enhanced by the integration of AI. For example, when you don an advanced VR headset equipped with AI features, its sensors will empower you to analyze and predict mechanical and electrical patterns, enabling you to trace your movements throughout the Metaverse. In order to recreate a true touch sensation in VR programs, AI is used. Additionally, it helps with voice-activated navigation to communicate with digital characters and virtual items [81]. To solve these problems, [82] discussed Human-machine interaction, which has evolved to include Hybrid Human-Artificial Intelligence (H-AI), which combines human intellect and AI to create a new, enhanced intelligence. H-AI offers a significant edge over more conventional AI approaches in social computing (produced by social and interactive human behaviours utilizing computing technology) when it comes to solving social-oriented problems.

The provision of languages for every user is the primary definition of multilingual accessibility. It incorporates several linguistic elements. This capability is used by digital humans for communication and language. The ability to turn the language into any language is known as multiple language accessibility. It is only accessible to those with good training in AI and its uses. As a solution to the multilingual accessibility, a variety of ML methodologies proposed in [83] are utilized, especially Bernoulli Naive Bayes, Linear Support Vector Classifier (SVC), Chi-squared SVC, and Multinomial Naive Bayes algorithms are used, and packages of NLP are used for the data pre-processing.

### 4.1 Security & Privacy Challenges

The surface area for cyberattacks has considerably increased in the Metaverse [84], [85]. IoT devices, wearables, and sensors are commonplace in the Metaverse ecosystem, and many hardware vendors process a great deal of private user behaviour in real-time. Producers and stakeholders in the Metaverse will need to be able to verify that users are who they say they are. For user authentication, numerous other researchers are already looking into biometrics, such as fingerprints, facial recognition, and retinal imaging. Biometric data can now be added to the massive amount of financial and personal information acquired while we work, socialize, and shop in the Metaverse. These concerns were divided into four categories, which are mentioned below and discussed by Ruoyu Zhao in [86] which are overlapping with B. Falchuk's ideas [41], where privacy was categorized into three different types: privacy of personal info, privacy of behaviour, and privacy of communications which are discussed below in separate sections.

- **User information:** can be treated as any information regarding one's economic, cultural, social, or biological standing and physical, medical, or physiologic details. Without a doubt, sensors are vital since they help users enhance the experience, which results in immersion in the Metaverse by themselves. On the other hand, many users might not recognize or even be aware that the physical and biometric data are viewed as too sensitive. If they are disclosed, they could put people's lives in grave danger as malicious third parties will be more interested in this information and might have a chance to attack through any network. Therefore, ensuring that the information obtained is secured or protected is important. Effective communication plays a pivotal role within the Metaverse, enabling seamless social interactions and information sharing. Protecting sensitive communication within this digital realm is essential.
- **Communication:**
  Communication is a crucial aspect of the Metaverse, facilitating social interactions and information sharing. Protecting sensitive communication within this digital realm is essential. Encryption and decryption techniques play a key role in verifying the legitimacy of recipients and ensuring data security. Only authorized parties with the correct decryption key can access transmitted information, enhancing privacy and trust in the Metaverse.
- **Scenario:** These are the details regarding routines, pursuits, scenarios, decisions, etc. [41]. In the Metaverse, the avatar can be described as a digital representation of a person which is customizable and often used in online or virtual environments. There also exists malicious avatars that can annoy, spam, do unwanted following, and virtually stalk other people. In order to create a user-friendly Metaverse, a setting window should be made available to users. This window should allow users to prevent certain scenarios from occurring around their avatars, such as conflicts that occasionally arise in the real world due to different cultures and viewpoints, such as those involving religious, political, gender, and sexual minorities.
- **Goods:** For various reasons, the owner of goods would naturally want to prevent any misuse or unlawful copying of their property. To address this concern, it is essential to implement measures for safeguarding these assets. One effective approach to tackle this issue is the use of invisible watermarking. This method is designed to embed a unique identifier into products as they are created or ownership changes hands without affecting their visual appearance in the Metaverse. When necessary, this watermark can be either removed or identified. Additionally, the realization of multiple capabilities, such as content protection, authentication, and resistance against tampering, as discussed in Begum's work [87], acts as a deterrent against malicious avatars attempting theft or illegal copying of goods. The blockchain, with its attributes of decentralization, tamper resistance, and anonymity, provides an ideal solution for addressing ownership, traceability, and product transfer concerns, as highlighted in Dai's research [88]. Decentralization ensures that every avatar can actively participate in blockchain activities, allowing them to independently record their ownership of each item, which forms the foundation of protection. Moreover, the tamper resistance of the blockchain is enforced by the requirement of controlling more than 51% of the system's computational power to make any alterations.

Other than these, there are other security threats mentioned below related to cybercrime, which are addressed in [89]. On the internet, phishing emails and messaging schemes are already sufficiently effective, as cybercriminals adeptly utilize social engineering techniques to obtain passwords, personal data, and financial assets illicitly.

That might be even simpler in the Metaverse, particularly if individuals mistakenly believe they are speaking to the actual person they know and trust when they are actually communicating with someone else totally. This can be possible when a scammer makes an avatar that resembles you and uses it to help carry out assaults on your friends or coworkers; alternatively, just like with any online account, they might simply breach through into an actual one. It could be quite difficult to recognize whether someone can take control of someone else's account when you are transacting business with them in the virtual world. Another possible threat that's crucial to keep in mind is that software plays a big role in it as well; individuals will need to acquire software in order to access virtual spaces, use business tools, play games, and more. The software we download for our computers or cellphones can be dangerous, just like everything else we download for non-trustable websites, especially if it originates from unofficial sources or is cracked software.

### 4.2 Machine Learning: A Solution to Metaverse Security Challenges

Improving and Analysing a security posture is no longer a problem on a human scale. Also, from [90], it is mentioned that because the underlying technologies are rapidly evolving, cybersecurity is highly dynamic, and the offence and defence are locked in a threat-response-threat co-evolution. This dynamic and ever-changing environment necessitates constant vigilance and updates to threat classification, identification, and response. In order to solve this, ML has become a critical information security technology because it can analyze millions of events quickly and identify a wide range of threats, from exploiting zero-day vulnerabilities in malware to identifying risky behaviour that could lead to phishing attacks or malicious code downloads [91]. One significant advantage of ML in cybersecurity is its ability to automate repetitive and time-consuming tasks such as intelligence triage, malware analysis, network log analysis, and vulnerability assessments [92]. By incorporating this into the existing workflow of the Metaverse security layer, it will be feasible to respond to and remediate threats at a rate that would be impossible with only manual human capability. Therefore, ML algorithms for the majority of the possible security threats in Metaverse are explored later in Section 5.

## 5 SURVEY ON THE STATE-OF-THE-ART MACHINE LEARNING BASED TECHNIQUES FOR METAVERSE SECURITY

### 5.1 Authentication, Access Control, and Session Management in Metaverse

These are the three significant risks that come under security and privacy threats. This section will discuss the measures and their feasibility in developing a secure and privacy-preserving Metaverse paradigm. According to [49], identity authentication and access control are crucial for large numbers of users and avatars in the Metaverse service offerings. Also, the main threats or attacks in the Metaverse related to Authentication are identity theft, where the user's personal information is stolen, hacking personal assets like VR glasses, and attempts to cyber-fraud. In avatar authentication issues, it is easier for hackers to create voice personas through several bots and imitate the user's voice, behaviour, and appearance of other users in the Metaverse. In order to achieve secure avatar authentication, more personal information might be needed as proof, along with suitable fraud-detecting mechanisms using ML, which could lead to new privacy breach risks. Related to the threats to access control in the Metaverse, there will be a high chance of misuse of avatars, where the attackers can disclose the avatar intentionally to target the advertising organization's data. This can lead to one more issue called unauthorized data access, where it gets complicated for users to decide on what information should be shared.

In the paper [47], Ning et al. explained the session management issues in heterogeneous networks, which are seen in two categories. First comes single-session management, where page views, events, social interactions, and online purchases are just a few examples of the various activities that can be included in a single session. These activities are all saved in the session, while the single instance is designed to communicate with just one user. The main issues include time management and resource joining/quitting management. Second is the multi-session, which enables simultaneous interaction between multiple users and an application. The same application procedure could be accessible to numerous individuals at once. Collision, deadlock, and mutual exclusion are considered typical issues. All the issues in single- and multi-session management are handled through priority comparison, bankers' algorithms, and other protocols.

The issues outlined above for authentication and access control, traffic, and behaviour monitoring systems are summarized in the paper [93] using AI-based approaches. All the threats to authentication in the Metaverse, such as one-time multi-authentications, are addressed using Random Forest (RF), which uses techniques such as word matching in the password authentication system and Support Vector Regression (SVR) for security authentication using a kernel function. Some techniques also involved transfer learning, RL, and CNN in creating a system for physical authentication. While dealing with biometric authentication, the fingerprint feature is solved using the proposed Artificial Neural Network (ANN) algorithm, Extreme Learning Machine (ELM), and end-to-end recognition model using CNN, ANN, and a few other combinations. Session Management issues, as discussed above, such as the deadlock problem, can be solved using numerous algorithms and strategies, but one of the most effective solutions is proposed by Rabie Ahmed, Taoufik Saidani, and Malek Rababa to the use of meta-heuristics. Numerous optimization-related problems, including the deadlock problem, have been successfully resolved by genetic algorithms.

In the paper [94], a more effective and economic adaptation of the evolutionary algorithm's parallel framework to the problem of deadlock is presented. The experiment done by the authors in the paper demonstrates that the suggested approach can yield the most viable solutions in each advanced generation regarding burst time. Additionally, the suggested method ensures excellent performance for all crossovers. Security strategies that emphasize identity management and user behaviour analysis will benefit end users because identity and behaviour are two essential elements of the Metaverse. Also, we can adapt the collision solution from [95], which presents the discussion on avoiding the chain collision by proposing a new technique called "reinforcement learning based on a decision-making strategy". Here, we can consider a chain collision avoidance taxonomy for session management as shown in Fig:6.

### 5.2 Attack Detection and Mitigation

The attack is an effort to access a device, system, or organization without authorization and with the intent of stealing information or carrying out other destructive behaviour [96]. Attacks generally fall into several categories, which are discussed below:

- **Network attacks:** This Is an effort to access a company's network without authorization with the intent of stealing information or carrying out other destructive behaviour.
- **Endpoint attacks:** Getting unauthorized access to consumer devices, servers, or other endpoints, usually by infecting them with malware to compromise them.
- **Malware attacks:** Introducing malware into IT resources enables attackers to take control of systems, steal data, and cause harm. Attacks using ransomware are also among them.
- **Advanced persistent threats:** These are sophisticated, multi-layered threats encompassing network and other assault types.
- **Vulnerabilities, exploits, and attacks:** Using software flaws in the organization's software to compromise, sabotage, or obtain illegal access to systems.

For the purpose of detecting and mitigating attacks, various ML techniques have been developed. The Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Firefly Algorithm (FF), Whale Optimization Algorithm (WOA), Rider Optimization Algorithm (ROA), and others are a few of them [97]. Since the aforementioned techniques have significant drawbacks, several hybrid and improved algorithms have been presented for attack detection and mitigation. These algorithms improve overall performance by combining the actual ML algorithms.

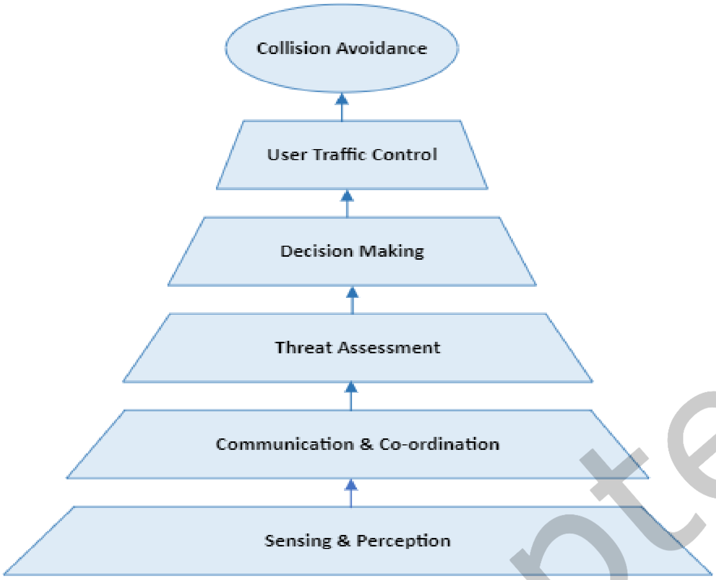

Fig. 6. Taxonomy of chain collision avoidance in Session Management

The proposed Attack Detection System (ADS) in this work is divided into two stages: Deep Belief Network (DBN) and Median Fitness oriented Sea Lion Optimization algorithm (MFSLoN). The initial categorization step for the data set is DBN. Further classification is carried out using MFSLoN because there is a significant volume of data and to preserve it appropriately. Following attack identification, the bait strategy is employed to mitigate the attacks. Attacks are neutralized using the bait strategy if an attack is detected; otherwise, the packet is forwarded through conventional routing. Thus, the cooperative bait strategy got its name.

Bharot et al. [98] proposed a DDoS attack detection and mitigation model using the J-48 algorithm, the Intensive Care Request Processing Unit, and the feature selection approach (ICRPU). In this work, the Hellinger distance function is initially used to analyze traffic. The unique feature of ICRPU is that the attacker won't ever be aware that the request they issued to deplete the resources is a trap, preventing the attacker from acting reflexively. It becomes simple to find the assailant.

To identify and combat DDoS TCP flood attacks in public clouds, Sahi et al. in 2017 [99] proposed a brand-new classifier system. The classifier system for DDoS recognizes packets and assesses whether they are standard or come from an attacker during the detection phase. The source IP will be banned, and malicious packets will not be allowed to reach the cloud service during the preventive phase. A K-fold cross-validation model is used to validate the results in the end, and when the Least Square Support Vector Machine (LS-SVM) classifier is used, the classifier system DDoS performs at its best.

Fatima Khashab et al. [100] suggested an ML model able to automatically detect and prevent assaults in Software-Defined Networks (SDN). The suggested model extends the native features, in contrast to existing methods that are found in other studies that employ the native flow features exclusively for attack detection. The extended flow features are the average flow packet size, the number of flows to the same host as the current flow in the previous five seconds, and the number of flows to the same host and port over that time frame. Six ML methods, including Logistic Regression (LR), Naive Bayes (NB), K-Nearest Neighbor (KNN), Support Vector

Machine (SVM), Decision Tree (DT), and Random Forest (RF) were examined, and studies revealed that RF is the most effective ML algorithm. Additionally, results demonstrated that the proposed algorithm could reliably and quickly identify assaults with a low likelihood of disrupting regular traffic. Most of the approaches using the aforementioned ML algorithms follow the below architecture Fig:7 for attack detection and mitigation.

In [101], the authors proposed a platypus framework that can be used for solving multi-objective optimization problems. It is a type of issue with competing goals that never has a single ideal solution but rather a collection of them, and that necessitates the simultaneous optimization of numerous goal functions [102]. The creation and improvement of signature-based rules is the main goal of the proposed detection and mitigation scheme. To solve this optimization problem, network traffic is observed, and the required packet-level data are processed to create signatures, which are distinct sets of packet field values. These are fed into ML models to determine whether they are malicious/benign. Finally, the proposed method is tested using production environment traces and attack traffic that is generated at high rates to assess detection accuracy and packet filtering performance. Results demonstrate that, in high-speed traffic conditions, the suggested solution outperforms the synchronize (SYN) cookies mechanism, achieves high detection accuracy, and greatly decreases the number of filtering rules.

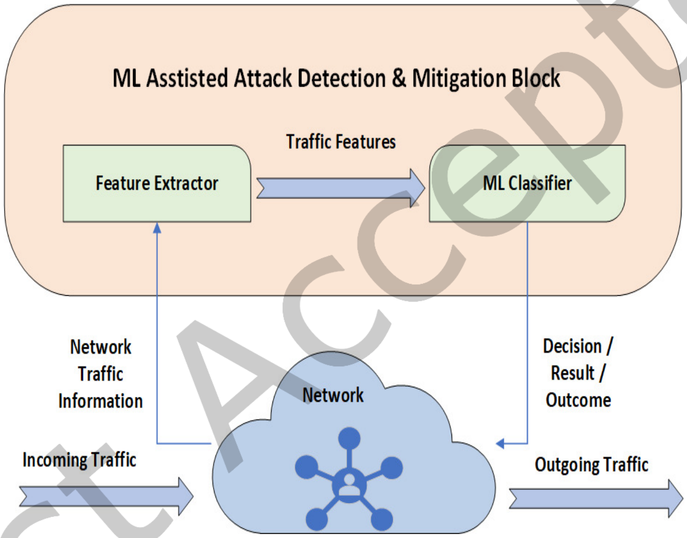
ML Asstisted Attack Detection & Mitigation Block
Traffic Features
Feature Extractor
ML Classifier
Network Traffic Information
Decision / Result / Outcome
Network
Incoming Traffic
Outgoing Traffic

Fig. 7. High-Level Architecture for Attack Detection and Mitigation

## 5.3 Anomaly-based Intrusion Detection

Any tool or program that actively scans your network for malicious activity and notifies you when it finds an attack qualifies as an Intrusion Detection System (IDS). Different IDS types and configurations exist, but they all record data, alert security administrators to unusual activity and generate reports. Some IDSs can also detect attempted attacks and take action to stop them [103]. To get a clear context and difference between intrusion and attack, all successful attacks are intrusions. Now, an anomaly IDS is based on statistical analysis. It detects attacks based on irregularities in the pattern w.r.t the normal pattern. For this, it creates the model of the normal behaviour of the IDS and looks for activities that differ from the created model. The main advantage of having the anomaly IDS is that it can detect unknown threats. Therefore, the term "attack" refers to both successful and unsuccessful incursions [104].

The work in [105] explores the security challenges posed by the Metaverse and its wireless systems, particularly focusing on detecting malware and wormhole attacks. The Metaverse's potential for new technologies has led to concerns about its security. The paper highlights the need for enhanced security between physical and virtual sensing models in Metaverse-based wireless systems. It emphasizes the threat of wormhole attacks, which can compromise network protocols and collect significant amounts of data, especially with the rise of IoT applications. While existing countermeasures assume static networks, the paper investigates the security impact of mobile cloud and Metaverse environments, proposing the use of statistical methods like the sequential probability ratio test (SPRT) for wormhole detection and exploring innovative defence mechanisms against such attacks. While the paper addresses the challenge of loose node employment, it could benefit from further investigation and refinement of Bernoulli random variable conditions and parameters to enhance performance.

Adhering to the fact that techniques for unsupervised anomaly traffic detection are getting better over time, Fekadu Yihunie et al. in [106] did research that aims to find a powerful classifier that detects anomaly traffic from the NSL-KDD dataset with a high level of accuracy and a low error rate has been developed experimenting with five ML algorithms. The outcome is produced by testing and validating five binary classifiers: LR, SVM, Stochastic Gradient Decent (SGD), Sequential Model (SM), and RF. The results show that the RF classifier performs better than the other four classifiers, both with and without normalizing the dataset.

Because supervised network intrusion detection systems have a high probability of false positives when there are changes to the network environment, services, or patterns of regular traffic, unsupervised outlier detection can overcome the limitations of supervised anomaly detection. Therefore, authors in [107] applied one of the effective data mining systems referred to as RF algorithms. The proposed framework collects network activity and builds a dataset using pre-processing. Following that, the RF algorithm is used to build the service-based patterns over the dataset to identify outliers associated with each created pattern. When outliers are found, the system will then provide alerts. Processing takes place offline after network traffic has been captured. Online processing is inappropriate in a real network setting because of the high CPU needs for outlier detection algorithm execution.

The study performed in [108] examines attempted network intrusions using anomaly-based ML models to offer superior protection over the established misuse-based approaches. On the UNSW-NB15 benchmark data set acquired from a real-world institutional production setting, two models — an ensemble learning model and a CNN model — were developed and put into use, demonstrating the models' validity and dependability. To keep the study's scope modest, the attack type was restricted to probing attacks. High accuracy rates were found, with the CNN model being more accurate.

In [109], Tushar Rakshe and Vishal Gonjari created a classifier model for network intrusion detection based on SVM and RF- based methods. They evaluated the effectiveness of their system using the NSL-KDD dataset, a vastly enhanced version of the real-time KDDCUP'99 dataset. The detection algorithm's primary objective was to determine using 41 attributes that describe every pattern of network traffic whether the incoming network traffic was legitimate or an attack. The results of two algorithms were examined, and it was found that RF's classification algorithm outperformed SVM's primary classification method. This demonstrates that the anomaly intrusion detection system can successfully use ML techniques.

Instead of using conventional shallow ML techniques, the authors in [110] tried improving the performance of anomaly detection necessitates the use of seven commonly used DL techniques, such as DNN, Deep Migration Learning (DML), Deep Belief Network (DBN), Recurrent Neural Network (RNN), CNN, Graph Neural Network (GNN), Long Short-Term Memory (LSTM), and Auto-encoders (AE). With a focus on resource-constrained devices utilized in real-world IoT situations, the study gives an overview of anomaly intrusion detection using DL algorithms. In terms of high detection accuracy and low false alarm rates, the results from the evaluated research demonstrated that DL is superior to other methods for detecting anomalies.

N. Satheesh et al. [111] implemented a Flow-based anomaly intrusion detection using an ML model with software-defined networking for the OpenFlow network and believe that the ML model continuously monitors the system's network activity for the transmission of both normal and abnormal traffic data in order to find anomaly intrusions. They propose that a flow-based ML model combined with SDN function as an intelligent system to limit throughput virtually through the flow of reserved bandwidth and utilize extra bandwidth, which presents more than the utilization bandwidth for priority-based applications at minimal cost when compared to the conventional methods. The suggested ML technique is known as flow-based because the entire process is described and implemented in a 4-layer structure, where the top layer removes an incoherent and unrelated feature and the bottom layer supplies chosen functions for the top layer. Later, it uses certain effective and symmetrical ML techniques to categorize the condensed dataset. Then, using the 10-fold cross-validation (CV) procedure, this model is trained and tested once more. Additionally, it employs a number of accurate metrics to assess how well the technique works.

On the DARPA KDDCUP'99 dataset, the paper [112] implements a DL strategy for anomaly detection utilizing a Restricted Boltzmann Machine (RBM) and a deep belief network. Unsupervised feature reduction is accomplished by their method using a single hidden layer RBM. A deep belief network is created with the weights that come from this RBM being sent to another RBM. The pre-trained weights are fed into a layer for fine-tuning that consists of a multi-class soft-max LR classifier. On the entire 10% test dataset, they were able to achieve a detection rate of 97.9%. They were also able to achieve a low false negative rate of 2.47% by optimizing the simulation's training procedure.

## 5.4 Malware Analysis in IoT

Malware is software created to prevent a computer from operating normally. A file or piece of code known as malware is capable of nearly any task that an attacker may require using a network that is frequently used to spread it [113]. In contrast to conventional software, malware frequently has the ability to proliferate throughout a network, go unnoticed, alter or damage an infected system or network, and persist. They have the ability to impair machine performance and destroy the network seriously. There are different types of malware, such as viruses, Trojan horses, worms, spyware, Botnets, ransomware, and rootkits. Experts claim that malware attacks can target IoT systems because these devices are constantly online and lack security.

In [114] research, the authors offer an ML-based method for identifying IoT device ransomware. In terms of accuracy rate, recall rate, and precision rate, the suggested method, which is the combination of Mutual Information (feature selection) and K-NN (ML algorithm), performs better than Neural Networks, SVM, and RF, which is also easy to update, train, fast and achieved a detection rate of 93.76% and a precision rate of 89.85%.

Rajesh Kumar et al. proposed a novel framework in their paper [115], which is presented for improving malware detection for Android IoT devices. It combines the benefits of ML techniques and blockchain technology. Clustering, classification, and blockchain are used in the sequential implementation of the suggested technique. Using clustering and classification techniques, ML automatically collects information about malware and stores it on the blockchain. By communicating through the network, authentic information of extracted features in distributed malware database blocks are stored in the blockchain's history is able to boost the run-time detection of malware with more speed and accuracy and to declare malware information for all users further.

Authors in [116] showed their interest in improving the security of IoT devices in the year 2020 and proposed a model to detect the malware based on its behaviour in terms of system call sequences that occurred during its execution. These system calls of IoT malware are gathered using the Strace tool in the Ubuntu operating system. 'n-gram' techniques are used to pre-process the generated malicious system calls in order to retrieve required features. Using a recurrent neural network, the extracted system calls were classified into two classes: normal and malicious. The effectiveness of this DL approach is evaluated using a variety of performance metrics where the real-time IoT malware samples were obtained from the IOTPOT honeypot, which emulates various CPU architectures of IoT devices.

The study conducted in [117] employs ML models and provides an efficient method for identifying IoT malware through forensic analysis of their network traffic features by selecting the most distinctive features and combining them with the binary features of the malware families. A large dataset with many network traffic collections used various network traffic features. To achieve the study's goal, three phases were followed in an extremely conceptual manner: pre-processing, processing, and post-processing. As a result of the feature extraction process for each malware type, the proposed model's detection accuracy was nearly 100% during the experimental phase of the Quantitative research study. Also mentioned in the paper is that this model can be improved further by considering the fog-level implementation of the IoT layer, where learning will aid in identifying a malicious packet transfer to the network at level zero.

Throughout the study, Mohammad Masum et al. [118] have presented a feature selection-based framework for ransomware detection and prevention that uses various ML algorithms, including neural network-based architectures. On a subset of ransomware features, they used a variety of ML algorithms, including DT, RF, NB, LR, and Neural Network (NN)-based classifiers. To evaluate the proposed framework, they ran all of the experiments on a single ransomware dataset from the GitHub repository [119]. The experimental results show that RF classifiers outperform other methods in terms of accuracy, F-beta, and precision scores.

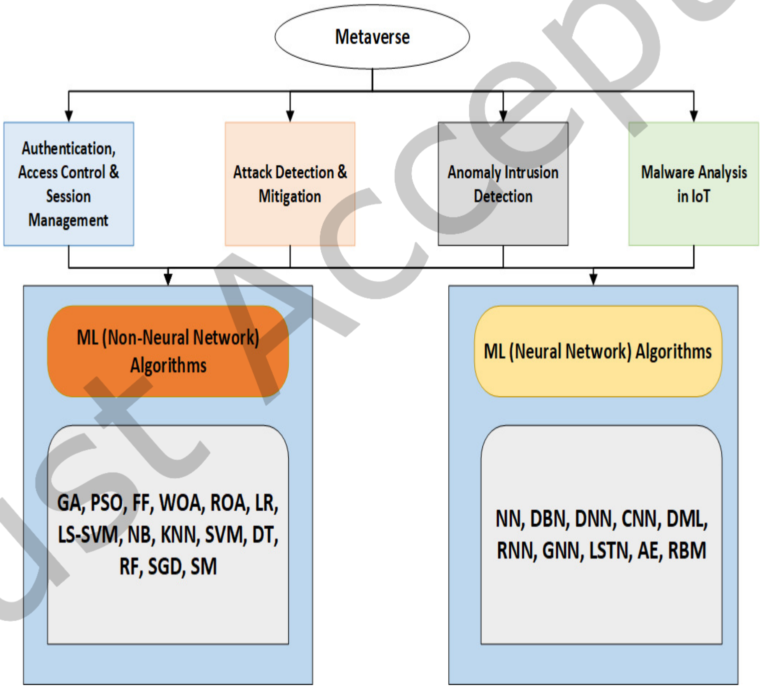
Metaverse
Authentication, Access Control & Session Management
Attack Detection & Mitigation
Anomaly Intrusion Detection
Malware Analysis in IoT
ML (Non-Neural Network) Algorithms
GA, PSO, FF, WOA, ROA, LR, LS-SVM, NB, KNN, SVM, DT, RF, SGD, SM
ML (Neural Network) Algorithms
NN, DBN, DNN, CNN, DML, RNN, GNN, LSTN, AE, RBM

Fig. 8. Consolidated List of ML Algorithms for all the Security Problems

At last, all the ML algorithms used in each subsection of security challenges are consolidated and shown in Fig:8, where all the ML algorithms were classified into Non-NN and NN algorithms. However, as the number and variety of ML applications have grown, so has the number of malicious actors.

## 5.5 Security for Machine Learning Based Systems

In ML-based systems, security challenges have become more complex and diverse. This indicates that the world is still in the early stages of ML security research and development. To ensure the security of ML-based applications/systems, one needs to be sure of their services/users, such as below, which are mentioned in [120].

- **Manufactures**: Malicious hardware inclusion during hardware implementation if the manufacturers are untrustworthy.
- **Internet Protocol (IP) providers**: IP provider that can also be untrustworthy because it can contaminate training datasets and manipulate baseline ML models/architectures or other hyper-parameters that third-party cloud providers do not have access to.
- **Users**: An attacker can compromise the security of the ML-based system even after deployment and during inference by tampering with the inference data or the corresponding hardware and can use side-channel attacks to obtain the IP address.
- **3rd party cloud platforms**: If the cloud platform provider is untrustworthy, it has the ability to manipulate the training dataset as well as the baseline neural networks or ML algorithms. Even if the cloud platform provider is trusted, another client can perform a man-in-the-middle attack to steal the IP or even tamper with the IP or the training process.

Ignoring these issues may lead to experimental bias or incorrect conclusions, particularly in computer security. For example, if any of the aforementioned factors is untrustworthy, it can be regarded as a potential threat model. Some of the most prevalent security vulnerabilities in ML and their countermeasures are shown in Fig:9 are explained below [120]:

- **Data Encryption:** In the following approach, the training dataset set is encrypted before training [121–123]. This countermeasure, however, includes additional hardware for encrypting the inference dataset.
- **Local Training based Transfer-Learning:** To reduce weight/model manipulations, the dataset is divided into two parts: one for outsourced training and one for locally training the model, which can be used to overwrite the model via transfer-learning [124],[125].
- **Redundant Outbound Training:** To reduce the possibility of trained model/data manipulation, training is outsourced to multiple third-party cloud platforms. During testing, triple/multi-modular redundancy is used to detect intrusions [126].
- **Hardware Implementation:** Because hardware intrusions in ML-based systems are similar to traditional hardware attacks, traditional hardware security techniques, such as traditional obfuscation techniques, run-time anomaly detection using side-channel, formal method-based analysis [127–129], and communication analysis techniques are used counter stealing hardware IP's.
- **Inference:** To mitigate IP stealing, run-time anomaly detection, traditional obfuscation techniques, side channel (SC) analysis, and security measures for remote cyber-attacks [130] can be used. The selection & development of appropriate inference security measures is a time-consuming and complex process. For example, encryption is one of the possible countermeasures to avoid data poisoning attacks, but its applicability is limited due to limited energy resources.

## 5.6 Generative AI (GAI) for Metaverse Security

In the evolving landscape of the Metaverse, the role of generative AI (GAI) in enhancing security is becoming increasingly pivotal. GAI technologies, such as advanced machine learning algorithms, offer novel approaches to detecting and mitigating security threats in these complex virtual environments. GAI can provide dynamic, real-time solutions to safeguard users and digital assets by analyzing vast amounts of data and learning from evolving security incidents. Moreover, GAI's ability to simulate potential security breaches and generate predictive

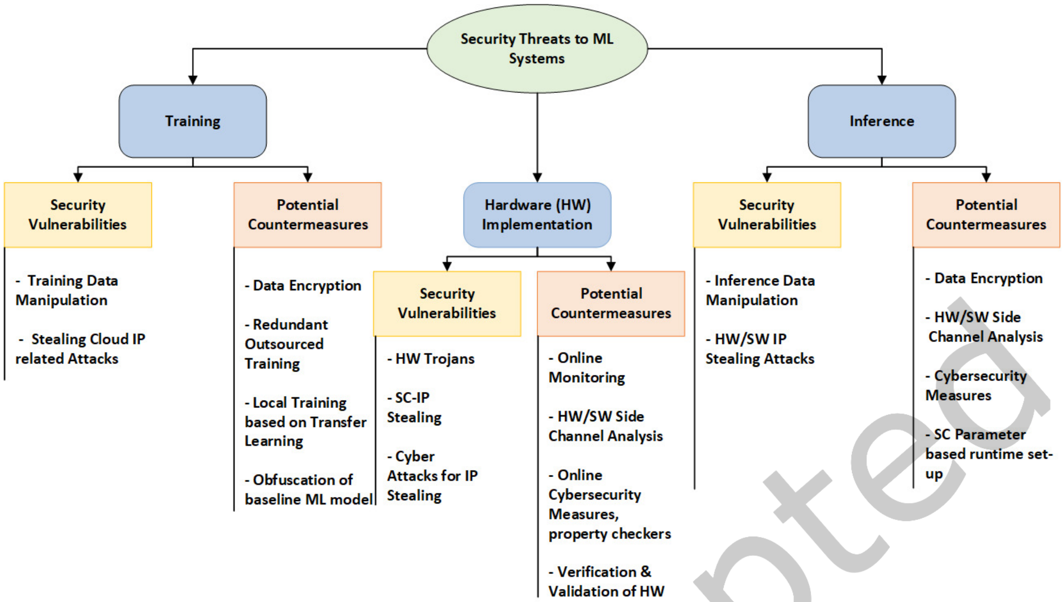
Security Threats to ML Systems
Training
Inference
Hardware (HW) Implementation
Security Vulnerabilities
- Training Data Manipulation
- Stealing Cloud IP related Attacks
Potential Countermeasures
- Data Encryption
- Redundant Outsourced Training
- Local Training based on Transfer Learning
- Obfuscation of baseline ML modell
Security Vulnerabilities
- HW Trojans
- SC-IP Stealing
- Cyber Attacks for IP Stealing
Potential Countermeasures
- Online Monitoring
- HW/SW Side Channel Analysis
- Online Cybersecurity Measures, property checkers
- Verification & Validation of HW
Security Vulnerabilities
- Inference Data Manipulation
- HW/SW IP Stealing Attacks
Potential Countermeasures
- Data Encryption
- HW/SW Side Channel Analysis
- Cybersecurity Measures
- SC Parameter based runtime set-up

Fig. 9. Potential Security Vulnerabilities and Their Countermeasures in ML-based Systems

models is crucial for proactively strengthening Metaverse security frameworks. This integration of GAI into Metaverse security represents a significant step towards ensuring safe, reliable virtual experiences.

The survey paper [131] extensively covers the evolving landscape of AI in content generation, with a particular emphasis on its application in the Metaverse. It explores how AI models, especially large-scale ones like GPT-3, are revolutionizing content creation, offering insights into their potential, limitations, and ethical considerations. This paper is particularly relevant for understanding the integration of AI in the Metaverse, highlighting how AI can facilitate the creation of more dynamic, interactive, and personalized virtual environments. This dovetails with the need for constant innovation in the Metaverse, where AI's role rapidly expands in virtual reality interactions, digital asset creation, and user experience enhancement. The survey also sheds light on the challenges and future directions of AIGC, underscoring its significance in shaping the Metaverse's evolution.

The paper [132] explores how generative AI, exemplified by technologies like ChatGPT, can revolutionize content creation in the Metaverse. It focuses on the applications and potential of these technologies in enhancing user experiences within virtual environments. The survey details how generative AI can assist in creating complex virtual structures, engaging user avatars, and facilitating multilingual interactions in the Metaverse. This is particularly relevant to Metaverse security as the integration of generative AI introduces new dimensions in ensuring the integrity, authenticity, and safety of user-generated content. The paper underscores the potential of generative AI to reshape Metaverse dynamics, stressing the need for robust security measures in these rapidly evolving digital landscapes. Authors in [133] provide a comprehensive overview of the AIGC operating principles, security and privacy issues, cutting-edge solutions, and future challenges.

## 6 FUTURE RESEARCH DIRECTIONS & CHALLENGES

The Metaverse presents a multifaceted environment where numerous complex tasks unfold simultaneously, often requiring multi-mode and multi-task approaches. For newcomers to Metaverse development, there exists a significant learning curve, as practical details for complex and realistic implementations are still relatively scarce. To address this challenge, the importance of a collaborative system that seamlessly integrates with a platform and an active developer community cannot be overstated. Such a system is indispensable for those new to Metaverse development, as it eliminates the need to design the entire system from scratch, promoting knowledge sharing and facilitating secure Metaverse development [7]. Here are some key directions for enhancing security in the Metaverse using ML:

- Develop ML models that continuously analyze and authenticate user behaviours within the Metaverse, focusing on specific activities such as financial transactions or access to sensitive data. These models can detect anomalies or suspicious activities in real-time and trigger authentication challenges or alerts when necessary, providing an extra layer of security.
- Given the rising threat of deepfake technology, ML algorithms can be trained to recognize deepfake avatars and content. These algorithms can help authenticate the identity of avatars and prevent impersonation and misinformation.
- Explore techniques for AI and ML models that can operate while preserving user privacy. This includes differential privacy, federated learning [134], generative AI, homomorphic encryption, and other privacy-preserving technologies to ensure data security and privacy within the Metaverse.
- Implement ML-driven access control mechanisms that adapt to user behaviour and context. These systems can automatically adjust access permissions based on the user's actions and risk profile.
- Implement blockchain technology to establish and verify user identities within the Metaverse securely. Blockchain can provide a decentralized and tamper-resistant system for identity management.
- Employ predictive ML models to anticipate potential security threats and take proactive measures to prevent them. This can include predictive analytics for identifying likely attack vectors.
- Explore the application of zero-trust security principles in the Metaverse, employing ML for continuous user and device authentication, dynamic access controls, and real-time risk assessment. This approach establishes a security framework that never assumes trust and continuously verifies trustworthiness within the Metaverse environment.

However, having explored numerous ML and AI algorithms for addressing security concerns, it is essential to acknowledge the specific challenges that arise when implementing them in the context of the Metaverse. These challenges must be carefully weighed and considered when choosing the appropriate algorithms to ensure seamless integration of ML and AI within the Metaverse without causing any disruptions.

- Designing AI models that are lightweight yet efficient to accommodate mobile devices with limited resources.
- Adapting AI models for different problem domains within the Metaverse, which may require retraining with appropriate data.
- Addressing the challenge of RL convergence, as many RL algorithms have a slow convergence rate, making it a complex problem.
- Shifting from making hardware intelligent with AI algorithms to building intelligent hardware with AI algorithms for end-to-end solutions.
- Managing the enormous amount of data generated in the Metaverse, ensuring data quality, and addressing storage, interoperability, and privacy issues.
- Enhancing security with avatar two-factor authentication, protecting transmitted data, and preventing various threats and cyber-attacks.
- Dealing with the high computing power demands of the Metaverse, including supercomputers and edge computing solutions.

## 7 CONCLUSION

As a future paradigm of the internet, the Metaverse aims to create a virtual shared space that is immersive, hyper-spatiotemporal, and self-sustaining. The Metaverse is transitioning from science fiction to an imminent reality, thanks to recent technological advancements such as AI, XR, and blockchain. However, the widespread adoption of the Metaverse can be hindered by severe privacy invasions and security breaches, which may stem from underlying technologies or emerge within the new digital ecosystem. Due to the intrinsic characteristics of the Metaverse, such as immersive realism, hyper spatiotemporality, sustainability, and heterogeneity, several fundamental challenges, including scalability and interoperability, can arise in Metaverse security provisioning. This paper aims to comprehensively overview the security and privacy challenges of the Metaverse using ML models. In particular, we examine a new distributed Metaverse architecture with interactions between 3D worlds. Subsequently, we review the current state-of-the-art countermeasures for Metaverse systems and discuss security and privacy threats. For the future of Metaverse systems, we outline open research directions. Following are some points that summarize our findings:

- Complexity of the Metaverse: Securing the Metaverse is highly complex due to its immersive, interconnected, and multi-dimensional nature. ML models need to adapt to this complexity by considering various data sources, communication channels, and interaction modes.
- Privacy Challenges: Protecting user privacy is paramount in the Metaverse. ML models must be designed to ensure that personal data remains secure and confidential while allowing meaningful interactions and experiences.
- Behavioral Analysis: ML models that can continuously monitor user behaviours are crucial for detecting anomalies and potential security threats. Behavioural analysis plays a vital role in identifying suspicious activities within the Metaverse.
- Zero-Trust Architecture: Implementing a zero-trust security model is essential in the Metaverse, where trust cannot be assumed. ML can contribute by continuously verifying user identities and devices, ensuring access is granted on a need-to-know basis.
- Authentication Mechanisms: Research into alternative authentication mechanisms beyond text-based passwords is needed to streamline authentications in the Metaverse. Methods like body gestures, iris authentication, and biometric recognition can enhance security and user experience.
- On-Device Intelligence: As the Metaverse shifts towards on-device intelligence, ML models need to adapt to provide real-time security without heavy reliance on centralized cloud technologies. This is essential for ensuring consistent user experiences even in remote areas with poor connectivity.
- Phishing and Deep Fakes: ML models should be equipped to detect and mitigate phishing scams and deep fake attacks that can impersonate trusted organizations or avatars within the Metaverse.
- Collaborative Security: Developing a collaborative security ecosystem that involves the Metaverse platform, developers, and the community is essential. It allows for collective efforts in identifying and addressing security vulnerabilities.
- Ethical Considerations: ML in the Metaverse must consider ethical aspects such as data privacy, consent, and the potential for bias in algorithms. Ensuring ethical AI practices is crucial to building trust in the Metaverse.
- Continuous Adaptation: Security in the Metaverse is an ongoing process. ML models and security measures must continually adapt to emerging threats and changing user behaviours within this dynamic digital environment.

## REFERENCES

[1] Yan Huang, Yi Joy Li, and Zhipeng Cai. 2023. Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics* 6, 2 (2023), 234–247.

[2] A Short History Of The Metaverse. https://bernardmarr.com/a-short-history-of-the-metaverse/. ([n. d.]). Accessed: 2022-11-21.

[3] Jie Guan, Jay Irizawa, and Alexis Morris. 2022. Extended Reality and Internet of Things for Hyper-Connected Metaverse Environments. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 163–168.

[4] What is IoT? https://www.oracle.com/ca-en/internet-of-things/what-is-iot/. ([n. d.]). Accessed: 2022-09-11.

[5] Abbas M Al-Ghaili, Hairoladenan Kasim, Naif M Al-Hada, Zainuddin Hassan, Marini Othman, Tharik J Hussain, Rafiziana Md Kasmani, and Ibraheem Shayea. 2022. A review of metaverse's definitions, architecture, applications, challenges, issues, solutions, and future trends. *IEEE Access* (2022).

[6] Danda B Rawat and Hassan El Alami. 2023. Metaverse: Requirements, architecture, standards, status, challenges, and perspectives. *IEEE Internet of Things Magazine* 6, 1 (2023), 14–18.

[7] Sang-Min Park and Young-Gab Kim. 2022. A Metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access* 10 (2022), 4209–4251.

[8] Lik-Hang Lee, Tristan Braud, Pengyuan Zhou, Lin Wang, Dianlei Xu, Zijun Lin, Abhishek Kumar, Carlos Bermejo, and Pan Hui. 2021. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352* (2021).

[9] Metaverse Vs. Virtual Reality: A Detailed Comparison? https://www.blockchain-council.org/metaverse/metaverse-vs-virtual-reality/. ([n. d.]). Accessed: 2022-09-11.

[10] What is augmented reality and why is it important for the Metaverse? https://cointelegraph.com/explained/what-is-augmented-reality-and-why-is-it-important-for-the-metaverse. ([n. d.]). Accessed: 2022-09-11.

[11] Kemal Gökhan Nalbant and Şevval UYANIK. 2021. Computer vision in the metaverse. *Journal of Metaverse* 1, 1 (2021), 9–12.

[12] The Intersection of Metaverse and AI: How AI Can Help Deliver Metaverse Promises? https://www.hcltech.com/blogs/intersection-metaverse-and-ai-how-ai-can-help-deliver-metaverse-promises. ([n. d.]). Accessed: 2022-09-11.

[13] Qinglin Yang, Yetong Zhao, Huawei Huang, Zehui Xiong, Jiawen Kang, and Zibin Zheng. 2022. Fusing blockchain and AI with metaverse: A survey. *IEEE Open Journal of the Computer Society* 3 (2022), 122–136.

[14] Thien Huynh-The, Quoc-Viet Pham, Xuan-Qui Pham, Thanh Thi Nguyen, Zhu Han, and Dong-Seong Kim. 2023. Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence* 117 (2023), 105581.

[15] The First IEEE International Workshop on Communications in Digital Twins and Metaverse. http://commetaverse.site/. ([n. d.]). Accessed: 2022-11-21.

[16] Yijing Lin, Hongyang Du, Dusit Niyato, Jiangtian Nie, Jiayi Zhang, Yanyu Cheng, and Zhaohui Yang. 2023. Blockchain-aided secure semantic communication for ai-generated content in metaverse. *IEEE Open Journal of the Computer Society* 4 (2023), 72–83.

[17] Hamed Taherdoost. 2023. Blockchain and Machine Learning: A Critical Review on Security. *Information* 14, 5 (2023), 295.

[18] Yue Han, Dusit Niyato, Cyril Leung, Chunyan Miao, and Dong In Kim. 2022. A dynamic resource allocation framework for synchronizing metaverse with iot service and data. In *ICC 2022-IEEE International Conference on Communications*. IEEE, 1196–1201.

[19] Abdenacer Naouri, Hangxing Wu, Nabil Abdelkader Nouri, Sahraoui Dhelim, and Huansheng Ning. 2021. A novel framework for mobile-edge computing by optimizing task offloading. *IEEE Internet of Things Journal* 8, 16 (2021), 13065–13076.

[20] Pengfei Hu, Sahraoui Dhelim, Huansheng Ning, and Tie Qiu. 2017. Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network and Computer Applications* 98 (2017), 27–42.

[21] Sahraoui Dhelim, Tahar Kechadi, Liming Chen, Nyothiri Aung, Huansheng Ning, and Luigi Atzori. 2022. Edge-enabled Metaverse: The Convergence of Metaverse and Mobile Edge Computing. *arXiv preprint arXiv:2205.02764* (2022).

[22] Jian Liu, Hongbo Liu, Yingying Chen, Yan Wang, and Chen Wang. 2019. Wireless sensing for human activity: A survey. *IEEE Communications Surveys & Tutorials* 22, 3 (2019), 1629–1645.

[23] Yuanhao Cui, Fan Liu, Xiaojun Jing, and Junsheng Mu. 2021. Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges. *IEEE Network* 35, 5 (2021), 158–167.

[24] An Liu, Zhe Huang, Min Li, Yubo Wan, Wenrui Li, Tony Xiao Han, Chenchen Liu, Rui Du, Danny Kai Pin Tan, Jianmin Lu, et al. 2022. A survey on fundamental limits of integrated sensing and communication. *IEEE Communications Surveys & Tutorials* 24, 2 (2022), 994–1034.

[25] Dhanashree Shukla and Sudhir D. Sawarkar. 2022. A study of wireless network evolution from 4G to 5G: standalone vs non-standalone. In *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*. 1–6. DOI: http://dx.doi.org/10.1109/SMARTGENCON56628.2022.10084020

[26] Cloud Computing, 5G, Metaverse, Electric Vehicles Among the Most Important Areas of Technology in 2023, Says New IEEE Study. https://www.ieee.org/about/news/2022/news-release-2022-survey-results.html. ([n. d.]). Accessed: 2022-11-18.

[27] Why 6G is essential to bring the metaverse vision into fruition. https://telecom.economictimes.indiatimes.com/news/why-6g-is-essential-to-bring-the-metaverse-vision-into-fruition/93591820. ([n. d.]). Accessed: 2022-11-18.

[28] Fengxiao Tang, Xuehan Chen, Ming Zhao, and Nei Kato. 2022. The Roadmap of Communication and Networking in 6G for the Metaverse. *IEEE Wireless Communications* (2022).

[29] Muhammad Zawish, Fayaz Ali Dharejo, Sunder Ali Khowaja, Kapal Dev, Steven Davy, Nawab Muhammad Faseeh Qureshi, and Paolo Bellavista. 2022. AI and 6G into the Metaverse: Fundamentals, Challenges and Future Research Trends. *arXiv preprint arXiv:2208.10921* (2022).

[30] Walid Saad, Mehdi Bennis, and Mingzhe Chen. 2019. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network* 34, 3 (2019), 134–142.

[31] Trung Q Duong, Dang Van Huynh, Saeed R Khosravirad, Vishal Sharma, Octavia A Dobre, and Hyundong Shin. 2023. From Digital Twin to Metaverse: The Role of 6G Ultra-Reliable and Low-Latency Communications with Multi-Tier Computing. *IEEE Wireless Communications* 30, 3 (2023), 140–146.

[32] Avatar. https://blog.hootsuite.com/social-media-definitions/avatar/. ([n. d.]). Accessed: 2022-09-11.

[33] Metaverse Avatar Guide; Embody Yourself in the Metaverse. https://metamandrill.com/metaverse-avatar/. ([n. d.]). Accessed: 2022-09-11.

[34] The Metaverse Will Radically Change Content Creation Forever. https://www.forbes.com/sites/falonfatemi/2022/03/07/the-metaverse-will-radically-change-content-creation-forever/?sh=7938c2784a7f. ([n. d.]). Accessed: 2022-09-17.

[35] Shu-Ching Chen. 2022. Multimedia Research Toward the Metaverse. *IEEE MultiMedia* 29, 1 (2022), 125–127.

[36] Ben Mildenhall, Pratul P Srinivasan, Matthew Tancik, Jonathan T Barron, Ravi Ramamoorthi, and Ren Ng. 2021. Nerf: Representing scenes as neural radiance fields for view synthesis. *Commun. ACM* 65, 1 (2021), 99–106.

[37] NFTs: The metaverse economy. https://www.ft.com/partnercontent/crypto-com/nfts-the-metaverse-economy.html. ([n. d.]). Accessed: 2022-09-18.

[38] Calkin S Montero, Jason Alexander, Mark T Marshall, and Sriram Subramanian. 2010. Would you do that? Understanding social acceptance of gestural interfaces. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services*. 275–278.

[39] Giluk Kang, Jahoon Koo, and Young-Gab Kim. 2023. Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective. *IEEE Communications Magazine* (2023).

[40] Mona M Soliman, Ashraf Darwish, and Aboul Ella Hassanien. 2023. The Threat of the Digital Human in the Metaverse: Security and Privacy. In *The Future of Metaverse in the Virtual Era and Physical World*. Springer, 247–265.

[41] Ben Falchuk, Shoshana Loeb, and Ralph Neff. 2018. The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine* 37, 2 (2018), 52–61.

[42] Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy. 2017. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 Internet Measurement Conference*. 432–444.

[43] Jiliang Tang and Huan Liu. 2015. Trust in social media. *Synthesis lectures on information security, privacy, & trust* 10, 1 (2015), 1–129.

[44] Trust and Safety in the Metaverse. https://cesium.com/open-metaverse-podcast/trust-and-safety-in-the-metaverse/. ([n. d.]). Accessed: 2022-09-18.

[45] In the Metaverse, Blockchain Will be the Foundation of Trust. https://thegrand.space/blockchain-will-be-the-foundation-of-trust-in-metaverse/. ([n. d.]). Accessed: 2022-09-18.

[46] When the Virtual Became Real. https://medium.com/building-the-metaverse/when-the-virtual-became-real-4168809879f5. ([n. d.]). Accessed: 2022-09-18.

[47] HuanSheng Ning and Hong Liu. 2015. Cyber-physical-social-thinking space based science and technology framework for the Internet of Things. *Science China Information Sciences* 58, 3 (2015), 1–19.

[48] Quoc-Viet Pham, Xuan-Qui Pham, Thanh Thi Nguyen, Zhu Han, Dong-Seong Kim, et al. 2022. Artificial Intelligence for the Metaverse: A Survey. *arXiv e-prints* (2022), arXiv–2202.

[49] Yuntao Wang, Zhou Su, Ning Zhang, Dongxiao Liu, Rui Xing, Tom H Luan, and Xuemin Shen. 2022. A survey on metaverse: Fundamentals, security, and privacy. *arXiv preprint arXiv:2203.02662* (2022).

[50] Mark Wright, Henrik Ekeus, Richard Coyne, James Stewart, Penny Travlou, and Robin Williams. 2008. Augmented duality: overlapping a metaverse with the real world. In *Proceedings of the 2008 International Conference on Advances in Computer Entertainment Technology*. 263–266.

[51] Eliane Schlemmer Grings, Diana Trein, and Cristofer Oliveira. 2009. The Metaverse: Telepresence in 3D Avatar-Driven Digital-Virtual Worlds. *@ tic. revista d'innovació educativa* 2 (2009), 26–32.

[52] Christopher Jaynes, Williams B Seales, Kenneth Calvert, Zongming Fei, and Jim Griffioen. 2003. The Metaverse: a networked collection of inexpensive, self-configuring, immersive environments. In *Proceedings of the workshop on Virtual environments 2003*. 115–124.

[53] Cory Ondrejka. 2004. Escaping the gilded cage: User created content and building the metaverse. *NYL Sch. L. Rev.* 49 (2004), 81.

[54] Dawn Owens, Alanah Mitchell, Deepak Khazanchi, and Ilze Zigurs. 2011. An empirical investigation of virtual world projects and metaverse technology capabilities. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 42, 1 (2011), 74–101.

[55] Haihan Duan, Jiaye Li, Sizheng Fan, Zhonghao Lin, Xiao Wu, and Wei Cai. 2021. Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia*. 153–161.

[56] Amina Almarzouqi, Ahmad Aburayya, and Said A Salloum. 2022. Prediction of User's Intention to Use Metaverse System in Medical Education: A Hybrid SEM-ML Learning Approach. *IEEE Access* 10 (2022), 43421–43434.

[57] Roberto Di Pietro and Stefano Cresci. 2021. Metaverse: Security and Privacy Issues. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 281–288.

[58] Huansheng Ning, Hang Wang, Yujia Lin, Wenxi Wang, Sahraoui Dhelim, Fadi Farha, Jianguo Ding, and Mahmoud Daneshmand. 2023. A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges. *IEEE Internet of Things Journal* (2023).

[59] Abhimanyu S Ahuja, Bryce W Polascik, Divyesh Doddapaneni, Eamonn S Byrnes, and Jayanth Sridhar. 2023. The digital metaverse: Applications in artificial intelligence, medical education, and integrative health. *Integrative Medicine Research* 12, 1 (2023), 100917.

[60] Yuntao Wang, Zhou Su, and Miao Yan. 2023. Social Metaverse: Challenges and Solutions. *arXiv preprint arXiv:2301.10221* (2023).

[61] Rajeswari Chengoden, Nancy Victor, Thien Huynh-The, Gokul Yenduri, Rutvij H Jhaveri, Mamoun Alazab, Sweta Bhattacharya, Pawan Hegde, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2023. Metaverse for healthcare: A survey on potential applications, challenges and future directions. *IEEE Access* (2023).

[62] Sikandar Ali, Abdullah, Tagne Poupi Theodore Armand, Ali Athar, Ali Hussain, Maisam Ali, Muhammad Yaseen, Moon-Il Joo, and Hee-Cheol Kim. 2023. Metaverse in healthcare integrated with explainable ai and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors* 23, 2 (2023), 565.

[63] Pronaya Bhattacharya, Ashwin Verma, Vivek Kumar Prasad, Sudeep Tanwar, Bharat Bhushan, Bogdan Cristian Florea, Dragos Daniel Taralunga, Fayez Alqahtani, and Amr Tolba. 2023. Game-o-Meta: Trusted Federated Learning Scheme for P2P Gaming Metaverse beyond 5G Networks. *Sensors* 23, 9 (2023), 4201.

[64] Shahab S Band, Sina Ardabili, Mehdi Sookhak, Anthony Theodore Chronopoulos, Said Elnaffar, Massoud Moslehpour, Mako Csaba, Bernat Torok, Hao-Ting Pai, and Amir Mosavi. 2022. When smart cities get smarter via machine learning: An in-depth literature review. *IEEE Access* 10 (2022), 60985–61015.

[65] Varun Kohli, Utkarsh Tripathi, Vinay Chamola, Bijay Kumar Rout, and Salil S Kanhere. 2022. A review on Virtual Reality and Augmented Reality use-cases of Brain Computer Interface based applications for smart cities. *Microprocessors and Microsystems* 88 (2022), 104392.

[66] Gordana Zeba, Marina Dabić, Mirjana Čičak, and Tugrul Daim. 2020. Artificial Intelligence in Manufacturing: Bibliometric and Content Analysis. In *2020 IEEE/ITU International Conference on Artificial Intelligence for Good (AI4G)*. IEEE, 95–100.

[67] Moslem Azamfar, Xiang Li, and Jay Lee. 2020. Deep learning-based domain adaptation method for fault diagnosis in semiconductor manufacturing. *IEEE Transactions on Semiconductor Manufacturing* 33, 3 (2020), 445–453.

[68] Zhiyu Lin, Peng Xiangli, Zhi Li, Fuhe Liang, and Aofei Li. 2022. Towards metaverse manufacturing: a blockchain-based trusted collaborative governance system. In *The 2022 4th International Conference on Blockchain Technology*. 171–177.

[69] IEEE Special Issue on Metaverse and the Future of Education. https://ieee-edusociety.org/ieee-special-issue-metaverse-and-future-education. ([n. d.]). Accessed: 2022-12-09.

[70] Jinping Zhong and Yunxiang Zheng. 2022. Empowering future education: Learning in the Edu-Metaverse. In *2022 International Symposium on Educational Technology (ISET)*. IEEE, 292–295.

[71] Emily Hedrick, Michael Harper, Eric Oliver, and Daniel Hatch. 2022. Teaching & learning in virtual reality: Metaverse classroom exploration. In *2022 Intermountain Engineering, Technology and Computing (IETC)*. IEEE, 1–5.

[72] Qifen Zhang. 2023. Secure Preschool Education Using Machine Learning and Metaverse Technologies. *Applied Artificial Intelligence* 37, 1 (2023), 2222496.

[73] Why the Military Needs a Metaverse. https://www.antiersolutions.com/why-the-military-needs-a-metaverse.. ([n. d.]). Accessed: 2022-12-30.

[74] What is Military Metaverse and How is it Different from Commercial Metaverse. https://www.geospatialworld.net/prime/interviews/what-is-military-metaverse-and-how-is-it-different-from-commercial-metaverse/. ([n. d.]). Accessed: 2022-12-30.

[75] Thien Huynh-The, Quoc-Viet Pham, Xuan-Qui Pham, Thanh Thi Nguyen, Zhu Han, and Dong-Seong Kim. 2022. Artificial Intelligence for the Metaverse: A Survey. *arXiv preprint arXiv:2202.10336* (2022).

[76] Roman V Yampolskiy, Brendan Klare, and Anil K Jain. 2012. Face recognition in the virtual world: recognizing avatar faces. In *2012 11th International Conference on Machine Learning and Applications*, Vol. 1. IEEE, 40–45.

[77] Aitor Rovira and Mel Slater. 2017. Reinforcement learning as a tool to make people move to a specific location in immersive virtual reality. *International Journal of Human-Computer Studies* 98 (2017), 89–94.

[78] Iason Kastanis and Mel Slater. 2012. Reinforcement learning utilizes proxemics: An avatar learns to manipulate the position of people in immersive virtual reality. *ACM Transactions on Applied Perception (TAP)* 9, 1 (2012), 1–15.

[79] The Metaverse: Driven By AI, Along With The Old Fashioned Kind Of Intelligence. https://www.forbes.com/sites/forbestechcouncil/2022/04/18/the-metaverse-driven-by-ai-along-with-the-old-fashioned-kind-of-intelligence/sh=19a2cd9c1b36. ([n. d.]). Accessed: 2022-10-24.

[80] AI will help realize the true vision the Metaverse hopes to achieve. https://cointelegraph.com/news/ai-will-help-realize-the-true-vision-the-metaverse-hopes-to-achieve. ([n. d.]). Accessed: 2022-10-24.

[81] 6 Use Cases of AI in Metaverse. https://analyticssteps.com/blogs/6-use-cases-ai-metaverse. ([n. d.]). Accessed: 2022-10-25.

[82] Merylin Monaro, Emilia Barakova, and Nicol Navarin. 2022. Editorial Special Issue Interaction With Artificial Intelligence Systems: New Human-Centered Perspectives and Challenges. *IEEE Transactions on Human-Machine Systems* 52, 3 (2022), 326–331.

[83] Nitesh Khadka, Mir Ragib Ishraq, Asif Mohammed Samir, and Mohammad Shahidur Rahman. 2019. Multilingual text categorization of indo-aryan languages. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, 1–5.

[84] Why the metaverse is filled with security, privacy and safety issues. https://venturebeat.com/security/why-the-metaverse-is-filled-with-security-privacy-and-safety-issues/. ([n. d.]). Accessed: 2022-10-17.

[85] Mohammad Alja'afreh, Ranwa Al Mallah, Ali Karime, and Abdulmotaleb El Saddik. 2023. Cybersecurity in the Metaverse: Challenges and Approaches. In *2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)*. IEEE, 1–8.

[86] Ruoyu Zhao, Yushu Zhang, Youwen Zhu, Rushi Lan, and Zhongyun Hua. 2022. Metaverse: Security and Privacy Concerns. *arXiv preprint arXiv:2203.03854* (2022).

[87] Mahbuba Begum and Mohammad Shorif Uddin. 2020. Digital image watermarking techniques: a review. *Information* 11, 2 (2020), 110.

[88] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. 2019. Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal* 6, 5 (2019), 8076–8094.

[89] The metaverse is coming, and the security threats have already arrived. https://www.zdnet.com/article/the-metaverse-is-coming-and-the-security-threats-have-already-arrived/. ([n. d.]). Accessed: 2022-10-20.

[90] Artificial Intelligence. 2017. Machine Learning Applied to Cybersecurity. (2017).

[91] Using Artificial Intelligence in Cybersecurity. https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/. ([n. d.]). Accessed: 2022-11-6.

[92] Debunking the Myths. How Machine Learning (ML) Benefits Cyber Security. https://www.securityhq.com/blog/debunking-the-myths-how-machine-learning-ml-benefits-cyber-security/. ([n. d.]). Accessed: 2022-11-6.

[93] Zhimin Zhang, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, and Kim-Kwang Raymond Choo. 2021. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review* (2021), 1–25.

[94] Rabie Ahmed, Taoufik Saidani, and Malek Rababa. 2021. A Parallel Genetic Algorithm for Solving Deadlock Problem within Multi-Unit Resources Systems. *International Journal of Computer Science & Network Security* 21, 12 (2021), 175–182.

[95] Abu Jafar Md Muzahid, Syafiq Fauzi Kamarulzaman, Md Arafatur Rahman, and Ali H Alenezi. 2022. Deep Reinforcement Learning-Based Driving Strategy for Avoidance of Chain Collisions and Its Safety Efficiency Analysis in Autonomous Vehicles. *IEEE Access* 10 (2022), 43303–43319.

[96] Network Attacks and Network Security Threats. https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/. ([n. d.]). Accessed: 2022-10-27.

[97] SaiSindhuTheja Reddy and Gopal K Shyam. 2020. A machine learning based attack detection and mitigation using a secure SaaS framework. *Journal of King Saud University-Computer and Information Sciences* (2020).

[98] Nitesh Bharot, Priyanka Verma, Sangeeta Sharma, and Veenadhari Suraparaju. 2018. Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. *Arabian Journal for Science and Engineering* 43, 2 (2018), 959–967.

[99] Aqeel Sahi, David Lai, Yan Li, and Mohammed Diykh. 2017. An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. *IEEE Access* 5 (2017), 6036–6048.

[100] Fatima Khashab, Joanna Moubarak, Antoine Feghali, and Carole Bassil. 2021. DDoS attack detection and mitigation in SDN using machine learning. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*. IEEE, 395–401.

[101] Marinos Dimolianis, Adam Pavlidis, and Vasilis Maglaris. 2021. SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering. In *2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 126–133.

[102] MOW Grond, NH Luong, J Morren, and JG Slootweg. 2012. Multi-objective optimization techniques and applications in electric power systems. In *2012 47th International Universities Power Engineering Conference (UPEC)*. IEEE, 1–6.

[103] Yazan Otoum, Sai Krishna Yadlapalli, and Amiya Nayak. 2022. FTLIoT: A Federated Transfer Learning Framework for Securing IoT. In *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 1146–1151.

[104] What is Attack vs. Intrusion. https://www.igi-global.com/dictionary/attack-vs-intrusion/1751. ([n. d.]). Accessed: 2022-10-29.

[105] Shu-Yu Kuo, Fan-Hsun Tseng, and Yao-Hsin Chou. 2023. Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism. *Future Generation Computer Systems* 143 (2023), 179–190.

[106] Fekadu Yihunie, Eman Abdelfattah, and Amish Regmi. 2019. Applying machine learning to anomaly-based intrusion detection systems. In *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 1–5.

[107] Jiong Zhang and Mohammad Zulkernine. 2006. Anomaly based network intrusion detection with unsupervised outlier detection. In *2006 IEEE International Conference on Communications*, Vol. 5. IEEE, 2388–2393.

[108] Emrah Tufan, Cihangir Tezcan, and Cengiz Acartürk. 2021. Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network. *IEEE Access* 9 (2021), 50078–50092.

[109] Tushar Rakshe and Vishal Gonjari. 2017. Anomaly based network intrusion detection using machine learning techniques. *International Journal of Engineering Research and Technology* 6, 5 (2017), 216–220.

[110] Muaadh Alsoufi, Shukor Razak, Maheyzah Md Siraj, Abdulalem Ali, Maged Nasser, Salah Abdo, et al. 2020. Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey. In *International Conference of Reliable Information and Communication Technology*. Springer, 659–675.

[111] N Satheesh, MV Rathnamma, G Rajeshkumar, P Vidya Sagar, Pankaj Dadheech, SR Dogiwal, Priya Velayutham, and Sudhakar Sengan. 2020. Flow-based anomaly intrusion detection using machine learning model with software defined networking for OpenFlow network. *Microprocessors and Microsystems* 79 (2020), 103285.

[112] Khaled Alrawashdeh and Carla Purdy. 2016. Toward an online anomaly intrusion detection system based on deep learning. In *2016 15th IEEE international conference on machine learning and applications (ICMLA)*. IEEE, 195–200.

[113] Malware is a growing threat to IoT devices- find out how to protect your device! https://www.einfochips.com/blog/malware-is-a-growing-threat-to-iot-devices-find-out-how-to-protect-your-device/. ([n. d.]). Accessed: 2022-10-30.

[114] Anshuman Dash, Satyajit Pal, and Chinmay Hegde. 2018. Ransomware auto-detection in IoT devices using machine learning. *no. December* (2018), 0–10.

[115] Rajesh Kumar, Xiaosong Zhang, Wenyong Wang, Riaz Ullah Khan, Jay Kumar, and Abubakar Sharif. 2019. A multimodal malware detection technique for Android IoT devices using various features. *IEEE Access* 7 (2019), 64411–64430.

[116] M Shobana and S Poonkuzhali. 2020. A novel approach to detect IoT malware by system calls using Deep learning techniques. In *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*. IEEE, 1–5.

[117] Nisais Nimalasingam, Janaka Senanayake, and Chathura Rajapakse. 2022. Detection of IoT Malware Based on Forensic Analysis of Network Traffic Features. In *2022 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, Vol. 5. IEEE, 122–130.

[118] Mohammad Masum, Md Jobair Hossain Faruk, Hossain Shahriar, Kai Qian, Dan Lo, and Muhaiminul Islam Adnan. 2022. Ransomware classification and detection with machine learning algorithms. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 0316–0322.

[119] Ransomware Detection using Machine Learning. https://github.com/muditmathur2020/RansomwareDetection. ([n. d.]). Accessed: 2022-10-30.

[120] Faiq Khalid, Muhammad Abdullah Hanif, Semeen Rehman, and Muhammad Shafique. 2018. Security for machine learning-based systems: Attacks and challenges during training and inference. In *2018 International Conference on Frontiers of Information Technology (FIT)*. IEEE, 327–332.

[121] Ran Gilad-Bachrach, Nathan Dowlin, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. 2016. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In *International conference on machine learning*. PMLR, 201–210.

[122] Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K Reiter. 2016. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 acm sigsac conference on computer and communications security*. 1528–1540.

[123] Ehsan Hesamifard, Hassan Takabi, and Mehdi Ghasemi. 2017. Cryptodl: Deep neural networks over encrypted data. *arXiv preprint arXiv:1711.05189* (2017).

[124] Francisco-Javier González-Serrano, Adrián Amor-Martín, and Jorge Casamayón-Antón. 2018. Supervised machine learning using encrypted training data. *International Journal of Information Security* 17, 4 (2018), 365–377.

[125] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. 2009. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition*. Ieee, 248–255.

[126] Tong Li, Zhengan Huang, Ping Li, Zheli Liu, and Chunfu Jia. 2018. Outsourced privacy-preserving classification service over encrypted data. *Journal of Network and Computer Applications* 106 (2018), 100–110.

[127] Divya Gopinath, Guy Katz, Corina S Pasareanu, and Clark Barrett. 2017. Deep-Safe: A Data-driven Approach for Checking Adversarial Robustness in Neural Networks. CoRR abs/1710.00486 (2017). *arXiv preprint arXiv:1710.00486* (2017).

[128] Xiaowei Huang, Marta Kwiatkowska, Sen Wang, and Min Wu. 2017. Safety verification of deep neural networks. In *International conference on computer aided verification*. Springer, 3–29.

[129] Ishai Rosenberg, Guillaume Sicard, and Eli Omid David. 2017. DeepAPT: nation-state APT attribution using end-to-end deep neural networks. In *International Conference on Artificial Neural Networks*. Springer, 91–99.

[130] Ximeng Liu, Robert H Deng, Kim-Kwang Raymond Choo, and Yang Yang. 2018. Privacy-preserving outsourced support vector machine design for secure drug discovery. *IEEE Transactions on Cloud Computing* 8, 2 (2018), 610–622.

[131] Jiayang Wu, Wensheng Gan, Zefeng Chen, Shicheng Wan, and Hong Lin. 2023. AI-Generated Content (AIGC): A Survey. *arXiv preprint arXiv:2304.06632* (2023).

[132] Zhihan Lv. 2023. Generative Artificial Intelligence in the Metaverse Era. *Cognitive Robotics* (2023).

[133] Y. Wang, Y. Pan, M. Yan, Z. Su, and T. H. Luan. 2023. A Survey on ChatGPT: AI–Generated Contents, Challenges, and Solutions. *IEEE Open Journal of the Computer Society* 4, 01 (jan 2023), 280–302. DOI: http://dx.doi.org/10.1109/OJCS.2023.3300321

[134] Yazan Otoum, Vinay Chamola, and Amiya Nayak. 2022. Federated and Transfer Learning-Empowered Intrusion Detection for IoT Applications. *IEEE Internet of Things Magazine* 5, 3 (2022), 50–54.