A Survey on Metaverse: Fundamentals, Security, and Privacy

Yuntao Wang†, Zhou Su†, Ning Zhang‡, Dongxiao Liu§, Rui Xing†, Tom H. Luan¶, Xuemin Shen§
†School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an, China
‡Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada
§Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada
¶School of Cyber Engineering, Xidian University, Xi'an, China

***Abstract*—Metaverse, as an evolving paradigm of the next-generation Internet, aims to build a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space for humans to play, work, and socialize. Driven by recent advances in emerging technologies such as extended reality, artificial intelligence, and blockchain, metaverse is stepping from the science fiction to an upcoming reality. However, severe privacy invasions and security breaches (inherited from underlying technologies or emerged in the new digital ecology) of metaverse can impede its wide deployment. At the same time, a series of fundamental challenges (e.g., scalability and interoperability) can arise in metaverse security provisioning owing to the intrinsic characteristics of metaverse, such as immersive realism, hyper spatiotemporality, sustainability, and heterogeneity. In this paper, we present a comprehensive survey of the fundamentals, security, and privacy of metaverse. Specifically, we first investigate a novel distributed metaverse architecture and its key characteristics with ternary-world interactions. Then, we discuss the security and privacy threats, present the critical challenges of metaverse systems, and review the state-of-the-art countermeasures. Finally, we draw open research directions for building future metaverse systems.**

***Index Terms*—Metaverse, security, privacy, distributed virtual worlds, extended reality, artificial intelligence, and blockchain.**

I. Introduction

The metaverse, literally a combination of the prefix "meta" (meaning transcendence) and the suffix "verse" (shorthand for universe), is a computer-generated world with a consistent value system and an independent economic system linked to the physical world [1]. The term metaverse was created by Neil Stephenson in his science fiction novel named *Snow Crash* in 1992. In this novel, humans in the physical world enter and live in the metaverse (a parallel virtual world) through digital avatars (in analogy to user's physical self) via virtual reality (VR) equipment. Since its first appearance, the concept of metaverse is still evolving with various descriptions, such as a second life [2], 3D virtual worlds [3], and life-logging [4]. Commonly, the metaverse is regarded as a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space blending the ternary physical, human, and digital worlds [5], [6]. Metaverse is recognized as an evolving paradigm of the next-generation Internet after the web and the mobile Internet revolutions [7], where users can live as digital natives and experience an alternate life in virtuality.

The metaverse integrates a variety of emerging technologies [1], [6], [8]. In particular, digital twin produces a mirror image of the real world, VR and augmented reality (AR) provide immersive 3D experience, 5G and beyond offers ultra-high reliable and ultra-low latency connections for massive metaverse devices, wearable sensors and brain-computer interface (BCI) enable user/avatar interaction in the metaverse, artificial intelligence (AI) enables the large-scale metaverse creation and rendering, and blockchain and non-fungible token (NFT) play an important role in determining authentic rights for metaverse assets [1]. Currently, with the popularity of smart devices and the maturity of enabling technologies, the metaverse is stepping out of its infancy into an upcoming reality in the near future. Furthermore, significant innovations and advances in above emerging technologies are giving birth to a new information ecology and new demands for applications, as well as the metaverse for becoming a platform of the new ecology and applications [8]. Driven by realistic demands and the prospect of feasibility of metaverse construction, metaverse recently has attracted increasing attention from around the world and many tech giants such as Facebook, Microsoft, Tencent, and NVIDIA have announced their ventures into Metaverse. Particularly, Facebook rebranded itself as "meta" to dedicate itself to building the future metaverse [9].

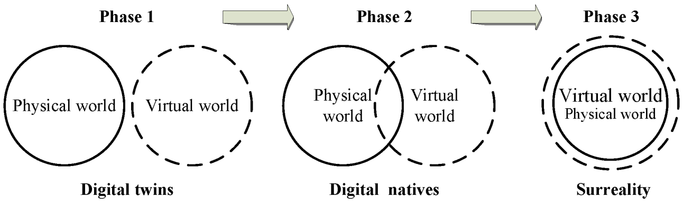

Fig. 1. Three phases of the development of the metaverse.

Generally, the development of metaverse consists of three successive phases from a macro perspective [6]: (i) *digital twins*, (ii) *digital natives*, and eventually (iii) *surreality*, as depicted in Fig. 1. The first phase produces a mirror world consisting of large-scale and high-fidelity digital twins of humans and things in virtual environments, aimed for a vivid digital representation of the physical reality. In this phase, virtual activities and properties such as user emotion and movement are imitations of their physical counterparts, where reality and virtuality are two parallel spaces. The second phase mainly focuses on the native content creation, where digital natives represented by avatars can produce innovations and insights inside the digital worlds and such digital creations may only exist in the virtual spaces. In this phase, the massively created contents in the digital world become equal with their physical counterparts, and the digital world has the ability to transform and innovate the production process of the physical world, thereby creating more intersections between these two worlds. The metaverse grows to its maturity in the last phase and turns into a persistent and self-sustaining surreality world which assimilates the reality into itself. The seamless integration and mutual symbiosis of physical and virtual worlds will be realized in this phase, where the scope of virtual world will be larger than that of real world and more scenes and lives that do not exist in reality can exist in virtual realms.

A. Challenges for Securing Metaverse

In spite of the promising sign of metaverse, security and privacy issues are the prime concerns that hinder its further development. A wide range of security breaches and privacy invasions may arise in the metaverse from the management of massive data streams, pervasive user profiling activities, unfair outcomes of AI algorithms, to the safety of physical infrastructures and human bodies. Firstly, since metaverse integrates a variety of latest technologies and systems built on them as its basis, their vulnerabilities and intrinsic flaws may also be inherited by the metaverse. There have been risk incidents of emerging technologies, such as hijacking of wearable devices or cloud storage, theft of virtual currencies, and the misconduct of AI to produce fake news. Secondly, driven by the interweaving of various technologies, the effects of existing threats can be amplified and become more severe in virtual worlds, while new threats nonexistent in physical and cyber spaces can breed such as virtual stalking and virtual spying [10]. Particularly, the personal data involved in the metaverse can be more granular and unprecedentedly ubiquitous to build a digital copy of the real world, which opens new horizons for crimes on private big data [11]. For example, to build a virtual scene using AI algorithms, users will inevitably wear wearable AR/VR devices with built-in sensors to comprehensively collect brain wave patterns, facial expressions, eye movements, hand movements, speech and biometric features, as well as the surrounding environment. Besides, as users need to be uniquely identified in the metaverse, it means that headsets, VR glasses, or other devices can be used for tracking of users' real locations illegally. Lastly, hackers can exploit system vulnerabilities and compromise devices as entry points to invade real-world equipments such as household appliances to threaten personal safety, and even threaten critical infrastructures such as power grid systems, high-speed rail systems, and water supply systems via advanced persistent threat (APT) attacks [12].

Nevertheless, existing security countermeasures can still be ineffective and lack adaptability for metaverse applications. Particularly, the intrinsic characteristics of metaverse including *immersiveness*, *hyper spatiotemporality*, *sustainability*, *interoperability*, *scalability*, and *heterogeneity* may bring about a series of challenges for efficient security provision. 1) The real-time fully immersive experience in the metaverse brings not only sensual pleasures of the flawless virtual environment, but also challenges in the secure fusion of massive multimodal user-sensitive big data for interactions between users and avatars/environments. 2) The integration of the ternary world contributes to the hyper spatiotemporality in the metaverse [13], which greatly increases the complexity and difficulty of trust management. Due to the deepening blurring of the boundary between the real and the virtual, the metaverse will make the fact and fiction more confusing such as Deepfake event, especially for regulations and digital forensics. 3) To get rid of the single point of failure (SPoF) and the control by a few powerful entities, the metaverse should be built on a decentralized architecture to be self-sustaining and persistent [14], which raises severe challenges in reaching unambiguous consensus among massive entities in the time-varying metaverse. 4) The interoperability and scalability in the metaverse indicates users can freely shuttle across various sub-metaverses concurrently under different scenes and interaction modes [15], which also pose challenges to ensure fast service authorization, compliance auditing, and accountability enforcement in seamless service mitigation and multi-source data fusion. 5) The virtual worlds in the large-scale metaverse can be highly heterogeneous in terms of hardware implementation, communication interfaces, and softwares, which poses huge interoperability difficulties.

B. Related Works

The topic of metaverse has attracted various research attention. Until now, there have been several survey papers from different aspects of the metaverse. For example, Dionisio *et al.* [3] specify four characteristics of viable 3D virtual worlds (or metaverse) including ubiquity, realism, scalability, and interoperability, and discuss ongoing improvements of the underlying virtual world technology. Lee *et al.* [6] review and examine eight fundamental technologies to build up the metaverse as well as its opportunities from six user-centric factors. Yang *et al.* [1] investigate the potential of AI and blockchain technologies for future metaverse construction. Ning *et al.* [5] present a survey of the development status of metaverse in terms of national policies, industrial projects, infrastructures, supporting technologies, VR, and social metaverse. Park *et al.* [16] discuss three components (i.e., hardware, software, and content) of metaverse and review the user interaction, implementation, and representative applications in the metaverse. Leenes [10] investigate potential privacy risks in the online game *Second Life* from both social and legal perspectives. Different from the above existing surveys on the general metaverse [3], [5], [6], [10] or the potential in service provisioning in social VR/AR games [11], retailing [17], education [18], social goods [8], and computational arts [19], we focus on the perspective of metaverse security and privacy such as potential security/privacy threats, critical security/privacy challenges, and state-of-the-art defenses, etc.

In this paper, we present a comprehensive survey on the fundamentals of metaverse, as well as the key challenges and solutions to build the secure and privacy-preserving metaverse. The contributions of this survey are four-fold.

- We discuss the fundamentals of metaverse including the general architecture, key characteristics, and enabling tech-

TABLE I
A Comparison of Contribution Between Our Survey and Relevant Surveys

Year.	Refs.	Contribution
2008	[10]	Discussions on privacy risks in the game *Second Life* from both social and legal perspectives.
2009	[17]	Survey on metaverse applications in terms of retailing.
2013	[3]	Discussions on key features of metaverse and ongoing improvements of the underlying virtual world technology.
2018	[11]	Survey on privacy issues and countermeasures related to digital footprints in social metaverse games.
2020	[18]	Survey on metaverse applications in terms of education.
2021	[8]	Survey on metaverse applications in terms of social goods.
2021	[6]	Review on eight fundamental technologies to build up the metaverse and its opportunities from six user-centric factors.
2021	[5]	Overview of metaverse development in terms of national policies, industrial projects, infrastructures, supporting technologies, VR, and social metaverse.
2021	[19]	Survey on metaverse applications in terms of digital arts.
2022	[1]	Discuss the potential of AI and blockchain technologies in future metaverse construction.
2022	[16]	Discuss the hardware, software, and content components of metaverse and review user interaction, implementation, and representative applications in the metaverse.
Now	**Ours**	Comprehensive survey of the fundamentals, security, and privacy of metaverse, discussions on the general architecture, characteristics, and security/privacy threats of the metaverse, discussions on critical challenges, state-of-the-art solutions, and future research directions in building the secure metaverse.

nologies, as well as existing modern prototypes of metaverse applications.
- We investigate the security and privacy threats in the metaverse from seven aspects (i.e., identity, data, privacy, network, economy, governance, and physical/social effects) and discuss the critical challenges to address them.
- We survey the state-of-the-art security and privacy countermeasures and discuss their feasibility toward building the secure and privacy-preserving metaverse paradigm.
- We outline open future research directions in building the secure, privacy-preserving, and efficient metaverse realm.

Table I summarizes the contribution of our work in comparison to previous relevant surveys in the metaverse.

The remainder of this paper is organized as follows. Section II presents the architecture, characteristics, supporting technologies, and current prototypes of the metaverse. Section III presents the taxonomy of security and privacy threats in the metaverse and Section IV discusses the critical challenges and existing/potential solutions to resolve them. Then, we discuss open research issues in Section V. Finally, we draw the conclusions in Section VI. The key acronyms are listed in Table II.

II. An Overview of Metaverse

In this section, we introduce the metaverse from the following aspects: the general architecture, key characteristics, enabling technologies, potential applications, and existing prototypes.

A. *Metaverse Architecture*

Metaverse is a self-sustaining, hyper spatiotemporal, and 3D immersive virtual shared space, created by the convergence of physically persistent virtual space and virtually enhanced physical reality. The construction of metaverse blends the ternary physical, human, and digital worlds. Fig. 2 shows the general architecture of the metaverse with consideration of its intrinsic ternicity. Human users along with their inner psychologies and social interactions constitute the human world. The physical world contains the smart objects/devices (to interact with both the digital and human worlds) and network and computing infrastructures (to support efficient data transmission and processing). According to IEEE 2888 standards [15], the digital world can be composed of a series of interconnected distributed virtual worlds (i.e., sub-metaverses), and each sub-metaverse can offer certain kinds of services (e.g., gaming, social dating, online museum, and online concert) to users represented as avatars.

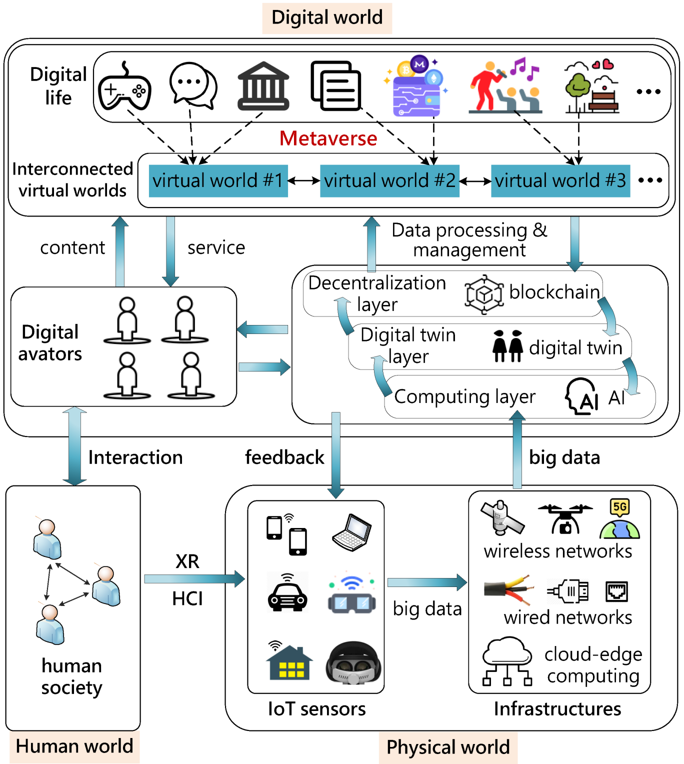

Fig. 2. The architecture of metaverse in integration of the human, physical, and digital worlds.

1) Information Sources of Metaverse: There are two main sources of information in the metaverse: one is the input of the real world (i.e., the knowledge and information of real space digitally displayed in virtual space), and the other is the output of virtual worlds (i.e., the information generated by avatars, digital objects, and metaverse services in virtual space).

The metaverse is regarded as human-centric [20]. Generally, with the assistance of human-computer interaction (HCI) and extended reality (XR) technologies [21], users situated in physical environments are able to control their digital avatars in the metaverse for diverse collective and social activities such as car racing, dating, and virtual item trading (as depicted in the film *Ready Player One*). The virtual economy as a spontaneous derivative of such activities can be built in the metaverse. Information is the core resource of the metaverse and the free data flow in the ternary world makes the digital ecology, which eventually promotes the integration of virtual

TABLE II
SUMMARY OF IMPORTANT ABBREVIATIONS IN ALPHABETICAL ORDER

Abbr.	Definition	Abbr.	Definition	Abbr.	Definition
ABE	Attribute-Based Encryption	AR	Augmented Reality	AI	Artificial Intelligence
APT	Advanced Persistent Threat	BCI	Brain-Computer Interface	B5G	Beyond 5G
CA	Certificate Authority	CPSS	Cyber-Physical-Social System	DL	Deep Learning
DP	Differential Privacy	ECG	Electrocardiogram	FL	Federated Learning
GDPR	General Data Protection Regulation	HCI	Human-Computer Interaction	HE	Homomorphic Encryption
IoT	Internet of Things	MMO	Massive Multi-player Online	MR	Mixed Reality
NFT	Non-Fungible Token	NPC	Non-Player Character	OSN	Online Social Network
PUGC	Professional- and User-Generated Content	PGC	Professional-Generated Content	PKI	Public Key Infrastructure
PPG	Photoplethysmography	SDN	Software-Defined Network	SSI	Self-Sovereign Identity
SMC	Secure Multi-party Computation	SPoF	Single Point of Failure	SVM	Support Vector Machine
QoE	Quality-of-Experience	QoS	Quality-of-Service	UGC	User-Generated Content
VR	Virtual Reality	XR	Extended Reality	ZKP	Zero-Knowledge Proof

and actual worlds. Particularly, AI algorithms perform large-scale metaverse rending and service offering in the computing layer. The knowledge derived from the computing layer can be beneficial to perform digitalizing and mirroring the real world via digital twin technology in the digital twin layer. Finally, the created digital twins, as well as created naive contents by avatars, can be transparently managed, uniquely tokenized, and monetized by the blockchain technology in the decentralization layer to build the economic system and value system in the metaverse. More details of these technologies are elaborated at Sect. II-C. Next, we discuss the information flow in a single world and across different worlds, respectively.

2) In-World Information Flow: The human society or human world is interconnected by the social network and formed based on common activities and mutual interactions among human beings.

In the physical world, IoT plays an important role in digitalizing the physical world via pervasive sensors and the generated IoT big data is transmitted and processed via physical infrastructures. Specifically, networking connectivity is provided via wireless or wired networks and powerful computation and storage capacities are provisioned via cloud-edge computing. For data communications, cellular base stations, unmanned aerial vehicle (UAV) networks, satellite networks, etc., form heterogeneous space-air-ground integrated networks (SAGINs) [22], together with wired networks, provide seamless, ubiquitous, and low-latency network accesses to metaverse services.

In the digital world, the produced digital information of the physical and human worlds are processed and managed via technologies such as AI, blockchain, and digital twin to support large-scale metaverse creation and various services built upon it. Besides, users, represented as avatars in the metaverse, can produce and distribute digital contents across various platforms in different sub-metaverses to promote the creativity of metaverse ecology.

3) Information Flow Across Worlds: As depicted in Fig. 2, the subjective consciousness, the Internet, and the IoT are the main media among the three worlds.

Humans observe objective information from the physical world, transform it into knowledge and intelligence through subjective consciousness, and then use them as guidance to change the objective world. Besides, humans can interact with the physical objects via HCI technology and experience virtually augmented reality (e.g., holographic telepresence) via XR technology.

The human world and the digital world are connected through the Internet, i.e., the largest computer network in the world. Users can interact with the digital world via smart devices such as smartphones, wearable sensors, and VR helmets, for creation, sharing, and acquisition of knowledge.

The IoT bridges the physical world and the digital world by using inter-connected smart devices for digitalization, and thereby information can flow freely between the two worlds [23]. Besides, the feedback information from the digital world (e.g., processed results of big data and intelligent decisions) can guide the process of physical world to realize smart manufacturing, intelligent transportation, etc.

B. Key Characteristics of Metaverse

In web 1.0, Internet users are just content consumers, where contents are provided by the websites. In web 2.0 (i.e., mobile Internet), users are both content producers and consumers, and the websites turn into platforms for service offering. Typical such platforms include Wikipedia, WeChat, and TikTok. Metaverse is recognized as the evolving paradigm of web 3.0. In metaverse, we live as digital natives and create digital contents with avatars, which opens a new horizon for new services and applications, as shown in Fig. 3. Specifically, metaverse exhibits unique features from the following perspectives.

1) Immersiveness: The immersiveness means that the computer-generated virtual space is sufficiently realistic to allow users to feel psychologically and emotionally immersed. It can be also called *immersive realism* [3]. According to the perspective of realism, human beings interact with the environment through their senses and their bodies. The immersive realism can be approached through the structure of sensory perception (e.g., sight, sound, touch, temperature, and balance) and expression (e.g., gestures).

2) Hyper Spatiotemporality: The real world is restricted by the finiteness of space and the irreversibility of time. As metaverse is a virtual space-time continuum parallel to the real one, the hyper spatiotemporality refers to the break of limitations of time and space [5]. As such, users can freely shuttle across various worlds with different spatiotemporal

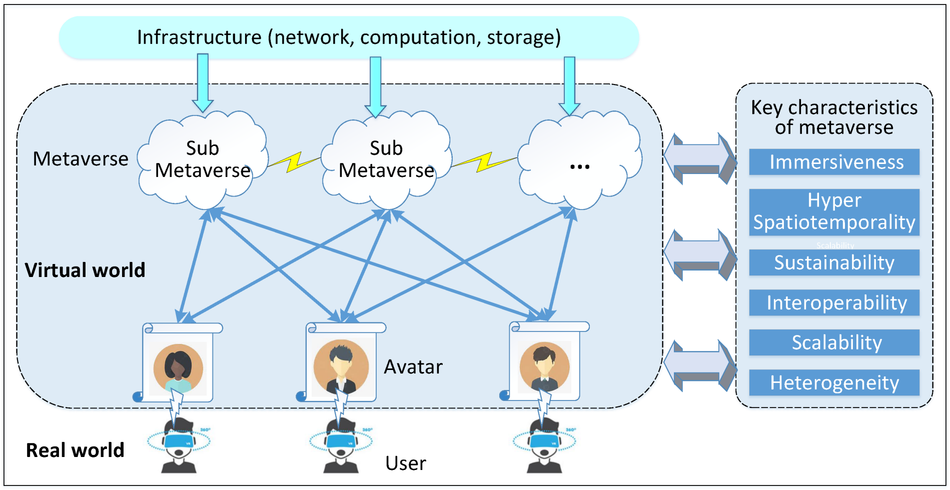

Fig. 3. General network architecture and key characteristics of the metaverse.

dimensions to experience an alternate life with seamless scene transformation.

3) Sustainability: The sustainability indicates that the metaverse maintains a closed economic loop and a consistent value system with a high level of independence. On the one hand, it should be *open*, i.e., continuously arousing users' enthusiasm in digital content creation as well as open innovations. On the other hand, to remain persistent, it should be built on a *decentralized* architecture to get rid of SPoF risks and prevent from being controlled by a few powerful entities.

4) Interoperability: The interoperability in the metaverse represents that (i) users can seamlessly move across virtual worlds (i.e., sub-metaverses) without interruption of the immersive experience [6], and (ii) digital assets for the rendering or reconstruction of virtual worlds are interchangeable across distinct platforms [3].

5) Scalability: The scalability refers to the capacity of metaverse to remain efficient with the number of concurrent users/avatars, the level of scene complexity, and the mode of user/avatar interactions (in terms of type, scope, and range) [3].

6) Heterogeneity: The heterogeneity of metaverse includes heterogeneous virtual spaces (e.g., with distinct implementations), heterogeneous physical devices (e.g., with distinct interfaces), heterogeneous data types (e.g., unstructured and structured), heterogeneous communication modes (e.g., cellular and satellite communications), as well as the diversity of human psychology. It also entails the poor interoperability of metaverse systems.

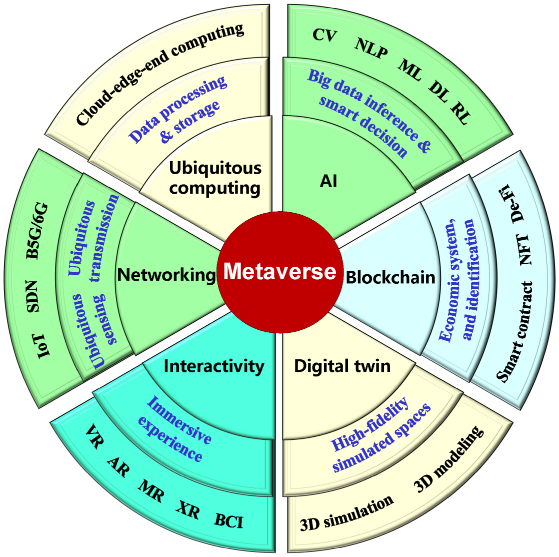

Fig. 4. The illustration of six underlying technologies including its roles and key components in the metaverse.

C. Enabling Technologies of Metaverse

As shown in Fig. 4, there are the following six enabling technologies underlying the metaverse.

1) Interactivity: With the maturity of miniaturized sensors, embedded technology, and XR technology, head-mounted displays or helmets are expected to be the main terminal for entering the metaverse [24]. The XR deeply incorporates virtual reality/augmented reality/mixed reality (VR/AR/MR) technologies to offer multi-sensory immersiveness, augmented experience, and real-time user/avator/environment interaction via front-projected holographic display, HCI (especially BCI), and large-scale 3D modeling [21]. The wearable sensors and XR devices perform fine-grained human-specific information perception, and indoor smart devices (e.g., cameras) perform ubiquitous sensing for objects and surroundings. In this manner, the user/avatar interactivity will no longer be limited to mobile inputs (e.g., hand-held phones and laptops), but all kinds of interactive devices connected to the metaverse. Besides, negative experience such as dizziness in wearing XR helmets can be resolved by low-latency edge computing systems and AI-based real-time rendering.

2) Digital Twin: Digital twin represents the digital clone of objects and systems in the real world with high integrity and consciousness [25]. It enables the mirroring of physical entities, as well as prediction and optimization of their virtual bodies, by analyzing real-time streams of sensory data, physical models, and historical information. In digital twin, data fed back from physical entities can be used for self-learning and self-adaption in the mirrored space. Moreover, digital twins can provide digital models of the expected objects with intended attributes in the metaverse with high accuracy through the simulation of complex physical processes and the assistance of AI technologies, which is beneficial for large-scale metaverse creation and rendering. Besides, digital twin enables predictive maintenance and accident traceability for physical safety, due to the bidirectional connection between physical entities and their virtual counterparts, thereby improving efficiency and reducing risks in the physical world.

3) Networking: In the metaverse, networking technologies such as 6G, software-defined network (SDN), and IoT empower the ubiquitous network access and real-time massive data transmission between real and virtual worlds, as well as between sub-metaverses. Beyond 5G (B5G) and 6G offer possibilities for ubiquitous, real-time, and ultra-reliable communications for massive metaverse devices with enhanced mobility support [26]. SDN enables the flexible and scalable management of large-scale metaverse network via the separation of the control plane and data plane. In SDN-based metaverse, the physical devices and resources are managed by a logically centralized controller using a standardized interface such as OpenFlow, thereby virtualized computation, storage, and bandwidth resources can be dynamically allocated according to real-time demands of various sub-metaverses [27]. Besides, IoT is a network of numerous physical objects that are embedded with sensors, softwares, communication components, and other technologies with the aim to connect, exchange, and process data between things, systems, clouds, and users over the Internet [28]. In the metaverse, IoT sensors are extensions of human senses.

4) Ubiquitous Computing: Ubiquitous computing, or ubicomp aims to create an environment where computing appears anytime and everywhere for users [29]. Through pervasive (often mobile) smart objects embedded in the environment or carried on the human body, ubiquitous computing enables smooth adaptation to the interactions between human users and the physical space. With ubicomp, instead of using specific equipment (e.g., laptop), human users can freely interact with their avatars and experience real-time immersive metaverse services via ubiquitous smart objects and network access in the environment. For improved user quality-of-experience (QoE) in ubicomp, the cloud-edge-end computing [30] orchestrates the highly scalable cloud infrastructures (with powerful computation and storage capacity) and heterogeneous edge computing infrastructures (closer to end users/devices) for flexible and on-demand resource allocation to satisfy various requirements of end users/devices in metaverse applications.

5) AI: AI technology acts as the "brain" of metaverse which empowers personalized metaverse services (e.g., vivid and customized avatar creation), massive metaverse scene creation and rendering, multilingual support in the metaverse by learning from historical experience via big data inference [1]. Moreover, AI enables the smart interaction (e.g., smart shopping guider and user movement prediction) between user and avatar/NPC (non-player character) via intelligent decision-making. For example, by continuously learning users' facial expressions, emotions, hairstyles, and so on, AI algorithms can create vivid and personalized avatars and intelligently recommend interested goods or information to users in the metaverse. Typically, there exist four types of AI models: supervised, unsupervised, semi-supervised, and reinforcement learning [31]. In supervised learning, labeled training samples are required, while unlabeled data applies to unsupervised learning. Semi-supervised learning falls in between these two. Reinforcement learning mainly focuses on smart decision-making under uncertain environments. Inspired by biological neural networks, deep learning (DL) has gained exciting advances in practice and becomes the hottest paradigm in the AI realm.

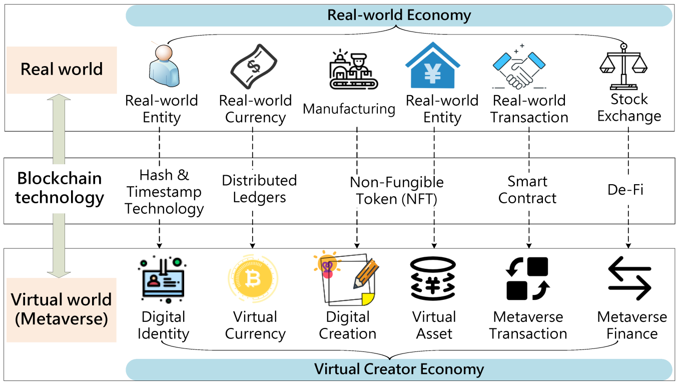

Fig. 5. The role of blockchain technologies in bridging the conventional economy and metaverse economy.

6) Blockchain: To be persistent, the metaverse should be constructed on a decentralized architecture to avoid centralization risks such as SPoF, low transparency, and control by a few entities [14]. Besides, the virtual economy and value system provided by the blockchain are essential components of the metaverse. As shown in Fig. 5, blockchain technologies offer an open and decentralized solution for building the sustainable virtual economy, as well as constructing the value system in the metaverse. Blockchain is a distributed ledger, in which data is structured into hash-chained blocks and featured with decentralization, immutability, transparency, and auditability [22]. The blockchain can be classified into three categories, i.e., public, consortium, and private, based on the decentralization degree [22]. The consensus protocols are the key component of blockchain, which determines the ledger consistency and system scalability. Besides, smart contracts can be deployed atop the blockchain to allow automatic function execution among distrustful parties in a prescribed fashion. NFT represents irreplaceable and indivisible tokens [32], which can help asset identification and ownership provenance with the assistance of distributed ledgers in the blockchain. De-Fi stands for the decentralized finance, which aims to deliver secure, transparent, and efficient financial services (e.g., stock/currency exchange) in the metaverse.

D. Existing Modern Prototypes of Metaverse Applications

In this subsection, we introduce existing representative prototypes in the following metaverse applications.

1) Game: Game is the current hottest metaverse application. Considering the technological maturity, user matching, and content adaptability, games are an excellent way to explore the metaverse. We list some representative examples of metaverse games. The sandbox game *Second Life*[1] offers a modifiable 3D virtual world where players can join in as avatars and create their virtual architectures and sell them, as well as participate in social activities such as art shows and even political gatherings and visiting embassy. *Roblox*[2] is a global user-created game platform, in which players can create games and design items such as skins and clothes. It proposes eight key features of the metaverse: identity, friends, immersion, anywhere, diversity, low latency, economy, and civilization [33]. *Fortnite*[3] is a massive multi-player online (MMO) shooter game designed by Epic Games, where players can build buildings and bunkers as well as construct islands, while the in-game items such as skins can only be designed by the platform.

2) Social Experience: Metaverse can revolutionize our society and enable a series of immersive social applications such as virtual lives, virtual shopping, virtual dating, virtual chatting, global travel, and even space/time travel. For example, Lil Nas X held a virtual concert on Roblox in 2020, with over 30 million fans participating. Players can unlock special Lil Nas X goods in the digital store, e.g., commemorative items and emotions. Due to the COVID-19 situation, UC Berkeley celebrated graduation festivities virtually in Minecraft by digitally copying the campus scenery in 2020. Besides, Tencent developed a *Digital Palace Museum*[4] in 2018 which allows tourists to freely visit the palace museum and its exhibitions with a panoramic and immersive view by wearing VR helmets in their homes.

3) Online Collaboration: Metaverse also opens new possibilities for immersive virtual collaboration in terms of telecommuting in virtual workplaces, study and learning in virtual classrooms, and panel discussion and meeting in virtual conference rooms. For example, *Horizon Workroom*[5] is an office collaboration software (run in Oculus Quest 2 helmet) released by Facebook, which allows people in any physical location to work and meet together in the same virtual room.

4) Simulation & Design: Another promising application is 3D simulation, modeling, and architectural design on metaverse. For example, NVIDIA has built its open platform named *Omniverse*[6] to support multi-user real-time 3D simulation and visualization of physical objects and attributes in a shared virtual space for industrial applications, e.g., automotive design. Besides, Omniverse can be compatible with Disney Pixart's open-source platform *Universal Scene Description (USD).*

5) Creator Economy: The metaverse mainly includes three modes of content creation: professional-generated content (PGC), professional- and user-generated content (PUGC), and user-generated content (UGC), as illustrated in Table III. In PGC mode, contents (e.g., games) are created by professional content producers on the platform, and ordinary users are just participants and content viewers/experiencers. In UGC mode, all users produce contents and trade them freely in the marketplace provided by the platform, which is featured with high freedom degree, low cost, high diversification, and decentralization. Users are dominant in the content production process under the UGC mode. For example, creators of game scenes, skins, and items in Roblox can earn a certain percentage of Robux (i.e., virtual tokens exchangeable with real-world currency) paid by their experiencers, leading to a virtuous cycle. The PUGC mode is the combination of PGC and UGC modes, in which contents are jointly produced by professionals and ordinary users.

TABLE III
A SUMMARY OF CONTENT CREATION MODES IN THE METAVERSE

Mode	Description	Feature	Instance
PGC	Contents are produced by professionals	Centralization, low diversification, high quality & cost	GTA, Unity
PUGC	Contents are produced by professionals and users	Semi-centralization, medium diversification, medium cost	Second Life, Minecraft, Fortnite
UGC	Contents are produced and traded among users	Decentralization, high diversification, uneven quality & low cost	Roblox, Decentraland, Cryptovoxels

There are existing decentralized virtual worlds with built-in creator economy supported by the Ethereum blockchain such as Decentraland[7] and Cryptovoxels[8]. In *Decentraland*, users can trade the land parcel and equipments in the marketplace and build their own buildings as well as social games by calling the builder function, where the trading details are immutably recorded in Ethereum for auditablility. In *Cryptovoxels*, players can trade the lands and build virtual stores and art galleries in the virtual world "Origin City". Besides, users can display and trade their digital assets such as artwork inside buildings.

Table IV summarizes existing modern prototypes in different metaverse applications in terms of the six key characteristics of the metaverse.

III. Security and Privacy Threats to Metaverse

In this section, we elaborate on the typical security threats in the metaverse by classifying them from the following seven dimensions: identity, data, privacy, network, economy, governance, and physical/social effects. Fig. 6 depicts the proposed taxonomy of security threats in the metaverse.

A. Identity-related Threats

In the metaverse, identity management plays a vital role for massive users/avatars in metaverse service offering. The identities of users/avatars in the metaverse can be illegally stolen, impersonated, and interoperability issues can be encountered in authentication across virtual worlds.

1) Identity Theft. If the identity of a user is stolen, his/her avatars, digital assets, social relationships, and even the digital life in the metaverse can be leaked, which can be more severe

[1] https://secondlife.com/

[2] https://developer.roblox.com/en-us/

[3] https://www.epicgames.com/fortnite/en-US/home

[4] https://en.dpm.org.cn/about/news/2019-09-18/3089.html

[5] https://www.theverge.com/2021/8/19/22629942/facebook-workrooms-horizon-oculus-vr

[6] https://www.nvidia.com/en-us/omniverse/

[7] https://decentraland.org/

[8] https://www.cryptovoxels.com/

TABLE IV
SUMMARY OF EXISTING METAVERSE PROTOTYPES IN DIFFERENT APPLICATIONS

Prototype	Application	Immersive	Hyper Spatiotemporal	Sustainable		Interoperable	Scalable	Heterogeneous
				Open	Decentralized			
Second Life	MMO Game	Partly	✓	Partly	×	×	✓	N/A
Roblox	MMO Game	✓	✓	✓	×	Partly	✓	N/A
Fortnite	MMO Game	✓	✓	Partly	×	Partly	✓	N/A
Digital Palace Museum	Travelling	✓	×	×	×	×	Partly	N/A
Horizon Workroom	Working	✓	×	×	×	×	Partly	N/A
Omniverse	Platform	✓	✓	✓	×	Partly	✓	✓
Decentraland	Game	✓	✓	✓	✓	×	✓	Partly
Cryptovoxels	Game	✓	✓	✓	✓	×	✓	Partly

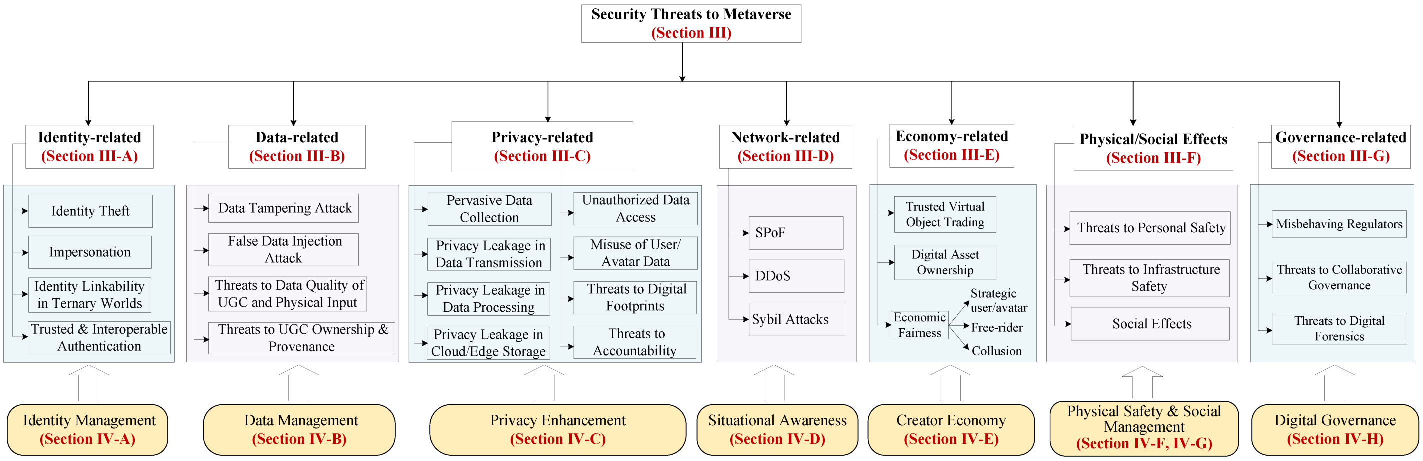

Fig. 6. The taxonomy of security threats in the metaverse.

than that in traditional information systems. For example, hackers can steal users' personal information (e.g., full names, social security numbers, secret keys of digital assets, and banking details) through hacked personal devices, phishing email scams, and the stolen customer data of companies to commit fraud and crimes (e.g., steal the victim's avatar and digital assets) in the metaverse.

2) Impersonation Attack. An attacker can carry out the impersonation attack by pretending to be another authorized entity to gain access to a service or system in the metaverse [34]. For example, attackers can exploit Bluetooth impersonation threats [35] to impersonate trusted endpoints and illegally access metaverse services by inserting rogue devices into the established Bluetooth pairing. Another example is that hackers can invade helmets or wearable devices and exploit them as entry points to impersonate the victim and illegally gain his/her service privileges.

3) Identity Linkability in Ternary Worlds. As the metaverse assimilates the reality into itself, the human, physical, and virtual worlds are seamlessly integrated into the metaverse, causing identity linkability concerns across the ternary worlds [11]. For example, a malicious player A can track another player B by the name appeared above the corresponding avatar of player B and infer his/her position in the real world. Another example is that hackers may track the position of users via compromised VR headsets or glasses.

4) Trusted and Interoperable Authentication. For users/avatars in the metaverse, it is fundamental to ensure fast, efficient, and trusted cross-platform and cross-domain identity authentication, i.e., across various service domains and virtual worlds (built on distinct platforms such as blockchains) [3].

B. Data-related Threats

The data collected or generated by users, IoT devices, and avatars may suffer from threats in terms of confidentiality, integrity, availability, false data injection, and UGC ownership/provenance tracing in the metaverse.

1) Data Tampering Attack. Integrity features ensure effective checking and detection of any modification during data communication among the ternary worlds and various sub-metaverses. Adversaries may modify, forge, replace, and remove the raw data to interfere with the normal activities of users, avatars, or physical entities [36]. Besides, adversaries may remain undetected by falsifying corresponding log files or message-digest results to hide their criminal traces.

2) False Data Injection Attack. Attackers can inject falsified information such as false messages and wrong instructions to mislead metaverse systems [37]. For example, AI-aided content creation can help improve user immersiveness in the early stage of the metaverse, and adversaries can inject adversary training samples or poisoned gradients during centralized or distributed AI training, respectively, to generate biased AI models.

3) Threats to Data Quality of UGC and Physical Input. In metaverse, selfish users/avatars may contribute low-quality contents under the UGC mode to save their costs, thereby compromising UGC utility such as data quality [38]. For example, they may share unaligned and severe non-IID data during the collaborative training process of the content recommendation model in the metaverse. Another example is that uncalibrated wearable sensors can generate inaccurate and even erroneous sensory data to mislead the creation of digital twins in the metaverse.

4) Threats to UGC Ownership and Provenance. Different from the asset registration supervised by the government in the real world, the metaverse is an open and fully autonomous space and there exists no centralized authority. Due to the lack of authority, it is hard to trace the ownership and provenance of various UGCs produced by massive avatars under different virtual worlds in the metaverse, as well as turn UGCs into protected assets [39].

C. Privacy Threats

When enjoying digital lives in the metaverse, user privacy including location privacy, habit, living styles, and so on may be offended during the life-cycle of data services including data perception, transmission, processing, governance, and storage.

1) Pervasive Data Collection. The construction of an avatar requires pervasive user profiling activities [11] including facial expressions, eye/hand movements, speech and biometric features, brain wave patterns, and the surroundings. For example, the motion sensors and four built-in cameras in the Oculus helmet help track the head direction and movement, draw our rooms, as well as track our positions and environment in real time with submillimeter accuracy. If it is hacked by attackers, severe crimes can be committed on the basis of these sensitive data.

2) Privacy Leakage in Data Transmission. In metaverse systems, massive private and sensitive user data collected from various XR devices (e.g., helmets) are transferred via wired and wireless communications, the confidentiality of which should be prohibited from unauthorized individuals/services. Although communications are encrypted and information is confidentially transmitted, adversaries may still access the raw data by eavesdropping on the specific channel and even track users' locations via differential attacks [40] and advanced inference attacks [41].

3) Privacy Leakage in Data Processing. In metaverse, the aggregation and processing of massive data collected from human bodies and environments are essential for the creation and rendering of avatars and metaverse, in which users' sensitive information may be leaked [42]. For example, the aggregation of private data (belonging to different users) to a central storage for training may offend user privacy and violate existing regulations such as General Data Protection Regulation (GDPR)[9]. Besides, adversaries may infer users' privacy (e.g., preferences) from the published processing results (e.g., synthetic avatars) in the metaverse.

4) Privacy Leakage in Cloud/Edge Storage. The storage of these private and sensitive information (e.g., user profiling) of massive users in cloud servers or edge devices may also raise privacy disclosure issues. For example, hackers may deduce users' privacy information by frequent queries via differential attacks [40] and even compromise the cloud/edge storage via DDoS attacks [43].

5) Unauthorized Data Access. To deliver seamless personalized services (e.g., customized avatar appearance) in the metaverse, different service providers in distinct sub-metaverses need to access real-time user/avatar profiling activities. Malicious service providers may illegally elevate their rights in data access via attacks such as buffer overflow and tampering access control lists [44].

6) Misuse of User/Avatar Data. In the life-cycle of data services in the metaverse, user/avatar-related data can be disclosed intentionally by attackers or unintentionally by service providers to facilitate user profiling and precision marketing activities.

7) Threats to Digital Footprints. As the behavior pattern, preferences, habits, and activities of avatars in the metaverse can reflect the real statuses of its physical counterpart, attackers can collect the digital footprints of avatars and exploit the similarity linked to real users to facilitate accurate user profiling and even illegal activities [5]. Besides, metaverse usually offers the third person view with a wider viewing angle of their avatar's surroundings than that in the real world [10], which may infringe on other players' behavior privacy without awareness. For example, an avatar may conduct the virtual stalking/spying attack by following your avatar and record all your digital footprints, e.g., purchasing behaviors, to facilitate social engineering attacks.

8) Threats to Accountability. As XR devices intrinsically gather more sensitive data such as locations and surroundings of users than traditional smart devices, the accountability in the metaverse is important to ensure users' data are handled with privacy compliance. For metaverse service providers, the audit process of the compliance of privacy regulations (e.g., GDPR) for accountability can be clumpy and time-consuming under the centralized service offering architecture. Besides, it is hard for them to ensure the transparency of regulation compliance during the life-cycle of data management [45], especially in the new digital ecology of metaverse.

D. Network-related Threats

In the metaverse, traditional threats to the communication networks can also be effective, as the metaverse evolves from the current Internet and incorporates existing wireless communication technologies. Here, we list some typical threats as below.

1) SPoF. In the construction of metaverse systems, the centralized architecture (e.g., cloud-based system) brings convenience for user/avatar management and cost saving in operations [46]. Nevertheless, it can be prone to the SPoF caused by the damage of physical root servers and DDoS attacks. Besides, it raises challenges for free exchange of tokens or virtual currencies across various virtual worlds.

2) DDoS. Adversaries may exploit IoT botnets [43] (e.g., Mirai) composed of massive victimized IoT devices to conduct DDoS attacks to make network outage and service unavailability by overwhelming the centralized server with giant traffic within a short time.

3) Sybil Attacks. Sybil adversaries may manipulate multiple faked/stolen identities to gain disproportionately large influence [47] on metaverse services (e.g., reputation service and voting-based service), thereby compromising system effectiveness.

[9] https://gdpr-info.eu/

E. Economy-related Threats

Various attacks may threaten the creator economy in the metaverse from the service trust, digital asset ownership, and economic fairness aspects.

1) Service Trust Issues in Virtual Object Trading. In the open metaverse marketplace, avatars may be distrustful entities without historical interactions. There exist inherent fraud risks [48] (e.g., repudiation and refusal to pay) during virtual object trading among different stakeholders in the metaverse. Besides, in the construction of virtual objects via digital twin, the metaverse has to guarantee that the produced and deployed digital copies are authentic and trustworthy [49].

2) Threats to Digital Asset Ownership. Due to the lack of central authority and the complex circulation and ownership forms (e.g., collective ownership and shared ownership [50]) in the distributed metaverse system, it poses huge challenges for the generation, pricing, trusted trading, and ownership traceability in the life-cycle of digital assets in the creator economy.

3) Threats to Economic Fairness in Creator Economy. Well-designed incentives [51], [52] are benign impetuses to promote fairness and efficiency in resource sharing and digital asset trading in the creator economy. The following three adversaries are considered.

- *Strategic* users/avatars may manipulate the digital market in the metaverse to make enormous profits by breaking the supply and demand status [51].
- *Free-riding* users/avatars may unfairly gain revenues and enjoy metaverse services without contributing to the metaverse market [53], thereby compromising the sustainability of creator economy.
- *Collusive* users/avatars in the metaverse may collude with each other or with the service provider to perform market manipulation and gain economic benefits [52].

F. Threats to Physical World and Human Society

The metaverse is an extended form of the cyber-physical-social system (CPSS) [54], in which physical systems, human society, and cyber systems are interconnected with complex interactions. The threats in virtual worlds also severely affect physical infrastructures, personal safety, and human society.

1) Threats to Personal Safety. In the metaverse, hackers can attack wearable devices, XR helmets, and other indoor sensors (e.g., cameras) to obtain the life routine and track the real-time position of users to facilitate burglary, which may threaten their safety [55]. Besides, due to the immersive realism of metaverse, hackers can suddenly display harmful and scary content (e.g., ghost pictures) in the virtual environment in front of the avatar, which may lead to the death of fright of the corresponding user.

2) Threats to Infrastructure Safety. By sniffing the software or system vulnerabilities in the highly integrated metaverse, hackers may exploit the compromised devices as entry points [56] to invade critical national infrastructures (e.g., power grid systems and high-speed rail systems) via APT attacks [12].

3) Social Effects. Although metaverse offers an exciting digital society, severe side effects can also raise in human society such as user addiction [57], rumor prevention [58], biased outcomes, and simulated facts. For example, the metaverse, in its ultimate form, is fully controlled by AI algorithms (as depicted in the film *Matrix*), in which the code can be the law to rule everything and severe ethical issues such as race/gender bias may arise.

G. Governance-related Threats

In analogy to the social norms and regulations in the real world, content creation, data processing, and virtual economy in the metaverse should align with the digital norms and regulations [59]. In the supervision and governance process of metaverse, the following threats may deteriorate system efficiency and security.

1) Misbehaving Regulators. Regulators may misbehave and cause system paralysis, and their authorities also need supervision. Dynamic and effective punishment/reward mechanisms should be enforced for misbehaving/honest regulators, respectively. To ensure sustainability, punishment and reward rules should be maintained by the majority of avatars in a decentralized and democratic manner [60].

2) Threats to Collaborative Governance. To avoid the concentration of regulation rights, collaborative governance under hierarchical or flat mode is more suitable for large-scale metaverse maintenance [61]. Collusive regulators may undermine the system even under collaborative governance. For example, they can collude to make a certain regulator partitioned from the network via wormhole attacks.

3) Threats to Digital Forensics. Digital forensics in the metaverse means the virtual reconstruction of cybercrimes by identifying, extracting, fusing, and analyzing evidences obtained from both real and virtual worlds [62]. Nevertheless, due to the high dynamics and interoperability issues of various virtual worlds, it is challenging for efficient forensics investigation including entity-behavior association, identification, and tracing among anonymous users/avatars with diverse behavior patterns in the metaverse. In addition, due to the blurred boundary between real and virtual worlds, the metaverse can make us confused to distinguish the true and false (e.g., Deepfake event).

IV. Security Countermeasures in Metaverse

In this section, we review existing and potential defense mechanisms for the above security and privacy threats in the metaverse.

A. Identity Management

For the metaverse, secure and efficient identity management are the basis for user/avatar interaction and service provisioning. Generally, digital identities can be classified into three kinds from the identity management perspective, i.e.,

- *Centralized identity.* Centralized identity refers to the digital identity authenticated and managed by a single institution, such as the Gmail account.
- *Federated identity [63].* Federated identity refers to the digital identity managed by multiple institutions or federations. It can reduce the administrative cost in identity

authentication for cross-platform and cross-domain operations, and alleviate the cumbersome process of typing personal information repeatedly for users.

- *Self-sovereign identity (SSI) [64].* SSI refers to the digital identity which is fully controlled by individual users. It allows users to autonomously share and associate different personal information (e.g., username, education information, and career information) in performing cross-domain operations to enable identity interoperability with users' consent.

In the metaverse, centralized identity systems can be prone to SPoF risks and suffer potential leakage risks. Federated identity systems are semi-centralized and the management of identities is controlled by a few institutions or federations, which may also suffer potential centralization risks. The identity systems built on SSIs will be dominant in future metaverse construction [7]. According to [65], identity management schemes in the metaverse should follow the following design principles: (i) *scalability* to massive users/avatars, (ii) *resilience* to node damage, and (iii) *interoperability* across various sub-metaverse during authentication.

In the metaverse, empowered by HCI technologies, wearable devices such as head-mounted displays enable user/avatar interactions and are expected as the major terminal to enter the metaverse [6]. Besides, the metaverse usually includes various administrative domains and the sub-metaverses can be implemented on distinct blockchain platforms [14]. In the following, we first review existing works on the metaverse in terms of key management and identity authentication for wearable devices. Then, we give the literature review in cross-domain and cross-chain identity authentication in the metaverse.

1) Key Management for Wearable Devices: Wearable devices such as Oculus helmet and HoloLen headset are anticipated to be the major terminal to enter the metaverse. Key management (including generation, negotiation, distribution, update, revocation, and recovery) is essential for wearable devices to establish secure communication, deliver sensory data, receive immersive service, etc. In the literature, works [66]–[68] take the intrinsic features of distinct wearable devices into account in designing efficient key management schemes, which can be beneficial for future metaverse construction.

To secure communications between wearable devices integrated with accelerometers, Sun *et al.* [66] exploit the gait-based biometric cryptography to design a group key generation and distribution scheme for wearable devices based on signed sliding window coding and fuzzy vault. To further reduce system overheads and reduce response delay for resource-limited wearable devices, Chen *et al.* [67] introduce a lightweight and real-time key establishment model with gait regularity hiding functions for wearables by analyzing gestures and motions through the integrated accelerometer. To protect patients from fatal cyber attacks, Zheng *et al.* [68] propose an electrocardiogram (ECG) signal based key distribution mechanism for wearable and implantable medical devices (WIMDs) via the fuzzy commitment and fuzzy vault primitives. Experimental results validate that the proposed mechanism attains a high false acceptance rate.

2) Identity Authentication for Wearable Devices: Identity authentication for wearable devices to guarantee device/user authenticity is also a promising topic in the metaverse. To adapt to wearable devices with extremely low computing/storage capacity, Srinivas *et al.* [69] present a cloud-based mutual authentication model with low system cost for wearable medical devices to prevent device impersonation in healthcare monitoring systems with password change and smart card revocation functions. Rigorous security analysis proves the security of session key in defense against active and passive attacks. However, the one-time authentication in [69] may cause friction such as unauthorized privileges. To resolve this issue, Zhao *et al.* [70] propose a novel continuous authentication model to support seamless device authentication at low cost. In [70], unique cardiac biometrics are extracted from photoplethysmography (PPG) sensors (embedded in wrist-worn wearables) for user authentication. Experimental results show that their proposed system obtains a high average continuous authentication accuracy rate of 90.73%. To further protect user privacy during authentication, Liu *et al.* [71] design a privacy-preserving identity authentication mechanism for wearable devices with consideration of spatiotemporal contexts. By combing MinHash, bloom filter, and ciphertext-policy attribute-based encryption (CP-ABE) in the edge computing environment, the proposed scheme in [71] can achieve cooperative privacy preservation.

3) Cross-Domain Identity Authentication: The metaverse typically contains various administrative security domains created by distinct operators/standards. Identity authentication across distinct security domains in the metaverse is critical to deliver seamless metaverse services for users/avatars. Based on the virtual heterogeneous cross-domain authentication model, Wang *et al.* [72] realize the security authentication between public key infrastructure (PKI) and Kerberos. However, the work [72] relies on a trusted third party and brings heavy key management overhead. To address this issue, Shen *et al.* [73] employ the blockchain technology to design a decentralized and transparent cross-domain authentication scheme for industrial IoT devices. An anonymous identity authentication protocol is also proposed to protect user privacy during device authentication. To further improve the response speed arising from the low throughput of blockchains, Chen *et al.* [74] propose an efficient cross-domain authentication scheme named XAuth under optimized blockchain systems. Within the proposed scheme, a lightweight verification protocol is developed based on the multiple Merkle hash tree structure to support rapid response.

4) Cross-Chain Identity Authentication: By getting rid of trusted third parties, blockchain technology is fundamental to build trust-free digital identities for users in various domains in the metaverse [73], [74]. As distinct sub-metaverses may deploy services on heterogeneous blockchains to meet quality-of-service (QoS) requirements, efficient cross-chain authentication is needed for seamless services across multiple sub-metaverses. Fromknecht *et al.* [75] design a decentralized authentication protocol based on blockchain to resolve identity retention concerns under PKI, where identity certificates are stored in blockchain ledgers to eliminate certificate authority (CA) centralization risks. Besides, the authors employ cryptographic accumulators to support fast verification of public keys, and use distributed hash tables to enable fast public key lookup. Current cross-chain mechanisms mainly focus on digital asset transfer, and few of them consider cross-chain identity authentication in the metaverse. The implementation, efficiency, and security of identity authentication across various domains and blockchains in the metaverse remain to be further investigated.

B. Data Management

The metaverse is a digital world built on digital copies of the physical environment and avatars' digital creations. Analogy to the value created by human activities in the real world, digital twins and UGCs as well as avatars' behaviors (e.g., chat records and browsing records) will produce certain value in the metaverse [8]. Information security is an important prerequisite for the development and prosperity of the metaverse. In the following, we discuss the data security in metaverse in terms of data reliability, data quality, and provenance.

1) Data Reliability of AI-generated Content, Digital Twin, and Physical Input: In the metaverse, AI such as generative adversarial network (GAN) can help generate high-quality dynamic game scenarios and context images in the metaverse, but also poses security threats such as adversarial threats which is hard to detect for humans. Zhu *et al*. [76] propose a tensor-based adversarial training to resist adversarial samples in AI model training and improve learning robustness by taking adversarial samples as part of training data, which can be beneficial to resist adversarial threats in the scene construction in the metaverse.

The works [77], [78] discuss the data reliability in the metaverse in terms of AR device inputs and digital twin. Gharsallaoui *et al*. [77] introduce the authenticity threat of inputs of physical AR devices in location-based AR games (e.g., Pokemon Go). A novel image authentication method is also presented by the authors which allows players to upload an authenticated proof of game results to ensure authenticity without revealing the private positioning data. Gehrmann *et al*. [78] propose a reliable state replication method for digital twin synchronization and identify seven key requirements in architecture design. However, the trustworthiness of data collected from disparate data silos is not studied in [78]. To address this issue in the metaverse, Suhail *et al*. [49] combine the blockchain technology to build a trustworthy data dissemination and fault diagnosis platform for digital twin construction using disparate data sources.

2) Data Quality of UGC and Physical Input: Low-quality data input from physical sensors and the UGCs produced by avatars can deteriorate the QoS of metaverse services and the QoE of users. Effective quality control mechanisms are important to offer efficient metaverse services and maintain sustainability of creator economy.

Considering human's psychological status, Guo *et al*. [38] present a safety management method to ensure the availability of physical data generated from wearable devices in the metaverse. Considering multi-hop transmissions and potential node failures, Qaim *et al*. [79] propose a hop-by-hop data replication scheme for IoT sensors, which can ensure the data availability even under high node failure scenarios. Moreover, the replica spread of data is also optimized in their scheme. Ning *et al*. [80] propose a quality-aware vehicular service access model, where the access quality is assessed via a generation tree and access service routing strategies are designed based on network states. By using k-means and differential privacy, Xiong *et al*. [81] design a privacy-aware data clustering method to improve the quality of clustering results for intelligent IoT services. However, the proposed method in [81] overlooks the precision of data clustering results, which is also critical and should be optimized.

3) Provenance of UGC: Data provenance can realize the traceability of historical archives of a piece of UGC, which is essential to evaluate data quality, trace data source, reproduce data generation process, and conduct audit trail to quickly identify data responsible subjects. In the metaverse, UGC provenance information such as the source, circulation, and intermediate processing information is often stored in disparate data silos (e.g., distinct blockchains), making it difficult to monitor and track in real time. Existing works on IoT data provenance can offer some lessons for UGC provenance design in the metaverse.

Liang *et al*. [39] present a blockchain-based cloud file provenance architecture named ProvChain with three stages, i.e., collection, storage, and verification of provenance information. ProvChain ensures source tamper resistance, user privacy, and reliability of cloud storage. For multi-hop IoT, Mohsin *et al*. [82] design a lightweight protocol to enable data provenance in wireless communications, where the received signal strength indicator (RSSI) of the communicating IoT node is exploited to produce the unique link fingerprint. In the metaverse, the lifecycle of UGCs involves the ternary worlds and multiple submetaverses, which can be more complex than that in traditional IoT. Besides, the scalability, trust, and efficiency (e.g., response delay) are still challenging in the provenance of massive UGCs in the large-scale metaverse.

C. Privacy Enhancement

1) Privacy in Metaverse Games: AR/VR games are the current most popular metaverse application for users. AR/VR games usually contain three steps: the game platform (i) collects sensory data from users and their surroundings, (ii) identifies objects according to these contexts, and lastly (iii) performs rendering on game senses for immersiveness.

Existing works have demonstrated the security and safety concerns related to metaverse games using case studies [83] and qualitative studies [84], [85]. Bono *et al*. [83] offer two case studies (i.e., *Second Life* and *Anarchy Online*) and show that a hacker can exploit the features and vulnerabilities of MMO metaverse games to fully compromise and take over players' devices (e.g., laptops). Lebeck *et al*. [84] carry out a qualitative lab study using Microsoft HoloLen (an AR headset), whose result shows that players can easily be immersed in AR experiences and treat virtual objects as real, as well as various security, privacy, and safety issues are uncovered. Shang *et al*. [85] identify a novel user location tracking attack in location-based AR games by solely exploiting the network traffic of the player, and real-world experiments on 12 volunteers validate that the proposed attack model attains fine-grained geolocation of any player with high accuracy. Besides, three possible mitigation approaches are presented in [85] to alleviate attack effects.

To prevent potential privacy issues in metaverse games, Laakkonen *et al.* [86] introduce privacy-by-design principles in digital games from both qualitative and quantitative perspectives, where nineteen privacy attributes divided into three levels are accounted for privacy evaluation. In [87], Corcoran *et al.* distinguish the *individual privacy* and *group privacy* in privacy-preserving interactive metaverse game design. The former refers to the purchasing patterns, behavioral traits, communication, image/video data, and location/space related to an individual, while the latter refers to the privacy associated with a group of individuals (e.g., a social group, an organization, and a nation).

2) Fine-grained Access Control and Usage Audit for UGC: The naive content creation (e.g., UGCs) produced by avatars is essential to maintain the creativity and sustainability of the metaverse. As UGCs inevitably contain sensitive and private user information, efficient UGC access control and usage audit schemes should be designed. The following works [88]–[90] discuss the UGC access control. Different from conventional access control schemes which enforce a single access policy for a specific content, Ma *et al.* [88] design a scalable access control scheme to allow multiple levels of access privileges for sharing user-generated media contents (UGMCs) in the cloud. The detailed construction based on scalable CP-ABE mechanism is also presented with formal security proof. However, the above scheme cannot support time-domain UGMC access control. To address this issue, Yang *et al.* [89] propose a time-domain attribute-based access control mechanism with provable security for sharing user-generated video contents (UGVCs) in the cloud. In their mechanism, the allowed time slots for access are embedded into both ciphertexts and keys in CP-ABE, thereby only authorized users in specific time slots can decrypt the UGVCs. Moreover, queries on UGVCs created in previous time slots along with efficient attribute updating and revoking are supported. Nevertheless, the above works overlook that authorized entities may become traitors to illegally redistribute UGCs to the public, i.e., *illegal UGC redistribution*. To address this realistic threat, Zhang *et al.* [90] propose a novel secure encrypted UGMC sharing scheme with traitor tracing in the cloud via the proxy re-encryption mechanism (for secure UGMC sharing) and watermarking mechanism (for traitor tracing).

The above works mainly focus on the access control of UGCs, while the usage control (i.e., shared UGCs can be only used for intended purposes) is ignored. To bridge this gap, Wang *et al.* [45] propose a novel data processing-as-a-service (DPaaS) mode to complement current data sharing ecosystem and exploit blockchain technologies for fine-grained data usage policy making on user's side, policy execution atop smart contracts, and policy audit on transparent ledgers. Yu *et al.* [44] combine both sensitiveness of UGMC (to be shared) and trustworthiness of user (being granted) to train a tree classifier for fine-grained privacy setting configurations. In their scheme, a deep network is utilized to extract discriminative features and identify privacy-sensitive object classes/events, and users are clustered into social groups for trustworthiness characterization.

3) Privacy-Preserving UGC Sharing and Processing: Existing privacy-preserving schemes for data sharing and processing mainly focus on four fields: differential privacy (DP), federated learning (FL), cryptographic approaches (e.g., secure multiparty computation (SMC), homomorphic encryption (HE), and zero-knowledge proof (ZKP)), and trusted computing. The following works [40], [91]–[94] discuss privacy-preserving UGC sharing in the metaverse. To offer privacy-preserving trending topic recommendation services in the metaverse, Wei *et al.* [40] propose a graph-based local DP mechanism, where a compressive sensing indistinguishability method is devised to produce noisy social topics to prevent user-linkage association and protect keyword correlation privacy with high efficiency. To enable smart health sensing without violating users' private data in the metaverse, Zhang *et al.* [91] present a FL-based secure data collaboration framework where wearable sensors periodically send local model updates trained on their private sensory data to the server which synthesizes a global abnormal health detection model. To resolve class imbalance concerns of participants under FL, the authors in [91] further design a novel local update method based on reinforcement learning and an adaptive global update method via online regret minimization. To enhance privacy protection in blockchain-based metaverse, Guan *et al.* [93] utilize ZKP to empower current account-model blockchains (e.g., Ethereum) with privacy preservation functions in terms of hiding sender-recipient linkage, account balances, and transaction amounts. Xu *et al.* [94] identify the *co-photo privacy* threat in social metaverse that a shared photo may contain not only the individual privacy but also the privacy of others in photos. Besides, by utilizing SMC and SVM techniques, the authors design a personalized facial recognition method to differentiate photo co-owners without disclosing their privacy in users' private photos.

Privacy-preserving UGC processing in the metaverse has also attracted various attention. Based on Okamoto-Uchiyama HE, Li *et al.* [42] present a verifiable privacy-preserving method for data processing result prediction in edge-enabled CPSSs. Besides, batch verification is supported for multiple prediction results at one time to reduce communication burdens. Wang *et al.* [45] leverage the trusted computing technique to design a privacy-preserving off-chain data processing mechanism, where private UGC datasets are processed in an off-chain trusted enclave and the exchange of processed results and payment are securely executed via the designed fair exchange smart contract.

4) Confidentiality Protection of UGC and Physical Input: The confidentiality of UGCs (inside the metaverse) along with physical inputs (to the metaverse) should be ensured to prevent private data leakage and sensitive data exposure. The identity management (in Sect. IV-A), access control (in Sect. IV-C2), and privacy computing technologies (in Sect. IV-C3) are enablers to maintain UGC confidentiality in the metaverse. For confidentiality of physical inputs, Raguram *et al.* [95] propose a novel threat named *compromising reflections*, which can automatically reconstruct user typing on virtual keyboards, thereby compromising data confidentiality and user privacy.

Experiment results show that compromising reflections of a device's screen (e.g., sunglass reflections) are sufficient for automatic and accurate reconstruction with no limitation on the motion of handheld cameras even in challenging scenarios such as a bus and even at long distances (e.g., 12m for sunglass reflections).

5) Digital Footprints Protection: In the metaverse, privacy inside avatars' digital footprints can be classified into three types [11]: (i) personal information (e.g., avatar profiling), (ii) virtual behaviors, and (iii) interactions or communications between avatars or between avatar and NPC. Avatars' digital footprints can be tracked via virtual stalking/spying attacks in the metaverse to disclose user's real identity and other private information, e.g., shopping preferences, location, and even banking details. A potential solution is *avatar clone* [5], which creates multiple virtual clones of the avatar which appear identical to confuse the attackers. Nevertheless, it brings other challenging issues such as managing multiple representations of each user and managing millions of clones roaming around the metaverse.

Another potential solution is *disguise* by periodically changing avatar's appearance to confuse attackers, or *mannequin* by replacing with the avatar with a single clone (e.g., bot) which imitates user's behavior and *teleport* user's true avatar to another location when being tracked. Other privacy preservation mechanisms [11] include invisibility, private enclave, lockout. *Invisibility* indicates the avatar is made to be temporarily invisible in case of suspected stalking. *Private enclaves* allow certain locations inside the metaverse to be occupied by individuals, which are unobserved by others. In private enclaves, owners have control over who can enter into the enclave by teleporting, thereby offering a maximum level of privacy. *Lockout* means certain areas inside the metaverse are temporarily locked out for private use. After the lock expires, the restriction is lifted and other users are allowed to enter the area.

D. Situational Awareness

Situational awareness is an effective tool for security monitoring and threat early-warning in large-scale complex systems such as the metaverse [96]. In the metaverse, local situational awareness is essential for monitoring a single security domain and global situational awareness can assist early-warning of large-scale distributed threats target at multiple sub-metaverses.

1) Local Situational Awareness: Situational awareness for devices and systems built on XR technology has received increasing attention in the metaverse [96]–[98]. Woodward *et al.* [96] review the presentation of information in AR headsets, and discuss the potential in applying AR technologies to enhance users' situational awareness in perception and understanding the surroundings. Apart from the AR technology, the VR technology can enhance situational awareness capacities in various applications. Ju *et al.* [97] carry out realistic and immersive driving simulations, whose findings validate that acoustic cues can help VR drivers remain alert in emergencies (e.g., accidents) under VR car-driving scenarios. Lv *et al.* [98] present a smart intrusion detection model to detect attack behaviors in 3D VR environments based on support vector machine (SVM). However, the proposed model cannot resist unknown/new attack types.

To effectively detect unknown/new threats, Vu *et al.* [99] design a representation learning approach for better prediction of unknown attacks, where three regularized autoencoders (AEs) are deployed to learn the latent representation. The effectiveness of their work is evaluated on nine recent IoT datasets. To be further adaptive to wearable devices with extreme size and energy constraints, Heartfield *et al.* [100] propose a multi-layered lightweight anomaly detection method by exploiting radio-frequency wireless communications to/from them to identify potentially malicious transactions. In [101], reinforcement learning methods are employed for intrusion detection in small-scale applications such as smart homes. The above defense approaches can provide some lessons to resist unknown/new threats in the metaverse.

2) Global Situational Awareness: The above works mainly focus on situational awareness in a local security domain. Global situational awareness can facilitate understanding global security statuses in defending large-scale attacks in the metaverse. Both works [102], [103] utilize data-driven approaches for global situational awareness in large-scale distributed power grids. In [102], Shahsavari *et al.* propose a multi-class SVM classifier to extract malicious events from collected raw metering data. However, their approach relies on additional expert knowledge for costly event labeling. To resolve this issue, Wu *et al.* [103] further model legitimate users and attackers as an evolutionary game and devise a two-phase reinforcement learning algorithm to solve the game. Profiling of potential attack behaviors is another challenge in the metaverse. Krishnan *et al.* [104] combine digital twin and SDN to build a behavioral monitoring and profiling system where security strategies are evaluated on digital twins before being deployed in the real network.

Honeynets consisting of collaborative honeypots offer an alternative solution for building a secure metaverse to defend against large-scale distributed attacks. Zhang *et al.* [105] propose a honeynet-based situational awareness system where each honeypot built on the Docker environment traps attackers, monitors their attack behaviors, and exchanges these information with each other coordinated by the honeynet controller. However, the work [105] has a drawback in terms of scalability and programmability in large-scale deployment. Zarca *et al.* [106] further propose SDN-enabled virtual honeynet services with higher degree of scalability and flexibility, and the efficiency of the proposed approach is validated using real implementations and tests. However, the trust issues and resilience of compromised domain operators in aggregating local situational awareness into the global one require further investigation.

E. Open and Decentralized Creator Economy

Creator economy is an essential component of the metaverse to maintain its sustainability and promote avatars' open creativity. Besides, it should be built on a decentralized architecture to prevent centralization risks, e.g., SPoF, non-transparency, and control by a few entities.

1) Trusted UGC/Asset/Resource Trading: As shown in Fig. 5, blockchain technologies (e.g., NFT and smart contract) provide a decentralized solution to construct the sustainable creator economy. NFT is the irreplaceable and indivisible token in the blockchain [32] and is regarded as the unique tradable digital asset associated with virtual objects (e.g., land parcel and digital painting). For example, in the game Cryptokitties, players can buy virtual pet cats with unique genetic attributes identified by NFT and breed them. Besides, smart contracts enable the automatic transaction enforcement and financial settlement in trading virtual objects, items, and assets. The works [48], [107], [108] discuss the usage of blockchain technology for virtual economy design.

Rehman *et al.* [107] discuss several design principles in cryptocurrency ecosystems including centrality, privacy, price manipulation, insider trading, parallel and shadow economy, governance, usability, and security. Considering the cooperation of heterogeneous smart devices, Biase *et al.* [48] propose a swarm economy model for digital resource sharing which incorporates their spontaneous collaboration and dynamic organization in large-scale networks. A blockchain-based transaction model is also developed in [48] for transparent and immutable currency audit, thereby ensuring trading trust among distrustful devices. However, the work [48] has drawbacks in terms of non-automatic transaction settlement, high computational overhead, and non-supervisability. To address these issues, Liu *et al.* [108] propose a blockchain-based automatic transaction settlement framework, in which a three-layer sharding blockchain architecture is devised for enhanced system scalability. Moreover, the authors in [108] devise an encryption scheme with keyword search to uncover criminal transactions and achieve crime traceability, where the supervision right is equally allocated among all participants.

In the creator economy, trust or reputation management offer a quantifiable solution to evaluate the trustworthiness of participants and services. Das *et al.* [109] propose dynamic trust models and metrics based on user interactions including direct/indirect trust (derived from local/recommendation experience) and recent/historical trust (considering time decay effects). To achieve "trust without identify", Wang *et al.* [110] present an anonymous trust and reputation management system in mobile crowdsensing. However, most of current works on trust or reputation evaluation may rely on the specific rules to determine trust scores and cannot intelligently learn from historical interaction information. To cope with this issue, Jayasinghe *et al.* [23] exploit AI techniques to design an intelligent trust model, which classifies various individual trust attributes (e.g., frequency, duration, and cooperativeness) and aggregates them to produce final trust values.

2) Economic Fairness for Manipulation Prevention: As described in Sect. III-E, the economic fairness in the metaverse market may be violated by strategic, free-riding, and collusive users/avatars. Strategy-proof incentive mechanisms, e.g., truthful auctions [111] and truthful contracts [112], can prevent strategic users/avatars from market manipulating. However, truthful participation also violates user's privacy, e.g., the true bid in auctions may reveal user's true valuation on the items. Existing strategy-proof and privacy-preserving auctions mainly depend on cryptographic mechanisms (e.g., ZKP [113], HE [114]), DP [51]), which may bring large system burdens for energy-limited wearable devices or large data utility decrease in practical metaverse applications.

Existing schemes to prevent free-riders (who try to enjoy benefits of the good/service without contributing to it) mainly focus on node behavior modeling [53], cryptographic mechanism [115], contribution certification [116], and blockchain [117]. For example, Li *et al.* [53] design a fluid model for non-free-riders and free-riders in peer-to-peer (P2P) file sharing systems to capture free-riding effects in designing optimal bandwidth allocation strategies. Based on symmetric key cryptography, Shin *et al.* [115] design a lightweight and almost-fair exchange algorithm to prevent free-riders under cooperative computing scenarios. Ma *et al.* [116] propose a differentiated service framework with free-rider prevention in P2P networks, where the differentiation is based on prior contribution levels of individuals. To mitigate free-riding attacks, Li *et al.* [117] utilize smart contracts and ZKP to generate the proof-of-ad-receiving commitments in blockchain systems with anonymity and conditional linkability guarantees.

Multi-user/avatar collusion prevention is also important for fairness in the creator economy. Existing collusion-resistant mechanisms mainly focus on AI-based collusion behavior detection [118], [119], cryptography-based approaches [120], [121], game theory [52], and optimization methods [122]. In the metaverse, future research efforts are required in designing fair mechanisms with the combination of strategy-proofness, collusion-resistance, free-rider prevention, along with privacy preservation.

3) Ownership Traceability of Digital Assets: In the metaverse, blockchain provides a promising solution to manage the complex asset provenance and ownership tracing in the lifecycle of digital assets by recording the evidence of content/asset originality and involved operations on the public ledgers. As the recorded historical activities on blockchain ledgers are maintained by the majority of entities in the metaverse, it is ensured to be democratic, immutable, transparent, auditable, and non-repudiable. Besides, smart contracts offer an intelligent traceability solution by coding the ownership management logic into scripts which is run atop the blockchain. Existing works have utilized blockchain technologies for food supply [123], [124], product supply [125], charging pile sharing [126], and ride sharing [127]. In addition of private ownership, there can exist multiple types of ownership forms in the metaverse such as collective ownership and shared ownership [50], which raise extra challenges in ownership management of virtual objects and metaverse assets.

F. Physical Safety

In this subsection, we review existing potential solutions to the physical safety in the metaverse from the following two aspects.

1) Insurance-based Solutions: Cyber-insurance offers a financial instrument for risk mitigation of critical infrastructures in cyberthreats. To resolve the high premium stipulation in traditional insurance offered by insurance companies, Lau *et al.* [128] propose the coalitional insurance in power systems where the coalitional premium is computed by considering loss distributions, vulnerabilities, and budget compliance in an insurance coalition. However, when applying to the metaverse, the scalable and dynamic insurance coalition formation along with fair premium design under diverse cyber threats (e.g., anti-forensics) require further investigation.

2) CPSS-based Solutions: Existing CPSS-based solutions afford lessons for cyberthreat defense to safeguard physical safety in the metaverse. Vellaithurai *et al.* [56] introduce cyber-physical security indices for security measurement of power grid infrastructures. The cyber probes are deployed on host systems to profile system activities, where the generated logs along with the topology information are to build stochastic Bayesian models using belief propagation algorithms. Satchidanandan *et al.* [129] design a dynamic watermarking technique which exploits indelible patterns imprinted in the medium to detect misbehaviors (e.g., signal tampering) of malicious sensors or actuators. To resolve the issues (e.g., low-level abstraction) in task-based programming paradigm, Tariq *et al.* [130] propose a service-oriented paradigm with QoS-aware operation and resource-aware deployment for better support of disruption-free incremental system implementation and reconfiguration. Different from CPSSs, metaverse is an immersive and hyper spatiotemporal virtual space with a sustainable economy ecosystem, which adds extra challenges in migration these solutions.

G. Social Management

In this subsection, we review existing works on social management in the metaverse from the following two perspectives.

1) Misinformation Spreading Mitigation: The extremely rapid information spreading (e.g., gossip) in the metaverse makes the so-called "butterfly effect" more challenging in social governance and public safety in the real world. As an attempt to address this issue, Zhu *et al.* [58] propose to minimize the misinformation influence in online social networks (OSNs) by dynamically selecting a series of nodes to be blocked from the OSN. However, it only works in traditional static OSNs and it is challenging to be applied in the fully interactive metaverse with a huge and time-varying social graph structure.

2) Human Safety and Cyber syndromes: The full immersiveness in metaverse can also raise immersion concerns, e.g., occlusion and chaperone attack, as well as cybersickness. Casey *et al.* [55] investigate a new attack named *human joystick attack* in immersive VR systems such as Oculus Rift and HTC Vive. In their work, adversaries can modify VR environmental factors to deceive, disorient, and control immersed human players and move them to other physical locations without consciousness. Valluripally *et al.* [57] present a novel cybersickness mitigation method and several design principles in social VR learning scenarios via threat quantification and attack-fault tree model construction. However, the ethical issues and adaptations to different attack-defense strategies are not considered in their work, which is an important factor for future metaverse construction.

H. Digital Governance

Almeida *et al.* [59] highlight three principles in the digital governance of content moderation ecosystems: (i) open, transparent, and consensus-driven, (ii) respect human rights, and (iii) publicly accountable. Here, we review existing potential solutions to digital governance in the metaverse from the following three fields.

1) AI Governance: With the pervasive fusion of perception, computing, and actuation, AI will play a leading role to allow digital self-governance of individuals and society in the metaverse in a fully automatic manner. AI approaches can be employed for detecting misbehaving entities and abnormal or Sybil accounts in the metaverse. He *et al.* [131] exploit a multi-factor attention-enhanced LSTM model to dynamically reveal suspicious signals of malicious accounts in online dating applications by mining the user-generated textual information and the interplay of accounts' temporal-spatial activities. Experiments performed on the real-world dataset demonstrate its effectiveness in detection accuracy. However, the outcomes of AI governance algorithms can be biased and unfair (e.g., race bias), thereby arising ethical concerns. Gasser *et al.* [132] propose a three-layer AI governance model from the sociological perspective, where the bottom technical layer allows the data governance and algorithm accountability; the middle ethical layer guides decision-making and data processing via ethical criteria and norms; and the top social and legal layer addresses the allocation of responsibilities in regulation. Zambonelli *et al.* [133] investigate the potential risks including interpretability, trust, autocracy, and ethic issues in delegating the governance of human activities and society to the algorithmic engines in the metaverse. To summarize, both technological and sociological insights are required to build an AI-governed future metaverse.

2) Decentralized Governance: For governance in the large-scale metaverse maintenance, collaborative governance can avoid concentration of regulation rights and promote democracy for avatars. Blockchain technologies offer potential decentralized solutions for collaborative governance in the metaverse, where smart contracts offer a straightforward approach for decentralized governance in an automatic manner. Febrero *et al.* [60] present a blockchain-based decentralized framework in digital city governance to encourage users' active engagement and witness in all administrative processes. In their approach, a verifier group is dynamically selected from digital citizens for transaction verification in the hybrid blockchain. A private-prior peer prediction mechanism is devised for collusion prevention among verifiers, and a Stackelberg game theoretical approach is designed to motivate citizens' participation. Agudo *et al.* [61] design a fair and transparent vehicular governance system based on blockchain, which requires no trusted authorities. Based on SDN, Bai *et al.* [134] design a decentralized data lifecycle governance architecture, where UGC owners can implement customized governance rules for data usage to service providers, aiming to promote an open environment to satisfy users' diverse requirements. To further defend against opportunistic attackers in market manipulation, Li *et al.* [135] study a Dirichlet-based probabilistic detection model to detect compromised local agents in decentralized power grid control systems by evaluating their reputation levels using historical operating observations. The implementation of AI governance under decentralized architectures is a future trend for metaverse governance.

3) Trusted Digital Forensics: Digital forensics is an enabler for accountability in the metaverse under disputes, which has been widely investigated in images and videos. For example, Swaminathan *et al.* [136] develop a general forensic mechanism for digital camera images, according to the observation that in-camera and post-camera image processing leaves a series of distinct fingerprint traces on the digital camera image. The estimated post-camera fingerprints can be employed to validate image authenticity (i.e., whether a specific digital image is from a specific scanner, camera, or computer graphics program). However, the use of anti-forensics makes trusted digital forensics challenging. To address this issue, Stamm *et al.* [137] propose an automatic video frame addition or deletion forensics method with anti-forensics detection, according to the observation that a modified video's motion vectors (i.e., fingerprint) can be imposed in the anti-forensics process.

An obstacle of digital forensics in the metaverse lies in trustworthiness. Blockchain can offer a decentralized solution to establish trust in digital forensics. For example, Li *et al.* [62] utilize blockchain to design a decentralized forensics method, where customized cryptography enables fine-grained forensics data access control and smart contracts enforce auditable forensics execution. Digital forensics can be utilized for accountability of privacy violations. Zou *et al.* [138] propose a privacy leakage forensics scheme with taint analysis and RAM mirroring to obtain digital evidences without touching user's privacy data in a simulated virtual environment. More research efforts are required in terms of resilience, collaboration, QoS enhancement, and privacy preservation in the implementation of digital forensics for metaverse applications.

I. Summary and Insights

From the macro level, the metaverse blends the ternary physical, human, and digital worlds, and blurs the border between the reality and virtuality. From the micro level, the metaverse is composed of multiple interconnected virtual worlds to collectively maintain personalized services for massive users represented by avatars.

For identity management in the metaverse, we have learned that apart from traditional cryptography system design, the fusion of sensory signals (e.g., ECG and PPG) of wearable devices and biometrics (e.g., face and gait) of users can be beneficial for efficient key generation and identity authentication in the metaverse. Besides, blockchain can build trust-free digital identities for metaverse users. Moreover, continuous-time dynamic authentication, as well as cross-chain and cross-domain authentication need further investigation under the metaverse environment. For data management in the metaverse, we have learned that the integration of various cutting-edge technologies in the metaverse results in more attack surfaces on UGC, physical inputs, and metaverse outputs. Besides, blockchain offers a potential solution to ensure data reliability in digital twin creation and mitigation. For privacy in the metaverse, we have learned that users may suffer more privacy exposure in the digital world. In the metaverse, existing privacy threats can be amplified, and new threats related to digital footprints can emerge. For situational awareness in the metaverse, we have learned that AR, AI, honeypot, and SDN technologies can help build situational awareness systems in the metaverse. Besides, global situational awareness can assist monitoring and early-warning of large-scale distributed threats target at multiple sub-metaverses. For creator economy in the metaverse, we have learned that blockchain technology is the key to build the decentralized virtual economy ecosystem from virtual currency creation and trusted UGC/asset/resource trading to economic fairness and ownership traceability. Moreover, the interoperability, resilience, and efficiency issues are prime concerns to construct the sustainable creator economy. For physical safety and social effect in the metaverse, we have learned that existing cyber-insurance and CPSS based approaches can offer some insights for protecting physical devices. More related technological and sociological efforts in this field considering the characteristics of metaverse are required. For digital governance in the metaverse, we have learned that AI-enabled governance and decentralized governance are two trends for future metaverse regulation. Besides, trusted digital forensics offers a promising tool to regulate the metaverse. More research efforts are required from both technological and sociological perspectives.

A comparison of existing/potential security countermeasures in the metaverse is presented in Tables V and VI.

V. Future Research Directions

In this section, we discuss several future research directions in the metaverse from the following aspects.

A. Endogenous Security Empowered Metaverse

Existing commercial metaverse systems mainly depends on the *brought-in security* such as frequent security patch upgrades after the system deployment. Although security upgrades can enhance system security to an extent, the passive defense mechanisms built on security patching strategies inevitably result in the curse of being continuously broken. With the continuity of ubiquitous cyber-physical attack surfaces in the metaverse, current bring-in security defenses can be fragile and costly in practical use, like the sword of Damocles hanging overhead. Endogenous security theory offers a promising solution for provisioning *built-in security* or called *secure by design* mechanisms with self-protection, self-evolution, and autoimmunity capabilities [139], which takes security and privacy factors into account before the system design. Thereby, the future metaverse can resist the ever-increasing known/unknown security vulnerabilities and privacy threats. An example of endogenous security is the quantum key distribution [140], which utilizes channel-based secret keys to resolve information disclosure in wireless transmissions via quantum entanglement properties.

B. Energy-Efficient and Collaborative Metaverse

In the metaverse, the wearable XR devices may be resource-constrained and their communication/computation capacities

TABLE V
SUMMARY OF EXISTING/POTENTIAL SECURITY COUNTERMEASURES IN METAVERSE

Ref.	Security Threat	Threat Type	⋆ Purpose ● Advantages ○ Limitations	Utilized Technology
[66]	Robust key sequence generation	①	⋆Gait-based biometric group key management for wearable devices ●Pass both Diehard and NIST tests with high efficiency ○Lack real-world thorough test	Fuzzy vault
[67]	Gait predictability	①	⋆Real-time and lightweight key establishment for wearable devices ●High matching rate of shake-to-generate secret keys ○Lack complete and thorough evaluation (e.g., NIST tests)	HCI
[68]	Hijack of WIMDs	①	⋆Efficient ECG-based key distribution for WIMDs ●High false acceptance rate ○Relatively low precision in ECG signal processing	Fuzzy commitment, fuzzy vault
[69]	Dolev-Yao threat	①	⋆Low-cost mutual authentication for wearable medical devices ●Efficient authentication with low communication cost ○Without consideration of the immersiveness of users	Real-or-Random model
[70]	Random attack, synthesis attack	①	⋆Low-cost PPG-based continuous authentication for wearables ●Low communication overhead and computation cost ○Unscalable to large-scale networks	Motion artifacts, gradient boosting tree
[71]	Privacy leakage	①,③	⋆Privacy-preserving identity authentication for wearable devices ●Ensure privacy protection with low system overheads ○Lack real-world thorough evaluation	MinHash, CP-ABE, bloom filter, edge computing
[73]	Eavesdropping, impersonation, man-in-the-middle	①,③	⋆Decentralized cross-domain authentication in industrial IoT ●Anonymous identity authentication and low overhead ○Low response speed due to the low throughput of blockchains	Blockchain
[74]	Data tampering, impersonation	①,③	⋆Efficient cross-domain authentication in optimized blockchain ●Fast response, anonymous authentication, and low overhead ○Lack large-scale real-world test	Blockchain, multiple Merkle tree
[75]	Identity retention under PKI	①	⋆Decentralized PKI with strong identity retention ●Eliminate the risk of CA centralization ○Lack large-scale real-world test	Blockchain
[78]	Threats to digital twin	②	⋆Reliable state replication method for digital twin synchronization ●Low computational cost and synchronization latency ○Lack trustworthiness guarantee of data collected from disparate data silos	Cloud computing, digital twin
[49]	Trustworthiness of digital twin	②	⋆Trustworthy data dissemination and fault diagnosis for digital twins ●High reliability of data sources in digital twin creation ○Lack accurate representation of digital footprints	Blockchain
[80]	Low data quality	②	⋆Quality-aware vehicular service access with mobility support ●High average service quality and network success rate ○Lack impact analysis on trust management and security issues	Generation tree, bi-direction buffering
[85]	Location tracking in AR games	③	⋆Attack model construction and possible mitigation design ●Fine-grained and high-accuracy location tracking attack modeling ○Lack complete defense analysis under real-world test	Cloud, AR, access control
[89]	Unauthorized UGVC access	③	⋆Time-domain access control with provable security for UGVC sharing ●Support time-domain UGVC access control ○Lack consideration of illegal UGC redistribution	CP-ABE
[90]	Illegal UGC redistribution	③	⋆Secure encrypted UGMC sharing scheme with fair traitor tracing ●High traitor tracing accuracy and perceptual quality ○Ignore UGMC usage control	Proxy re-encryption, fair watermarking
[45]	Unintended UGC usage	③	⋆Fine-grained and transparent UGC usage/processing audit ●Low computational overheads in UGC usage/processing audit ○Lack large-scale and real-world performance test	Smart contract, trusted computing
[40]	Privacy exposure in UGC sharing	③	⋆Graph-based local DP for privacy-preserving topic recommendation ●High-level privacy and high efficiency in user-linkage unassociation ○Lack image indistinguishability mechanism in practical use	Local DP
[91]	Privacy exposure in UGC sharing	③	⋆Secure data collaboration with class imbalance scenarios ●High accuracy in abnormal health detection ○Lack Byzantine robustness in FL	FL
[94]	Co-photo privacy	③	⋆Personalized facial recognition with privacy protection in photo sharing ●High recognition ratio and efficiency in OSNs ○Lack implementation and test on personal clouds (e.g., Dropbox)	Facial recognition
[95]	Compromising reflections	③	⋆Automatically reconstruct user typing on virtual keyboards ●Effective attack execution with high robustness and accuracy ○Lack effective defense design	Feature extraction and matching
[11]	Threats to digital footprints	③	⋆Privacy preservation tools for digital footprints in social metaverse ●Offer complete confusion and private copy tools for avatars ○Lack user experience analysis and practical deployment of such tools	Avatar confusion, private copy

①: identity-related threats; ②: data-related threats; ③: privacy threats; ④: network-related threats; ⑤: economy-related threats; ⑥: physical/social effects; ⑦: governance-related threats.

TABLE VI
SUMMARY OF EXISTING/POTENTIAL SECURITY COUNTERMEASURES IN METAVERSE (CONTINUED)

Continued from previous page

Ref.	**Security Threat**	**Threat Type**	⋆ **Purpose** ● **Advantages** ○ **Limitations**	**Utilized Technology**
[98]	Intrusion of VR control system	④	⋆Smart intrusion detection to detect attacks in 3D VR environments ●High classification and detection accuracy ○Cannot resist unknown/new attack types	SVM
[102]	Malicious events in distribution grid	④	⋆Data-driven situational awareness in large-scale distributed power grids ●High accuracy in malicious event labeling ○Rely on additional expert knowledge for costly event labeling	Multi-class SVM
[104]	Intrusion of indistrial control system	④	⋆Monitoring and profiling of potential attack behaviors ●High detection/prediction accuracy and low response time ○Lack merging other cutting-edge technologies into this framework	SDN, digital twin
[105]	Large-scale network intrusion	④	⋆Honeynet-based situational awareness to deceive attackers ●Rapid honeynet deployment with adaptability to unknown threats ○Low scalability and programmability in large-scale deployment	Honeynet
[106]	Large-scale network intrusion	④	⋆SDN-enabled virtual honeynet with high scalability and flexibility ●Successful implementation and test in real-world EU project ○Lack resilience of compromised domain operators	SDN, honeynet
[48]	Low cooperation in creator economy	⑤	⋆Swarm economy model for cooperative and dynamic digital resource sharing ●Real-world implementation of blockchain in such economy model ○Non-supervisability in transaction settlement and high computational overhead	Blockchain
[108]	Lack supervisability on criminal transaction	⑤	⋆Three-layer sharding blockchain for scalable and automatic transaction ●Enhanced system scalability and traceability of criminal transactions ○Lack vulnerability analysis and large-scale real-world simulations	Blockchain sharding
[23]	Compromised nodes/services	⑤	⋆Intelligent trust model to quantitatively evaluate user/service trustworthiness ●Aggregate multi-dimensional trust attributes for high-accuracy trust computing ○Lack complexity and scalability analysis, as well as cold start issues	Machine learning
[114]	Economic fairness, strategic users	⑤	⋆Strategy-proof and privacy-preserving auction for heterogeneous spectrum ●Privacy protection, strategy-proofness, and high social welfare ○Vulnerable to collusive bidders in auction	HE, auction
[117]	Economic fairness, free-riding attack	⑤	⋆Blockchain-based fair ad delivery among connected vehicles ●Enable anonymity and conditional linkability ○Not support batch verification of aggregated dissemination proofs	Smart contracts, ZKP
[52]	Economic fairness, collusion attack	⑤	⋆Collusion-resistant auction design in cooperative communications ●Truthfulness, collusion-resistance, and budget-balance ○Only apply to wireless cooperative communications	Game theory
[56]	Stochastic risk on power system	⑥	⋆Cyber-physical security indices for security measurement of power systems ●Efficient indices computing under actual attacks in real-world test-bed ○Lack merging other cutting-edge technologies into this framework	Graph theory
[128]	High premium stipulation	⑥	⋆Coalitional insurance with budget compliance for risk control in power grids ●High defense level with long-term reduced premiums ○Lack dynamic insurance design and dependence analysis of cyberthreats	Cyber-insurance
[58]	Butterfly effect in information spreading	⑥	⋆Minimize misinformation influence via dynamic node blocking in OSNs ●Low misinformation spreading value and misinformation interactions ○Challenging to be applied to the dynamic and time-varying metaverse	Heuristic greedy
[55]	Human joystick attack	⑥	⋆Construct human joystick attack model in immersive VR systems ●Deceive and move immersed players to intended physical locations unconsciously ○Lack effective defense design	HCI, VR
[131]	Abnormal social accounts	⑦	⋆Dynamically reveal suspicious signals of malicious accounts in online dating ●High F1-score and AUC on a real-world dataset gathered from Momo ○Challenging to be applied to dating services atop the blockchain	Attention-based LSTM
[60]	Centralized governance risks	⑦	⋆Decentralized digital city governance with incentives for user engagement/witness ●High user utility and time efficiency in decentralized governance ○Scalability and security issues in practical system deployment	Blockchain, Stackelberg game
[135]	Opportunistic attacks for price manipulation	⑦	⋆Detect compromised local agents in decentralized power systems using reputation ●Fast aggressive attacker detection using the PowerWorld simulator ○Lack credibility analysis for historical operations in reputation evaluation	Dirichlet-based probabilistic model
[136]	Image authenticity	⑦	⋆General camera image forensic via post-camera fingerprints ●High efficiency in non-intrusive digital image forensics ○Absense of anti-forensics defense	Image fingerprints
[137]	Anti-forensics attack	⑦	⋆Automatic video frame addition or deletion forensics with anti-forensics detection ●Able to automatically detect video tampering/forgeries with high accuracy ○Lack trusted whole-process video forensics	Anti-forensic, game theory
[138]	Privacy violation	⑦	⋆Privacy leakage forensics to ensure accountability of privacy violations ●High detection efficiency of privacy leakage paths on real malware samples ○Only consider limited detection attributes and privacy leakage paths	Cloud forensics

①: identity-related threats; ②: data-related threats; ③: privacy threats; ④: network-related threats; ⑤: economy-related threats;
⑥: physical/social effects; ⑦: governance-related threats.

can be highly heterogeneous. The future metaverse design should be energy-efficient and incorporate users/avatars' cooperation in terms of UGC dissemination, resource sharing, security provision, and privacy preservation. For example, users' social cooperation can be beneficial to create and distribute high-quality UGC games via the formation of social groups. Besides, the collaboration among heterogeneous metaverse devices with temporal and spatial correlations, along with the orchestration with edge-cloud computing, can be leveraged to design lightweight and energy-efficient consensus protocols [22] tailored to specific resource-limited metaverse environments. In addition, by analyzing the metaverse system as a whole, the cooperation among various sub-metaverses is essential to facilitate seamless security provision and privacy protection and requires further investigation. An example is to dynamically allocate spatiotemporal security resource (e.g., intrusion detection and prevention system (IDPS)) allocation among heterogeneous sub-metaverses with unbalanced resource distribution.

C. Content-Centric and Human-Centric Metaverse

In the future metaverse, a surge of UGC is expected to be created, requested, and delivered across various sub-metaverses. Existing IP-based content transmissions can face critical challenges in securing UGC dissemination to massive heterogeneous end devices over the large-scale metaverse across virtual worlds. Content-centric networking (CCN) stands for a paradigm shift of current Internet architecture. In contrast to current IP-based and host-oriented Internet architecture, contents are addressed and routed directly by their naming information in CCN instead of IP addresses. In CCN-based metaverse, the UGC consumer can request the desired UGC object by sending an interest message to any CCN node that hosts the matched UGC. Besides, CCN embodies a security model which explicitly ensures the security of individual content pieces instead of securing the "pipe" or the connection. Therefore, the deployment of CCN can offer a more flexible, scalable, and secure network in the metaverse. However, CCN can also bring new security concerns in the metaverse and one of that is content poisoning, in which adversaries can contaminate the cache space of metaverse nodes by injecting poisoned UGCs and further cause the delay and even failure in retrieving valid UGCs via flooding attacks. In addition, the design of metaverse should be human-centric. For example, users/avatars' personalized privacy preferences should be ensured in developing privacy-preserving approaches in metaverse environments.

D. Cross-Chain Interoperable and Regulatory Metaverse

Blockchain is recognized as the underlying technology to build the future virtual economy ecosystem in the metaverse. However, blockchain itself also faces interoperability concerns as different sub-metaverses can be built on heterogeneous blockchains (e.g., using different transaction formats, block structures, and consensus protocols) to satisfy diverse QoS requirements. An example is the exchange of different cryptocurrencies such as Bitcoin and Ethereum. Cross-chain governance is essential to ensure the security and legitimacy of digital asset related activities (e.g., asset trading) across different sub-metaverses built on heterogeneous blockchains. Open challenges include the programmable and scalable cross-chain governance architecture design, on-chain entity identification and risk assessment, dynamic and collaborative cross-chain supervision, etc.

VI. Conclusion

In this paper, we have presented an in-depth survey of the fundamentals, security, and privacy of metaverse. Specifically, we have introduced a novel distributed metaverse architecture and discussed its key characteristics, enabling technologies, and modern prototypes. Afterward, the security and privacy threats, as well as the critical challenges in security defenses and privacy preservation, have been investigated under the distributed metaverse architecture. Furthermore, we have reviewed the existing/potential solutions in designing tailored security and privacy countermeasures for the metaverse. We expect that this survey can shed light on the security and privacy provision in metaverse applications, and inspire more pioneering research in this emerging area.

References

[1] Q. Yang, Y. Zhao, H. Huang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *arXiv preprint arXiv:2201.03201*, 2022.

[2] J. Sanchez, "Second life: An interactive qualitative analysis," in *Society for Information Technology & Teacher Education International Conference*, 2007, pp. 1240–1243.

[3] J. D. N. Dionisio, W. G. B. III, and R. Gilbert, "3D virtual worlds and the metaverse: Current status and future possibilities," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, pp. 1–38, 2013.

[4] A. Bruun and M. L. Stentoft, "Lifelogging in the wild: Participant experiences of using lifelogging as a research tool," in *IFIP Conference on Human-Computer Interaction*, 2019, pp. 431–451.

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

[6] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," *arXiv preprint arXiv:2110.05352*, 2021.

[7] D. Grider and M. Maximo. (2021) The metaverse: Web3.0 virtual cloud economies. Accessed: Nov. 1, 2021. [Online]. Available: https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf

[8] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in *Proceedings of ACM Multimedia (MM)*, Oct. 2021, pp. 153—161.

[9] (2021) Facebook Inc. rebrands as Meta to stress 'metaverse' plan. Accessed: October 28, 2021. [Online]. Available: https://machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/

[10] R. E. Leenes, "Privacy in the metaverse: Regulating a complex social construct in a virtual world," *Proceedings of the Ifip/fidis Summer School on the Future of Identity in the Information Society*, pp. 1–18, 2008.

[11] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 52–61, 2018.

[12] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *IEEE Conference on Computer Communications (INFOCOM)*, 2015, pp. 747–755.

[13] K. J. Nevelsteen, "Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the metaverse," *Computer Animation and Virtual Worlds*, vol. 29, no. 1, pp. 1–22, 2018.

[14] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "Metachain: A novel blockchain-based framework for metaverse applications," *arXiv preprint arXiv:2201.00759*, 2021.

[15] K. Yoon, S.-K. Kim, S. P. Jeong, and J.-H. Choi, "Interfacing cyber and physical worlds: Introduction to IEEE 2888 standards," in *IEEE International Conference on Intelligent Reality (ICIR)*, 2021, pp. 49–50.

[16] S.-M. Park and Y.-G. Kim, "A metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 10, pp. 4209–4251, 2022.

[17] M. Bourlakis, S. Papagiannidis, and F. Li, "Retail spatial evolution: Paving the way from traditional to metaverse retailing," *Electronic Commerce Research*, vol. 9, no. 1–2, pp. 135–148, Jun 2009.

[18] J. Díaz, C. Andrés, D. Saldaa, C. Alberto, and R. Avila, "Virtual world as a resource for hybrid education," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 15, pp. 94–109, 2020.

[19] L. Lee, Z. Lin, R. Hu, Z. Gong, A. Kumar, T. Li, S. Li, and P. Hui, "When creators meet the metaverse: A survey on computational arts," *CoRR*, vol. abs/2111.13486, 2021.

[20] L. Heller and L. Goodman, "What do avatars want now? posthuman embodiment and the technological sublime," in *International Conference on Virtual System Multimedia (VSMM)*, 2016, pp. 1–4.

[21] A. C. S. Genay, A. Lecuyer, and M. Hachet, "Being an avatar "for real": a survey on virtual embodiment in augmented reality," *IEEE Transactions on Visualization and Computer Graphics*, 2021, doi: 10.1109/TVCG.2021.3099290.

[22] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 160–209, 2022.

[23] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for IoT services," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39–52, 2019.

[24] M. Sugimoto, "Extended reality (XR: VR/AR/MR), 3D printing, holography, AI, radiomics, and online VR Tele-medicine for precision surgery," in *Surgery and Operating Room Innovation*. Springer, 2021, pp. 65–70.

[25] Y. Wu, K. Zhang, and Y. Zhang, "Digital twin networks: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13 789–13 804, 2021.

[26] H. Du, D. Niyato, J. Kang, D. I. Kim, and C. Miao, "Optimal targeted advertising strategy for secure wireless edge metaverse," *arXiv preprint arXiv:2111.00511*, 2021.

[27] E. H.-K. Wu, C.-S. Chen, T.-K. Yeh, and S.-C. Yeh, "Interactive medical VR streaming service based on software-defined network: Design and implementation," in *IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*, 2020, pp. 1–2.

[28] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[29] S. Vural, D. Wei, and K. Moessner, "Survey of experimental evaluation studies for wireless mesh network deployments in urban areas towards ubiquitous Internet," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 223–239, 2013.

[30] C. Kai, H. Zhou, Y. Yi, and W. Huang, "Collaborative cloud-edge-end task offloading in mobile-edge computing networks with limited communication capability," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 2, pp. 624–634, 2021.

[31] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li, A. Seneviratne, Y. Li, and H. V. Poor, "Enabling AI in future wireless networks: A data life cycle perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 553–595, 2021.

[32] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (nft): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*, 2021.

[33] J. Han, J. Heo, and E. You, "Analysis of metaverse platform as a new play culture: Focusing on Roblox and ZEPETO," in *International Conference on Human-centered Artificial Intelligence*, 2021, pp. 1–10.

[34] F. L. Greitzer, A. P. Moore, D. M. Cappelli, D. H. Andrews, L. A. Carroll, and T. D. Hull, "Combating the insider cyber threat," *IEEE Security & Privacy*, vol. 6, no. 1, pp. 61–64, 2008.

[35] D. Antonioli, N. Tippenhauer, and K. Rasmussen, "BIAS: Bluetooth impersonation attacks," in *IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 549–562.

[36] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 19–32, 2022.

[37] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[38] H. Guo, Y. Yu, T. Xiang, H. Li, and D. Zhang, "The availability of wearable-device-based physical data for the measurement of construction workers' psychological status on site: From the perspective of safety management," *Automation in Construction*, vol. 82, pp. 207–217, 2017.

[39] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2017, pp. 468–477.

[40] J. Wei, J. Li, Y. Lin, and J. Zhang, "LDP-based social content protection for trending topic recommendation," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4353–4372, 2021.

[41] S. Wasserkrug, A. Gal, and O. Etzion, "Inference of security hazards from event composition based on incomplete or uncertain information," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, pp. 1111–1114, 2008.

[42] X. Li, J. He, P. Vijayakumar, X. Zhang, and V. Chang, "A verifiable privacy-preserving machine learning prediction scheme for edge-enhanced HCPSs," *IEEE Transactions on Industrial Informatics*, 2021, doi: 10.1109/TII.2021.3110808.

[43] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[44] J. Yu, Z. Kuang, B. Zhang, W. Zhang, D. Lin, and J. Fan, "Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1317–1332, 2018.

[45] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7688–7699, 2021.

[46] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[47] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[48] L. C. C. De Biase, P. C. Calcina-Ccori, G. Fedrecheski, G. M. Duarte, P. S. S. Rangel, and M. K. Zuffo, "Swarm economy: A model for transactions in a distributed and organic IoT platform," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4561–4572, 2019.

[49] S. Suhail, R. Hussain, R. Jurdak, and C. S. Hong, "Trustworthy digital twins in the industrial internet of things with blockchain," *IEEE Internet Computing*, 2021, doi: 10.1109/MIC.2021.3059320.

[50] H. Ritzdorf, C. Soriente, G. O. Karame, S. Marinovic, D. Gruber, and S. Capkun, "Toward shared ownership in the cloud," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3019–3034, 2018.

[51] M. Zhang, L. Yang, S. He, M. Li, and J. Zhang, "Privacy-preserving data aggregation for mobile crowdsensing with externality: An auction approach," *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1046–1059, 2021.

[52] Z. Xu and W. Liang, "Collusion-resistant repeated double auctions for relay assignment in cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1196–1207, 2014.

[53] M. Li, J. Yu, and J. Wu, "Free-riding on BitTorrent-like peer-to-peer file sharing systems: Modeling analysis and improvement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 7, pp. 954–966, 2008.

[54] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 389–425, 2020.

[55] P. Casey, I. Baggili, and A. Yarramreddy, "Immersive virtual reality attacks and the human joystick," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 550–562, 2021.

[56] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.

[57] S. Valluripally, A. Gulhane, K. A. Hoque, and P. Calyam, "Modeling and defense of social virtual reality attacks inducing cybersickness," *IEEE Transactions on Dependable and Secure Computing*, 2021, doi: 10.1109/TDSC.2021.3121216.

[58] J. Zhu, P. Ni, and G. Wang, "Activity minimization of misinformation influence in online social networks," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 4, pp. 897–906, 2020.

[59] V. Almeida, F. Filgueiras, and D. Doneda, "The ecosystem of digital content governance," *IEEE Internet Computing*, vol. 25, no. 3, pp. 13–17, 2021.

[60] Y. Bai, Q. Hu, S.-H. Seo, K. Kang, and J. J. Lee, "Public participation consortium blockchain for smart city governance," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2094–2108, 2022.

[61] I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A blockchain approach for decentralized V2X (D-V2X)," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4001–4010, 2021.

[62] M. Li, J. Weng, J.-N. Liu, X. Lin, and C. Obimbo, "Towards vehicular digital forensics from decentralized trust: An accountable, privacy-preserving, and secure realization," *IEEE Internet of Things Journal*, 2021, doi: 10.1109/JIOT.2021.3116957.

[63] J. Jensen and M. G. Jaatun, "Federated identity management - we built it; why won't they come?" *IEEE Security Privacy*, vol. 11, no. 2, pp. 34–41, 2013.

[64] E. Samir, H. Wu, M. Azab, C. S. Xin, and Q. Zhang, "DT-SSIM: A decentralized trustworthy self-sovereign identity management framework," *IEEE Internet of Things Journal*, 2021, doi: 10.1109/JIOT.2021.3112537.

[65] M. De Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. E. Otung, "Key management for beyond 5G mobile small cells: A survey," *IEEE Access*, vol. 7, pp. 59 200–59 236, 2019.

[66] F. Sun, W. Zang, H. Huang, I. Farkhatdinov, and Y. Li, "Accelerometer-based key generation and distribution method for wearable IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1636–1650, 2020.

[67] Z. Chen, W. Ren, Y. Ren, and K.-K. R. Choo, "LiReK: A lightweight and real-time key establishment scheme for wearable embedded devices by gestures or motions," *Future Generation Computer Systems*, vol. 84, pp. 126–138, 2018.

[68] G. Zheng, R. Shankaran, W. Yang, C. Valli, L. Qiao, M. A. Orgun, and S. C. Mukhopadhyay, "A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices," *IEEE Sensors Journal*, vol. 19, no. 3, pp. 1186–1198, 2018.

[69] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 942–956, 2018.

[70] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, "Trueheart: Continuous authentication on wrist-worn wearables using PPG-based biometrics," in *IEEE Conference on Computer Communications (INFOCOM)*, 2020, pp. 30–39.

[71] H. Liu, X. Yao, T. Yang, and H. Ning, "Cooperative privacy preservation for wearable devices in hybrid computing-based smart health," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1352–1362, 2018.

[72] Y. Wang and Y. L. Wang, "A heterogeneous cross-domain authentication model based on access tickets in virtual cable television network," in *Applied Mechanics and Materials*, vol. 742, 2015, pp. 717–720.

[73] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[74] J. Chen, Z. Zhan, K. He, R. Du, D. Wang, and F. Liu, "XAuth: Efficient privacy-preserving cross-domain authentication," *IEEE Transactions on Dependable and Secure Computing*, 2021, doi: 10.1109/TDSC.2021.3092375.

[75] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized public key infrastructure with identity retention." *IACR Cryptology ePrint Archive*, vol. 2014, p. 803, 2014.

[76] Y. Zhu, L. T. Yang, J. Feng, and X. Xie, "Tensor-based GAN to defense adversarial attacks for cyber-physical-social system," *IEEE Transactions on Network Science and Engineering*, 2021, doi: 10.1109/TNSE.2021.3077305.

[77] R. Gharsallaoui, M. Hamdi, and T.-H. Kim, "A novel privacy technique for augmented reality cloud gaming based on image authentication," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 252–257.

[78] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 669–680, 2020.

[79] W. B. Qaim and O. Ozkasap, "DRAW: Data replication for enhanced data availability in IoT-based sensor systems," in *Proceedings of IEEE DASC/PiCom/DataCom/CyberSciTech*, 2018, pp. 770–775.

[80] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, "A cooperative quality-aware service access system for social internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2506–2517, 2018.

[81] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1530–1540, 2018.

[82] M. Kamal *et al.*, "Light-weight security and data provenance for multi-hop internet of things," *IEEE Access*, vol. 6, pp. 34 439–34 448, 2018.

[83] S. Bono, D. Caselden, G. Landau, and C. Miller, "Reducing the attack surface in massively multiplayer online role-playing games," *IEEE Security Privacy*, vol. 7, no. 3, pp. 13–19, 2009.

[84] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, "Towards security and privacy for multi-user augmented reality: Foundations with end users," in *IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 392–408.

[85] J. Shang, S. Chen, J. Wu, and S. Yin, "ARSpy: Breaking location-based multi-player augmented reality application for user location tracking," *IEEE Transactions on Mobile Computing*, vol. 21, no. 2, pp. 433–447, 2022.

[86] J. Laakkonen, J. Parkkila, P. Jäppinen, J. Ikonen, and A. Seffah, "Incorporating privacy into digital game platform design: The what, why, and how," *IEEE Security & Privacy*, vol. 14, no. 4, pp. 22–32, 2016.

[87] P. M. Corcoran and C. Costache, "A privacy framework for games & interactive media," in *IEEE Games, Entertainment, Media Conference (GEM)*, 2018, pp. 1–9.

[88] C. Ma, Z. Yan, and C. W. Chen, "Scalable access control for privacy-aware media sharing," *IEEE Transactions on Multimedia*, vol. 21, no. 1, pp. 173–183, 2019.

[89] K. Yang, Z. Liu, X. Jia, and X. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," *IEEE Transactions on Multimedia*, vol. 18, no. 5, pp. 940–950, 2016.

[90] L. Y. Zhang, Y. Zheng, J. Weng, C. Wang, Z. Shan, and K. Ren, "You can access but you cannot leak: Defending against illegal content redistribution in encrypted cloud media center," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1218–1231, 2020.

[91] D. Y. Zhang, Z. Kou, and D. Wang, "FedSens: A federated learning approach for smart health sensing with class imbalance in resource constrained edge computing," in *IEEE Conference on Computer Communications (INFOCOM)*, 2021, pp. 1–10.

[92] L. Jiang, H. Zheng, H. Tian, S. Xie, and Y. Zhang, "Cooperative federated learning and model update verification in blockchain empowered digital twin edge networks," *IEEE Internet of Things Journal*, 2021, doi: 10.1109/JIOT.2021.3126207.

[93] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang, "BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs," *IEEE Transactions on Dependable and Secure Computing*, 2020, doi: 10.1109/TDSC.2020.3025129.

[94] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 199–210, 2017.

[95] R. Raguram, A. M. White, Y. Xu, J.-M. Frahm, P. Georgel, and F. Monrose, "On the privacy risks of virtual keyboards: Automatic reconstruction of typed input from compromising reflections," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 3, pp. 154–167, 2013.

[96] J. Woodward and J. Ruiz, "Analytic review of using augmented reality for situational awareness," *IEEE Transactions on Visualization and Computer Graphics*, 2022, doi: 10.1109/TVCG.2022.3141585.

[97] U. Ju, L. L. Chuang, and C. Wallraven, "Acoustic cues increase situational awareness in accident situations: A VR car-driving study," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2020.

[98] Z. Lv, D. Chen, R. Lou, and H. Song, "Industrial security solution for virtual reality," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6273–6281, 2021.

[99] L. Vu, V. L. Cao, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Learning latent representation for IoT anomaly detection," *IEEE Transactions on Cybernetics*, pp. 1–14, 2020.

[100] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 7, no. 6, pp. 871–881, 2013.

[101] R. Heartfield, G. Loukas, A. Bezemskij, and E. Panaousis, "Self-configurable cyber-physical intrusion detection for smart homes using

reinforcement learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1720–1735, 2021.

[102] A. Shahsavari, M. Farajollahi, E. M. Stewart, E. Cortez, and H. Mohsenian-Rad, "Situational awareness in distribution grid using micro-PMU data: A machine learning approach," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6167–6177, 2019.

[103] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big data analysis-based security situational awareness for smart grid," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 408–417, 2018.

[104] P. Krishnan, K. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal, and H. Song, "MUD-based behavioral profiling security framework for software-defined IoT networks," *IEEE Internet of Things Journal*, 2021, doi: 10.1109/JIOT.2021.3113577.

[105] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, "An IoT honeynet based on multiport honeypots for capturing IoT attacks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3991–3999, 2020.

[106] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. Alcaraz Calero, "Virtual IoT honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1262–1277, 2020.

[107] M. H. u. Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1196–1212, 2020.

[108] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4680–4693, 2019.

[109] A. Das and M. M. Islam, "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 261–274, 2012.

[110] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling reputation and trust in privacy-preserving mobile sensing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2777–2790, 2013.

[111] F. Wu, T. Zhang, C. Qiao, and G. Chen, "A strategy-proof auction mechanism for adaptive-width channel allocation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2678–2689, 2016.

[112] Y. Wang, Z. Su, T. Luan, R. Li, and K. Zhang, "Federated learning with fair incentives and robust aggregation for UAV-aided crowdsensing," *IEEE Transactions on Network Science and Engineering*, 2021, doi: 10.1109/TNSE.2021.3138928.

[113] Z. Wan, T. Zhang, W. Liu, M. Wang, and L. Zhu, "Decentralized privacy-preserving fair exchange scheme for V2G based on blockchain," *IEEE Transactions on Dependable and Secure Computing*, 2021, doi: 10.1109/TDSC.2021.3059345.

[114] Y. Chen, X. Tian, Q. Wang, M. Li, M. Du, and Q. Li, "ARMOR: A secure combinatorial auction for heterogeneous spectrum," *IEEE Transactions on Mobile Computing*, vol. 18, no. 10, pp. 2270–2284, 2019.

[115] K. Shin, C. Joe-Wong, S. Ha, Y. Yi, I. Rhee, and D. S. Reeves, "T-Chain: A general incentive scheme for cooperative computing," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2122–2137, 2017.

[116] R. Ma, S. Lee, J. Lui, and D. Yau, "Incentive and service differentiation in P2P networks: A game theoretic approach," *IEEE/ACM Transactions on Networking*, vol. 14, no. 5, pp. 978–991, 2006.

[117] M. Li, J. Weng, A. Yang, J.-N. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 248–11 259, 2019.

[118] P. Razmi, M. O. Buygi, and M. Esmalifalak, "A machine learning approach for collusion detection in electricity markets based on nash equilibrium theory," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 1, pp. 170–180, 2021.

[119] H. Shen, Y. Lin, K. Sapra, and Z. Li, "Enhancing collusion resilience in reputation systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 8, pp. 2274–2287, 2016.

[120] J. Liu and B. Yang, "Collusion-resistant multicast key distribution based on homomorphic one-way function trees," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 980–991, 2011.

[121] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, "User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Transactions on Computers*, vol. 65, no. 9, pp. 2939–2946, 2016.

[122] K. Li, S. Wang, X. Cheng, and Q. Hu, "A misreport- and collusion-proof crowdsourcing mechanism without quality verification," *IEEE Transactions on Mobile Computing*, 2021, doi: 10.1109/TMC.2021.3052873.

[123] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, 2019.

[124] S. Malik, S. S. Kanhere, and R. Jurdak, "ProductChain: Scalable blockchain framework to support provenance in supply chains," in *IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 2018, pp. 1–10.

[125] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17 465–17 477, 2017.

[126] Y. Wang, Z. Su, J. Li, N. Zhang, K. Zhang, K.-K. R. Choo, and Y. Liu, "Blockchain-based secure and cooperative private charging pile sharing services for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1857–1874, 2022.

[127] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-Ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1214–1229, 2021.

[128] P. Lau, L. Wang, Z. Liu, W. Wei, and C.-W. Ten, "A coalitional cyber-insurance design considering power system reliability and cyber vulnerability," *IEEE Transactions on Power Systems*, vol. 36, no. 6, pp. 5512–5524, 2021.

[129] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," *Proceedings of the IEEE*, vol. 105, no. 2, pp. 219–240, 2017.

[130] M. U. Tariq, J. Florence, and M. Wolf, "Improving the safety and security of wide-area cyber–physical systems through a resource-aware, service-oriented development methodology," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 144–159, 2018.

[131] X. He, Q. Gong, Y. Chen, Y. Zhang, X. Wang, and X. Fu, "DatingSec: Detecting malicious accounts in dating apps using a content-based attention network," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2193–2208, 2021.

[132] U. Gasser and V. A. Almeida, "A layered model for AI governance," *IEEE Internet Computing*, vol. 21, no. 6, pp. 58–62, 2017.

[133] F. Zambonelli, F. Salim, S. W. Loke, W. De Meuter, and S. Kanhere, "Algorithmic governance in smart cities: The conundrum and the potential of pervasive computing solutions," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 80–87, 2018.

[134] G. Huang, C. Luo, K. Wu, Y. Ma, Y. Zhang, and X. Liu, "Software-defined infrastructure for decentralized data lifecycle governance: Principled design and open challenges," in *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 1674–1683.

[135] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415–2425, 2016.

[136] A. Swaminathan, M. Wu, and K. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 101–117, 2008.

[137] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Temporal forensics and anti-forensics for motion compensated video," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1315–1329, 2012.

[138] D. Zou, J. Zhao, W. Li, Y. Wu, W. Qiang, H. Jin, Y. Wu, and Y. Yang, "A multigranularity forensics and analysis method on privacy leakage in cloud environment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1484–1494, 2019.

[139] Z. Zhou, X. Kuang, L. Sun, L. Zhong, and C. Xu, "Endogenous security defense against deductive attack: When artificial intelligence meets active defense for online service," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 58–64, 2020.

[140] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, "Field test of measurement-device-independent quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 116–122, 2015.