Guest Editorial Introduction to the Special Section on Computational Intelligence and Advanced Learning for Next-Generation Industrial IoT

THE rapid development of real-time Industrial Internet-of-Things (IIoT) applications including green infrastructure, smart grids, smart city, intelligent transport networks, etc. enables green communication between tens of billions of end devices such as wearable devices and sensors. As a result, a tremendous amount of data is generated from massively distributed sources, which require computational intelligence techniques to fulfill high computing and communication demand that frequently exceeds energy consumption. Many emerging IIoT applications including remote surgery, machine monitoring and control, fault detection, and healthcare generate delay-sensitive tasks, which require timely processing with minimum delay. Besides, according to the energy consumption formulation, the required energy consumption for processing real-time tasks on remote computing devices should be the accumulation of data transmission time, transmission power, and processing capacity. Thereby, the energy emission rate can be controlled by balancing the trade-off between the transmission power and transmission time. IIoT covers a broad domain of real-time IIoT applications and refers to the combination of IoT technologies and computational intelligence techniques for processing real-time data with minimum delay. In addition, energy-efficient communication and computation of the real-time IIoT applications target to increase efficiency, automation, and productivity.

Recent advances in artificial intelligence (AI)-enabled techniques including advanced machine learning (ML) and deep learning (DL), bring many key research directions to analyze the computational intelligence framework by monitoring the real-time information and sensed data. Despite various advantages of the integration of computational intelligence techniques for various IIoT applications, the appropriate application of the AI model poses several challenges including data volume and quality, integration, and accuracy of the inferences drawn from the collected data. Besides that, advanced computational intelligence techniques such as distributed and federated learning are selected to train the local edge/fog devices locally and produce a global model under the coordination of a central edge/fog/cloud server. In recent times, advanced computational intelligence techniques for IIoT have attracted great interest from academia and industry.

The special section focused on the recent advances and novel contributions from academic researchers and industry practitioners in the area of computational intelligence techniques for the Next-generation IIoT applications to fully leverage the potential capabilities and opportunities brought by this area. Thanks to the extensive efforts of the reviewers and the great support from the Editor-in-Chief, Dr. Jianwei Huang, we were able to accept 27 contributed articles covering several important topics related to IIoT application [A1], mobile edge resource allocation [A2], Federated Learning (FL) in edge computing [A3], intelligent transportation system [A4], digital-twin in edge computing [A5], Blockchain and digital-twin in IIoT [A6], robust graph clustering [A7], distributed split mechanism in wireless communication system [A8], task offloading in D2D-based IIoT application [A9], prediction-based task allocation [A10], secured FL mechanism in healthcare system [A11], computational intelligence and deep learning in edge networks [A12], intrusion detection for IIoT applications [A13], privacy preservation in edge networks [A14], federated analysis in distributed IIoT network [A15], resource allocation using deep reinforcement learning [A16], securing IIoT applications using hybrid deep learning [A17], security enhancement using deep learning [A18], anomaly detection in IIoT application [A19], partial task offloading and resource allocation [A20], anomaly detection in IIoT application [A21], resource allocation in vehicular social networks [A22], computational offloading and resource allocation in end-edge-cloud framework [A23], privacy preserving data aggregation using FL [A24], secure framework for Internet of Drones [A25], accelerating CNN for IIoT applications [A26], object detection in edge networks [A27], dynamic tracking in IIoT [A1]. A brief review follows:

Li et al. in [A1], addressed that earlier research has attempted to follow the demographic trends, even though many have looked at tracking population dynamics. In this regard, their work suggested a widely used, reliable IIoT-based approach for tracking built environment demographic dynamics.

Zhang et al. [A2], proposed a proactive downlink system framework in which a proactive task-based data transmission problem is decomposed into multiple sub-problems and improves the low latency communication scenario.

Chakraborty and Misra in [A3], addressed the resource allocation problem to improve the quality of IIoT. Motivated by this, they proposed the framework using the Nah-Bargaining game approach that optimizes the service delay in edge networks.

Zhou et al. in [A4], considered the challenges in the vehicle re-identification area for cross-domain. To address this problem,

Digital Object Identifier 10.1109/TNSE.2023.3293695

they proposed a generative adversarial network to transform the identical vehicle into other domains.

Wen et al. [A5] considered the delays and communication failures in ocean monitoring platforms. To address this issue, they propose an artificial platform method based on maritime IoT where multi-autonomous underwater glider (AUG) systems are used to reduce communication delays.

Kumar et al. [A6] found different kinds of threats and attacks on ongoing communication by unreliable public communication channels and a lack of confidence among participating entities. In response to these difficulties, they provide an integrated framework of blockchain and Deep Learning (DL) for delivering decentralised data processing and learning in the IIoT network, where the DL scheme is created to apply the Intrusion Detection System (IDS) on legitimate data obtained from the blockchain.

Wang et al. [A7] found that many of the consolidation solutions now in use are unaware of the significance of an appropriate consolidation schema. They concentrate on offering a strong and efficient consolidation schema in their article. They consider the workload uncertainty issue and provide a graph-clustering-based approach that is more resilient to workload uncertainty in the future than the majority of existing methods, which primarily concentrate on the past workload. To achieve this, they present robust optimization, a mathematical approach that offers support theoretically for resolving uncertainty problems.

Sun et al. [A8] found wireless communication system dependability faces difficulties due to the stringent requirements for industrial applications. So, they suggest a distributed split mechanism with a cross-level dependability assessment model in their study. The distributed split mechanism splits and deploys the model's device-level assessment sub-models and system-level assessment sub-models independently once they have been trained together.

Ibrar et al. [A9] addressed the Social IIoT (SIIoT) problems due to uneven job offloading which actually worsens system performance. In this research, they offer an adaptive capacity task offloading solution for D2D-based social industrial IoT (ToSIIoT) that takes into account the strength of social links and device utilization ratio to enhance resource utilization, raise QoS, and achieve higher task completion rates. The suggested method has three components: selecting a socially conscious relay in a multi-hop D2D communication context, selecting a resource-rich SIIoT device for task offloading, and adaptive workload redistribution.

Peng et al. in [A10] found the efficiency of crowdsourcing job allocation is decreased by the fact that existing spatial crowdsourcing task allocation technologies overlook the temporal and spatial continuity of previous work data. For addressing this issue, they suggested a Spatiotemporal Prediction based Spatial Crowdsourcing technique, known as SPSC, utilizing blockchain and artificial intelligence to address these issues. The SPSC lowers the possibility of crowdsourcing employees banding together to steal the private data of crowdsourcing projects utilizing blockchain technology by classifying crowdsourcing activities and grouping crowdsourcing workers.

Zhang et al. [A11] introduced the deep learning of medical models in an Internet of Things (IoT)-based healthcare system. To further secure local models, cryptographic primitives like masks and homomorphic encryption are used. This prevents the adversary from deducing sensitive medical data through various methods like model reconstruction attacks or model inversion attacks. The security study demonstrates that the suggested solution fulfills data privacy.

Tang et al. [A12] found that it is difficult for multiple devices to complete local training and upload weights to the edge server promptly due to the constrained resources in industrial IoT networks, including CPU power, bandwidth, and channel status. So, they offer a novel multi-exit-based federated edge learning (ME-FEEL) framework to address this problem, allowing the deep model to be partitioned into numerous sub-models of varying depths and output prediction from the exit in each sub-model.

Zhang et al. [A13] noticed that intrusion detection is a practical way to increase security in the Industrial Internet of Things (IIoT) which are so susceptible to cyberattacks. However, since labeled examples are hard to come by, finding a trustworthy model is also challenging. They use graph neural network technologies to deal with the high dimensional, redundant, but categorically imbalanced and scarce labeled data in IIoT. This network constructor with refinement regularisation is created to alter the network structure to reduce the impact produced by the erroneous network structure.

Wang et al. in [A14] discussed that outsourcing data to far-away clouds always carries a risk to privacy and has a significant latency. As a result, they develop a new framework (called PCNNCEC) based on cloud-edge-client collaboration for effective and privacy-preserving CNN inference. In PCNNCEC, the cloud model and client data for the IIoT are divided into two shares and sent to two edge servers without collusion.

Wang et al. [A15] described that all types of federated industrial IoT learning tasks suffer considerably from the intrinsic data heterogeneity (skewness) of many industrial IoT data holders. They suggest a Federated skewness Analytics and Client Selection mechanism (FedACS) to quantify the skewness of the data while protecting privacy and use this knowledge to support subsequent tasks including federated learning.

Chang et al. [A16] present unique machine learning-based resource allocation and trajectory planning strategies for a multi-UAV communications system. They first provide a machine learning-based strategic resource allocation algorithm that uses deep learning and reinforcement learning to create the best possible policy for every UAV to address the issue created by the large dimensionality in state space. With no prior knowledge of the dynamic nature of networks, they then also provide a multi-agent deep reinforcement learning technique for distributed implementation.

Hasan et al. [A17] found that the attacks by smart and persistent multi-variant bots are seen as disastrous for connected IIoTs. Additionally, botnet attack detection is quite difficult and precise. Therefore, the prompt and effective identification of IIoT botnets is an urgent current demand. To protect IIoT infrastructure from deadly and complex multi-variant botnet attacks, they provide a hybrid intelligent Deep Learning (DL)-enabled technique.

Ye et al. [A18] discussed that the widespread adoption of WiFi fingerprinting of Received Signal Strength (RSS) for indoor localization is challenging. Current RSS fingerprint-based techniques lack security-related concerns and are open to hostile intrusions. They suggested suggesting SE-Loc, a strategy based on semi-supervised learning to increase the security and

robustness of fingerprint-based localization. The SE-Loc architecture consists of two components: (1) a correlation-based AP selection for handling RSS fingerprints and generating fingerprint images, and (2) a deep learning model based on a denoising autoencoder and convolutional neural networks for robust feature learning and location matching.

Gao et al. [A19] discovered that anomaly detection is crucial to assure hardware and software security since the IoT's time-series feature increases data density and dimension. The conventional anomaly detection technique, however, has trouble satisfying this requirement. So, in their research, they offer a memory-augmented autoencoder technique that uses reconstruction errors to identify data anomalies in IoT data.

Zhang et al. [A20] discussed that IIoT resources must be used effectively because IIoT devices have a finite capacity. Finding the best option for effective resource allocations is also difficult because of the variety of services customers can choose from and the dynamic nature of wireless networks. To address this issue, they suggested a partial task offloading and resource allocation strategy, aiming to maximize user work completed within a reasonable time frame while reducing energy consumption.

Yang and Zhou [A21] discovered that the data on intrusion detection is in the form of a dynamic data stream with infiniteness, correlations, and changing data distribution features. These characteristics, however, provide some challenges for the existing anomaly detection methods. To achieve accurate and effective anomaly detection with improved scalability, thus they offer ASTREAM (anomaly detection in data streams), a unique anomaly detection approach that combines sliding window, model updating, and change detection algorithms into LSHiForest.

Zhang and Zhou [A22] found that, due to the narrow range of vehicular social networks and the uneven distribution of cache resources, issues including low vehicle data transfer rates, subpar service quality, and poor service content delivery efficiency of streaming media are present. To address these issues, they offer an approach to resource distribution in vehicle social networks (RATG) based on tripartite graphs. Using vehicle mobility and social similarity as its foundations, this technique creates a mobile vehicular social network model.

Peng et al. [A23] discussed about the large scale of IIoT devices and the nature of the applications, as well as the constrained and heterogeneous resources of edge servers, prevent the direct deployment of the existing MEC approaches for IIoT situations. In light of this, they develop an end-edge-cloud collaborative intelligent optimization technique and formulate the offloading of computation and resource allocation as a multi-objective optimization issue.

Song et al. in [A24] showed that FL is vulnerable to a reverse attack, in which a foe might obtain user information by scrutinizing the user-uploaded model. Thus, they created EPPDA, an effective privacy-preserving data aggregation mechanism for FL, based on secret sharing to resist the reverse attack, which can aggregate users trained models covertly without disclosing the user models.

Tanveer et al. [A25] discussed the requirements of the authentication key exchange between users and drones in the Internet of Drones (IoD) networks for users to be able to communicate securely with the drone through the public communication infrastructure. In their study, they present a REAS-IoD authentication mechanism for IoD networks. The AKE process is carried out securely by the proposed REAS-IoD using the ACE authentication primitive and lightweight hash function.

Li et al. in [A26], offer ABM-SpConv-SIMD, an on-device inference optimization framework, to expedite the network inference by fully using the low-cost and common CPU resource. This model optimizer with pruning and quantization is used initially by ABM-SpConv SIMD to create models with sparse convolutions.

Wu et al.[A27], presented an edge computing and multi-task-driven framework to fulfill tasks of image enhancement and object detection with quick response, in contrast to previous techniques to acquire enhanced images before detection with various types of manually constructed filters.

In summary, the collected articles provide innovative application scenarios and shed light on the computational intelligence and advanced learning for next-generation Industrial IoT. We hope that this timely special section will trigger more future work in the emerging area.

MAINAK ADHIKARI, *Lead Guest Editor*
Department of Computer Science
Indian Institute of Information Technology
Lucknow 226002, India
mainak@iiitl.ac.in

VARUN G. MENON, *Guest Editor*
Computer Science and Engineering
SCMS Group of Educational Institutions
Kerala 683 106, India
varunmenon@ieee.org

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

XINGWANG LI, *Guest Editor*
Henan Polytechnic University
Henan 454099, China
lixingwang@hpu.edu.cn

APPENDIX
RELATED ARTICLES

[A1] P. Li et al., "IIoT based trustworthy demographic dynamics tracking with advanced Bayesian learning," *IEEE Trans. Netw. Sci. Eng.*, early access, Jan. 25, 2022, doi: 10.1109/TNSE.2022.3145572.

[A2] P. Zhang, H. Tian, P. Zhao, and S. Fan, "Context-aware mobile edge resource allocation in OFDMA downlink system," *IEEE Trans. Netw. Sci. Eng.*, early access, Nov. 24, 2022, doi: 10.1109/TNSE.2022.3224258.

[A3] A. Chakraborty and S. Misra, "QoS-aware resource bargaining for federated learning over edge networks in industrial IoT," *IEEE Trans. Netw. Sci. Eng.*, early access, Sep. 14, 2022, doi: 10.1109/TNSE.2022.3206474.

[A4] Z. Zhou et al., "GAN-Siamese network for cross-domain vehicle re-identification in intelligent transport systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 18, 2022, doi: 10.1109/TNSE.2022.3199919.

[A5] J. Wen, J. Yang, Y. Li, J. He, Z. Li, and H. Song, "Behavior-based formation control digital twin for multi-AUG in edge computing," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 19, 2022, doi: 10.1109/TNSE.2022.3198818.

[A6] P. Kumar et al., "Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 18, 2022, doi: 10.1109/TNSE.2022.3191601.

[A7] S. Wang, H. Lan, Y. Peng, and Z. Peng, "Consolidating industrial small files using robust graph clustering," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 01, 2022, doi: 10.1109/TNSE.2022.3195350.

[A8] D. Sun, J. Zhao, B. Chen, H. Wu, and J. Wu, "Cross-level dependability assessment with a distributed split mechanism for wireless communication systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 28, 2022, doi: 10.1109/TNSE.2022.3194535.

[A9] M. Ibrar et al., "Adaptive capacity task offloading in multi-hop D2D-based social industrial IoT," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 19, 2022, doi: 10.1109/TNSE.2022.3192478.

[A10] M. Peng et al., "Spatiotemporal prediction based intelligent task allocation for secure spatial crowdsourcing in industrial IoT," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 16, 2022, doi: 10.1109/TNSE.2022.3198675.

[A11] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system," *IEEE Trans. Netw. Sci. Eng.*, early access, Jun. 30, 2022, doi: 10.1109/TNSE.2022.3185327.

[A12] S. Tang et al., "Computational intelligence and deep learning for next-generation edge-enabled industrial IoT," *IEEE Trans. Netw. Sci. Eng.*, early access, Jun. 08, 2022, doi: 10.1109/TNSE.2022.3180632.

[A13] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Jun. 21, 2022, doi: 10.1109/TNSE.2022.3184975.

[A14] J. Wang, D. He, A. Castiglione, B. B. Gupta, M. Karuppiah, and L. Wu, "PCNNCEC: Efficient and privacy-preserving convolutional neural network inference based on cloud-edge-client collaboration," *IEEE Trans. Netw. Sci. Eng.*, early access, May 26, 2022, doi: 10.1109/TNSE.2022.3177755.

[A15] Z. Wang, Y. Zhu, D. Wang, and Z. Han, "Federated analytics informed distributed industrial IoT learning with non-IID data," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 04, 2022, doi: 10.1109/TNSE.2022.3187992.

[A16] Z. Chang et al., "Trajectory design and resource allocation for multi-UAV networks: Deep reinforcement learning approaches," *IEEE Trans. Netw. Sci. Eng.*, early access, May 03, 2022, doi: 10.1109/TNSE.2022.3171600.

[A17] T. Hasan et al., "Securing industrial internet of things against botnet attacks using hybrid deep learning approach," *IEEE Trans. Netw. Sci. Eng.*, early access, Apr. 22, 2022, doi: 10.1109/TNSE.2022.3168533.

[A18] Q. Ye et al., "SE-Loc: Security-enhanced indoor localization with semi-supervised deep learning," *IEEE Trans. Netw. Sci. Eng.*, early access, May 23, 2022, doi: 10.1109/TNSE.2022.3174674.

[A19] H. Gao et al., "TSMAE: A novel anomaly detection approach for internet of things time series data using memory-augmented autoencoder," *IEEE Trans. Netw. Sci. Eng.*, early access, Mar. 29, 2022, doi: 10.1109/TNSE.2022.3163144.

[A20] F. Zhang et al., "Deep reinforcement learning based cooperative partial task offloading and resource allocation for IIoT applications," *IEEE Trans. Netw. Sci. Eng.,* early access, Apr. 19, 2022, doi: 10.1109/TNSE.2022.3167949.

[A21] Y. Yang et al., "ASTREAM: Data-stream-driven scalable anomaly detection with accuracy guarantee in IIoT environment," *IEEE Trans. Netw. Sci. Eng.*, early access, Mar. 08, 2022, doi: 10.1109/TNSE.2022.3157730.

[A22] Y. Zhang and Y. Zhou, "Resource allocation strategy based on tripartite graph in vehicular social networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 23, 2022, doi: 10.1109/TNSE.2022.3153511.

[A23] K. Peng et al., "Intelligent computation offloading and resource allocation in IIoT with end-edge-cloud computing using NSGA-III," *IEEE Trans. Netw. Sci. Eng.*, early access, Mar. 08, 2022, doi: 10.1109/TNSE.2022.3155490.

[A24] J. Song et al., "EPPDA: An efficient privacy-preserving data aggregation federated learning scheme," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 25, 2022, doi: 10.1109/TNSE.2022.3153519.

[A25] M. Tanveer, A. U. Khan, T. Nguyen, M. Ahmad, and A. Abdei-Latif, "Towards a secure and computational framework for Internet of Drones enabled aerial computing," *IEEE Trans. Netw. Sci. Eng.,* early access, Feb. 15, 2022, doi: 10.1109/TNSE.2022.3151843.

[A26] X. Li et al., "ABM-SpConv-SIMD: Accelerating convolutional neural network inference for industrial IoT applications on edge devices," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 25, 2022, doi: 10.1109/TNSE.2022.3154412.

[A27] Y. Wu et al., "Edge computing driven low-light image dynamic enhancement for object detection," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 14, 2022, doi: 10.1109/TNSE.2022.3151502.

Mainak Adhikari (Senior Member, IEEE) received the B.Tech degree in computer science and engineering from the West Bengal University of Technology, Kolkata, India, and the M.Tech. degree in computer science and engineering from the University of Kalyani, Kalyani, India, and the Ph.D. degree from the Indian Institute of Technology Dhanbad, Dhanbad, India. He completed his Postdoctoral Research Fellowship from the Mobile & Cloud Lab, Institute of Computer Science, University of Tartu, Tartu, Estonia. He is currently the Head of Department and Assistant Professor of Indian Institute of Information Technology Lucknow, Lucknow, India. His research interests include distributed computing such as serverless computing, fog computing, and cloud computing, wearable sensors for healthcare, Internet-of-Things, and data analysis with AI approaches. He has contributed to numerous research articles/papers in various national and international journals such as IEEE, ACM, Elsevier, and Springer and conferences such as IEEE and Springer.

Varun G. Menon (Senior Member, IEEE) is currently an Associate Professor of computer science and engineering, international collaborations and a Corporate Relations in-charge with the SCMS School of Engineering and Technology, SCMS Group of Educational Institutions, Cochin, India. His research interests include the Internet of medical Things, Wearable sensor for healthcare, Ad Hoc network, wireless networks, 5G, fog computing and networking, underwater acoustic sensor networks, information science, scientometrics, opportunistic routing, and wireless sensor networks.

Danda B. Rawat (Fellow, IEEE) is currently a Professor with the Department of Electrical Engineering and Computer Science, the Founding Director of the Data Science and Cybersecurity Center, Graduate Program Director of Howard-CS Graduate Programs, Director of Graduate Cybersecurity Certificate Program, and Founding Director of Cyber-security and Wireless Networking Innovations Research Lab, Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning, and wireless networking for emerging networked systems including cyber-physical systems, Internet of Things, smart cities, software-defined systems, and vehicular networks.

Xingwang Li (Senior Member, IEEE) received the M.Sc. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2010, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015. From 2010 to 2012, he was an Engineer with Comba Telecom Ltd., Guangzhou, China. From 2017 to 2018, he was a Visiting Scholar with Queen's University Belfast, Belfast, U.K. His research interests include MIMO communication, cooperative communication, hardware constrained communication, nonorthogonal multiple access, physical layer security, unmanned aerial vehicles, and Internet of Things.