Guest Editorial: Federated Learning for Industrial IoT in Industry 4.0

THE development and evolution of modern information and communication technologies is leading us to the fourth industrial revolution, in which the Industrial Internet of Things (IIoT) is assumed to be one of the key aspects to realize Industry 4.0. With the increase of both quantity and type of IoT devices, a critical mass of data is collected from the real-world environment every day. The data need to be processed and analyzed to derive intelligence for further use in efficient, secure, and economic ways, and machine learning has been adopted in academia and industry to scrutinize and study the data for business decision-making. Nevertheless, data hungriness may hinder the development of machine-learning-enabled systems, with another growing challenge on protecting data privacy. To address the above issue, Google proposed the concept of federated learning in 2016. As an emerging machine learning paradigm, it allows clients at edge to perform model training locally and only send model parameter updates to a central server for the aggregation of the global model. All raw data are kept in respective local storage and not transferred to other clients.

Federated learning facilitates the implementation of secure platform with consideration on data privacy to support IIoT. Many researchers and practitioners have expressed their interest in this area with the expectation of profound effect in the context of Industry 4.0. However, the topic is quite new and has not been investigated under its different profiles until now. There is a lack of literature from both a theoretical and an empirical point of view. Therefore, this special sector is dedicated to provide cutting-edge technologies and novel studies, which can realize and elevate the effectiveness and advantages of federated learning for advancing industrial IoT. Eleven articles have been accepted by this Special Section based on review, and revision processing.

In the first article "FED-IIoT: A robust federated malware detection architecture in Industrial IoT," Taheri *et al.* [A1] present a method to detect Android malware in IIoT applications, enabled by a robust federated learning-based architecture. The architecture considers 1) a participant side with two dynamic poisoning attacks based on a generative adversarial network and federated generative adversarial network (GAN), and 2) a server side, which can monitor and shape collaboration training model, avoiding anomaly in aggregation by a GAN network and adjust two GAN-based countermeasure algorithms. The three proposed algorithms were demonstrated with a detailed description. This approach was evaluated on accuracy by conducting experiments on various features (i.e., different round, different number of clients, and different number of adversaries) using three datasets.

The second article "Privacy-preserving aggregation for federated learning-based navigation in vehicular fog," authored by Kong *et al.* [A2], suggests a privacy-preserving model aggregation scheme with the federated learning-based navigation framework. In the proposed scheme, security is ensured by hiding the model hyperparameter within a predefined threshold number of users using the Shamir secret sharing scheme, and detecting and excluding unregistered users from the learning process via an identity-based signature. In addition, the scheme supports flexible onboarding and exiting rules for participants by exploiting a skip list for group division. The authors conducted security analysis and performance evaluation in terms of computational complexity for user joining/leaving, robustness against dishonest users, and the tradeoff between security and flexibility.

In "FASTGNN: A topological information protected federated learning approach for traffic speed forecasting," Zhang *et al.* [A3] addressed the issue of topological information in transportation networks when applying federated learning (FL). They designed an FL framework consisting of the following:

1) a differential privacy-based approach for adjacency matrix preserving to protect the topological information;
2) an adjacency matrix aggregation mechanism to generate a preserved global-network adjacency matrix;
3) a GNN-based model with advanced spatial-temporal techniques to forecast traffic speed.

Experiments were carried out to examine the accuracy of speed forecasting, critical components, and the overall performance of proposed GNN model on a real-world traffic dataset.

Zhang *et al.* [A4] focused on the increase of the model aggregation rate and reduction of communication cost in FL application when managing and training a large amount of data in the fourth article "Deep reinforcement learning assisted federated learning algorithm for data management of IIoT." The authors applied deep reinforcement learning (DRL) to assist the selection of nodes, of which the ones with high data quality are preferred. Afterward, the selected nodes perform local model training and send the parameters to the central server for global model aggregation. Performance evaluation was conducted based on MNIST and Fashion MNIST datasets in terms of the impact of number of clients on accuracy, communication rounds on accuracy, and the convergence of loss value. The DRL-based algorithm was compared with the baseline algorithm FedSGD, and the results showed that the proposed solution can have effective model training process and achieve higher accuracy.

In the fifth article "TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT," Rehman *et al.*

Digital Object Identifier 10.1109/TII.2021.3086509

[A5] utilized blockchain technology in federated learning systems, to maintain participants' reputation, as the decentralized nature of both blockchain and federated learning align with each other. All devices form a community on blockchain, which stores the reputation scores. In this article, Ethereum was selected and three types of smart contracts (i.e., reputation, aggregator, and incentive mechanism smart contracts) were deployed to provide different functionalities. Inter Planetary File System was used for the version control of the model. In addition, the proposed framework can detect adversarial behaviors and remove the malicious participants before aggregating the model updates through statistical methods. The authors evaluated their design on model loss and the ability to detect adversaries.

The sixth article "Diagnosis of inter-turn short circuit faults in permanent magnet synchronous motors based on few-shot learning under a federated learning framework," authored by Zhang *et al.* [A6], depicts a few-shot learning approach based on Stacked Sparse Autoencoders and Siamese networks for the diagnosis of inter-turn short circuit faults in permanent magnet synchronous motors (PMSMs). In this article, the authors provided a detailed description on the background of PMSMs. The framework incorporates Siamese network to improve the feature learning ability, uses L1 distance to determine the similarity identify classes of samples, and adopts federated learning for the optimization of the overall model. Experiments were conducted to examine the main parameters for the optimal branch structure, compare the model accuracy with state of the art, and also analyze the ability of learning unbalanced data.

In "Resource allocation for latency-aware federated learning in Industrial Internet-of-Things," Gao *et al.* [A7] employed a resource allocation scheme for federated learning to address the collision issue and reduce the overall training latency. The authors first formulated the resource allocation task as an optimization problem with NP-hardness, and then designed a heuristic algorithm in which the most appropriate clients can be selected, by greedily allocating the preferred resources to each device and calculating the training latency. In the evaluation part, the proposed solution was validated on both training latency and convergence speed using an RGB-D dataset. Further analysis on the impact of different factors (i.e., available channels, transmit power allocation, device selection, and active devices) was also discussed.

Jin *et al.* [A8] adopted multiple nested long short-term memory networks (MTMC-NLSTM) for the forecasting of air quality index (AQI) in the eighth article "Multivariate air quality forecasting with nested LSTM neural network." In their design, the training and testing of six core AQI components are enhanced by federated learning, which can extract the internal correlation between these components. There are three steps in the forecasting method: 1) normalizing AQI time series data by zero-score normalization; 2) dividing the processed data into training set and testing set, where 5% of training set is further split as the validation set, and conducting model training for prediction; and 3) denormalizing and testing the generated prediction results to check the performance. Experiments were carried out with four evaluation metrics (i.e., mean absolute error, root mean squared error, mean absolute percentage error, and r-square) over each AQI component. The results were compared with other 17 baseline algorithms.

In the ninth article "A federated learning-based license plate recognition scheme for 5G-enabled Internet of Vehicles," Kong *et al.* [A9] investigated a license plate recognition framework based on federated learning, to mitigate the privacy risks caused by centralized model training in Internet of Vehicles. First, a license plate detection model was designed to be directly deployed at the mobile devices by reducing the number of parameters. Second, a tilt license plate correction algorithm was integrated into the recognition model to improve the accuracy. Third, federated learning was applied to preserve individual data locally for model training, and only send update gradients to the central server. The detection and recognition models were tested on accuracy with several baseline methods, while the federated learning process was examined on the impact of dirty data.

The tenth article "An asynchronous and real-time update paradigm of federated learning for fault diagnosis," authored by Ma *et al.* [A6], aimed to address the issue of effectiveness and performance via an asynchronous federated learning scheme. The proposed method consists of four main steps: 1) clients decode the global model and form the fusion center; 2) each local model is updated using the decoded information and local data through the extended Kalman filter; 3) clients upload the model parameters to the fusion center; and 4) the center performs asynchronous fusion based on the sequential Kalman filter. Simulation was conducted to validate the proposed approach via two different cases, and the results showed that the method has high fault diagnostic accuracy.

In the final article "Federated tensor decomposition-based feature extraction approach for Industrial IoT," Gao *et al.* [A11] presented a federated tensor decomposition (FTD) model for feature extraction, which includes two core components: 1) a joint high-order orthogonal iteration method (JHOOI) and 2) an FTD approach. In JHOOI, the authors implemented simultaneous decomposition of high-dimensional tensors and extraction of low-dimensional features. The FTD combines both JHOOI and federated learning to analyze the patterns of collected industrial data while preserving the user privacy. Experiments were performed to evaluate reconstruction accuracy and classification precision of the proposed solution using ORL and Fabrics datasets.

Acknowledgment

The guest editors would like to thank all the authors who submitted their work to this Special Section. In addition, the guest editors would also like to thank all the reviewers for their great efforts. Finally, they sincerely appreciate the support from the Editor-in-Chief, Professor Ren C. Luo, for his support and guidance in administrative issues. The guest editors wish all readers enjoy the researches in this special sector.

Jiehan Zhou, *Guest Editor*
University of Oulu
FI-90014 Oulu, Finland

Qinghua Lu, *Guest Editor*
Data61, CSIRO
Sydney, NSW 2015, Australia

WENBIN DAI, *Guest Editor*
Shanghai Jiao Tong University
Shanghai 200232, China

ENRIQUE HERRERA-VIEDMA, *Guest Editor*
University of Granada
18071 Granada, Spain

APPENDIX
RELATED ARTICLES

[A1] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "FED-IIoT: A robust federated malware detection architecture in Industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8442–8452, Dec. 2021.
[A2] Q. Kong et al., "Privacy-preserving aggregation for federated learning-based navigation in vehicular fog," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8453–8463, Dec. 2021.
[A3] C. Zhang, S. Zhang, J. J. Q. Yu, and S. Yu, "FASTGNN: A topological information protected federated learning approach for traffic speed forecasting," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8464–8474, Dec. 2021.
[A4] P. Zhang, C. Wang, C. Jiang, and Z. Han, "Deep reinforcement learning assisted federated learning algorithm for data management of IIoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8475–8484, Dec. 2021.
[A5] M. H. u. Rehman, A. M. Dirir, K. Salah, E. Damiani, and D. Svetinovic, "TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8485–8494, Dec. 2021.
[A6] J. Zhang, Y. Wang, K. Zhu, Y. Zhang, and Y. Li, "Diagnosis of inter-turn short circuit faults in permanent magnet synchronous motors based on few-shot learning under a federated learning framework," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8495–8504, Dec. 2021.
[A7] W. Gao, Z. Zhao, G. Min, Q. Ni, and Y. Jiang, "Resource allocation for latency-aware federated learning in Industrial Internet-of-Things," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8505–8513, Dec. 2021.
[A8] N. Jin, Y. Zeng, K. Yan, and Z. Ji, "Multivariate air quality forecasting with nested LSTM neural network," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8514–8522, Dec. 2021.
[A9] X. Kong *et al.*, "A federated learning-based license plate recognition scheme for 5G-enabled Internet of Vehicles," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8523–8530, Dec. 2021.
[A10] X. Ma, C. Wen, and T. Wen, "An asynchronous and real-time update paradigm of federated learning for fault diagnosis," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8531–8540, Dec. 2021.
[A11] Y. Gao, G. Zhang, C. Zhang, J. Wang, L. T. Yang, and Y. Zhao, "Federated tensor decomposition-based feature extraction approach for Industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 12, pp. 8541–8549, Dec. 2021.

Jiehan Zhou received the Ph.D. degree in mechanical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2000, and the second Ph.D. degree in computer engineering from the University of Oulu, Oulu, Finland, in 2011.

He is currently a Docent Professor with the Faculty of Information Technology and Electrical Engineering, University of Oulu, Oulu, Finland, and a Visiting Professor with the School of Mechanical Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is also a Postdoctor the with Tsinghua University and University of Toronto. He has supervised and participated in more than 27 ICT projects funded by NSFC, Academy of Finland, EU FP6-IST, EU ITEA3, and Canada NSERC. He has authored or coauthored more than 150 scientific papers in the fields of industrial Internet, cloud computing, big data, machine learning, federated learning, and Internet of Things. His main research include intelligent manufacturing, industrial internet, big data, cloud computing, Semantic Web, knowledge engineering, and service-oriented computing.

Dr. Zhou is a recipient of the ERCIM Fellowship (European Researcher Consortium of Informatics and Mathematics) hosted by Finland VTT and France INRIA.

Qinghua Lu (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of New South Wales, Sydney, NSW, Australia, in 2013.

She is currently a Senior Research Scientist with Data61, CSIRO, Sydney, NSW, Australia. Before joining Data61, she was an Associate Professor with the China University of Petroleum, and she was a Researcher with National Information and Communications Technology Australia. She has authored or coauthored more than 100 academic papers in international journals and conferences. Her research interests include the software architecture, blockchain, software engineering for AI, and AI ethics.

Wenbin Dai received the B.Eng. (Hons.) degree in computer systems engineering from the University of Auckland, Auckland, New Zealand, in 2006 and the Ph.D. degree in electrical and electronic engineering from the Department of Electrical and Computer Engineering, The University of Auckland in 2012.

He is currently an Associate Professor with the Department of Automation, School of Electrical Information and Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China, and the Director of SJTU-Rockwell Automation Joint Research Laboratory. From 2013 to 2014, he was a Postdoc Fellow with the Lulea University of Technology, Sweden. In 2014, he joined the Shanghai Jiao Tong University, China, as an Assistant Professor. From 2007 to 2013, he was also a Software Engineer with Glidepath Limited, a New Zealand-based airport baggage-handling system provider, and designed and commissioned more than 30 airport baggage-handling systems.

Enrique Herrera-Viedma (Fellow, IEEE) received the Ph.D. degree in computer science from the University of Granada, Granada, Spain, in 1996.

He is currently a Professor with the Department of Computer Science and Artificial Intelligence, University of Granada, where he is currently the Vice-Rector for Research and Knowledge Transfer. He has also been a Guest Lecturer in plenary lectures and tutorials in multiple national and international conferences related to artificial intelligence (AI). He has authored or coauthored more than 300 papers in JCR journals. In 2013, he published in the prestigious journal *Science* about the new role of digital libraries in the era of the information society.

Prof. Herrera-Viedma was the Vice-President for Publications with the IEEE System Man and Cybernetics Society during 2019–2020. He is currently the VP for Cybernetics, founder of the IEEE TRANSACTIONS IN ARTIFICIAL INTELLIGENCE, and a Highly Cited Researcher by Clarivate Analytics in Computer Science and Engineering in 2014–2020. His H-index is 101 in Google Scholar (more than 33 000 citations) and 85 in WoS (more than 23 000 citations). He is an Associate Editor of several AI journals like IEEE TRANSACTIONS FUZZY SYSTEMS, IEEE TRANSACTIONS INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, *Knosys*, *Applied Soft Computing*, FUZZY OPTIMIZATION AND DECISION MAKING, *Information Sciences*, *Soft Computing*.