IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Security and Privacy of Federated Learning Solutions for Industrial IoT Applications

Theme: Industrial Internet of Things typically consists of several thousands of heterogeneous devices, such as sensors, actuators, access points, machinery, end-user's hand held equipment, and supply chain. In such industrial environment, multitude of data is generated from massive IoT devices, e.g., sensors for monitoring environment, reading temperature, and gauging pressure. Most of data is 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 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 new data samples by applying ML algorithms to this training dataset. However, the access to these datasets in centralized ML methods raises concerns about data privacy for users. To address a part of these issues, federated learning (FL) was designed to protect data privacy. In FL, each participant uses a global training model, without needing to upload their private data to a third-party server. Compared with conventional ML, FL can preserve data security, especially in terms of participant data during the learning process. 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, for example due to faulty software, hardware invasions, unreliable communication channels, malicious samples deliberately craft the model. To mitigate these challenges, we require robust policies to control the learning phases in FL.

Motivated by the above issues, this special section solicits original research and practical contributions which advance security and privacy of federated learning solutions for industrial IoT applications. Results obtained by simulations must be validated in bounds by experiments or analytical results. Surveys and state-of-the-art tutorials are also considered.

This special section will focus on (but not limited to) the following topics:

- Privacy preserving and security approaches for large scale analytics in IIoT
- Hardware-Level Attack and Defense in Federated Learning for IIoT
- Determining appropriate security measures in response to risk assessments in Federated Learning for IIoT
- Data-Centric Security in Federated Learning for IIoT
- Finding and evaluating vulnerabilities that threats might exploit in Federated Learning for IIoT
- Privacy and trust challenges associated with federated learning in IIoT
- Resilient decision making under security and privacy constraints in Federated Learning for IIoT
- Validation of security and privacy protection methods in real-world applications

Follow the guidelines in "Information for Authors" in the IEEE Transaction on Industrial Informatics http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics . Please submit your manuscript in electronic form through Manuscript Central web site: https://mc.manuscriptcentral.com/tii . On the submitting page #1 in popup menu of manuscript type, select: SS on **Security and Privacy of Federated Learning Solutions for Industrial IoT Applications**

Submissions to this Special Section must represent original material that has been neither submitted to, nor published in, any other journal. Regular manuscript length is 8 pages.

Note: The recommended papers for the section are subject to final approval by the Editor-in-Chief. Some papers may be published outside the special section, at the EIC discretion.

Timetable: Deadline for manuscript submissions **June 30, 2021**
Expected publication date (tentative) January 2022

Guest Editors:

Dr. Mohammad Shojafar, University of Surrey, UK m.shojafar@surrey.ac.uk
Dr. Mithun Mukherjee, Nanjing University of Inf.Sci. &Tech., China mithun@nuist.edu.cn
Prof. Vincenzo Piuri, University of Milan, Italy vincenzo.piuri@unimi.it
Prof. Jemal Abawajy, University of Deakin, Australia jemal.abawajy@deakin.edu.au