IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Trustworthiness of AI-ML-DL Approaches in Industrial Internet of Things and Applications

Theme: The impressive future influence of the Industrial Internet of Things (IIoT) and its applications in industry and commerce is already widely recognized. This includes automated environments, such as smart factories, smart airports, and smart healthcare systems. Artificial Intelligence (AI) approaches enable automation and data analytics across industrial technologies, including the IIoT, cloud and edge, and fog computing paradigms. Current machine learning (ML) models, such as deep learning (DL) models, still suffer from designing a generalized trustworthy architecture that reveals semantics and contexts of models and attacks threat surface. Recent cyberattack statistics show that complex cyberattacks on AI/ML/DL approaches in IIoT systems and applications are upcoming. One reason is that these approaches are often black-box, unexplainable, or not transparent, meaning that diverse issues associated with data security, data privacy, data transparency, and data quality are not explainable. If any concerns related to these issues appeared during the data processing through the AI/ML/DL approaches are not answered. Furthermore, data or decisions can be compromised at the time of data collection, during the processing, or before decision-making. For example, some models like adversarial machine learning (AML) have been widely utilized to fool ML/DL applications using malicious actors.

There can be more challenges that bring the trustworthiness issues with AI/ML/DL in IIoT. (1) Networked devices used in industrial IIoT applications have various constraints related to energy, processing, communication, while they are expected to provide high trustworthy and real-time processing, decision-making, and monitoring. It is assumed to be tough and complex to have full-scale AI/ML/DL approaches running on tiny devices. (2) Major security objectives, such as integrity, availability, and confidentiality, have not been measured while regularly training and validating ML/DL models in IIoT. (3) Numerous threat scenarios, such as causative, inference, data poisoning, data collusion, security violation, and indiscriminate attacks, make an optimization problem for self-tuning ML/DL components and refining their hyperparameters in the network for IIoT. (4) The development of trustworthy AI/DL/ML methods in IIoT networks, including sensors, actuators, and their telemetry data, is still in its infancy, due to the challenges and its practical insights. As a result, AI/ML/DL approaches should be developed to establish white-box models, rather than black-box ones in order to determine their trustworthiness and reliability in business problems in IIoT networks.

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

- Trustworthiness issues in AI/ML/DL in IIoT
- Trustworthy and secure learning architectures in IIoT
- Dependability in AI/ML/DL enabled IIoT system design and development
- Trustworthiness in AI-enabled predictive maintenance, equipment, and process monitoring
- Trustworthiness in AI integrated machines, tools, apps, and techniques for IIoT
- Trustworthiness in AI-enabled services and open-source software for IIoT
- Trustworthiness of AI-enabled tools and software dealing with privacy
- Trustworthiness in privacy-preserving DL/ML models for IIoT
- Trustworthy AI-based intrusion detection and prevention in IIoT
- Trustworthiness and resource constraint trade-offs in IIoT
- Trustworthiness in AI approaches used in cloud/edge/fog assisted IIoT
- ML/DL micro-algorithms for security applications at the edge in IIoT networks
- Trustworthiness in AI-enabled applications, including fingerprinting, healthcare, event tracking, robotics in IIoT
- Trustworthiness assessment, metrics, evaluation, and prediction in AI/ML/DL approaches for IIoT

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 **Trustworthiness of AI-ML-DL Approaches in Industrial Internet of Things and Applications in Industrial IoT Systems and 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**	**December 30, 2021**
	Expected publication date (tentative)	**August 2022**

Guest Editors:

Prof. Zakirul Alam Bhuiyan, Fordham University, USA zakirulalam@gmail.com; mbhuiyan3@fordham.edu
Prof, Sy-Yen Kuo, National Taiwan University, Taiwan sykuo@ntu.edu.tw
Prof. Guojun Wang, Guangzhou University, China csgjwang@gmail.com ; csgjwang@gzhu.edu.cn

Editor-in-Chief: Prof. Dr.-Ing; Ren C. Luo tii@ira.ee.ntu.edu.tw