IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Privacy-Preserving Federated Machine Learning Solutions for Enhanced Security of Critical Energy Infrastructures

Theme: The Critical Energy Infrastructure (CEI) is specific engineering information about proposed or existing critical infrastructure. Modern critical infrastructures are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks, and most importantly combined cyber-physical attacks, which are much more challenging and it is expected to become the most intrusive attack. This is particularly true for the Critical Energy Infrastructures (CEI). During 2015, the Industrial Control Systems Cyber Emergency Response Team in US responded to more than 245 incidents; the Energy sector tops the list with 32% incidents.

Taking into account the importance of energy in our daily life and its influence to other critical infrastructures, CEI requires significant attention comparatively. For example, wind-turbine system is considered one of the most complex Cyber-Physical infrastructures causing huge cascading effects to other Critical Energy Infrastructures (CEIs), such as Electrical Power and Energy Systems (EPES), transportation, healthcare sector, communications, industry and finance. Wind turbines are mainly composed of condition monitoring and operational data (i.e. Supervisory Command and Data Acquisition-SCADA), including air-temperature, air-pressure, voltage and power with multiple types of parameters and periodic characteristics.

Compared with legacy SCADA systems, recent-developed infrastructures utilize less expensive and scalable IOT that enables the data monitoring in near real-time conditions. However, the main limitations regarding wind turbine data monitoring still pertain. An innovative approach is to adopt Privacy-Preserving Federated Machine Learning solutions in order to detect any possible anomalies in such infrastructures. Instead of centralizing the wind-turbine data into a common server, Federated Machine Learning allows the data to remain on-premise in the infrastructure. This enables the responsible authorities to consider the advantages of Machine Learning, and simultaneously protect their privacy. Federated learning is able to train a model using data stored at multiple wind-turbine stations without the data leaving the station's premises as illustrated in figure below.

This special issue will respond to the research challenges by encouraging researchers in the computing world to bring to bear novel techniques, combinations of tools, and so forth to build effective ways to Enhancing the Security of Critical Energy Infrastructures.

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

- Federated Learning for Critical Infrastructure
- Enhancing the Security of Critical Energy Infrastructures
- Federated Learning in Energy Sector
- Model and Infrastructure for Federated Learning in Energy
- Advances and Open Problems in Federated Learning in Critical Infra Structure
- Scalable Federated in Energy sector
- Securing federated learning
- Federated Learning for Crisis in Critical Infrastructure

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 **Privacy-Preserving Federated Machine Learning Solutions for Enhanced Security of Critical Energy Infrastructures**

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 **March 30, 2021**

Expected publication date (tentative) December 2021

Guest Editors:

- Dr. Imran Razzak, Deakin University, Victoria, Australia. imran.razzak@deakin.edu.au
- Prof. Guandong Xu, University of Technology, Sydney, Australia Guandong.xu@uts.edu.au
- Prof. Muhammad Khurram Khan, King Saud University, Saudi Arabia mkhurram@ksu.edu.sa