Guest Editorial: Security and Privacy of Federated Learning Solutions for Industrial IoT Applications

THE Industrial Internet of Things (IoT) typically consists of several thousands of heterogeneous devices, such as sensors, actuators, access points, machinery, end-users' handheld equipment, and supply chain. In such an industrial environment, a multitude of data is generated from massive IoT devices, e.g., sensors for monitoring the environment, reading temperature, and gauging pressure. Most of the data are from delay-sensitive and computation-intensive applications, such as real-time manufacturing and automated diagnostics, which require big data analytics with low latency. Machine learning (ML) has been witnessed as an efficient solution for big data analytics. The majority of such ML algorithms are centralized methods, meaning that they first gather data from different users for use as a training dataset, which is placed on the ML server, and then build a model to classify the new data samples by applying the ML algorithms to this training dataset. However, the access to these datasets in the centralized ML methods raises concerns about data privacy for users. Federated learning (FL) was designed to protect data privacy to address a part of these issues. In FL, each participant uses a global training model without uploading their private data to a third-party server. Compared with the conventional ML, FL can preserve data security, especially in terms of participant data during the learning process. In particular, FL can also help in updating server-side data for the global model, and the participant is not required to provide their data. However, in FL, individual computing units may show abnormal actions, such as faulty software, hardware invasions, unreliable communication channels, and malicious samples deliberately crafting the model. To mitigate these challenges, we require robust policies to control the learning phases in FL. Motivated by the abovementioned issues, this special section solicits original research and practical contributions that advance the security and privacy of the FL solutions for industrial IoT applications as follows.

In [A1], Golec *et al.* propose a security and privacy-based lightweight framework called iFaaSBus, which uses the concept of IoT, ML, and function as a service (FaaS) or serverless computing to diagnose the COVID-19 disease and manages resources automatically to enable dynamic scalability. Furthermore, trust mechanisms, such as blockchain and biometric authentication, can be incorporated within iFaaSBus to prevent future attacks, such as denial of service. Moreover, iFaaSBus can be tested using other quality of services parameters, such as energy, reliability, availability, cost, and other issues, such as platform migration and debugging.

Digital Object Identifier 10.1109/TII.2021.3128972

IoT devices are widely considered in smart cities, intelligent medicine, intelligent transportation, among other fields that facilitate people's lives, and producing a large amount of private data. However, due to the mobility, limited performance, and distributed deployment of IoT, the traditional access control methods cannot support the security of private data's access control process in the current IoT environments. To solve this issue, in [A2], Han *et al.* propose a blockchain-based auditable access control system based on the Hyperledger Fabric platform by applying the blockchain technology and the attribute-based access control model. The proposed approach can track the request record, response record, and access record of private data through the distributed network and consensus authentication.

Customer baseline load (CBL) reconstruction is a critical problem in residential demand response (DR). The difficulty of residential CBL lies in the variability of both irregular consumption and on-site distributed energy resources. In [A3], Chen *et al.* propose a privacy-preserving CBL estimation scheme for the DR-participating residents. With the aid of FL, a three-layer hierarchical estimation architecture is established to manage the residential participants, residential unit, and independent third party. This article addresses how to prevent the leakage of private data when training the client model.

In [A4], Zhang *et al.* propose an FL model used in IIoT data transmission that combine blockchain and edge computing. Their proposed model underlies devices and allocates computing tasks to the edge server with rich computing resources. Their method could solve the problem and provide low computing power by uploading data information to the blockchain for the verification of the devices. They analytically verified the reduction of the risk of information disclosure for the devices.

FL is vulnerable to the backdoor attack from strong malicious participants. The backdoor attack is inconspicuous and may result in devastating consequences. To resist the attack on IIoT applications, in [A5], Hou *et al.* propose a novel federated backdoor filter defense algorithm dealing with inputs, identifying the malicious inputs, and restoring the data to availability by the blur-label-flipping strategy. To do this, they present an effective filter-training approach with the help of XAI models and clean the backdoor trigger area for suspicious backdoor data.

In [A6], Qu *et al*. propose ChainFL, a novel simulation platform that could simulate multiple IoT devices, edges, and clouds. ChainFL is a lightweight mechanism that is compatible with the blockchain embedding and distributed learning, such as FL and cope with a complex task offloading in such networks.

The traditional FL models are strongly dependent on a centralized aggregation server, which will cause the system to crash if the server is compromised. Such models are vulnerable to neat communication among the clients and server, and cause

issues for complex cross-domain devices, such as 5G UAVs. To address such issues, in [A7], Feng *et al.* designe a BE-DHFL, blockchain-empowered decentralized horizontal FL, framework for 5G-enabled UAVs. Their decentralized FL framework could employ blockchain technology for model aggregation to avoid the single point of failure represented by a centralized aggregator.

MOHAMMAD SHOJAFAR, *Guest Editor*
5G & 6G Innovation Centre (5GIC & 6GIC)
University of Surrey
GU2 7XH Guildford, U.K.

MITHUN MUKHERJEE, *Guest Editor*
Nanjing University of Information
Science and Technology
Nanjing 210044, China

VINCENZO PIURI, *Guest Editor*
Computer Science Department
University of Milan
20122 Milano, Italy

JEMAL ABAWAJY, *Guest Editor*
School of Info Technology
Deakin University
Burwood, VIC 3125, Australia

APPENDIX
RELATED WORKS

[A1] M. Golec, R. Ozturac, Z. Pooranian, S. S. Gill, and R. Buyya, "iFaaSBus: A security and privacy based lightweight framework for serverless computing using IoT and machine learning," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3095466.

[A2] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri, and K. -C. Li, "A blockchain-based auditable access control system for private data in service-centric IoT environments," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3114621.

[A3] Y. Chen *et al.*, "Privacy-preserving baseline load reconstruction for residential demand response considering distributed energy resources," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3107400.

[A4] P. Zhang, Y. Hong, N. Kumar, M. Alazab, M. D. Alshehri, and C. Jiang, "BC-EdgeFL: Defensive transmission model based on blockchain assisted reinforced federated learning in IIoT environment," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3116037.

[A5] B. Hou *et al.*, "Mitigating the backdoor attack by federated filters for industrial IoT applications," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3112100.

[A6] G. Qu, N. Cui, H. Wu, R. Li, and Y. M. Ding, "ChainFL: A simulation platform for joint federated learning and blockchain in edge/cloud computing environments," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3117481.

[A7] C. Feng, B. Liu, K. Yu, S. K. Goudos, and S. Wan, "Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3116132.

ACKNOWLEDGMENT

The Guest Editors would like to thank all the authors who have submitted their valuable contributions and to the numerous and highly qualified anonymous reviewers. They believe that the selected contributions, which represent the current state of the art in the field, will be of great interest to the industrial electronics community. They would also like to thank Prof. R. Luo, Editor-in-Chief of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, for giving them the opportunity to organize this Special Section and for all the encouragement, help, and support given throughout the process, and Linda, TII staff, for her professional support and assistance during the whole preparation of this Special Section.

Mohammad Shojafar (Senior Member, IEEE) received the Ph.D. (Hons.) degree in ICT from the Sapienza University of Rome, Rome, Italy, in 2016.

He is currently a Senior Lecturer (Associate Professor) in network security and an Intel Innovator. He is currently working with the 5G & 6G Innovation Centre (5GIC & 6GIC), Institute for Communication Systems (ICS), University of Surrey, Guildford, U.K. Before joining 5GIC & 6GIC, he was a Senior Researcher and a Marie Curie Fellow with the SPRITZ Security and Privacy Research Group, University of Padua, Padua, Italy.

Prof. Shojafar is an IES Member, a Professional ACM Member, an ACM Distinguished Speaker, and a Marie Curie Alumni. He is an Associate Editor for the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE SYSTEMS JOURNAL, and *Computer Networks*. He is a PI of AutoTrust, a 750k euros 5G secure autonomous vehicular communication project supported by the European Space Agency (ESA) in 2021 and was a PI of PRISENODE Project, a 275k euros Horizon 2020 Marie Curie Global Fellowship Project in the areas of fog/cloud security collaborating with the University of Padua. He was also a PI of an Italian SDN security and privacy (60k euros) supported by the University of Padua in 2018. He has contributed to some Italian projects in telecommunications, such as GAUChO, SAMMClouds, and SC2.

Mithun Mukherjee (Senior Member, IEEE) received the B.E. degree in electronics and communication engineering from the University Institute of Technology, The University of Burdwan, Bardhaman, India, in 2007, the M.E. degree in information and communication engineering from the Indian Institute of Science and Technology, Shibpur, India, in 2009, and the Ph.D. degree in electrical engineering from the Indian Institute of Technology Patna, Patna, India, in 2015.

He is currently an Assistant Professor with the School of Artificial Intelligence, Nanjing University of Information Science and Technology, Nanjing, China. His research interests include wireless communications and intelligent edge computing.

Dr. Mukherjee was the recipient of the 2016 EAI WICON, 2017 IEEE SigTelCom Best Paper Award, and 2018 IEEE SYSTEMS JOURNALBest Paper Award. He was the Guest Editor for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, *ACM/Springer Mobile Networks and Applications*, and *Sensors*.

Vincenzo Piuri (Fellow, IEEE) received the Ph.D. degree in computer engineering from Politecnico di Milano, Milan, Italy, in 1989.

Since 2000, he has been a Full Professor of computer engineering with the Università degli Studi di Milano, Milan, Italy. He was an Associate Professor with Politecnico di Milano, a Visiting Professor with The University of Texas at Austin, Austin, TX, USA, and a Visiting Researcher with George Mason University, Fairfax, VA, USA. He is also an Honorary Professor with Obuda University, Budapest, Hungary, Guangdong University of Petrochemical Technology, Maoming, China, Northeastern University, Shenyang, China, Muroran Institute of Technology, Muroran, Japan, Amity University, Noida, India, and Galgotias University, Noida, India. He has authored or coauthored in more than 400 articles in international journals, proceedings of international conferences, books, and book chapters. His research interests include artificial intelligence, computational intelligence, intelligent systems, machine learning, pattern analysis and recognition, signal and image processing, biometrics, intelligent measurement systems, industrial applications, digital processing architectures, fault tolerance, dependability, and cloud-computing infrastructures.

Dr. Piuri is the IEEE Region 8 Director-elect (2021–2022) and the President of the IEEE Systems Council (2020–2021). He was the IEEE Vice President for Technical Activities (2015), IEEE Director, President of the IEEE Computational Intelligence Society, Vice President of Education of the IEEE Biometrics Council, Vice President of Publications of the IEEE Instrumentation and Measurement Society and the IEEE Systems Council, and Vice President of Membership of the IEEE Computational Intelligence Society. He was the Editor-in-Chief for the IEEE SYSTEMS JOURNAL (2013–2019) and an Associate Editor for the IEEE TRANSACTIONS ON CLOUD COMPUTING. He was an Associate Editor for the IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON NEURAL NETWORKS, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, and IEEE ACCESS. He was the recipient of the IEEE Instrumentation and Measurement Society Technical Award (2002) and the IEEE TAB Hall of Honor (2019). He is a Distinguished Scientist of ACM and a Senior Member of INNS.

Jemal Abawajy (Senior Member, IEEE) is currently a Full Professor with the Faculty of Science, Engineering and Built Environment, Deakin University, Burwood, VIC, Australia. He has authored or coauthored more than 400 refereed articles and supervised numerous Ph.D. students to completion.

Prof. Abawajy is currently an Associate Editor for many journals, including the IEEE ACCESS, *Electronic Commerce Research*(Springer), *Sensors*(MDPI), and *Parallel, Emergent and Distributed Systems*(Taylor & Francis). He has delivered more than 50 keynote and seminars worldwide and has been involved in the organization of more than 300 international conferences in various capacity, including the Chair and the General Co-Chair. He was also on the editorial board of numerous international journals, including the IEEE TRANSACTIONS ON CLOUD COMPUTING.