ParaDefender: A Scenario-Driven Parallel System for Defending Metaverses

Jinpeng Han, *Student Member, IEEE*, Manzhi Yang, Xiaoguang Chen, Hongtao Liu, Yuntao Wang, Jianhao Li, Zhou Su, Zhen Li, and Xiaobo Ma

***Abstract*—The metaverse, as an instance of cyber–physical–social systems (CPSS) that originates in cyber–physical systems (CPS), features growing complexity, and diversity in terms of functionalities, as well as the exponentially increasing demand in network bandwidth and computational resources, thereby leading to exaggerated security threats. However, compared with the extensive attention received by the metaverse, solutions defending against the threats have not kept pace. A major obstacle to such solutions is virtuality–reality-synthesized threats. Therefore, it is imperative to design new paradigms to defend the metaverse effectively. In this article, we advance a parallel system, dubbed ParaDefender, to defend the metaverse against emerging new threats effectively. Inspired by parallel intelligence, ParaDefender comprises artificial cyberspace, computational experiments, and parallel execution. The basic idea is to make artificial and real cyberspaces executed in parallel to mutually guide each other for enhanced security, wherein the parallel execution is scenario driven in the sense that the scenarios originate from all possible spatial–temporal combinations of security threats in the metaverse. We also demonstrate how to land ParaDefender onto real-world applications, including the Industrial Internet of Things (IIoT) security operation application in the industrial metaverse, and the social governance application.**

***Index Terms*—Cyber–physical–social systems (CPSS), parallel intelligence (PI), parallel security, scenario engineering (SE), security in metaverses.**

Manuscript received 15 November 2022; revised 8 December 2022; accepted 10 December 2022. Date of publication 22 December 2022; date of current version 17 March 2023. This work was supported by the National Key Research and Development Program of China under Grant 2018AAA0101502 and the Joint Science and Technology Project of SGCC (State Grid Corporation of China): Fundamental Theory of Human-in-the-Loop Hybrid-Augmented Intelligence for Power Grid Dispatch and Control. This article was recommended by Associate Editor F. Y. Wang. *(Jinpeng Han and Manzhi Yang contributed equally to this work.) (Corresponding author: Xiaobo Ma.)*

Jinpeng Han is with the School of Software Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: jinpeng.han@stu.xjtu.edu.cn).

Manzhi Yang and Xiaoguang Chen are with the Macau Institute of Systems Engineering, Macau University of Science and Technology, Macau, China (e-mail: yangmanzhi@eversec.cn; chenxiaoguang@eversec.cn).

Hongtao Liu, Yuntao Wang, Jianhao Li, Zhou Su, and Xiaobo Ma are with the MOE Key Laboratory for Intelligent Networks and Network Security, Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: lht974868031@stu.xjtu.edu.cn; yuntao.wang@xjtu.edu.cn; 1269047508@stu.xjtu.edu.cn; zhousu@xjtu.edu.cn; xma.cs@xjtu.edu.cn).

Zhen Li is with North Automatic Control Technology Institute, Taiyuan 030006, China (e-mail: zhen.li@qaii.ac.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2022.3228928.

Digital Object Identifier 10.1109/TSMC.2022.3228928

I. Introduction

CLOSELY following the birth of mirror worlds in 1991, wherein every real scene in the real world could be projected into a software model and interact with the model through a monitor [1], the metaverse was conceptualized from the cyberpunk culture in a science fiction novel "Snow Crash" in 1992. It is actually a socialized cyberspace (inclusive of cybernetics and space) parallel yet interactive to the real world. Since the metaverse is built upon cyberspace, all security threats, such as botnets [2], website fingerprinting [3], [4], phishing [5], sybil attacks [6], and frauds [7], would be inherited. Additionally, the metaverse's growing complexity and diversity in terms of functionalities [8], as well the exponentially increasing demand in network bandwidth and computational resources [9], [10], makes security big concerns. On the one hand, complex and diverse functionalities introduce extra vulnerabilities, exposing the metaverse to new unexpected threats [11]. On the other hand, the increasing resource consumption renders the metaverse susceptible to distributed denial-of-service (DDoS) attacks.

Despite the substantially exaggerated security threats, solutions defending against them have not kept pace. A major obstacle to such solutions is virtuality–reality synthesized threats, e.g., virtual espionage [12]. In light of the widespread attention that the metaverse has received [13], [14], [15], [16], it is imperative to design new paradigms to effectively defend the metaverse against new threats. Designing new paradigms is not an easy task. In particular, it needs theoretical guidance. As a piece of pioneer work, Wang proposed that the metaverse could be abstracted as cyber–physical–social systems (CPSS) in which the system behaviors are guided by Merton's Laws [17], [18], a concept developed from cyber–physical systems (CPS) [19], [20]. In other words, CPSS can be instantiated into the metaverse [17]. Fig. 1 demonstrates the relationship among CPS, CPSS, digital twins (DT), and metaverses. We see the metaverse's interactive nature between the actual reality and virtual reality (VR), as well as the fundamental importance of CPSS in representing the metaverse.

Following the concept of CPSS, new paradigms addressing the security threats not only in CPS [21], [22] but also in CPSS (e.g., dynamic Cyber Movement Organizations) are required [23]. However, such requirements are full of uncertainty, diversity and complexity, which are typical problems of complex systems [24]. To tackle such problems in CPSS,

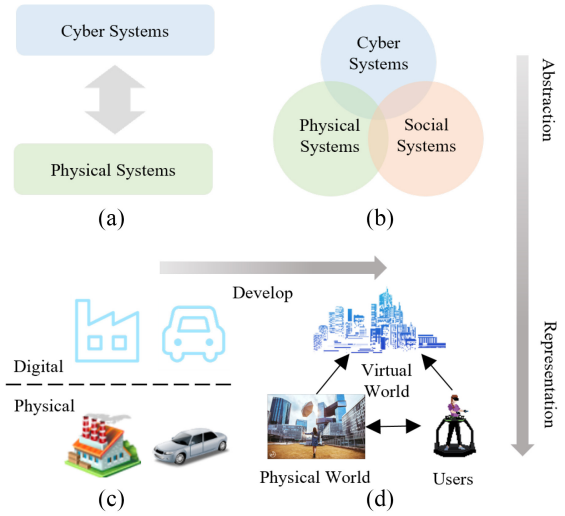


Fig. 1. Relationship among (a) CPS, (b) CPSS, (c) DTs, and (d) metaverses.

parallel intelligence (PI) is proposed [25]. Its main objective is to bridge the big modeling gap in CPSS using the ACP method that consists of artificial societies, computational experiments, and parallel execution [26], and to transform problems of complex systems into domain-specific tasks characterized by agility, dedication, and convergence [24].

Inspired by PI, we advance a parallel system, dubbed ParaDefender, to effectively defend the metaverse against emerging new threats. The main contributions of this article are threefold.

1) We present a novel cyberspace defender named ParaDefender based on the ACP method. ParaDefender comprises artificial cyberspace, computational experiments, and parallel execution. Artificial cyberspace is to mirror real cyberspace into artificial cyberspace, while computational experiments explore uncertainties in artificial cyberspace that may happen in real cyberspace. Parallel execution eventually makes artificial and real cyberspaces executed in parallel for mutually guiding each other for enhanced security.
2) ParaDefender features with scenario-driven computational experiments and parallel execution, wherein the scenarios originate from all possible spatial–temporal combinations of security threats in the metaverse.
3) We demonstrate how to land ParaDefender onto real-world applications, including the Industrial Internet of Things (IIoT) security operation application in the industrial metaverse, and the social governance application.

The remainder of this article is structured as follows. Sections II and III present the system overview and implementation of ParaDefender, respectively. In Section IV, we land ParaDefender onto real-world applications. We perform a literature survey in Section V and finally conclude this article in Section VI.

II. ParaDefender Overview

The metaverse blends the virtual and physical worlds. The avatar, in the virtual world, is released under the constraints of the physical world. As a result, modeling avatars' behavior and governing virtual society are more challenging. Moreover, as the metaverse infrastructure, information systems are more exposed to cyberattacks [27], [28]. Avatar-based attacks against information systems and virtual societies also become commonplace. To safeguard metaverses, we construct the system framework of ParaDefender using the ACP method as shown in Fig. 2. The ACP method contains artificial cyberspace for modeling, computer experiments for analysis and parallel execution for control [26]. Furthermore, ParaDefender uses the 6S (Safety, Security, Sustainability, Sensitivity, Service, and Smartness) as a benchmark for evaluation. Then, we introduce the ParaDefender framework from the perspective of ACP methods.

A. Artificial Cyberspace

Existing defense mechanisms of cybersecurity mainly rely on event-triggered responses [29], [30], [31]. The scale, depth, and frequency of security events are fast increasing as the continual development cyberspace [32]. Plain event-driven mechanisms [33], [34], [35], [36] hardly describe the complex security situation of metaverses. Therefore, the new mechanism should be capable of modeling the structure and dynamic activities of cyberspace. Then, the new mechanism is used to analyze and respond to security problems through the cyberspace model [37], [38], [39], [40]. We introduce a new Scenario-driven protection mechanism for ParaDefender. This mechanism builds an artificial cyberspace based on scenarios. Unlike the event-triggered response, this artificial cyberspace can retrace the event formation process, reconstruct the event-triggered state, and evolve with the post-event cyberspace. The diversified capabilities make the cyberspace defense process credible and visible.

B. Computational Experiments

Based on artificial cyberspace, ParaDefender analyzes security problems and provides solutions through computational experiments. For a complex security problem, it is unlikely to verify the effectiveness of a solution using a single experiment with a scenario. Therefore, we need a novel way of cross-testing multiple experiments with multiple scenarios. The artificial cyberspace described previously can construct different experimental environments based on scenarios. The scenario's architecture, components, and parameters can be modified in artificial cyberspace to meet the experimental requirements. Moreover, artificial cyberspace simulates real and unreal security events. Multiple experiments are conducted to optimize the solution's efficacy by analyzing the solution's statistics. However, it is impossible to infinitely approximate real security scenarios due to the finite composition division of artificial cyberspace. The purpose of computational experiments is not to discover the most realistic solution in artificial cyberspace but rather to provide some solutions that enable implementation. Real cyberspace is an evolutionary path that emerges from computational experiments. Thus, the solutions obtained from computational experiments can meet the needs of real security problems.

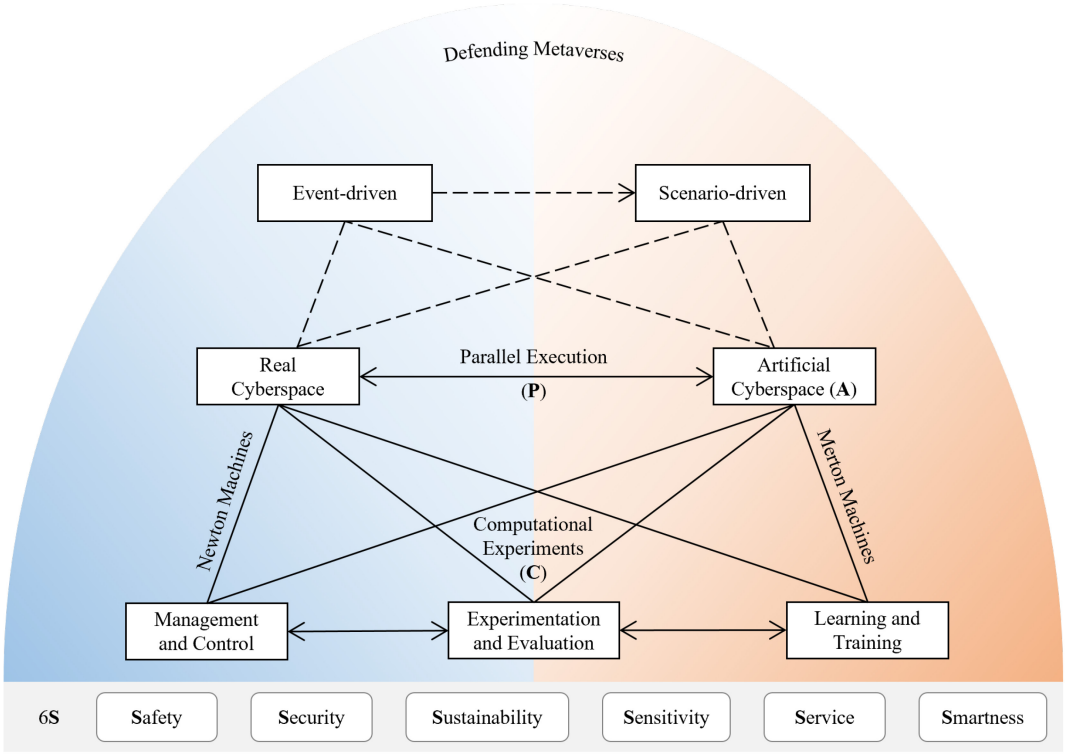


Fig. 2. Overall framework of ParaDefender.

C. Parallel Execution

Due to the distance between artificial and real cyberspaces, it is hard to directly apply defense solutions derived from computational experiments to real problems. Essentially, the conclusions of the computational experiments are only an analysis of security problems in artificial cyberspace. They are not optimized for real operational scenarios. The parallel execution links artificial and real cyberspaces with interactive data, models, and operations [41]. Generally, there is more than one artificial cyberspace operating in ParaDefender. We create different artificial cyberspaces based on cyberspace's history, performance, and operation. The initial state of these artificial cyberspaces is between best and worst. In addition, the basic architecture and elements of the artificial cyberspace map the real cyberspace, and ParaDefender enables control and management of both artificial and real cyberspaces through parallel execution. Online and offline evaluations and analyses are gathered in the parallel execution phase to support ParaDefender's decisions.

III. System Implementation

Next, we detail the system implementation of ParaDefender. As shown in Fig. 3, ParaDefender has three components, namely, cyberspace detection and response (CDR), scenario engineering (SE), and foundation models.

A. Exploiting Cyberspace Detection and Response

Detection and response in cyberspace are fundamental approaches to proactively defending against network attacks [42]. Salient methods and theories have been developed, such as endpoint detection and responses (EDRs) [43], network detection and responses (NDRs), extended detection and responses (XDRs), and managed detection and responses (MDRs). EDR and NDR work at the endpoint and network sides, respectively. The input of EDR comes from local security logs, while the input of NDR comes from traffic data obtained from network sniffing. XDR is a software-as-a-service (SaaS). Because XDR is deployed as a centralized vantage point and analyzes the data collected from both EDR and NDR, it has much higher identification efficiency and accuracy. In addition, based on the novel architecture of XDR, MDR is capable of situational awareness and analysis. XDR can explore automated response methods, such as security orchestration, automation and response (SOAR).

Based on the existing techniques, we leverage CDR as the monitoring and control component of ParaDefender for cyberspace in the metaverse. CDR functions as a link between SE and the cyberspace. It collects data regarding avatar activities and interactions in the metaverse. The data is the base for monitoring the cyberspace of metaverses. Furthermore, SE structures the data according to the metaverse's security requirements. Then, we feed structural data to the foundation models for computational experiments. SE examines the solutions obtained from computer experiments. Finally, the response component applies the feasible solutions to cyberspace.

B. Enabling Scenario Engineering

SE is a systems engineering solution providing all the elements involved in the evolution and observation of a scenario

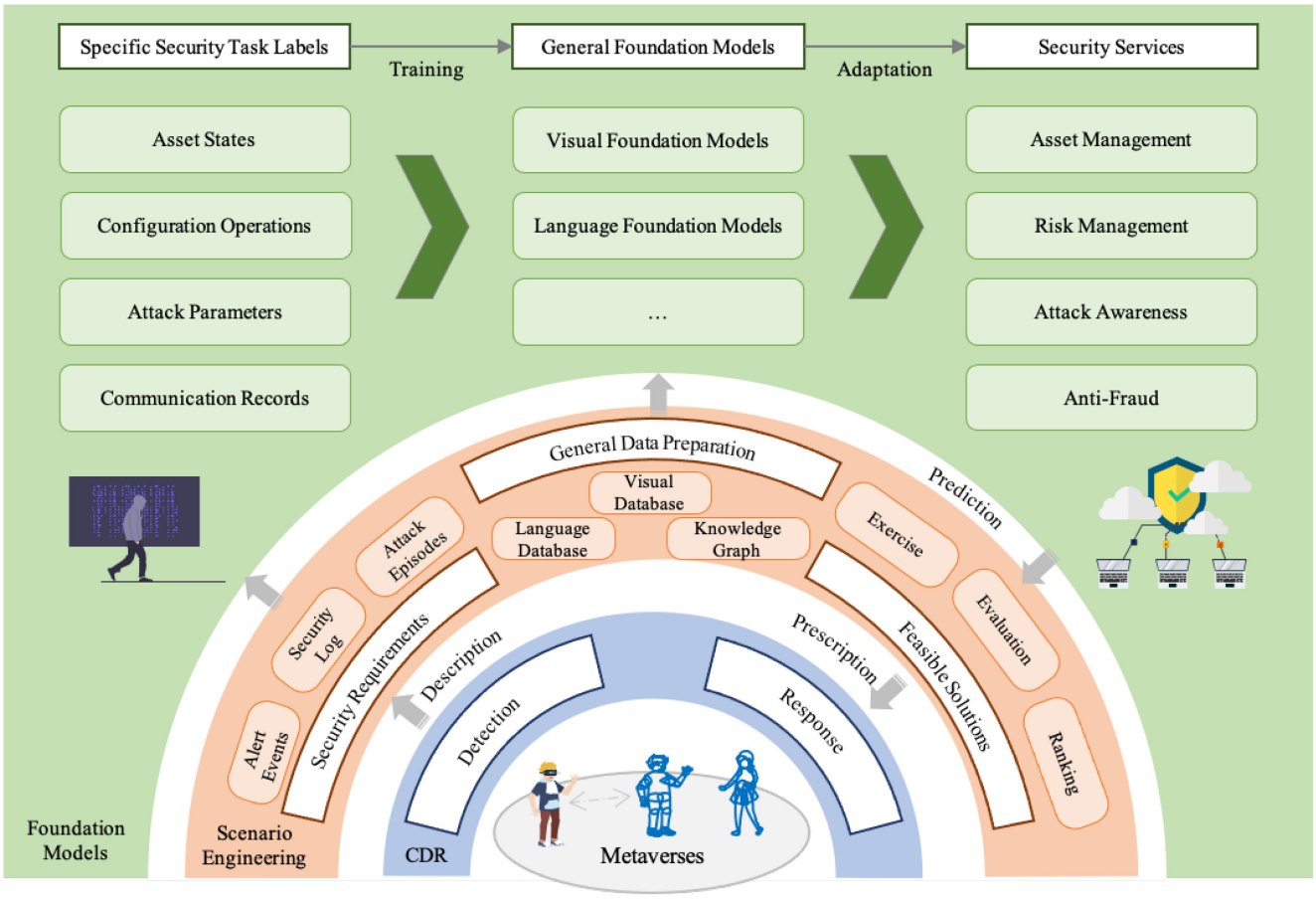


Fig. 3. System implementation of ParaDefender.

within a certain time and space range [44]. Its scenarios can be a series of activities or a branching structure of these activities. Moreover, the elements constituting a scenario can be real [45], virtual, parallel [46], or other forms. As for ParaDefender, SE provides a trustworthy and controllable architecture for building artificial cyberspace. SE verifies and certifies the real and artificial cybersecurity data.

As shown in Fig. 3, the original data of SE comes from the CDR of real cyberspace. Its data structure and quality are limited by the physical space, introducing challenges, such as less available information and more complex analysis. These challenges can be solved in SE by constructing scenario data based on security requirements. The scenario data will be mainly applied in the computational experiments using the foundation models. They will also be gradually used in actual cyberspace after the long-term observable, creditable, and controllable operation. Furthermore, foundation models are fine-tuned to fit the downstream tasks of specific security services. Before they can be implemented, security service solutions must be exercised, evaluated, and ranked by SE.

C. Exploring Foundation Models

Foundation models are emerging artificial intelligence methods with two training phases, i.e., obtaining pretrained models through large-scale self-supervised learning and then fine-tuning pretrained models to adapt to downstream tasks. BERT is an early effort of foundation models, and it outperforms previous algorithms in natural language processing. Moreover, its multitasking performance provides the basis for current multimodal research, and makes BERT evolve from natural language processing [47] to image-text [48] and control robotic arms [49]. Computational experiments have diverse tasks that include text, images, or other scenario elements. The cognitive and multimodal capabilities of foundation models well suit the task requirement of computational experiments.

In each computational experiment, the foundation model drives the evolution of the elements in SE to achieve a credible and visible process of computational experiments. During the application phase of foundation models, SE provides controllable elements, whereas SE provides structured and multimodal data during the training phase. The training data contains general knowledge (vision database, language database, and knowledge graph) and security requirements (alert events, security logs, and attack episodes) of the metaverse. The general data is used to pretrain the general foundation models, such as vision, language, and other foundation models. These general foundation models provide ParaDefender with text understanding, speech dialogue, image recognition, and other basic capabilities. Tokenizing the security requirement data produces labels for each task. Adjust the general foundation models to fit security services using data with labels [50].

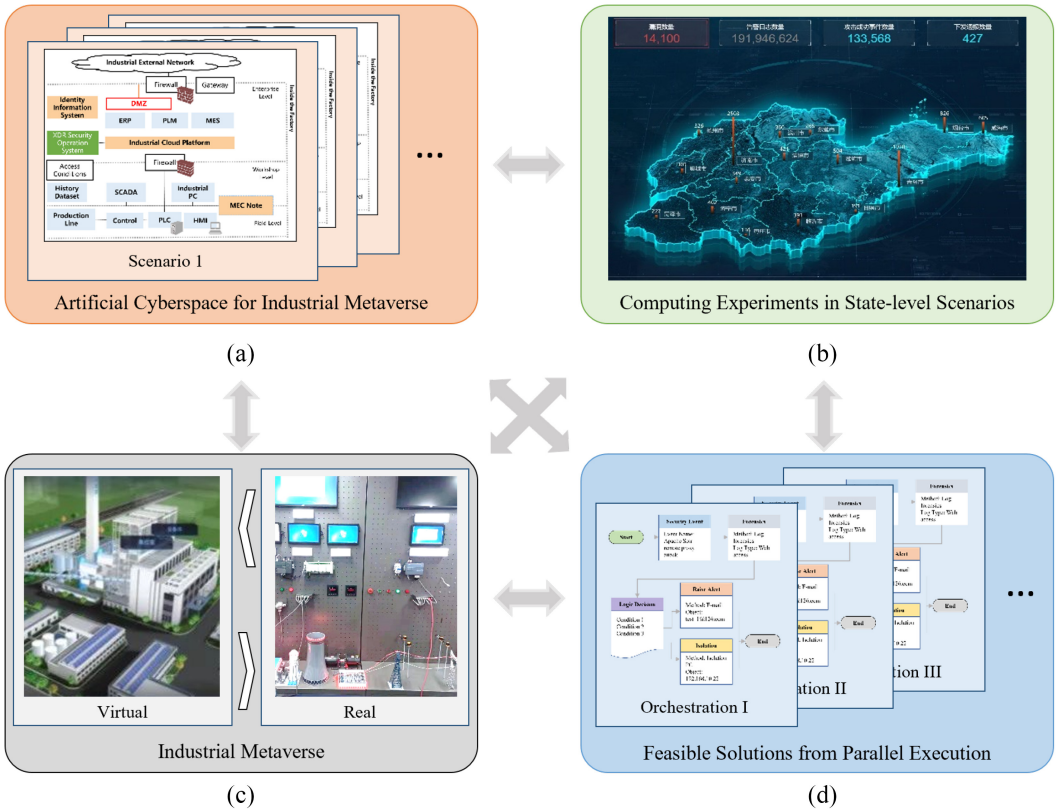


Fig. 4. IIoT defense process in ParaDefender: (a) real cyberspace, (b) artificial cyberspace, (c) computing experiments, and (d) parallel execution.

IV. Landing ParaDefender onto Real-World Applications

As a proof of concept, we demonstrate how to land ParaDefender onto real-world applications.

A. Application 1: Protecting Industrial Internet of Things

The industrial metaverse architecture is built upon the IIoT [51]. It creates functional avatars to describe industrial cyberspace in the physical world. As shown in Fig. 4, we apply ParaDefender to the industrial metaverse as a proof of concept. Fig. 4(c) shows the industrial metaverse representing real cyberspace, where the left image is a real IIoT environment of a thermal power plant, and the right image is a virtual scenario based on this power plant. Fig. 4(a) is a multivariate mapping of cyberspace in the industrial metaverse, where both the incarnations of the meta-universe and its network data are constructed as different scenarios based on SE. Fig. 4(b) shows the computational experiments on the state-level artificial cyberspace for IIoT identification, vulnerability, and communication mechanism analysis. Fig. 4(d) presents a set of orchestration schemes that translate solutions in cyberspace into executable operational processes.

B. Application 2: Anti-Fraud in CPSS

Communication fraud has become an important area of social governance. In particular, fraud in the metaverse will affect the stability and development of the virtual society in the metaverse. Fig. 5 shows the process of the traditional graph computation in ParaDefender. The connections between the avatars in the metaverse can form a graph. Nodes in this graph will be classified into different groups based on a social discovery algorithm. After that, the distribution of different group features will be analyzed by combining the fraudulent call labels. Finally, the features extracted are used to classify the fraudulent and normal users in the test scenario.

V. Related Work

In this section, we review related works concerning PI and metaverse security. These works are essential for building ParaDefender.

A. Parallel Intelligence

Users have experienced text communication in Web 1.0, video interactions in Web 2.0, and now are moving toward avatar activities in Web 3.0 [52], [53], [54], [55]. It is how users interact on the Internet and the deep integration of physical and social spaces within cyberspace that have been changing. The complete integration of the three spaces develops CPSS, also known as cyber–physical–human systems (CPHSs) [56]. CPS, as the basis of CPSS, enables the mapping of physical systems to cyber systems and the remote control and management of physical systems through cyber systems [57], [58]. The construction and operation of CPS rely on mathematical models driven by Newton's laws. However, human and social involvement in CPSS is difficult to describe through models, implying that the CPS approach applied to

Fig. 5. Anti-fraud process based on SE.

CPSS will be ineffective. Human activities are difficult to describe through models, but Merton's law of "self-fulfillment prophecy" provides the theoretical support for social governance [59]. Merton's law provides a way to implement CPSS systems but does not address how to describe social and physical spaces in cyberspace. The big data analysis from deep learning has inspired the method of describing CPSS. Through big data, the gap between cyberspace and other spaces is bridged. The artificial intelligence approach constructed by this idea is called PI [25], [60].

CPSS is the infrastructure of PI, and the ACP method is the basic method of PI deployment [61]. PI arises to solve the complex problems of CPSS and also to utilize the advantages of CPSS. Similarly, the ACP method is constructed on top of CPSS. The method consists of three parts artificial system, computational experiments, and parallel execution [23], [26]. In CPSS, the artificial system uses the descriptive capability of cyberspace to create multiple mappings of the physical system; the computational experiment uses the computational platform and energy of the physical space to optimize feasible solutions by repeated experiments; the parallel execution uses the self-fulfillment of the social space to deploy suitable solutions to the physical system; then the physical system after deploying solutions is mapped to the artificial system to build a closed-loop large system. Furthermore, theoretical approaches, such as parallel learning [62], [63], [64], parallel reinforcement learning [65], and parallel control [66], [67], [68], [69] are the inheritance and development of ACP methods. In particular, the parallel learning framework introduces the process of "small data to big data to deep intelligence" from the perspective of data and action [62], [70].

B. Metaverse Security

Metaverse is a persistent, immersive, and shared virtual space, which blends the physical, digital, and human worlds into itself. In the metaverse, security and privacy concerns are essential to the realization of the metaverse realm. Especially, driven by the interweaving impact of the enabling technologies, such as blockchain [71], [72], VR, augmented reality (AR), and beyond 5G (B5G), etc., the security vulnerabilities of each emerging technology will be magnified in the metaverse ecology, making security and privacy protection become huge challenges.

In the literature, there have been increasingly relevant surveys in this domain. For example, Yang et al. [73] investigated the integration of blockchain and AI technologies in the foundation of the metaverse from four aspects, i.e., digital content creation, digital currency, digital asset, and digital market. Falchuk et al. [74] explored the new privacy issues and the state-of-the-art solutions in protecting the privacy of users/avatars in social metaverse applications. In their survey, three main kinds of privacy information are discussed, i.e., privacy of user/avatar behavior, privacy of personal information, and privacy of user/avatar communications. Moreover, several privacy countermeasures are discussed including avatar confusion, digital clones, private copy, mannequin, disguise, lockout, and teleport. Recently, Wang et al. [11] provided a comprehensive review on the security threats in the metaverse from seven aspects: device authentication, data management, user privacy, physical/social effects, governance related, economy related, and network related. Besides, the existing and potential security and privacy countermeasures in both academia and industry are examined and discussed.

In the metaverse, AR/VR headsets are recognized as the entrance to the metaverse, and the security of real-time massive AR/VR contents is of significance. Lebeck et al. [75] conducted qualitative experiments on AR headsets (i.e., HoloLens) in multiuser settings (i.e., 22 players). Findings from the user study show that AR players can be easily immersed (i.e., treating virtual things as real) and deceptive virtual things can easily mislead participants (e.g., stepping out of the house and walking to the center of the street). Ruth et al. [76] identified the potential security risks in sharing private AR contents during multiuser interactions, and proposed a secure personal data-sharing control module under multiuser AR services such as multiplayer gaming. Their scheme allows participants to fully control the inbound and outbound AR/VR data, which is validated via a prototype implemented on HoloLens.

Aiming to prevent identity thieves and data misuse in the interactions between AR/VR headsets and users, Shen et al. [77] presented *GaitLock*, a novel and reliable authentication scheme by exploiting the intrinsic gait patterns of AR/VR headsets. In their work, a gait recognition model is proposed without the need of extra hardware, and intruders can be simply excluded by asking them to walk a few steps. A real implementation on Google Glass shows that GaitLock can achieve over 98% success in only 5 steps and

is energy efficient. For secure and efficient viewport rendering of VR devices, Lin et al. [78] proposed a blockchain and edge computing-based task offloading scheme. In their work, edge computing nodes perform the offloaded viewport rendering missions with much saved latency and the permissioned blockchain enforces transaction transparency and security. For disaster areas, drones can be utilized as edge computing nodes for efficient VR/AR rendering task offloading [79].

Apart from AR/VR contents, AI-generated contents (AIGC) and user-generated contents (UGC) can offer an immersive user experience and make users enjoy their digital lives in the metaverse, which also suffers various security risks. As an effort, Yu et al. [80] combined user trustworthiness and content sensitiveness to develop fine-grained privacy settings for UGC. In [80], an AI-based compact representation method is designed to measure UGC sensitiveness, and a social grouping method is devised to characterize users' trustworthiness. Moreover, for the dependability of AIGC, existing works on adversarial learning [81], [82] can offer some lessons for the resistance of adversarial samples during the construction of the metaverse.

Furthermore, the construction and synchronization of DT are essential to bridge the virtuality and reality in the metaverse. To ensure the reliability of DT in intelligent transportation systems, Lin et al. [78] presented a blockchain-based solution for on-demand DT construction and secure DT delivery. A pricing-based mechanism is also proposed in [78] to optimally match the DT service providers and metaverse users. To resolve the huge energy consumption in blockchains, a novel energy-recycling consensus mechanism is devised in [83] to enable sustainable blockchain systems and promote the seamless integration of blockchain and distributed AI in the metaverse palace.

For privacy threats in the metaverse, Raguram et al. [84] identified a new privacy risk in the metaverse named *compromising reflections*, such as the reflection of users' typing on virtual keyboards. They develop a fast reconstruction method to automatically reconstruct users' typed inputs based on compromising reflections (e.g., sunglass reflections). Extensive experiments demonstrate that the proposed attack can work even at long distances such as 12 m for sunglass reflections. Shang et al. [85] identified a new privacy threat named *ARSpy* to track users' locations in multiplayer AR games (e.g., Pokémon Go) via network traffic analysis. Real-world experiments show that the proposed threat can accurately attain any target's geolocation. Besides, three defense methods are developed to mitigate users/avatars' privacy leakage.

Observing that authorized users/avatars can be traitors to illegally redistribute UGC or AIGC to others, Zhang et al. [86] proposed a new *illegal content redistribution* threat on user/avatar privacy and develop a novel fair traitor tracing protocol based on proxy re-encryption and watermarking. For efficient UGC access control and usage audit, Wang et al. [87] developed a smart contract-based private UGC sharing and audit scheme, where the on-chain smart contract offers public audit functions for UGC access and usage behaviors while the off-chain trusted processor performs privacy-preserving UGC processing.

VI. Conclusion

The metaverse, as an instance of CPSS, is far beyond a simple combination of physical and virtual spaces. Rather, it involves complex and immersive spatial–temporal interactions among physical and virtual spaces, social networks, and cyber spaces. The unprecedented complexity involving multiple spaces and their interactions necessitates a new paradigm to address security concerns. We therefore take the first step to endeavor to fulfill such a goal. The proposed system ParaDefender fully exploits the ACP-based PI and comprises artificial cyberspace, computational experiments, and parallel execution. The design principle behind ParaDefender is to make artificial and real cyberspaces executed in parallel to mutually guide each other for enhanced security. More importantly, such parallel execution is scenario-driven in the sense that the scenarios originate from all possible spatial–temporal combinations of security threats in the metaverse. As a proof of concept, we also show the applications of ParaDefender in IIoT and anti-fraud systems. We expect our study could guide the paradigm how the metaverse is defended, and foster more research of metaverse solutions based on PI.

References

[1] D. H. Gelernter, *Mirror Worlds, or, the Day Software Puts the Universe in a Shoebox–: How it Will Happen and What it Will Mean*. New York, NY, USA: Oxford Univ. Press, 1991.

[2] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, Jul./Aug. 2020.

[3] M. S. Rahman, M. Imani, N. Mathews, and M. Wright, "Mockingbird: Defending against deep-learning-based website fingerprinting attacks with adversarial traces," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1594–1609, 2020.

[4] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y.-Q. Shi, "A novel weber local binary descriptor for fingerprint liveness detection," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 4, pp. 1526–1536, Apr. 2020.

[5] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2091–2121, 4th Quart., 2013.

[6] Y. Wang, W. Dai, Q. Jin, and J. Ma, "BciNet: A biased contest-based crowdsourcing incentive mechanism through exploiting social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 8, pp. 2926–2937, Aug. 2020.

[7] Y. Lin et al., "Dynamic control of fraud information spreading in mobile social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3725–3738, Jun. 2021.

[8] S. Mystakidis, "Metaverse," *Encyclopedia*, vol. 2, no. 1, pp. 486–497, 2022.

[9] Y. Jiang et al., "Reliable distributed computing for metaverse: A hierarchical game-theoretic approach," *IEEE Trans. Veh. Technol.*, early access, Sep. 7, 2022, doi: 10.1109/TVT.2022.3204839.

[10] F.-Y. Wang, R. Qin, X. Wang, and B. Hu, "MetaSocieties in metaverse: MetaEconomics and MetaManagement for MetaEnterprises and MetaCities," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 2–7, Feb. 2022.

[11] Y. Wang et al., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, early access, Sep. 7, 2022, doi: 10.1109/COMST.2022.3202047.

[12] R. Leenes, "Privacy in the metaverse," in *Proc. IFIP Int. Summer School Future Identity Inf. Soc.*, 2007, pp. 95–112.

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

[14] J. D. N. Dionisio, W. G. Burns, III, and R. Gilbert, "3D virtual worlds and the metaverse: Current status and future possibilities," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 1–38, 2013.

[15] J. Díaz, C. Saldaña, and C. Avila, "Virtual world as a resource for hybrid education," *Int. J. Emerg. Technol. Learn.*, vol. 15, no. 15, pp. 94–109, 2020.

[16] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in *Proc. 29th ACM Int. Conf. Multimedia*, 2021, pp. 153–161.

[17] F.-Y. Wang, "Parallel intelligence in metaverses: Welcome to Hanoi!" *IEEE Intell. Syst.*, vol. 37, no. 1, pp. 16–20, Jan./Feb. 2022.

[18] X. Wang, J. Yang, J. Han, W. Wang, and F.-Y. Wang, "Metaverses and DeMetaverses: From digital twins in CPS to parallel intelligence in CPSS," *IEEE Intell. Syst.*, vol. 37, no. 4, pp. 97–102, Jul./Aug. 2022.

[19] S. M. M. Rahman, "Cyber-physical-social system between a humanoid robot and a virtual human through a shared platform for adaptive agent ecology," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 190–203, Jan. 2018.

[20] W. Dai, C. Pang, V. Vyatkin, J. H. Christensen, and X. Guan, "Discrete-event-based deterministic execution semantics with timestamps for industrial cyber-physical systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 3, pp. 851–862, Mar. 2020.

[21] Y. Pang, H. Xia, and M. J. Grimble, "Resilient nonlinear control for attacked cyber-physical systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 6, pp. 2129–2138, Jun. 2020.

[22] X.-Y. Shen and X.-J. Li, "Data-driven output-feedback LQ secure control for unknown cyber-physical systems against sparse actuator attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 9, pp. 5708–5720, Sep. 2021.

[23] X. Wang, L. Li, Y. Yuan, P. Ye, and F.-Y. Wang, "ACP-based social computing and parallel intelligence: Societies 5.0 and beyond," *CAAI Trans. Intell. Technol.*, vol. 1, no. 4, pp. 377–393, Oct. 2016.

[24] F. Wang, "CC 5.0: Intelligent command and control systems in the parallel age," *J. Command Control*, vol. 1, no. 1, pp. 107–120, 2015.

[25] F.-Y. Wang, "Parallel intelligence: Belief and prescription for edge emergence and cloud convergence in CPSS," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 5, pp. 1105–1110, Oct. 2020.

[26] F.-Y. Wang, "Toward a paradigm shift in social computing: The ACP approach," *IEEE Intell. Syst.*, vol. 22, no. 5, pp. 65–67, Sep./Oct. 2007.

[27] Y. Wan, G. Wen, X. Yu, and T. Huang, "Distributed consensus tracking of networked agent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 10, pp. 6183–6196, Oct. 2021.

[28] B. Hu, C. Zhou, Y.-C. Tian, X. Hu, and X. Junping, "Decentralized consensus decision-making for cybersecurity protection in multimicrogrid systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 4, pp. 2187–2198, Apr. 2021.

[29] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[30] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," *IEEE Trans. Intell. Veh.*, vol. 5, no. 4, pp. 693–713, Dec. 2020.

[31] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, "Recursive filtering of distributed cyber-physical systems with attack detection," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 10, pp. 6466–6476, Oct. 2021.

[32] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021.

[33] Z. Gu, J. H. Park, D. Yue, Z.-G. Wu, and X. Xie, "Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 10, pp. 6197–6206, Oct. 2021.

[34] Q. Zhang, H. Yan, H. Zhang, S. Chen, and M. Wang, "H_∞ control of singular system based on stochastic cyber-attacks and dynamic event-triggered mechanism," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 12, pp. 7510–7516, Dec. 2021.

[35] J. Liu, T. Yin, J. Cao, D. Yue, and H. R. Karimi, "Security control for T–S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 10, pp. 6544–6554, Oct. 2021.

[36] S. Hu, D. Yue, X. Chen, Z. Cheng, and X. Xie, "Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 3, pp. 1392–1403, Mar. 2021.

[37] Z. Liu, R. Zheng, W. Lu, and S. Xu, "Using event-based method to estimate cybersecurity equilibrium," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 2, pp. 455–467, Feb. 2021.

[38] X. Yang et al., "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 2, pp. 273–302, Feb. 2021.

[39] M. A. Ferrag, L. Shu, and K.-K. R. Choo, "Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 9, pp. 1477–1499, Sep. 2021.

[40] M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions," *IEEE/CAA J. Automatica Sinica*, vol. 9, no. 3, pp. 407–436, Mar. 2022.

[41] T. Liu, B. Tian, Y. Ai, and F.-Y. Wang, "Parallel reinforcement learning-based energy efficiency improvement for a cyber-physical system," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 2, pp. 617–626, Mar. 2020.

[42] W. Contreras and S. Ziavras, "Low-cost, efficient output-only infrastructure damage detection with wireless sensor networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 3, pp. 1003–1012, Mar. 2020.

[43] C. Hwang, D. Kim, and T. Lee, "Semi-supervised based unknown attack detection in EDR environment," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 12, pp. 4909–4926, Dec. 2020.

[44] X. Li, P. Ye, J. Li, Z. Liu, L. Cao, and F.-Y. Wang, "From features engineering to scenarios engineering for trustworthy AI: I&I, C&C, and V&V," *IEEE Intell. Syst.*, vol. 37, no. 4, pp. 18–26, Jul./Aug. 2022.

[45] C. Sun et al., "Proximity based automatic data annotation for autonomous driving," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 2, pp. 395–404, Mar. 2020.

[46] S. Wang et al., "Robotic intra-operative ultrasound: Virtual environments and parallel systems," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 5, pp. 1095–1106, May 2021.

[47] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," in *Proc. Conf. North Amer. Ch. Assoc. Comput. Linguist. Human Lang. Technol. Vol. 1 (Long Short Papers)*, Minneapolis, MN, USA, Jun. 2019, pp. 4171–4186.

[48] A. Ramesh et al., "Zero-shot text-to-image generation," in *Proc. 38th Int. Conf. Mach. Learn.*, Feb. 2021, pp. 8821–8831.

[49] S. Reed et al., "A generalist agent," May 2022, *arXiv:2205.06175*.

[50] J. Han et al., "Parallel security for smart cyberspace operation: From AI model to foundational models," *J. Intell. Sci. Technol.*, vol. 2, no. 1, pp. 18–22, 2022.

[51] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarnè, "ResIoT: An IoT social framework resilient to malicious activities," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 5, pp. 1263–1278, Sep. 2020.

[52] S. L. France, Y. Shi, M. S. Vaghefi, and H. Zhao, "Online video channel management: An integrative decision support system framework," *Int. J. Inf. Manag.*, vol. 59, Aug. 2021, Art. no. 102244.

[53] L. Canales, W. Daelemans, E. Boldrini, and P. Martínez-Barco, "EmoLabel: Semi-automatic methodology for emotion annotation of social media text," *IEEE Trans. Affect. Comput.*, vol. 13, no. 2, pp. 579–591, Apr.–Jun. 2022.

[54] R. G. Crespo, R. F. Escobar, L. J. Aguilar, S. Velazco, and A. G. C. Sanz, "Use of ARIMA mathematical analysis to model the implementation of expert system courses by means of free software OpenSim and Sloodle platforms in virtual university campuses," *Expert Syst. Appl.*, vol. 40, no. 18, pp. 7381–7390, Dec. 2013.

[55] F.-Y. Wang, "Beyond X 2.0: Where should we go?" *IEEE Intell. Syst.*, vol. 24, no. 3, pp. 2–4, May/Jun. 2009.

[56] T. Yang, Q. Guo, L. Xu, and H. Sun, "Dynamic pricing for integrated energy-traffic systems from a cyber-physical-human perspective," *Renew. Sustain. Energy Rev.*, vol. 136, Feb. 2021, Art. no. 110419.

[57] F.-Y. Wang, "The emergence of intelligent enterprises: From CPS to CPSS," *IEEE Intell. Syst.*, vol. 25, no. 4, pp. 85–88, Jul./Aug. 2010.

[58] X. Wang, X. Zheng, W. Chen, and F.-Y. Wang, "Visual human–computer interactions for intelligent vehicles and intelligent transportation systems: The state of the art and future directions," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 253–265, Jan. 2021.

[59] P. Dick, "From rational myth to self-fulfilling prophecy? understanding the persistence of means—Ends decoupling as a consequence of the latent functions of policy enactment," *Org. Stud.*, vol. 36, no. 7, pp. 897–924, Jul. 2015.

[60] F.-Y. Wang, X. Wang, L. Li, and L. Li, "Steps toward parallel intelligence," *IEEE/CAA J. Automatica Sinica*, vol. 3, no. 4, pp. 345–348, Oct. 2016.

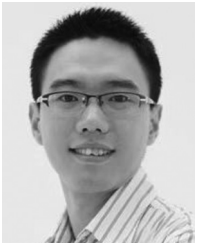
[61] F.-Y. Wang, J. J. Zhang, and X. Wang, "Parallel intelligence: Toward lifelong and eternal developmental AI and learning in cyber-physical-social spaces," *Front. Comput. Sci.*, vol. 12, no. 3, pp. 401–405, Jun. 2018.
[62] L. Li, Y. Lin, D. Cao, N. Zheng, and F.-Y. Wang, "Parallel learning—A new framework for machine learning," *Acta Automatica Sinica*, vol. 43, no. 1, pp. 1–8, 2017.
[63] L. Li, Y. Lin, N. Zheng, and F.-Y. Wang, "Parallel learning: A perspective and a framework," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 3, pp. 389–395, Jul. 2017.
[64] J. Jin, H. Guo, J. Xu, X. Wang, and F.-Y. Wang, "An end-to-end recommendation system for urban traffic controls and management under a parallel learning framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1616–1626, Mar. 2021.
[65] T. Liu, B. Tian, Y. Ai, L. Li, D. Cao, and F.-Y. Wang, "Parallel reinforcement learning: A framework and case study," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 4, pp. 827–835, Jul. 2018.
[66] F.-Y. Wang, "Parallel control and digital twins: Control theory revisited and reshaped," *Chin. J. Intell. Sci. Technol.*, vol. 52, no. 3, pp. 293–300, 2020.
[67] Q. Wei, H. Li, and F.-Y. Wang, "Parallel control for continuous-time linear systems: A case study," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 4, pp. 919–928, Jul. 2020.
[68] Q. Wei, L. Wang, J. Lu, and F.-Y. Wang, "Discrete-time self-learning parallel control," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 1, pp. 192–204, Jan. 2022.
[69] F.-Y. Wang, "The DAO to MetaControl for MetaSystems in metaverses: The system of parallel control systems for knowledge automation and control intelligence in CPSS," *IEEE/CAA J. Automatica Sinica*, vol. 9, no. 11, pp. 1899–1908, Nov. 2022.
[70] J. Han et al., "Desecurity: A framework of parallel intelligence for CPSS security," *Int. J. Intell. Control Syst.*, vol. 1, no. 4, pp. 27–31, 2021.
[71] J. Leng et al., "Blockchain-secured smart manufacturing in industry 4.0: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 237–252, Jan. 2021.
[72] Mamta, B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis, and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 12, pp. 1877–1890, Dec. 2021.
[73] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 122–136, 2022.
[74] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, Jun. 2018.
[75] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, "Towards security and privacy for multi-user augmented reality: Foundations with end users," in *Proc. IEEE Symp. Security Privacy (SP)*, 2018, pp. 392–408.
[76] K. Ruth, T. Kohno, and F. Roesner, "Secure multi-user content sharing for augmented reality applications," in *Proc. 28th USENIX Security Symp. (USENIX Security)*, Aug. 2019, pp. 141–158.
[77] Y. Shen et al., "GaitLock: Protect virtual and augmented reality headsets using gait," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 3, pp. 484–497, May/Jun. 2019.
[78] P. Lin, Q. Song, F. R. Yu, D. Wang, and L. Guo, "Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15749–15761, Nov. 2021.
[79] Y. Wang et al., "Task offloading for post-disaster rescue in unmanned aerial vehicles networks," *IEEE/ACM Trans. Netw.*, vol. 30, no. 4, pp. 1525–1539, Aug. 2022.
[80] 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 Trans. Inf. Forensics Security*, vol. 13, pp. 1317–1332, 2018.
[81] T. Miyato, S.-I. Maeda, M. Koyama, and S. Ishii, "Virtual adversarial training: A regularization method for supervised and semi-supervised learning," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 8, pp. 1979–1993, Aug. 2019.
[82] H. Zheng, Z. Zhang, J. Gu, H. Lee, and A. Prakash, "Efficient adversarial training with transferable adversarial examples," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2020, pp. 1–10.
[83] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane, and Y. Wu, "A platform-free proof of federated learning consensus mechanism for sustainable blockchains," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3305–3324, Dec. 2022, doi: 10.1109/JSAC.2022.3213347.
[84] 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 Trans. Dependable Secure Comput.*, vol. 10, no. 3, pp. 154–167, May–Jun. 2013.
[85] J. Shang, S. Chen, J. Wu, and S. Yin, "ARSpy: Breaking location-based multi-player augmented reality application for user location tracking," *IEEE Trans. Mobile Comput.*, vol. 21, no. 2, pp. 433–447, Feb. 2022.
[86] 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 Trans. Dependable Secure Comput.*, vol. 17, no. 6, pp. 1218–1231, Nov./Dec. 2020.
[87] Y. Wang et al., "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.

Jinpeng Han (Student Member, IEEE) received the B.E. degree in automation from the School of Automation, Wuhan University of Technology, Wuhan, China, in 2016. He is currently pursuing the Ph.D. degree with the School of Software Engineering, Xi'an Jiaotong University, Xi'an, China, as well as the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China.

His research interests include parallel intelligence, parallel security, and security games.

Manzhi Yang received the M.E. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, in 2005. He is currently pursuing the Ph.D. degree in intelligent science and systems engineering with the Macau University of Science and Technology, Macau, China.

He is currently a Senior Expert of Network Security Systems with Eversec Technology Company Ltd., Beijing. His research interests include parallel intelligence, parallel security, and cybersecurity.



Xiaoguang Chen received the M.E. degree in information security from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008. He is currently pursuing the Ph.D. degree in intelligent science and systems engineering with the Macau University of Science and Technology, Macau, China.

He is currently specialized in industrial IoT security systems with Eversec Technology Company Ltd., Beijing. His research interests include parallel intelligence, parallel security, and cybersecurity.

Hongtao Liu is currently pursuing the M.S. degree in software engineering with Xi'an Jiaotong University, Xi'an, China.

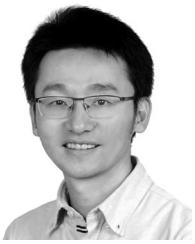
His research interests include network traffic analysis and cybersecurity.

Yuntao Wang received the Ph.D. degree in cyberspace security from Xi'an Jiaotong University Xi'an, China, in 2022.

He is currently an Assistant Professor with the School of Cyber Science and Engineering, Xi'an Jiaotong University. His research interests include security and privacy protection in general wireless networks and vehicular networks.

Jianhao Li is currently pursuing the B.E. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China.

His research interests include cybersecurity and network measurement.



Zhou Su received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2003.

He is a Professor with the MOE Key Laboratory for Intelligent Networks and Network Security, Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. His research interests include multimedia communication, wireless communication, and network traffic.

Dr. Su received the Best Paper Award of IEEE ICC2020, IEEE BigdataSE2019, and IEEE CyberSciTech2017. He is an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL, IEEE OPEN JOURNAL OF COMPUTER SOCIETY, and *IET Communications*.

Zhen Li received the B.S. and M.S. degrees in smart manufacturing from the North University of China, Taiyuan, China, in 2009 and 2012, respectively.

He is a Senior Engineer with North Automatic Control Technology Institute, Taiyuan. His research interests include data fusion, parallel theory, and artificial intelligence models and theory.

Xiaobo Ma received the Ph.D. degree in control science and engineering from Xi'an Jiaotong University, Xi'an, China, in 2014.

He is a Professor with the MOE Key Laboratory for Intelligent Networks and Network Security, Faculty of Electronic and Information Engineering, Xi'an Jiaotong University. He was a Postdoctoral Research Fellow with The Hong Kong Polytechnic University, Hong Kong, in 2015. His research interests include Internet measurement and cybersecurity.

Prof. Ma is a Tang Scholar.