Guest Editorial Special Issue on Knowledge- and Service-Oriented Industrial Internet of Things: Architectures, Challenges, and Methodologies

THE EVER-INCREASING evolution of technologies in communication, artificial intelligence (AI), manufacturing, etc., is promoting a new wave of industrial revolution. Industrial Internet of Things (IIoT) has been considered as a critical stimulator for both science and economics by amounts of countries.

Compared with the traditional consumer IoT with the purpose of improving human's awareness of the environment, IIoT is typically knowledge and service oriented. On the one hand, the data in IIoT is with high volume and diverse properties, which provides a great potential for IIoT to acquire different types of valuable knowledge. On the other hand, IIoT needs to fulfill various types of services with heterogeneous requirements on scalability, latency, throughput, reliability, robustness, privacy, and security. Additionally, those services may differ from each other in the data frame, communication carrier, etc. As a result, service requirement guarantees are more complex in IIoT than that in consumer IoT. The aim of this special issue is to foster novel and multidisciplinary approaches to realize efficient knowledge- and service-oriented IIoT.

The response to our call for this special issue was overwhelming, as we received in total 81 submissions from around the world. During the review process, each article was assigned to and reviewed by at least three experts in the field, with a rigorous multiround review process. Thanks to the great support from the Editor-in-Chief, Prof. Honggang Wang, and the dedicated work of numerous reviewers, we were able to accept 32 excellent articles covering various topics in knowledge- and service-oriented IIoT. In the following, we will introduce these articles and highlight their main contributions.

In [A1], Chen *et al.* investigated a long-term dynamic task allocation and service migration (DTASM) problem in edge-cloud IoT systems. A training architecture based on the twin-delayed deep deterministic policy gradient (DDPG) is devised. The proposed deep reinforcement learning (DRL)-based approach obtains the long-term optimal system performance and realizes seamless service migration.

[A2] optimizes the overall energy consumption of the massive IoT devices in IIoT. Yang *et al.* proposed a low-energy transmission strategy based on real-time edge layer traffic sensing. The designed energy-driven mapping strategy is effective in reducing the transmission energy consumption of IIoT devices and the overall system energy consumption in the massive device access scenario.

In [A3], Zhen *et al.* discussed the mobility of IIoT devices and the temporal dependence of content popularity. A multiagent cooperative caching policy is designed, exploiting these two features, to cooperatively learn the optimal caching decision. The proposed caching policy can efficiently improve the cache hit ratio, reduce the content access delay, and improve the Quality of Service (QoS) of IIoT applications.

In [A4], Liu *et al.* discussed the interconnections among physical and virtual entities and their roles in the interoperability of digital objects and the industrial efficiency of the supply chain. A general identification and resolution architecture is proposed as a guide to develop and improve technologies and schemes in terms of the joint requirements of service, role, function, implement, and security in Industrial Internet. An identifiable digital object model is constructed, a hybrid structure-based identification and resolution system is designed, and a trustable system based on blockchain is deployed on the designed architecture to realize the practical construction and deployment of national top-level nodes and secondary-level nodes and sustain the identification and resolution services for the Industrial Internet in China.

[A5] achieves the anonymous authentication and matching for task requirements and user reputation levels in a privacy-preserving way. Zhang *et al.* proposed a privacy-preserving multitask allocation (PMTA) scheme for mobile crowdsensing. PMTA exploits K-means clustering and matrix multiplication to realize a secure and efficient grouping mechanism, which realizes the selection of high-quality and accurate target users set with privacy-preserving.

In [A6], Hatcher *et al.* discussed various concepts for an open IoT search engine (IoT-SE). A study of security issues in IoT search is conducted to outline the challenges. A case study to resolve practical security vulnerabilities in IoT-SE systems is carried out. A case study is carried out to implement basic security features in IoT search, addressing the risk of false queries through the design of machine learning solutions. Most importantly, a roadmap for future research is provided, including the security and privacy for

Digital Object Identifier 10.1109/JIOT.2022.3187543

IoT systems connected to the IoT-SE, distributed edge computing in IoT-SE, privacy-preserving data markets in IoT-SE, and distributed machine learning in IoT-SE.

In [A7], Fan *et al.* explored a heat load prediction model based on feature fusion of dual-source data (DSDF). This model fully extracts the characteristics of the working condition data of pipe networks and the data of building energy consumption to make high-precision predictions of the ultrashort-term heat load of heat exchange stations. A calibrated prediction model can perform efficient ultrashort-term prediction of heat load.

[A8] presents a stacking model for diagnosing interturn short circuit (ITSC) faults in permanent magnet synchronous motors (PMSMs). Li *et al.* designed a verification strategy to update the global federated learning model and created a secondary server-side data set to validate the client weightings. The proposed dynamic verification model improves the diagnostic accuracy, incurs lower communication costs, and prevents local oscillations.

In [A9], Dong *et al.* implemented an efficient Tegra-based embedded GPU RSA acceleration server for IIoT. TEGRAS can deliver 34 kops/s of RSA2048 signature generation and 1007 kops/s of RSA signature verification. In real-world scenarios, TEGRAS can provide more than 34 and 978 kops of signature generation and signature verification, respectively, as a high-throughput, low-latency, and ready-to-use RSA accelerator for IIoT.

In [A10], Yang *et al.* proposed a novel high-efficiency and anti-jamming frequency hopping transmission scheme for IIoT. The combination of coherent fast frequency hopping (CFFH) and cyclic code shift key (CCSK) improves the power efficiency and spectrum efficiency by multiple times and inherits the excellent anti-jamming performance from conventional CFFH systems. PCSK-CFFH is a promising low-power and high-reliability transmission scheme for IIoT communications.

[A11] proposes a DRL-based resource allocation scheme to improve content distribution in a layered fog radio access network (FRAN). Fang *et al.* utilized a cloud-edge cooperation offloading scheme to realize the integrated allocation of caching, computing, and communication resources and joint optimization between in-network caching and routing. The designed resource allocation scheme promotes resource utilization and content delivery in FRAN.

[A12] addresses the problems of unbalanced distribution and inefficient use of computing resources during computing resource allocation. Huang *et al.* proposed a temporal computing resource allocation scheme with end device assistance to improve the efficiency of computing resource allocation and balance the distribution of computing resources in IIoT.

In [A13], Yi *et al.* explored a novel information dissemination model with the service-oriented incentive mechanism for IIoT. This model depicts the dynamical evolution of interactions among IIoT devices. A service-oriented incentive mechanism is devised to expand information diffusion by driving the participation of IIoT devices.

[A14] presents an end hopping scheme based on fixed hopping timeslot and strict time synchronization strategy by utilizing moving target defense (MTD). Fan *et al.* leveraged a Proof of Concept (PoC) to evaluate the scheme's theoretical protection performance for Distributed Denial of Service (DDoS). The proposed end hopping scheme is efficient in securing satellite communications in MTD.

In [A15], Li *et al.* designed a secure, efficient, and weighted access control scheme (SEWAC) for cloud-assisted IIoT applications. SEWAC enables the data owner to formulate any fine-grained access structure over weighted attributes without making it more complicated. SEWAC offloads the heavy decryption overhead to the cloud and achieves weighted access control, compressed ciphertext length, and efficient key generation and assurance of outsourced decryption results.

[A16] addresses the leakage of valuable industrial data and the loss of important cargos carried by UAVs. Tan *et al.* proposed a blockchain-assisted distributed and lightweight authentication service for industrial UAVs. This authentication service enables trustworthy communications for industrial drones, is resistant to various attacks, and achieves low computation and communication costs for industrial UAVs.

In [A17], Li *et al.* leveraged the time-varying user interest to design a recommendation-aided edge caching approach for Industrial Internet. A dynamic interest capture model is proposed to mine the individual user interest, a group interest aggregation algorithm is devised to determine content caching strategies, and an edge content recommendation model is designed to ensure a satisfying recommendation hit ratio and optimal caching decisions.

[A18] presents a DRL-based service provisioning strategy in software-defined industrial fog networks to minimize their energy consumption. Sarkar *et al.* leveraged a task migration policy to ensure the high availability of computing devices while addressing the single point of failure (SPOF) issue.

In [A19], Tang *et al.* maximized the energy efficiency (EE) by jointly optimizing the power allocation, analog and digital precoding in nonorthogonal multiple access (NOMA)-based cloud radio access networks (C-RANs). A joint digital precoding and power allocation algorithm is proposed to solve the optimization problem. The proposed hybrid precoding (HP) scheme improves the EE of NOMA-based C-RANs.

In [A20], Yang *et al.* investigated the problem of utilizing a sparse RFID tag array for backscatter indoor localization. The proposed SparseTag system leverages a novel sparse tag array for high-precision backscatter indoor localization. A robust channel selection method based on the RFID tag array is adopted for mitigating the multipath effect. The SparseTag system realizes high-precision RFID tag localization for IIoT.

[A21] proposes a privacy-preserving threshold spatial keyword search (TSKS) scheme. Yang *et al.* exploited the polynomial fitting technology, vector space model, and randomizable matrix multiplication technology to allow the cloud server to find relevant objects that are within some arbitrary geometric range and contain all query keywords. TSKS can protect the privacy of data sets and queries in IIoT.

In [A22], Fan *et al.* discussed the inherent defect of gradient-based adversarial attacks. A novel nongradient attack (NGA) is considered where the search strategy is effective but no longer depends on gradients to enhance the threat of adversarial examples. NGA outperforms the state-of-the-art adversarial attacks on attack success rate (ASR) significantly by up to 7%. A new evaluation metric, composite criterion (CC) based on both ASR and accuracy is proposed to measure the effectiveness of adversarial training more comprehensively for the reliability of IoT devices.

[A23] designs an optimal joint offloading scheme based on resource occupancy prediction for the problem of computing offloading with limited edge resources. Sun *et al.* utilized gate recurrent units to predict the multitask occupancy of edge resources. An optimal strategy of task offloading is produced by a reinforcement learning algorithm according to the network state. The proposed joint offloading scheme reduces the average delay of tasks and minimizes the task offloading failure rate for IIoT.

[A24] addresses the problems of cross-layer radio resource management, including power allocation in physical layer and random access in medium access layer. Liu *et al.* proposed a primal–dual DDPG algorithm for the cross-layer optimization. A multiagent primal–dual DDPG algorithm is devised for cell-free massive MIMO IIoT networks. The proposed primal–dual DDPG algorithm can realize efficient random access and power allocation.

In [A25], Li *et al.* designed a novel resource allocation and service co-placement (RaSP) algorithm to address the latency-aware online service reconfiguration problem for IoT. A RaSP prototype is implemented on the EdgeSim simulator. RaSP provides satisfying latency guarantees for newly incoming and previous requests of IoT services simultaneously and reduces the energy consumption of edge networks.

[A26] proposes a long short-term memory-based force reconstruction network (LSTM-FRN) by designing a novel sparse attention module for low-latency reconstruction and a novel metric-learning-based constraint for high-precision reconstruction. Li *et al.* constructed a large-scale data set of synchronous needle motion signals and haptic signals in acupuncture needle insertion. An interactive needle insertion training system (HapAR-NITS) integrating augmented reality (AR), the LSTM-FRN-based haptic reconstruction, and a skill assessment subsystem is established. HapAR-NITS enables satisfying immersive eHealth experiences.

In [A27], Ning *et al.* proposed malware traffic classification (MTC) methods based on semisupervised learning (SSL), transfer learning (TL), and domain adaptive (DA) to leverage a large amount of unlabeled data collected in the Internet traffic. The proposed MTC methods improve the classification accuracy with few labeled samples for IIoT.

In [A28], Gao *et al.* discussed the conflict between the operational performance and security of the blockchain system, the conflict between transparency and privacy, and the compatibility issues in IIoT. A novel system architecture is designed for IIoT devices to deploy high-performance blockchain systems. The sharding hashgraph consensus mechanism is exploited and a node evaluation mechanism based on node states is applied to divide IIoT nodes into shards dynamically, which can enhance the security of IIoT services.

[A29] achieves high accuracy and system scalability for IIoT multitask model sharing. Zhao *et al.* proposed an adaptively federated multitask learning (AFL) to generate subnets for each task using an iterative pruning network. The tailored task mask layers are devised to effectively train specialized subnets. An adaptive loss function is formulated to adjust the priority of IIoT tasks dynamically.

In [A30], Huang *et al.* proposed generative adversarial imitation learning (GAIL) to discover security risks in IIoT by training privacy protection agents using a large amount of expert data on privacy protection. GAIL has wide generalizability and high reliability in yielding the maximum payoff of the agents and reducing data security leakage risks.

[A31] introduces multikeyword conjunctive queries for using partial attributes to find target devices accurately and efficiently. Zhou *et al.* devised a universal device-oriented keyword searchable encryption scheme for cloud-assisted IIoT. The functions of a single and conjunctive keyword search are maintained to handle the device search requests using partial attributes. The proposed keyword searchable encryption scheme provides a lightweight index and query trapdoor for IIoT services.

In [A32], Kumar *et al.* presented BDTwin, a blockchain and deep-learning-based integrated framework to enhance security and privacy in cybertwin-driven V2X applications. A smart contract-based voting consensus mechanism is designed to ensure secure communications among vehicles, roadside units, cybertwin-edge servers, and cloud servers. Smart contracts are leveraged to enforce rules and regulations that govern the behavior of V2X entities in a nondeniable and automated manner. An autoregressive-deep variational autoencoder (AR-DVAE) model collaborates with attention-based bidirectional long short-term memory (A-BLSTM) for automatic feature extraction and attack detection in cybertwin-driven IIoT.

We would like to express our sincere thanks to all the authors for submitting their papers and to the reviewers for their valuable comments and suggestions that significantly enhanced the quality of these articles. We are also grateful to Prof. H. Wang, the Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL, for his great support throughout the whole review and publication process of this special issue, and, of course, all the editorial staff. We hope that this special issue will serve as a useful reference for researchers, scientists, engineers, and academics in the field of knowledge- and service-oriented IIoT.

DAPENG WU, *Guest Editor*
School of Communication and Information Engineering
Chongqing University of Posts and Telecommunications
Chongqing 400065, China

SHAOEN WU, *Guest Editor*
Department of Information Technology
Kennesaw State University
Marietta, GA 30060 USA

DANDA B. RAWAT, *Guest Editor*
Department of Electrical Engineering and Computer Science
Howard University
Washington, DC 20059 USA

PAULO R. L. GONDIM, *Guest Editor*
Electrical Engineering Department
University of Brasilia
Brasilia 70910-900, Brazil

PERIKLIS CHATZIMISIOS, *Guest Editor*
Department of Information and Electronic Engineering
International Hellenic University
Thessaloniki 57400, Greece
Department of Electrical and Computer Engineering
University of New Mexico
Albuquerque, NM 87106 USA

JINBO XIONG, *Guest Editor*
College of Computer and Cyber Security
Fujian Normal University
Fuzhou 350117, China

APPENDIX: RELATED ARTICLES

[A1] Y. Chen, Y. Sun, C. Wang, and T. Taleb, "Dynamic task allocation and service migration in edge-cloud IoT system based on deep reinforcement learning," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16742–16757, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3164441.

[A2] P. Yang, J. Hou, H. Zhang, P. Zhang, R. Wang, and Z. Li, "Traffic-aware transmission strategy of fog cell in green Industrial Internet," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16758–16769, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3164807.

[A3] Y. Zhen, W. Chen, L. Zheng, X. Li, and D. Mu, "Multiagent cooperative caching policy in Industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16770–16779, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3164447.

[A4] Y. Liu, C. Chi, Y. Zhang, and T. Tang, "Identification and resolution for Industrial Internet: Architecture and key technology," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16780–16794, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3160737.

[A5] Y. Zhang, Z. Ying, and C. L. P. Chen, "Achieving privacy-preserving multitask allocation for mobile crowdsensing," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16795–16806, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3153473.

[A6] W. G. Hatcher, C. Qian, F. Liang, W. Liao, E. Blasch, and W. Yu, "Secure IoT search engine: Survey, challenges issues, case study, and future research direction," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16807–16823, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3153171.

[A7] Q. Fan, S. Li, C. Qiu, X. Song, and W. Jie, "Ultrashort-term heat load prediction for heat exchange stations based on dual-source data feature fusion," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16824–16834, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3153453.

[A8] Y. Li, Y. Chen, K. Zhu, C. Bai, and J. Zhang, "An effective federated learning verification strategy and its applications for fault diagnosis in Industrial IoT systems," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16835–16849, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3153343.

[A9] J. Dong, G. Fan, F. Zheng, T. Mao, F. Xiao, and J. Lin, "TEGRAS: An efficient Tegra embedded GPU-based RSA acceleration server," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16850–16861, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3152203.

[A10] X. Yang, J. An, Z. Song, S. Luo, and A. Wang, "High-efficiency PCSK-CFFH system design for IoT networks," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16862–16873, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3147896.

[A11] C. Fang *et al.* "Deep-reinforcement-learning-based resource allocation for content distribution in fog radio access networks," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16874–16883, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3146239.

[A12] H. Huang, Y. Xue, J. Wu, Y. Tao, and M. Hu, "Temporal computing resource allocation scheme with end device assistance," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16884–16896, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3147238.

[A13] Y. Yi, Y. Yang, K. Cheng, Y. Wu, and X. Wang, "Information dissemination with service-oriented incentive mechanism in Industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16897–16907, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3147840.

[A14] Y. Fan, G. Wu, K.-C. Li, and A. Castiglione, "Robust end hopping for secure satellite communication in moving target defense," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16908–16916, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3144971.

[A15] Q. Li, Q. Zhang, H. Huang, W. Zhang, W. Chen, and H. Wang, "Secure, efficient and weighted access control for cloud-assisted Industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16917–16927, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3146197.

[A16] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16928–16940, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3142251.

[A17] Z. Li, X. Gao, Q. Li, J. Guo, and B. Yang, "Edge caching enhancement for Industrial Internet: A recommendation-aided approach," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16941–16952, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3143506.

[A18] I. Sarkar, M. Adhikari, S. Kumar, and V. G. Menon, "Deep reinforcement learning for intelligent service provisioning in software-defined industrial fog networks," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16953–16961, Sep. 15, 2022, doi: 10.1109/JIOT.2022.3142079.

[A19] J. Tang *et al.*, "Cross-layer optimization for Industrial Internet of Things in NOMA-based C-RANs," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16962–16975, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3138461.

[A20] C. Yang, X. Wang, and S. Mao, "RFID tag localization with a sparse tag array," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16976–16989, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3137723.

[A21] Y. Yang *et al.*, "Privacy-preserving threshold spatial keyword search in cloud-assisted IIoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16990–17001, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3138136.

[A22] M. Fan *et al.*, "Toward evaluating the reliability of deep-neural-network-based IoT devices," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17002–17013, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3138969.

[A23] Z. Sun *et al.*, "Cloud-edge collaboration in Industrial Internet of Things: A joint offloading scheme based on resource prediction," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17014–17025, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3137861.

[A24] X. Liu, H. Zhang, X. Wen, K. Long, J. Wang, and L. Sun, "Primal–dual learning for cross-layer resource management in cell-free massive MIMO IIoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17026–17034, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3137348.

[A25] X. Li, Z. Zhou, C. Zhu, L. Shu, and J. Zhou, "Online reconfiguration of latency-aware IoT services in edge networks," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17035–17046, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3135287.

[A26] A. Li, Y. Chen, S. Ni, J. Chen, and L. Zhou, "Haptic signal reconstruction in eHealth Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17047–17057, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3132771.

[A27] J. Ning *et al.*, "Malware traffic classification using domain adaptation and ladder network for secure Industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17058–17069, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3131981.

[A28] N. Gao, R. Huo, S. Wang, T. Huang, and Y. Liu, "Sharding-Hashgraph: A high-performance blockchain-based framework for Industrial Internet of Things with Hashgraph mechanism," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17070–17079, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3126895.

[A29] C. Zhao, Z. Gao, Q. Wang, K. Xiao, and Z. Mo, "AFL: An adaptively federated multitask learning for model sharing in Industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17080–17089, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3125989.

[A30] C. Huang, S. Chen, Y. Zhang, W. Zhou, J. J. P. C. Rodrigues, and V. H. C. de Albuquerque, "A robust approach for privacy data protection: IoT security assurance using generative adversarial imitation learning," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17089–17098, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3128531.

[A31] R. Zhou, X. Zhang, X. Wang, G. Yang, H.-N. Dai, and M. Liu, "Device-oriented keyword-searchable encryption scheme for cloud-assisted Industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17098–17109, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3124807.

[A32] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "BDTwin: An integrated framework for enhancing security and privacy in cybertwin-driven automotive Industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17110–17119, Sep. 15, 2022, doi: 10.1109/JIOT.2021.3122021.