Guest Editorial: Special Issue on Robustness and Efficiency in the Convergence of Artificial Intelligence and IoT

TODAY, the Internet of Things (IoT) is increasingly flourishing with establishing ubiquitous connections between smart devices and objects, and by 2020, there will be a total of 30 billion connected things reported by IDC. The unprecedented data explosion provides immense opportunities for valuable information mining. At the same time, it also floods the infrastructure with tremendous values it necessarily handles and proposes high challenges to traditional data storing or processing techniques. On the other hand, artificial intelligence (AI) has become a key component for many applications that profoundly change our lives. Machine learning, especially deep learning (DL) technologies, vastly improves traditional computer science and networking technologies. The convergence of AI and IoT enables data to be quickly explored and turned into significant decisions. For companies and enterprises, AI enhances the speed and accuracy of data processing for instant market strategies.

However, DL techniques also face the serious issue that the meticulously trained DL models are susceptible to the tiny perturbations in the input data called adversarial examples (AEs). This issue brings many attacks to mislead the DL models by generating AEs maliciously, or the "mess" objects in the physical world will challenge DL models' robustness. On the other hand, deploying AI methods on IoT systems must consider the efficiency issues. Therefore, this special issue aims to focus the research on the robustness and efficiency of the AI techniques in current IoT systems. First, the special issue will include novel research on vital issues, such as AE-based attacks and defense on the IoT systems. This special issue will also aim to bring attention to the convergence of AI solutions' efficiency issues with the IoT systems.

The response to our call for this special issue was overwhelming, as we received more than 90 submissions from around the world. Each article was assigned to and reviewed by at least three experts in the field during the review process, with a rigorous multiround review process. Thanks to the tremendous support from the Editor-in-Chief, Honggang Wang, and the dedicated work of numerous reviewers, we accepted 29 excellent articles regarding the robustness and efficiency in the convergence of AI and IoT. In the following, we will introduce these articles and highlight their main contributions.

In the article "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," Alkadi *et al.* investigate a blockchain-based framework with DL approach to identify the intrusion attacks while preserving data privacy. The intrusion detection method equipped a bidirectional long short-term memory (BiLSTM) DL algorithm to deal with sequential network data. The privacy-based blockchain and smart contract methods are developed using the Ethereum library to provide privacy to the distributed intrusion detection engines.

The article "A 3-D topology evolution scheme with self-adaption for Industrial Internet of Things" exploits the problem of building an energy-efficient topology based on the unique mine terrain characteristics. Qiu *et al.* propose a 3-D topology evolution scheme with self-adaption for mining areas to reduce energy consumption. The proposed scheme aims to determine the optimal number of sink nodes and find the best data transmission path between sensor nodes and multiple sink nodes for IIoT.

In the article "Car e-Talk: An IoT-enabled cloud-assisted smart fleet maintenance system," Hussain *et al.* propose a fleet maintenance system called Car e-Talk that uses Internet-of-Things technology and cloud computing to monitor vehicle health and report any anomalies along with information about the nearest maintenance center. The advantages of the proposed system are that it can monitor real-time vehicle health statistics, predict fleet health and maintenance, improve vehicle diagnostics, and perform automatic reporting, thus increasing the vehicle's usable life, fleet productivity, and performance.

The article "An adversarial examples identification method for time series in the Internet-of-Things system" exploits the problem of AEs that lies in time-series data in IoT systems. Jiang *et al.* propose a time-series representation method that can be adapted to detect AEs effectively. The proposed representation and metric are then being adopted in a supervised and unsupervised learning manner to evaluate the detection efficiency.

In the article "Joint multiuser DNN partitioning and computational resource allocation for collaborative edge intelligence," Tang *et al.* investigate the optimization problem of DNN partitioning in a realistic multiuser resource-constrained condition. The authors propose a novel algorithm with detailed theoretical analysis to solve the resource allocation problem in polynomial time.

Digital Object Identifier 10.1109/JIOT.2021.3073800

The article "IoT-inspired framework for athlete performance assessment in smart sport industry" presents an IoT-Fog computing-inspired game-theoretic model for provisioning in-depth analysis of athlete performance in real time. Sport-oriented parameters are acquired using smart devices. A game-theoretic mathematical model is proposed between the sports athlete and monitoring officials for effective decision-making services.

In the article "Deep-learning-enabled security issues in the Internet of Things," Lv *et al.* propose a hierarchical intrusion detection model based on IoT to improve detection efficiency. The autoencoder is specially studied in this work with detailed results. The model designed in this research can be applied to intrusion detection under IoT, reduce the detection load, and improve the detection effect and security stability.

The article "Network representation learning-enhanced multisource information fusion model for POI recommendation in smart city" proposes a network representation learning-enhanced multisource information fusion model for POI recommendation in the context of location-based social networks. The social influence is modeled by performing network representation learning methods on the constructed co-visiting user networks. A fusion model is designed to consider user preference, social influence, and geographical influence for POI recommendation.

In the article "Robust spammer detection using collaborative neural network in Internet-of-Things applications," Guo *et al.* propose a collaborative-neural-network-based spammer detection mechanism in social media applications. The proposed method introduces multisource information fusion by collaboratively encoding long-term behavioral and semantic patterns to achieve a comprehensive representation of the feature space to detect spam.

The article "TT-SVD: An efficient sparse decision-making model with two-way trust recommendation in the AI-enabled IoT systems" proposes an accurate sparse decision-making model with two-way trust recommendation in the AI-enabled IoT systems. The proposed model incorporates both trust information and rating information more thoroughly. A dual model, including a truster model and a trustee model, is integrated and proposed to achieve the goal.

In the article "Robust learning-enabled intelligence for the Internet of Things: A survey from the perspectives of noisy data and adversarial examples," Wu investigates the state-of-the-art and representative works of robust ML models that can enable high resilience and reliability of IoT intelligence. The work specifically focuses on two real-life cases, i.e., the training data contains noises and AEs.

The article "EBI-PAI: Toward an efficient edge-based IoT platform for artificial intelligence" proposes an edge-based IoT platform for AI based on the software-defined network and serverless technologies. The proposed platform provides a unified service calling interface and schedules the resources automatically to satisfy the QoE requirements of users

In the article "Distributed attention-based temporal convolutional network for remaining useful life prediction," Song *et al.* present a DL-based RUL prediction method with an attention mechanism to weight sequence data's representations. The proposed method weights different industrial sensors and time steps, respectively, based on the distributed attention mechanism. Then, temporal convolution modules with the shared weights are used for feature extraction of time series.

The article "Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices" presents a thorough study over adversarial attacks in COVID-19 diagnostic methods that rely on DL algorithms. The results show that DL-based COVID-19 diagnostic models that do not consider defensive models against adversarial perturbations remain vulnerable to adversarial attacks.

In the article "A robust deep-learning-enabled trust-boundary protection for adversarial Industrial IoT environment," Hassan *et al.* propose a downsampler-encoder-based cooperative data generator that trained using a proposed algorithm to ensure better capture of the actual distribution of attack models for the sizeable IIoT attack surface. The proposed downsampler-based data generator is updated and verified during training using a deep neural network discriminator to ensure robustness.

The article "ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes" presents a new privacy-preserving security architecture for SDN-based smart homes. Then, an anonymous lightweight authentication mechanism is designed based on the proposed security architecture core foundations. The proposed protocol's security characteristics are formally analyzed using Burrows–Abadi–Needham logic and ProVerif, followed by security analysis.

In the article "Multiview summarization and activity recognition meet edge computing in IoT environments," Hussain *et al.* propose an edge-intelligence-based multiview video summarization and activity recognition framework that combines AI with the IoT devices. The proposed work does not rely solely on a summary but encodes and transmits information to a master device using a neural computing stick for interview correlations computation and efficient activity recognition.

The article "A multicloud-model-based many-objective intelligent algorithm for efficient task scheduling in Internet of Things" constructs a many-objective distributed scheduling model, including six objectives: time, cost, cloud throughput, energy consumption, resource utilization, and balancing the load. This work also presents a many-objective intelligent algorithm with sine function to implement the model, which considers the variation tendency of diversity strategy in the population is similar to the sine function.

In the article "Deep reinforcement learning for scenario-based robust economic dispatch strategy in Internet of Energy," Fang *et al.* propose a scenario-based robust economic dispatch strategy for virtual power plants, aiming to reduce the operational costs of virtual power plants. Deep reinforcement learning (DRL) is adopted for historical data training, directly solving nonlinear and nonconvex problems to obtain a robust economic dispatch strategy.

The article "Toward convergence of AI and IoT for energy-efficient communication in smart homes" presents a study over the QoS optimization during video streaming through wireless micro medical devices in smart healthcare homes.

In the article "Memristor-based variation-enabled differentially private learning systems for edge computing in IoT," Fu *et al.* propose a noise distribution normalization method to add Gaussian distributed noise through hardware implementation, thereby achieving differential privacy in edge AI. The authors take advantage of inherent cycle-to-cycle variations of memristors during the weight-update process as the noise source, which does not incur extra software or hardware overhead.

The article "A model for joint planning of production and distribution of fresh produce in agricultural Internet of Things" presents a mixed-integer programming model, which covers labor and capital constraints. The decisions obtained are based not only on price estimation and resource availability but also on the impact of the agricultural IoT technology and each distribution channel's particular requirements.

In the article "Video scene segmentation using tensor-train faster-RCNN for multimedia IoT systems," Dai *et al.* propose a tensor-train video scene segmentation scheme that compares the local background information in regional scene boundary boxes in adjacent frames. The proposed scheme can achieve competitive performance in both segmentation accuracy and parameter compression rate compared to existing methods.

The article "Attacking and protecting data privacy in edge–cloud collaborative inference systems" conducts a systematic study about the opportunities of attacking and protecting the privacy of edge–cloud collaborative systems.

In the article "FSLM: An intelligent few-shot learning model based on Siamese networks for IoT technology," Yang *et al.* propose an intelligent few-shot learning model based on Siamese networks. The proposed model consists of two self-attention models with the same parameters divided into two parts. For two input texts, a self-attention model is used to extract sentiment features. The Mahalanobis distance is adopted to measure the similarity between two feature vectors to determine whether they belong to the same category.

The article "Multiple wavelet convolutional neural network for short-term load forecasting" proposes a multiple wavelet convolutional neural network for load forecasting.

In the article "DDLPF: A practical decentralized deep learning paradigm for Internet-of-Things applications," Wu *et al.* propose a decentralized DL paradigm with privacy-preservation and fast few-shot learning by exploiting federated learning, metalearning, and blockchain techniques.

The article "Energy-aware geographic routing for real-time workforce monitoring in industrial informatics" proposes a new energy-efficient routing algorithm geographic routing time transfer, to use topological information of sensor nodes for target tracking and coverage applications.

In the article "Multiagent deep reinforcement learning for vehicular computation offloading in IoT," Zhu *et al.* propose a multiagent DRL-based computation offloading scheme, in which the uncertainty of a multivehicle environment is considered.

We want to express our sincere thanks to all the authors for submitting their papers and the reviewers for their valuable comments and suggestions that significantly enhanced these articles' quality. We are also grateful to Prof. H. Wang, the Editor-in-Chief of IEEE INTERNET OF THINGS JOURNAL, for his tremendous 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 valuable reference for researchers, scientists, engineers, and academics in robustness and efficiency in the convergence of AI and IoT.

MEIKANG QIU, *Lead Guest Editor*
Department of Electrical Engineering
Columbia University
New York, NY 10027 USA

BHAVANI THURAISINGHAM, *Guest Editor*
Department of Computer Science
University of Texas at Dallas
Richardson, TX 75080 USA

MAHMOUD DANESHMAND, *Guest Editor*
School of Business
Stevens Institute of Technology
Hoboken, NJ 07030 USA

HUANSHENG NING, *Guest Editor*
School of Computer and
Communication Engineering
University of Science and Technology Beijing
Beijing 100083, China

PAYAM BARNAGHI, *Guest Editor*
Academic and Research Departments
University of Surrey
Guildford GU2 7XH, U.K.