BIG DATA MINING AND ANALYTICS
ISSN 1007-0214
DOI: 10.26599/BDMA.2022.9020047
Volume x, Number x, xxxxxxx 20xx

Security and Privacy in Metaverse: A Comprehensive Survey

Yan Huang, Yi (Joy) Li*, and Zhipeng Cai.

Abstract:

Metaverse describes a new shape of cyberspace and has become a hot-trending word since 2021. There are many explanations about what Meterverse is and attempts to provide a formal standard or definition of Metaverse. However, these definitions could hardly reach universal acceptance. Rather than providing a formal definition of the Metaverse, we list the four must-have characteristics of the Metaverse: Socialization, Immersive Interaction, Real World-building, and Expandability. These characteristics carve the Metaverse into a novel, fantastic digital world but also make it suffer from all security/privacy risks, such as personal information leakage, eavesdropping, unauthorized access, phishing, data injection, broken authentication, insecure design, and more. This paper first introduces the four characteristics, then the current progress and typical applications of the Metaverse are surveyed and categorized into four economic sectors. Based on the four characteristics and the findings of the current progress, the security and privacy issues in the Metaverse are investigated. We then identify and discuss more potential critical security and privacy issues that can be caused by combining the four characteristics. Lastly, the paper also raises some other concerns regarding society and humanity.

Keywords: Metaverse, cybersecurity, privacy protection, cyber infrastructure, extended reality

1 Introduction

Metaverse, a word coined in the 1992 novel *Snow Crash*, became popular in 2021 after Mark Zuckerberg bet the future of Meta (former Facebook) on it. It describes a virtual space accessible to everyone through the Internet and defines a new generation of the social world on the Internet. The Times Journal says the Metaverse is the next digital era that will change everything (Fig. 1 [78]). For any emerging technology in cyberspace, it is reasonable to be cautious, and one should consider its security and privacy issues from day one. Likewise, we must be fully prepared for security and privacy protection in the Metaverse before it flourishes in our daily lives. In order to do that, a good understanding of what exactly Metaverse is and an investigation of its current progress will be needed.

What is Metaverse? There are many discussions about what the Metaverse is and how it fits into current cyberspace. Different from other virtual spaces, Metaverse is targeting to build a digital copy mapped from our real world with imaginary extension. The Metaverse is still in the early development stage. Many new technologies are on the way to carve the shape of the immersive digital space. Therefore, it is challenging to define this term elaborately and accurately in academia. On the other hand, to become the new generation of cy-

• Yan Huang and Yi (Joy) Li are with the Department of Software Engineering and Game Development, Kennesaw State University, Atlanta 30060, USA. E-mail: yhuang24@kennesaw.edu and joy.li@kennesaw.edu
• Zhipeng Cai is with the Department of Computer Science, Georgia State University, Atlanta 30303, USA. E-mail: zcai@gsu.edu
* To whom correspondence should be addressed.
Manuscript received: 2022-10-4; accepted: 2022-11-16

berspace on the Internet, it is our insights that Metaverse has to include four characteristics: socialization, immersive interaction, imitation of the real world, and expandability. *(1) Socialization*: Metaverse connects people who have access to the Internet. Users in the Metaverse are able to post/share their social profiles and interact with other users. *(2) Immersive Interaction*: Users are able to have better machine-human interactions, such as extended reality (XR) and brain-computer interface, that are far more immersive and intuitive than traditional interactions based on sentences, images, and videos. *(3) Real World-building*: Metaverse is able to provide virtual world spaces for many kinds of real-life activities such as meeting, playing, shopping, traveling, etc. *(4) Expandability:* Metaverse has more possibilities and extensions than the real world, especially in science fiction and fantasy. In Metaverse, users can enjoy more functionalities that they cannot achieve in the real world, such as digital modeling and virtual educational science exploration. In addition, Metaverse not only contains the summation of these four characteristics but also reaches the next level of user experiences with cross-reinforcement of the four. For example, as the movie "Ready Player One" depicted, people can have a cyber-life in the virtual world, where they can make friends, play, do business, and have other real-life and fictional activities with immersive interactions.

Why we care about the Security and Privacy in Metaverse? Metaverse has all the benefits of the above four characteristics while also suffering from all their security/privacy risks, such as personal information leakage, eavesdropping, data theft, unauthorized access, phishing, data injection, broken authentication, insecure design, and more. What is worse, the combination of these four characteristics makes current security and privacy issues more critical. For example, personal information is more likely to be stolen because Metaverse includes more personal elements to build such immersive social cyberspace. Furthermore, Metaverse may cause issues that we have never experienced before. For instance, hackers may hack into a human's physical body from a brain-computer interface connected to Metaverse.

Therefore, it is high time for engineers, researchers, and entrepreneurs to discuss and understand the impact of the upcoming revolution. We wish to provide insights into future Metaverse and methodically address the challenges and practical solutions.

In this paper, we survey the current progress of Metaverse. Then we analyze and discuss security and privacy issues and solutions of current Metaverse applications. Lastly, we further explore and forecast possible security and privacy issues in the future Metaverse.

Fig. 1 The Metaverse Cover in Time Journal [78]

2 Metaverse Progress and Applications

Current progress of Metaverse?

Before the potable VR headsets or AR glasses became hot-trending gaming tools on the market, the closest implementation for metaverse was the *Second Life* platform, which many researchers referred to as "metaverse" when working on the platform. *Second Life* is a 3D digital gaming world that provides a digital replica of the real world. Users can interact with each other and the environment using textural, oral, gestural, and graphic languages. Educators treated the platform as an innovative teaching method for diverse classrooms [28,40], researchers used it for embodiment and behavioral change [15], healthcare professionals attempted to use it for advocating healthy behaviors in the treatment of substance abuse [15], companies made use of it for social networking and team building projects. However, as immersive technologies and IoT technologies emerged, Second Life soon lost its weight in the foundation of the new metaverse era.

Immersive technologies, including virtual reality, augmented reality, mixed reality, and extended reality, embraced a rapid development in both hardware and software through the 2010s. Meta Platform pushes the Metaverse industry further to a new level with 10 million Oculus Quest 2 headsets deliveries. The breakthrough in immersive technologies has enabled the fundamental infrastructure of the Metaverse. The internet has expanded into multiple dimensions, in which the real and virtual worlds have blended together. The human-computer interaction has ever become human-machine fusion. Digital twins, native virtualization, virtual and real fusion, and interaction, are the base structure of the Metaverse. Although the Metaverse is still merely at the beginning stage and far from taking shapes, many applications can serve as discrete pieces for later integration and formation.

Metaverse-related technologies include but are not limited to the combination of artificial intelligence (AI), data mining and deep learning, VR/AR/XR, the internet of things (IoT), blockchain, edge computing, cloud computing, and 3D reconstruction.

Research studies have explored using technologies for innovative education, healthcare, socialization, and more. The industry has also explored Metaverse economic activities such as entertainment experience, blockchain, non-fungible tokens (NFTs), Web 3.0, and so on. In this section, we discuss the typical applications in different fields based on the popular four-sector model in economy [36], how they match the four characteristics mentioned in the prior section, and their potential extension in the Metaverse. Figure 2 depicts how Metaverse technologies support innovative applications in three sectors. The applications on the list of each sector are not exhaustive but are some typical examples.

The primary sector of the economy is making direct use of natural resources, including agriculture, forestry and fishing, mining, and oil and gas extraction. Artificial intelligence and data mining construct reliable models for farmers and companies to optimize their operations based on computing and simulations. VR applications could provide a virtual farming experience, while AR applications can integrate with smart sensors to serve as a fully digitized virtual assistant. Precision farming [48], heavy equipment simulation and training, market learning and planning, remote experts consulting, hazards training for mining, and simulation of oil leakage are a few current typical applications in the fields. In this sector, the socialization character mainly

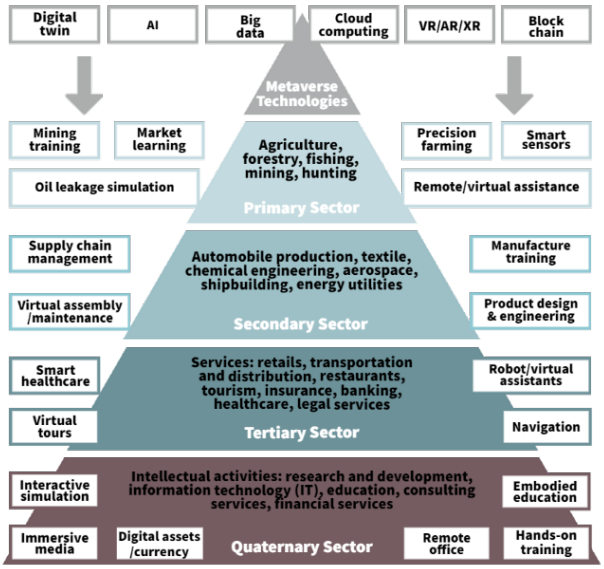


Fig. 2 Current technologies and applications in Metaverse economics

falls on the more convenient delivery of expert opinions and big data analysis to facilitate the activities. Smart appliances and tools enable real-world building, and applications can be easily expanded to other sectors, such as retail and virtual tours. Mixed reality technology and sensors are integrated to provide possible immersive interactions.

The secondary sector of the economy covers the manufacturing of goods, including the processing of materials produced by the primary sector, construction, and the public utility industries of electricity, gas, and water. Aerospace, shipbuilding and energy utilities are also included in this sector.

Digital human models (DHMs) are the main application intensively used in both the manufacturing industry and related academic research fields [102]. Six categories were identified that have utilized DHMs through prior study reports : (1) the Automotive industry; (2) Industrial plants; (3) the Aerospace industry; (4) the Military industry; (5) the Energy industry. Among them, assembly/maintenance, automotive interior assessment, and workplace design and optimization are the top three application type that DHMs are applied to, which add up to 76.1% of the total. Virtual assembly and maintenance have been largely used to replace physical prototyping and traditional procedures. On the other hand, AI and blockchain techniques are also playing growing roles in the manufacturing industries.

In aviation and aerospace, VR/AR/MR have played

essential roles in training pilots. Unanticipated events, weather changes, terrain, and airspace information can all be simulated with multiple variations for pilots to practice skills in safe environments. The technologies are also used in assisting aircraft maintenance and engineer training. Remote and virtual assistance can improve work efficiency. Furthermore, airlines are investing in bringing in VR headsets to enhance the inflight experience of their passengers [4].

In the second sector, real-world building and immersive interactions are realized by virtual planning, design, engineering, and management. Applications can be expanded to other sectors, such as educational training and remote management, thus also further enhancing socialization.

The tertiary sector involves services. Services include but are not limited to retail businesses, transportation and distribution, restaurants, tourism, insurance, banking, healthcare, and legal services. The following paragraphs list typical Metaverse applications and current progress in this sector.

Digital twins have gone a long way to provide more immersive interactions in displays, tours, and art presentations. With the support of scanning cameras and 3D reconstruction, VR can replicate existing masterpieces, galleries, and museums with incredible resolution, and bring the site to a remote user. One can stay at home and enjoy the virtual visits, with the ability to skip tour lines, 360 degrees of appreciation, and even possible interactions without causing any damage to the original items. On the other hand, onsite visits often integrate AR technology with geographic markers to enable virtual prompts of related information, audio tours, and possible interactions with the objects, eliminating the extra physical signs that are limited by space restriction and aesthetics concerns. These applications can be further extended with social attributes such as a virtual guestbook that allows visitors from different time dimensions to communicate, as well as trivia quizzes with a leaderboard to enable competition and better retention of knowledge after a virtual visit.

IoT and immersive technologies have made modern healthcare ever smarter. They provide assistance not only for clinical diagnosis, treatment and research [99], but also for prevention for onset and relapse [91], rehabilitation [83], and medical education [59]. Furthermore, not just benefiting people's health, but the embodiment and immersiveness of immersive technologies, and the remote distribution of IoT have made perspective-taking of public healthcare awareness easier. Empathy training can strengthen the social network and improve social support for suffering patients and families. Pilot studies have reported positive feedback using VR to cultivate empathy for older people [19], nausea and vomiting management [90], visual deficit [7], and Parkinson's Disease [63].

Virtual assistants based on AI [49] also started to serve in daily lives. From innovative IoT tools to humanoids, from completely virtual companions to virtual idols and virtual customer service, with the help of deep learning, big data, and AI, are replacing some actual human labor or assistants. Media, movies, entertainment tools, games, financial markets, tours, and more, are embracing new technologies and attempting to provide more customized services dedicated to their target audience.

In the tertiary sector, real-world building and immersive interactions are delivered through assistant services provided by robots or virtual agents that connect related fields. Added remote or virtual services further enhance the socialization characteristic in this sector. Applications can be expanded to different aspects within the sector or other sectors.

The quaternary sector includes intellectual activities and pursuits. Most businesses in this sector are engaged in research and development, information technology, education, and consulting services. The following paragraphs list typical Metaverse applications and current progress in this sector.

The most generic applications of Metaverse, especially services and solutions, would be education and remote office solutions. 3D reconstructions and simulations can be used to convey knowledge to teach any user in the world. From lower skills such as vocabulary and concept teaching to higher-order thinking skills such as cognition and leadership, immersive technologies can provide various help in the specific knowledge hierarchies. Complicated scenarios that are hard to elaborate in real life can be created virtually under carefully designed system constraints, to provide a repeatable and interactive experience for users to achieve their learning goals. On the other hand, the remote office can bring people together when necessary without limitations on physical distance and travel expenses. The current telecommunication or video calls may have provided essential solutions during the COVID-19 pandemic, but only being able to see facial expressions and hear voices are hardly natural office experiences. The

new Quest Pro released by Meta just recently will provide the features of facial tracking, eye tracking, and possible body tracking, increasing the presence to a great extent. Companies could customize their own virtual office or virtual campus and bring teams together with more native communications, thus increasing meeting and working efficiency.

Military in Metaverse mainly focus on training, experimentation, and mission rehearsal [5]. Many wargames and simulations are designed to utilize VR/AR technology with data analysis, to train the military on strategy, decision-making, reactions, and more, to enhance their defense strength in the absence of real-world combat [6]. More advanced mixed reality technologies have already been integrated into the navigation of navy ships and military flights, as well as their simulators. Furthermore, the social benefit of Metaverse can help recruitment and interconnections in teams.

Blockchain and decentralization technologies have made digital currency and assets so popular that they are closely involved with economic activities and investment. Non-fungible tokens (NFTs) are cryptographic tokens built on the Ethereum blockchain technology, which endorses their value in ownership and scarcity [58, 83]. People invest in cryptocurrencies, especially Bitcoin and Ethereum, not just to trade and exchange, but also to make profits just like other traditional financial investments. The mainstream use of NFTs today is for artwork. NFTs are used to mark and verify the origin of artwork, therefore asserting its investment value. Art galleries, game assets, virtual real estate, and other digital collectible assets are the top NFT marketplaces, which added up to $11.3 billion in the market value in 2021 [2].

In the quaternary sector, since the sector focuses on higher intellectual activities, immersive interactions are naturally embedded among many technology-related fields. Researches and development with the help of Metaverse technologies resolve real-world building issues, and further improve socialization through professional social computing methodologies. Applications can be expanded to serve all the above sectors.

The above-mentioned ongoing research and commercial usage of Metaverse technologies are continuously expanding. Infinite possibilities and extensions of innovative applications are yet to be explored. 5G/6G telecommunication network, cloud computing/edge computing, AI empowerment, industrial internet platform, blockchain, and the game engine will still be hot topics in the next decade on digital infrastructure construction. Based on the infrastructure, the ecosystem for both businesses and consumers will be built with innovative content and interactions. Entertainment, research, manufacturing, healthcare, and education will all benefit from the ecosystems.

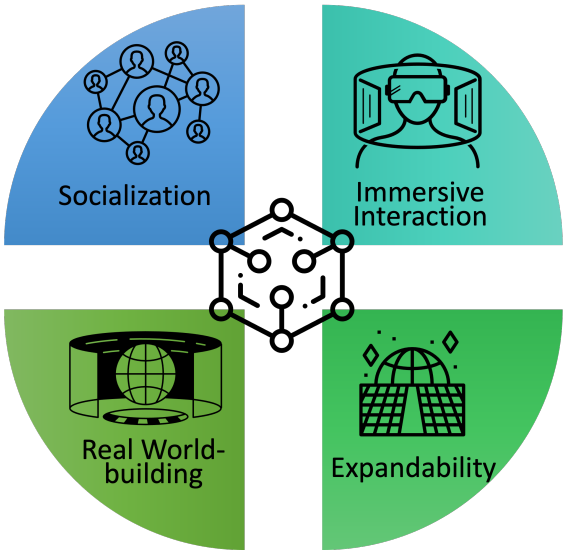


Fig. 3 Four characteristics of the Metaverse

3 Existing Security and Privacy Issues and Solutions in Metaverse

Based on the progress and vista of Metaverse, we analyze the existing security and privacy issues and solutions in Metaverse based on the four characteristics as shown in Fig. 3.

3.1 Socialization Related Security and Privacy Issues and Solutions

In the Metaverse, users can have social interactions with each other through the Internet, which means the Internet serves as the backbone for communication and connections. Therefore, Metaverse suffers from all the network-related security and privacy issues exposed in social networks.

3.1.1 Security issues and Solutions

The interactivity of online services accepts input from users, which gives hackers a chance to steal data from a venerable system by using **injection** attacks [32]. To prevent this, end-user devices should validate all user input, permit only minimally privileged accounts to send user input to the server, and run SQL Server with

Table 1 Metaverse Applications, Security and Privacy Issues and Solutions Comparison

	Security and Privacy Issues	**Solutions**
Socialization	Injection Attacks [32], Man-in-the-Middle Attacks [12], Cross Site Scripting [30], Privacy Leakage [13, 20, 70]	End User Validation [80], Strong Authentication and Cryptographic Protocols [11, 51], Attack Detection and Monitor [14, 54], Deep Learning-Based Detection [34], Secure Programming Practice [71] K-Anonymity [89], L-Diversity [66],Differential Privacy [31]
Immersive Interaction	Insecure Deserialization [57, 75, 96], Sensory Data Leakage [46, 47, 101], Biometrics Leakage [24, 25, 103]	Firewall [75],Static Scan [57], End-to-End Authentication Protocol [50], Two-Factor [94] or Three-Factor [81] Authentication, Local Storage [9]
Real World Building	Meta User Relations [44, 61, 65]	Graph-based framework for privacy preservation [62], Differential Privacy [100]
Expandability	Third-Party Tracking [56], Cross-App Tracking [79]	Third-Party Tracking/Cross-App Tracking Analysis Tools and Detection Algorithms [87], Machine Learning Based Blocking Model [27]
Combination	Virtual Economy Security [53], Data Security and Privacy in Digital Twin [74], Data Poison [45]	Blockchain [76], NFT [8], Cryptocurrency [33], Federated Learning [74, 97], Reinforcement Learning [73]

the least necessary privileges [80]. **Man-in-the-middle attacks** eavesdrop on or alter the communication between user and server and may intercept/modify data packets, thus compromising confidentiality, integrity, and availability of the system [12]. The most effective way to prevent this attack is by utilizing strong authentication and cryptographic protocols [11, 51]. Authentication algorithms can be applied to preserve the data integrity in communication channels [23], while cryptographic protocols can be used to achieve data availability [43]. Meanwhile, attack detection algorithms are necessary to monitor the system and prevent further attacks if detected [14]. **Cross Site Scripting (XSS)** attacks inject external malicious JavaScript code into websites. Attackers can inject malicious JavaScript code directly into the client website or into a store location where it will be requested by the client website [30]. Metaverse with embedded web pages is venerable to this type of attack. A web proxy with XXS detection algorithms can be used to mitigate possible cross-site scripting attempts [54]. Recently, deep learning model utilization improved the XXS detection accuracy and effectiveness [34]. From the software engineering aspect, the Open Web Application Security Project (OWASP) published XSS Prevention Cheat Sheet [71] to guide software engineers in preventing XXS attacks in web application development.

3.1.2 Privacy issues and Solutions

Privacy leakage happens almost every where in social networks, even in a well-maintained, secure platform. The private or sensitive information of users can be leaked from public information from a secure social network platform. Social network sites ask users to create a profile that contains sensitive information [20]. Users are willing to share their other activities to enjoy the services provided by the platform, such as shopping services from the business platform and friends-making services on Facebook, etc [20]. A malicious party can collect sensitive information of social network users from their online profiles and public information. In [77], the researcher found that privacy in publishing social network data is being used by unexpected people such as social network providers, analysts, adversaries, etc. Meanwhile, the social network platform provider may trade the collected users' profile and activity information in the data market [16, 18, 70], thus increasing the unpredictable risk of privacy leakage. Analysts can collect users' information from public data or purchase from the social network provider. These data can be used to mine purposely for marketing and advertising [64, 92]. Adversaries can utilize personal information to send phishing or scam messages. These messages with real personal information dramatically increase the success rate of phishing or scam, thus causing severe troubles to social network users [38]. Recently, Generative adversarial networks (GAN) have been employed to generate fake voices, images, or videos that hear/look real based on the public voice, image, or video data. These almost real fake data have caused more critical fraud and crime than ever before [52, 67].

The best way to protect users' privacy is to cut the data exposure on the clients' side. K-anonymity [89] and L-diversity [66] are algorithms to hide users' real data in a set of fake data, thus preventing users' real data be detected. Differential privacy [31] is a statistical disclosure control algorithm that can disturb each user's real data but still can have a relatively accurate statistical result from a group of people. To prevent GAN based attacks, anti-GAN algorithms [21, 88] are invented to add noise to users' different types of data to prevent fake data generation. The noise is invisible to people but will lead the GAN to generate fake data that are different from the real data.

Users' confidential information may also be leaked from data breaches. There are more than 9000 data breaches since 2005 that led to the loss of 11.5 billion individual records that made a significant financial and technical impact [39, 41]. In [22], Chen et al. proposed possible solutions to prevent and detect data breaches in the platform. Based on their analysis, we suggest the following defending strategies. Basic security protection mechanisms are always needed and should be enhanced, including firewall, antivirus, authentication, and access control. Besides, data leak prevention and detection techniques are necessary for platforms. These techniques can be categorized into content-based approaches and context-based approaches. Content-based approaches [82, 86] are mostly rule-based algorithms that detect data fingerprints that are added to or exist in stored data. A data leak is detected if a known fingerprint is detected in external space. Context-based approaches [68, 85, 85] use machine learning and data mining-based algorithms to detect abnormal access patterns to internal data or to detect the watermark in the unauthorized data. Context-based and content-based approaches are strongly encouraged to be performed simultaneously to keep monitoring the security status of data [26].

Sometimes, platforms can also leak information from inadvertent data publication or improper security or privacy protection configuration. For example, Netflix published an anonymized dataset for a $1 million prize recommendation competition [13]. However, the anonymized dataset was used to infer users' sensitive information by linking with other datasets. To avoid this kind of risk, platforms should employ high-level security and privacy protection mechanisms with proper configurations. The platform should always include experts to evaluate the impacts before any data release.

3.2 Immersive Interaction Related Security and Privacy Issues and Solutions

The immersive interaction involves many devices, such as wearable devices, headsets, base stations, and controllers, with massive data exchange. Data serialization and deserialization are essential to exchange (send and receive) data. However, attackers may be able to inject hostile serialized data into the communication and make it the initial entry point to a complex system. This kind of attack is called Insecure Deserialization which is one of the top 10 security risks [96]. For example, [75] shows a deserialization vulnerability in the Android system that allows for arbitrary code execution in the context of many apps and services and elevates the privileges of malicious applications. There are multiple methods to avoid insecure deserialization attacks: the data serialization should be encrypted and monitored; the data sources should always be authenticated; a firewall can be utilized in a computing-capable device [75]. The deserialization vulnerability can be analyzed with static scan [57]. Further improvement and enhancement can be executed based on the analysis report.

Communication among all these devices and remote/cloud services gives users an immersive experience. These devices are also embedded with many sensors that can collect more sensitive information, such as fingerprints, locations, and facial identities [46,47,101]. A security breach can cause more critical risks to users of these devices because many biometrics (*e. g.* fingerprint and facial identity) are unique and will not change throughout the life span of users. As a result, rigorous protection should be applied to each device and communication. An efficient end-to-end authentication protocol was proposed [50] to secure the information collected from wearable health monitoring sensors based on quadratic residues. For wearable devices with limited computational capability and battery, some lightweight authentication protocols can be applied. Das et al. [29] invented a scheme that allows users to mutually authenticate their wearable devices and the mobile terminal and establish a session key among these devices for secure communication between the wearable device and the mobile terminal. Two-factor [94] or three-factor [81] authentication methods are widely used to enhance security protection.

While biometrics-based authentication such as using voice [25], fingerprint [24], and face [103] is popular nowadays because of their convenience, these methods

may also cause the risk of leaking users' biometrics. Pagnin et al. [72] discussed the possibility and impact of biometrics leakage in authentication systems. The best practice is to keep all biometrics in the local device and never send them out. As Apple did for their touchID, the fingerprint will be stored and encrypted in the local chip instead of their remote server [9]. Their devices will compare the authenticating fingerprint with stored fingerprint records. The only output from the authentication system is TRUE or FALSE. Thus, even if the device or remote service provider is hacked, the fingerprints are still safe.

3.3 Real World-Building Related Security and Privacy Issues and Solutions

The world-building environment simulates the real world. Each user has character settings in the world-building environment with complete information on every aspect, including hobbies, interests, friendships, and expertise. The complete information of a user can build a user profile that reveals significant meta relations [65]. The user profiles, together with the knowledge graph, are typically used for recommendation systems [44,61]. However, massive users' privacy is at risk of being leaked from user profiling. Some privacy protection mechanisms should be applied to protect users' privacy while maintaining the world-building environment and accurate recommendation system. Hasan *et al.* [42] discussed user profiling with big data techniques, the associated privacy challenges, and the approaches to preserving user privacy. Li et al. proposed a graph-based framework for privacy preservation [62]. In their work, a graph was built for dataset representation, background knowledge specification, anonymity operation design, and attack inferring analysis. This framework can accommodate various datasets of the world-building environment. In [100], the authors added information perturbation mechanisms with differential privacy into the recommendation system and created an encryption paradigm to enforce privacy protection.

3.4 Expandability Related Security and Privacy Issues and Solutions

Metaverse extends the real-world building environment by adding more functions. For example, users can have "in-person" meetings in a VR room, shop in a virtual mall, or operate surgery remotely. These functionalities are added to the Metaverse system through many different applications. Communication channels are usually built among applications to compose a single multi-functional Metaverse, as in mobile devices. However, these communication channels allow one app to read the system component's status and the other app's outgoing information, which may create a back door for third-party tracking/cross-app tracking [79]. As a result, users' privacy can be leaked from third-party tracking/cross-app tracking.

The first step of the solution would be to prevent third-party tracking/cross-app tracking is to block unnecessary tracking channels in the system. Both Apple and Google have built strict cross-app tracking authentication in their iOS and Android mobile system [55]. Users get to decide which app can have the right to track other apps. Even with this, users may make mistakes in decisions or even simply click the wrong button and give away the control. On the other hand, seamlessly interconnected devices in the Metaverse via Bluetooth and other communication protocols promise unlimited room for third-party tracking/cross-app tracking [17,56]. To further improve the solution, third-party tracking/cross-app tracking analysis tools and detection algorithms should be applied [87]. Considering that the computational power of devices is usually limited in the early metaverse era, especially with mobile and other portable devices, a lightweight detection mechanism can be utilized to detect and block third-party tracking/cross-app tracking by using a blocklist to block known threat requests and some machine learning models to detect and block malicious activities from a third party [27].

4 Possible Security and Privacy Issues and Solutions in Metaverse

Metaverse simulates the real world with many extensions. The economy is one must-have factor to support all the activities in Metaverse. Some traditional companies, including restaurants such as McDonald's and retailers such as Nike, are preparing for the Metaverse to become a space where one can go shopping, play games, meet friends, attend concerts, work and generally build a virtual life [53]. In preparing for these activities, digital assets, such as digital arts, virtual goods, and services, have gained their investment value in Metaverse and become important in the virtual economy. Blockchain [76] technology, cryptocurrency, and NFT play a vital role in supporting and securing the virtual economy in Metaverse, by certificating the

unique identity (recorded in the blockchain) of virtual assets that can be owned and traded [8]. Normal currency may still be functioning in Metaverse, but the traditional centralized payment system has many problems people want to avoid in the new digital world, such as unreliability system, credit fraud, and privacy leakage. Cryptocurrency is a digital currency that is based on blockchain [33]. Thus, it does not rely on any central platform. Users can have an anonymized, secure payment experience based on cryptocurrency. Cryptocurrency and NFT also have their drawbacks, such as legal issues and collusion between majority entities. These issues are expected to be resolved or mitigated with technology improvement.

World-building is one of the necessary characteristics of the Metaverse. The real world simulation has been practiced for more than 50 years. Recently, a new technology, Digital Twin (DT), has the ability to present an up-to-date environment in operation that includes the environment's condition and relevant historical data. To be more sepecific, a DT system is a digital representation of a physical asset, environment, or system that was initially developed to automatically aggregate, analyze, and visualize complex information through continuous interactions with the real world [93]. The world-building utilizes DT to model not only the physical world but also the behavior and performance of physical entities in the digital world. That is to say, DT keeps querying massive of data from the environment or object it represents. These data are stored and processed in DT to decide the overall quality and utility of the DT. In other words, if we want to derive a DT that has no difference from the environment or object it represents, the environment or object should be transparent to DT and have no privacy. Federated Learning (FL) can serve as a solution for privacy protection because clients only upload training parameters to the DT instead of raw data. Pang et al. proposed a framework that fused city DT with FL to achieve a novel collaborative paradigm that allows multiple city DTs to share the local strategy and status quickly [74]. In their work, an FL central server serves as a global DT and gains the correlations between various response plans and infection trends. Communication during DT training among all the twins needs to be protected. Xiong et al. investigate the security vulnerabilities of the existing neural communication system and develop a new defense mechanism to facilitate secure two-way communication [98].

Besides privacy issues, data poison attack [45] is another security problem in DT. Data poisoning attacks pollute DT learning by tampering with the training data or labels, thus decreasing the model's utility. If the attacker dominates the training process, it can manipulate the training result. In [73], the authors proposed a reinforcement learning (RL)-based intelligent central server with the capability of recognizing heterogeneity or data poison attack in the FL training process. When minority clients or data poison attacks are detected, the central server will remove their updates to keep the best performance of the trained model.

In the complicated environment of the Metaverse, phishing also gets more sophisticated. Users create their avatars and deal with other users' avatars representing actual humans. Pictures or 3D models are used to build the avatars based on their real or preferred appearance. These avatars can be easily copied and used in phishing, which will not be similar to traditional phishing emails. It could be an avatar acting like users' friends or family in a virtual space like Meta Worlds Horizon. A form of deep learning technique may be maliciously used to imitate appearances, actions, and voices to deceive, thus getting credential information, digital assets, and NFTs from targeted users. Moreover, cybercriminals can copy known digital marketplaces and create fake replication to trap users into spending money. Fake replications can be exactly the same as the official virtual space, which makes businesses dangerous in Metaverse, especially for Metaverse newcomers.

For better comparison, all the discussed existing and possible security and privacy issues and solutions in Metaverse are listed in Table 1.

5 Other Related Issues in Metaverse

In addition to the issues discussed in the previous sections in more technological terms, possible mental and physical health concerns, safety issues, and societal problems raised by Metaverse cannot be overlooked. Similar cases have been identified in the Second Life [60] a few years earlier as the common issue of simulation and multi-player gaming platforms. Some of them can happen or even worsen in the upcoming Metaverse, since it consists of not only one gaming platform but an entire ecosystem.

The constant transition between the virtual world and reality and their mixtures can cause both **physical and mental problems**. Because of the limitation of the current immersive technologies, the hardware causes fa-

tigue and motion sickness in a relatively short period of time, typically after two or three hours of usage. This can cause longer reaction time, cognitive fatigue, concentration decrease, avoidance of deep thinking, or even loss of interest in real life. Similar to internet addiction, too much exposure to Metaverse could also cause cybersyndrome [69]. Physical disorders can be experienced, including weight gain or loss, neck or back pain, dry and red eyes, and other physical discomforts. Balance disorders, failure in hand-eye coordination, vision impairment, and spatial miscalculation can also happen. Mentally, social disorders could happen, such as neglecting friends and family, sociophobia, or even depression, because of the gap in self-expectation and real-life position.

In addition to the previous section mentioned privacy and security issues, social engineering attacks [84] will emerge more since more social communications are carried out in the digitized Metaverse. Social engineering often intentionally uses psychological manipulation to trick users. Human feelings, such as curiosity or fear, are made into traps to tempt victims. Baiting, Scareware, Pretexting, Phishing, and Spear phishing are commonly seen methods used by social engineering attackers. Social security numbers, health records, passwords, or even virtual identity, will be harvested if the Metaverse residents have no precautions or awareness.

In a larger **societal scale**, identity crisis can happen to people, especially teenagers who do not have mature cognition yet. The digital twin of the person or virtual avatar may create a mismatch between their real identity and the virtual world, both in appearance and internal mental status. Too much virtual involvement may blur the boundary of both worlds, and malicious ideology may be easily instilled, such as bias, discrimination, violence, and even viral propaganda.

Customizable avatars and more data computing powered AI will easily cause "information cocoons" or so-called "echo room effect" and thus shallow cognition [37]. Intelligent recommendations, big data analysis, adaptation engines, and IoT personalized digital assistants will isolate individuals, especially younger generations, who habitually rely on smart devices and their recommendations. What the individual receives is no longer comprehensive knowledge but fragmented and biased information source. It is threatening to the culture that the younger generations are vulnerable to the influence of the Metaverse, resulting in losing deep thinking and critical thinking skills.

Since the Metaverse is open to everyone, legit or malicious, the "Darkverse" is expected to flourish too, as long as malicious users master the necessary techniques. The darkverse is similar to the dark web, except it exists inside the Metaverse. Illegal or criminal activities will be more challenging to be detected and intercepted by law enforcement agencies because of the pseudo-physical presence of the users and non-so-easy-to-break tokens.

The *Second Life* was infamous once because of virtual grope and sexual harassment. Despite how advanced and wholesome the Metaverse may seem, the same problems could still happen. On Meta's Horizon Worlds, where a maximum of 20 avatars can hang out together and build within the virtual space, women are already complaining about sexual harassment [1]. Better mechanisms and safety solutions will be needed to regulate or prohibit the digital twin version of misconduct and toxic behaviors.

Other issues include technical difficulties and possible impact on the current economic activities. For example, customizable avatars, either humanoids or completely virtual, will still fall into the tricky "uncanny valley" [35] just like the *Second Life* [10]. Mori states that "as a robot is becoming more vivid, the emotional response from a human being to the robot will become increasingly positive and empathic, until a point is reached beyond which the response quickly becomes that of strong repulsion" [3]. Many researchers have investigated the situation but only to find it hard to resolve. This brings up even more challenges in the field since immersiveness will provide more presence and, thus, cause stronger repulsion if it falls into the uncanny valley. A careful balancing of human-like features in the design of virtual avatars or androids cannot be underestimated.

Last but not least, there are plenty of new words being coined along with "Metaverse", such as "Metasociety", "Metaeconomics", "Metamanagement", "Metaenterprise", "Metacity", and so on [95]. The job market may face a crisis and transition once more; some current and traditional profitable jobs may be replaced. New products and services, job profiles, and business models will be needed to adapt to the challenges and impacts.

6 Conclusions

In this paper, we have identified the four core characteristics that help define and summarize the current

progress of using cutting-edge technologies under the umbrella of Metaverse. Also investigated topics are the existing security and privacy issues and solutions of Metaverse accordingly to the four core characteristics. The discussion is then further expanded to other possible security and privacy issues. Finally, we also discussed other general related issues in Metaverse. By reviewing and summarizing the literature, we wish to inspire the discussions on necessary provisions for Metaverse-related research and applications regarding security and privacy issues, and provide insight for future studies.

Acknowledgement

This work is partially supported by National Science Foundation: NSF 1912753.

References

[1] The metaverse has a groping problem already.

[2] Non-fungible Token Market Size, Share, Trends, and Forecast 2030.

[3] The Uncanny Valley: The Original Essay by Masahiro Mori, June 2012.

[4] Emirates unveils first airline virtual reality app in Oculus store, September 2021.

[5] The Full Potential of a Military Metaverse, February 2022.

[6] Us military pioneers metaverse experiences that are amazingly sophisticated, May 2022.

[7] Drew Alexander, Thuy Nguyen, Patrick Keller, Jason Orlosky, Shilpa Brown, Elena Wood, Onyeka Ezenwoye, and Wanda Jirau-Rosaly. Design of Visual Deficit Simulation for Integration into a Geriatric Physical Diagnosis Course. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 838–839, March 2020.

[8] Lennart Ante. The non-fungible token (nft) market and its relationship with bitcoin and ethereum. *FinTech*, 1(3):216–224, 2022.

[9] Apple. About touch id advanced security technology, 2022.

[10] Elif Ayiter. Syncretia: A Sojourn into the Uncanny Valley. In Roy Ascott, Gerald Bast, Wolfgang Fiel, Margarete Jahrmann, and Ruth Schnell, editors, *New Realities: Being Syncretic*, pages 26–29. Springer Vienna, Vienna, 2009.

[11] Mourade Azrour, Jamal Mabrouki, Azedine Guezzaz, and Yousef Farhaoui. New enhanced authentication protocol for internet of things. *Big Data Mining and Analytics*, 4(1):1–9, 2021.

[12] Xiaolong Bai, Liang Hu, Zixing Song, Feiyan Chen, and Kuo Zhao. Defense against dns man-in-the-middle spoofing. In Zhiguo Gong, Xiangfeng Luo, Junjie Chen, Jingsheng Lei, and Fu Lee Wang, editors, *Web Information Systems and Mining*, pages 312–319, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[13] Robert M Bell, Yehuda Koren, and Chris Volinsky. The bellkor solution to the netflix prize. *KorBell Team's Report to Netflix*, 2007.

[14] Bharat Bhushan, G. Sahoo, and Amit Kumar Rai. Man-in-the-middle attack in wireless and computer networking — a review. In *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*, pages 1–6, 2017.

[15] Ana Boa-Ventura. Virtual Worlds and Behavioral Change. *Advances in Social Networking and Online Communities*, pages 271–286, 2011.

[16] Zhipeng Cai and Zaobo He. Trading private range counting over big iot data. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 144–153, 2019.

[17] Zhipeng Cai and Xu Zheng. A private and efficient mechanism for data uploading in smart cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, 7(2):766–775, 2020.

[18] Zhipeng Cai, Xu Zheng, Jinbao Wang, and Zaobo He. Private data trading towards range counting queries in internet of things. *IEEE Transactions on Mobile Computing*, pages 1–1, 2022.

[19] Aleda M. H. Chen, Mary E. Kiersma, Karen S. Yehle, and Kimberly S. Plake. Impact of an Aging Simulation Game on Pharmacy Students' Empathy for Older Adults. *American Journal of Pharmaceutical Education*, 79(5), June 2015.

[20] Xi Chen and Katina Michael. Privacy issues and solutions in social network sites. *IEEE Technology and Society Magazine*, 31(4):43–53, 2012.

[21] Zhenzhu Chen, Anmin Fu, Yinghui Zhang, Zhe Liu, Fanjian Zeng, and Robert H. Deng. Secure collaborative deep learning against gan attacks in the internet of things. *IEEE Internet of Things Journal*, 8(7):5839–5849, 2021.

[22] Long Cheng, Fang Liu, and Danfeng (Daphne) Yao. Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, 7(5):e1211, 2017.

[23] Stefano Chessa, Roberto Di Pietro, Erina Ferro, Gaetano Giunta, and Gabriele Oligeri. Mobile application security for video streaming authentication and data integrity combining digital signature and watermarking techniques. In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pages 634–638, 2007.

[24] T Charles Clancy, Negar Kiyavash, and Dennis J Lin. Secure smartcardbased fingerprint authentication. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52, 2003.

[25] A. Cocioceanu, M. Barbulescu, T. Ivanoaica, M. Raportaru, and A. I. Nicolin. Testing voice-based biometrics authentication platforms for romanian utterances through infrequent consonant clusters. In *2016 15th RoEduNet Conference: Networking in Education and Research*, pages 1–4, 2016.

[26] Elisa Costante, Davide Fauri, Sandro Etalle, Jerry Den Hartog, and Nicola Zannone. A hybrid framework for data loss prevention and detection. In *2016 IEEE security and privacy workshops*, pages 324–333. IEEE, 2016.

[27] Federico Cozza, Alfonso Guarino, Francesco Isernia, Delfina Malandrino, Antonio Rapuano, Raffaele Schiavone, and Rocco Zaccagnino. Hybrid and lightweight detection of third party tracking: Design, implementation, and evaluation. *Computer Networks*, 167:106993, 2020.

[28] Gibbons Damiana, Alecia Magnifico, Eduardo S. Junqueira, Laura Nicosia, and Michael Wagner. Book Review: Multimodal Pedagogies in Diverse Classrooms: Representation, Rights and Resources, the Digital Pencil: One-to-One Computing for Children, the Second Life Herald: The Virtual Tabloid That Witnessed the Dawn of the Metaverse, the Media and International Communication. *E-Learning and Digital Media*, 5(4):497–507, 2008.

[29] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and YoungHo Park. Design of secure and lightweight authentication protocol for wearable devices environment. *IEEE Journal of Biomedical and Health Informatics*, 22(4):1310–1322, 2018.

[30] G.A. Di Lucca, A.R. Fasolino, M. Mastoianni, and P. Tramontana. Identifying cross site scripting vulnerabilities in web applications. In *Proceedings. Sixth IEEE International Workshop on Web Site Evolution*, pages 71–80, 2004.

[31] Cynthia Dwork. Differential privacy: A survey of results. In Manindra Agrawal, Dingzhu Du, Zhenhua Duan, and Angsheng Li, editors, *Theory and Applications of Models of Computation*, pages 1–19, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[32] Khaled Elshazly, Yaser Fouad, Mohamed Saleh, and Adel Sewisy. A survey of sql injection attack detection and prevention. *Journal of Computer and Communications*, 02:1–9, 01 2014.

[33] Fan Fang, Carmine Ventre, Michail Basios, Leslie Kanthan, David Martinez-Rego, Fan Wu, and Lingbo Li. Cryptocurrency trading: a comprehensive survey. *Financial Innovation*, 8(1):1–59, 2022.

[34] Yong Fang, Yang Li, Liang Liu, and Cheng Huang. Deepxss: Cross site scripting detection based on deep learning. In *Proceedings of the 2018 International Conference on Computing and Artificial Intelligence*, ICCAI 2018, page 47–51, New York, NY, USA, 2018. Association for Computing Machinery.

[35] Zhixin Fang, Libai Cai, and Gang Wang. MetaHuman Creator The starting point of the metaverse. In *2021 International Symposium on Computer Technology and Information Science (ISCTIS)*, pages 154–157, June 2021.

[36] Allan G. B. Fisher. Production, Primary, Secondary and Tertiary. *Economic Record*, 15(1):24–38, 1939.

[37] Jiajia Ge. Multiple Influences of Intelligent Technology on Network Behavior of College Students in the Metaverse Age. *Journal of Environmental and Public Health*, 2022:e2750712, June 2022.

[38] Diksha Goel and Ankit Kumar Jain. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers Security*, 73:519–544, 2018.

[39] Seena Gressin. The equifax data breach: What to do. *Federal Trade Commission*, 8, 2017.

[40] Dean A. F. Gui, Lan Li, Dora Wong, and Gigi Au Yeung. 'Good to use for virtual consultation time': Second Life activities for and beyond the technical and web-based English writing classroom. *Metaverse Creativity*, 2(1):57–76, 2012.

[41] Hicham Hammouchi, Othmane Cherqi, Ghita Mezzour, Mounir Ghogho, and Mohammed El Koutbi. Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, 151:1004–1009, 2019.

[42] Omar Hasan, Benjamin Habegger, Lionel Brunie, Nadia Bennani, and Ernesto Damiani. A discussion of privacy challenges in user profiling with big data techniques: The eexcess use case. In *2013 IEEE International Congress on Big Data*, pages 25–30, 2013.

[43] Masahito Hayashi and Ángeles Vázquez-Castro. Physical layer security protocol for poisson channels for passive man-in-the-middle attack. *IEEE Transactions on Information Forensics and Security*, 15:2295–2305, 2020.

[44] Chu Huang, Qianzhen Zhang, Deke Guo, Xiang Zhao, and Xi Wang. Discovering association rules with graph patterns in temporal networks. *Tsinghua Science and Technology*, 28(2):344–359, 2023.

[45] W. Ronny Huang, Jonas Geiping, Liam Fowl, Gavin Taylor, and Tom Goldstein. Metapoison: Practical general-purpose clean-label data poisoning. In H. Larochelle, M. Ranzato, R. Hadsell, M.F. Balcan, and H. Lin, editors, *Advances in Neural Information Processing Systems*, volume 33, pages 12080–12091. Curran Associates, Inc., 2020.

[46] Yan Huang, Zhipeng Cai, and Anu G. Bourgeois. Search locations safely and accurately: A location privacy protection algorithm with accurate service. *Journal of Network and Computer Applications*, 103:146–156, 2018.

[47] Yan Huang, Xin Guan, Hongyang Chen, Yi Liang, Shanshan Yuan, and Tomoaki Ohtsuki. Risk assessment of private information inference for motion sensor embedded iot devices. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 4(3):265–275, 2020.

[48] William Hurst, Frida Ruiz Mendoza, and Bedir Tekinerdogan. Augmented Reality in Precision Farming: Concepts and Applications. *Smart Cities*, 4(4):1454–1468, December 2021.

[49] Thien Huynh-The, Quoc-Viet Pham, Xuan-Qui Pham, Thanh Thi Nguyen, Zhu Han, and Dong-Seong Kim. Artificial Intelligence for the Metaverse: A Survey, February 2022.

[50] Qi Jiang, Jianfeng Ma, Chao Yang, Xindi Ma, Jian Shen, and Shehzad Ashraf Chaudhry. Efficient end-to-end authentication protocol for wearable health monitoring sys-

tems. *Computers Electrical Engineering*, 63:182–195, 2017.

[51] Nikolaos Karapanos and Srdjan Capkun. On the effective prevention of tls man-in-the-middle attacks in web applications. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, page 671–686, USA, 2014. USENIX Association.

[52] Samar Samir Khalil, Sherin M. Youssef, and Sherine Nagy Saleh. icaps-dfake: An integrated capsule-based model for deepfake image and video detection. *Future Internet*, 13(4), 2021.

[53] Michel Kilzi. The new virtual economy of the metaverse, 2022.

[54] Engin Kirda, Nenad Jovanovic, Christopher Kruegel, and Giovanni Vigna. Client-side cross-site scripting protection. *Computers Security*, 28(7):592–604, 2009.

[55] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. Goodbye tracking? impact of iOS app tracking transparency and privacy labels. In *2022 ACM Conference on Fairness, Accountability, and Transparency*. ACM, jun 2022.

[56] Aleksandra Korolova and Vinod Sharma. Cross-app tracking via nearby bluetooth low energy devices. CODASPY '18, page 43–52, New York, NY, USA, 2018. Association for Computing Machinery.

[57] Nikolaos Koutroumpouchos, Georgios Lavdanis, Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. Objectmap: Detecting insecure object deserialization. In *Proceedings of the 23rd Pan-Hellenic Conference on Informatics*, pages 67–72, 2019.

[58] Logan Kugler. Non-fungible tokens and the future of art. *Communications of the ACM*, 64(9):19–20, September 2021.

[59] Bokyung Kye, Nara Han, Eunji Kim, Yeonjeong Park, and Soyoung Jo. Educational applications of metaverse: possibilities and limitations. *Journal of Educational Evaluation for Health Professions*, 18, December 2021.

[60] Ronald Leenes. Privacy Regulation in the Metaverse. pages 123–136, 2009.

[61] Guoliang Li, Chengliang Chai, Ju Fan, Xueping Weng, Jian Li, Yudian Zheng, Yuanbing Li, Xiang Yu, Xiaohang Zhang, and Haitao Yuan. Cdb: Optimizing queries with crowd-based selections and joins. In *Proceedings of the 2017 ACM International Conference on Management of Data*, New York, NY, USA, 2017. Association for Computing Machinery.

[62] Xiang-Yang Li, Chunhong Zhang, Taeho Jung, Jianwei Qian, and Linlin Chen. Graph-based privacy-preserving data publication. In *Proceedings ofhe 35th Annual IEEE International Conference on Computer Communications*, pages 1–9, 2016.

[63] Yi Joy Li, Cody Ducleroir, Tyler Ian Stollman, and Elena Wood. Parkinson's Disease Simulation in Virtual Reality for Empathy Training in Medical Education. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 56–59, March 2021.

[64] Xueting Liao, Danyang Zheng, and Xiaojun Cao. Coronavirus pandemic analysis through tripartite graph clustering in online social networks. *Big Data Mining and Analytics*, 4(4):242–251, 2021.

[65] Jiabin Liu, Chengliang Chai, Yuyu Luo, Yin Lou, Jianhua Feng, and Nan Tang. Feature augmentation with reinforcement learning. In *2022 IEEE 38th International Conference on Data Engineering (ICDE)*, pages 3360–3372, 2022.

[66] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, 1(1):3–es, mar 2007.

[67] Neal Mangaokar and Atul Prakash. Dispelling misconceptions and characterizing the failings of deepfake detection. *IEEE Security Privacy*, 20(2):61–67, 2022.

[68] Sunu Mathew, Michalis Petropoulos, Hung Q Ngo, and Shambhu Upadhyaya. A data-centric approach to insider attack detection in database systems. In *International Workshop on Recent Advances in Intrusion Detection*, pages 382–401. Springer, 2010.

[69] Huansheng Ning, Sahraoui Dhelim, Mohammed Amine Bouras, Amar Khelloufi, and Ata Ullah. Cyber-Syndrome and its Formation, Classification, Recovery and Prevention. *IEEE Access*, 6:35501–35511, 2018.

[70] Chaoyue Niu, Zhenzhe Zheng, Fan Wu, Shaojie Tang, Xiaofeng Gao, and Guihai Chen. Unlocking the value of privacy: Trading aggregate statistics over private correlated data. KDD '18, page 2031–2040, New York, NY, USA, 2018. Association for Computing Machinery.

[71] Open Web Application Security Project (OWASP). XSS Prevention Cheat Sheet. `https://cheatsheetseries.owasp.org/cheatsheets/DOM_based_XSS_Prevention_Cheat_Sheet.html`, 2021.

[72] Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin, and Aikaterini Mitrokotsa. On the leakage of information in biometric authentication. In *International Conference on Cryptology in India*, pages 265–280. Springer, 2014.

[73] Junjie Pang, Yan Huang, Zhenzhen Xie, Qilong Han, and Zhipeng Cai. Realizing the heterogeneity: A self-organized federated learning framework for iot. *IEEE Internet of Things Journal*, 8(5):3088–3098, 2021.

[74] Junjie Pang, Yan Huang, Zhenzhen Xie, Jianbo Li, and Zhipeng Cai. Collaborative city digital twin for the covid-19 pandemic: A federated learning solution. *Tsinghua Science and Technology*, 26(5):759–771, 2021.

[75] Or Peles and Roee Hay. One class to rule them all: 0-day deserialization vulnerabilities in android. In *9th USENIX workshop on offensive technologies (WOOT 15)*, 2015.

[76] Renana Peres, Martin Schreier, David A Schweidel, and Alina Sorescu. Blockchain meets marketing: Opportunities, threats, and avenues for future research, 2022.

[77] Vu Viet Hoang Pham, Shui Yu, Keshav Sood, and Lei Cui. Privacy issues in social networks and analysis: a comprehensive survey. *IET Networks*, 7(2):74–84, 2018.

[78] D.W. PINE. Into the metaverse. *Time*.

[79] Wen Qi, Yichen Xu, Wanfu Ding, Yonghang Jiang, Jianping Wang, and Kejie Lu. Privacy leaks when you play games: A novel user-behavior-based covert channel on smartphones. In *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*, pages 201–211, 2015.

[80] Li Qian, Zhenyuan Zhu, Jun Hu, and Shuying Liu. Research of sql injection attack and prevention technology. In *2015 International Conference on Estimation, Detection and Information Fusion*, pages 303–306, 2015.

[81] Shuming Qiu, Ding Wang, Guoai Xu, and Saru Kumari. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. *IEEE Transactions on Dependable and Secure Computing*, 19(2):1338–1351, 2022.

[82] Martin Roesch. Lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX conference on System administration, Nov.*, pages 229–238, 1999.

[83] F. David Rose, Barbara. M. Brooks, and Albert A. Rizzo. Virtual Reality in Brain Damage Rehabilitation: Review. *CyberPsychology & Behavior*, 8(3):241–262, June 2005.

[84] Fatima Salahdine and Naima Kaabouch. Social Engineering Attacks: A Survey. *Future Internet*, 11(4):89, April 2019.

[85] Ted E Senator, Henry G Goldberg, Alex Memory, William T Young, Brad Rees, Robert Pierce, Daniel Huang, Matthew Reardon, David A Bader, Edmond Chow, et al. Detecting insider threats in a real corporate database of computer usage activity. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1393–1401, 2013.

[86] Yuri Shapira, Bracha Shapira, and Asaf Shabtai. Content-based data leakage detection using extended fingerprinting. *arXiv preprint arXiv:1302.2028*, 2013.

[87] Jingxue Sun, Zhiqiu Huang, Ting Yang, Wengjie Wang, and Yuqing Zhang. A system for detecting third-party tracking through the combination of dynamic analysis and static analysis. In *IEEE Conference on Computer Communications Workshops*, pages 1–6, 2021.

[88] Miao Sun, Gurjeet Singh, and Patrick Yin Chiang. Antigan: Discriminating 3d reconstructed and real faces for robust facial identity in anti-spoofing generator adversarial network. In *2020 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pages 1–8, 2020.

[89] LATANYA SWEENEY. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[90] Mark Taubert, Lucie Webber, Timothy Hamilton, Madeleine Carr, and Mark Harvey. Virtual reality videos used in undergraduate palliative and oncology medical teaching: results of a pilot study. *BMJ supportive & palliative care*, 9(3):281–285, September 2019.

[91] Jane Thomason. Metaverse, Token Economies, and Chronic Diseases. *Global Health Journal*, July 2022.

[92] Bogdan Walek and Ondrej Pektor. Data mining of job requirements in online job advertisements using machine learning and sdca logistic regression. *Mathematics*, 9(19), 2021.

[93] Chenyu Wang, Zhipeng Cai, and Yingshu Li. Sustainable blockchain-based digital twin management architecture for iot devices. *IEEE Internet of Things Journal*, pages 1–1, 2022.

[94] Ding Wang and Ping Wang. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE transactions on dependable and secure computing*, 15(4):708–722, 2016.

[95] Fei-Yue Wang, Rui Qin, Xiao Wang, and Bin Hu. MetaSocieties in Metaverse: MetaEconomics and MetaManagement for MetaEnterprises and MetaCities. *IEEE Transactions on Computational Social Systems*, 9(1):2–7, February 2022.

[96] Dave Wichers and Jeff Williams. Owasp top-10 2017. *OWASP Foundation*, 3:4, 2017.

[97] Zhenzhen Xie, Yan Huang, Dongxiao Yu, Reza M. Parizi, Yanwei Zheng, and Junjie Pang. Fedee: A federated graph learning solution for extended enterprise collaboration. *IEEE Transactions on Industrial Informatics*, pages 1–10, 2022.

[98] Zuobin Xiong, Zhipeng Cai, Chunqiang Hu, Daniel Takabi, and Wei Li. Towards neural network-based communication system: Attack and defense. *IEEE Transactions on Dependable and Secure Computing*, pages 1–14, 2022.

[99] Dawei Yang, Jian Zhou, Rongchang Chen, Yuanlin Song, Zhenju Song, Xiaoju Zhang, Qi Wang, Kai Wang, Chengzhi Zhou, Jiayuan Sun, Lichuan Zhang, Li Bai, Yuehong Wang, Xu Wang, Yeting Lu, Hongyi Xin, Charles A. Powell, Christoph Thüemmler, Niels H. Chavannes, Wei Chen, Lian Wu, and Chunxue Bai. Expert consensus on the metaverse in medicine. *Clinical eHealth*, 5:1–9, December 2022.

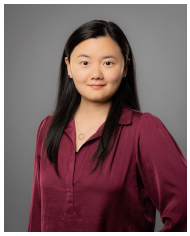
[100] Shijie Zhang, Hongzhi Yin, Tong Chen, Zi Huang, Lizhen Cui, and Xiangliang Zhang. Graph embedding for recommendation against attribute inference attacks. In *Proceedings of the Web Conference 2021*, WWW '21, page 3002–3014, New York, NY, USA, 2021. Association for Computing Machinery.

[101] Xu Zheng and Zhipeng Cai. Privacy-preserved data sharing towards multiple parties in industrial iots. *IEEE Journal on Selected Areas in Communications*, 38(5):968–979, 2020.

[102] Wenmin Zhu, Xiumin Fan, and Yanxin Zhang. Applications and research trends of digital human models in the manufacturing industry. *Virtual Reality & Intelligent Hardware*, 1(6):558–579, December 2019.

[103] Maheen Zulfiqar, Fatima Syed, Muhammad Jaleed Khan, and Khurram Khurshid. Deep face recognition for biometric authentication. In *2019 international conference on electrical, communication, and computer engineering (ICECCE)*, pages 1–6. IEEE, 2019.

Yan Huang is currently an Assistant Professor in the Department of Software Engineering Game Development at Kennesaw State University (KSU). Dr. Huang received his Ph.D. degree in the Department of Computing Science at Georgia State University. He is broadly interested in privacy and security, with particular emphasis on deep learning aided privacy protection solutions and cybersecurity challenges in the IoT environment.



Yi (Joy) Li received her Ph.D. and M.S. degree in Computer Science from the University of Louisville, KY in 2018. She is currently an assistant professor of Computer Game Design and Development in the Department of Software Engineering and Game Development at Kennesaw State University. Her research interests focus on affective gaming, eXtended reality (XR), and human-computer interaction. She has extensive experience in gamification for education, and makes an effort in applying gaming tools in healthcare, such as training for empathy or intervention on mental disorders.

Zhipeng Cai received his Ph.D. and M.S. degrees in the Department of Computing Science at the University of Alberta and a B.S. degree from Beijing Institute of Technology. Dr. Cai is currently an Assistant Professor in the Department of Computer Science at Georgia State University. His research agenda focuses on networking, privacy, and big data. He has published more than 50 journal papers, including more than 20 IEEE/ACM Transactions papers, such as in IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Dependable and Secure Computing, IEEE/ACM Transactions on Networking, and IEEE Transactions on Mobile Computing. Dr. Cai is the recipient of an NSF CAREER Award. He is an editor/guest editor for Algorithmica, Theoretical Computer Science, Journal of Combinatorial Optimization, and IEEE/ACM Transactions on Computational Biology and Bioinformatics. He is a senior member of the IEEE.