IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Emerging Privacy and Security Issues brought by Artificial Intelligence in Industrial Informatics

Theme: Nowadays, Artificial Intelligence (AI) based technologies have deeply changed people's daily lives. There are many AI-based applications used in industrial scenarios such as Internet of Things (IoT), smart grids, and edge computing. Although bringing AI into industrial scenarios could improve the performance in many aspects, new security and privacy issues are also introduced with it. Subsequently, machine learning technologies require a training process which introduces the protection problems in the training data and algorithms. As many machine learning and deep learning models are vulnerable against well-designed adversarial input samples, outsourcing data and algorithms for training will require the integrity of the training data. Also, data privacy of the end users must be protected. On the other hand, traditional solutions for industrial system (such as cyber, network, and communication) security could also be enhanced by these AI schemes. As AI-based protection and detection schemes could highly improve the countermeasures that used to be relying on human experts. Thus, this special section theme is expected to provide the primary and emerging research topics about bringing AI into industrial environments.

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

- Machine learning based security solutions for industrial informatics
- Deep learning based security solutions for industrial informatics
- Big data based security solutions for industrial informatics
- Privacy issues for machining learning in industrial informatics
- Attacks against machine learning in industrial informatics
- Emerging threat models for machining learning in industrial informatics
- Data privacy protection for machine learning in industrial informatics
- Data poison issues for machine learning in industrial informatics
- Data deception issues for machine learning in industrial informatics
- Security evaluation for the smart industrial systems
- Security M2M communications for the smart industrial systems
- Homomorphic computing in smart industrial systems

Manuscript Preparation and Submission

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 **Emerging Privacy and Security Issues brought by Artificial Intelligence in Industrial Informatics**

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**	**May 31, 2019**
	Expected publication date (tentative)	**October 2019**

Guest Editors:

Prof. Meikang Qiu, Columbia University, USA qiumeikang@yahoo.com
Prof. Hong-Ning Dai, Macau University of Science and Technology, Macau hndai@ieee.org
Prof. Arun Kumar Sangaiah, Vellore Institute of Technology, India arunkumarsangaiah@gmail.com
Prof. Kaitai Liang, University of Surrey, UK k.liang@surrey.ac.uk
Prof. Xi Zheng, Macquarie University, Sydney, Australia james.zheng@mq.edu.au

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