IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

" Security, Privacy, and Trust for Industrial Internet of Things "

Theme: Internet of Things (IoT) is heterogeneous networks provide ingenious services and applications in several fields, adopting IoT in the industry awards the Industrial IoT (IIoT) technology. IIoT has come to be an extensive trend in the business and commerce development as it helps organizations to attain extreme achievements with reduced expenses. However and regrettably the promising IIoT technology lacks of many security measures that make it vulnerable to many sorts of cyberattacks, for example and not limited to, node capture, side-channel analysis, eavesdropping, man-in-the-middle and distributed denial of service attacks. Moreover, the IIoT networks need challenging requirements to achieve the desired security and reliability. Unfortunately, traditional security solutions and even regular IoT solution cannot address the Industrial IoT security flaws due to the different nature of the IIoT. An integral part of IIoT is the Operational Technologies (OT), such as SCADA, needs to have a deep security examination. Present SCADA technology are distributed and networked over open internet protocols, which make it susceptible to cyber-attacks, an enhancement of the Modbus, Profibus, Fieldbus, and Hart protocols with digital authentication should promise, confidentiality, integrity, availability, and dynamic group management for OT. IIoT context has precise necessities when it comes to security and reliability, such as; i) Bounded and fast response is required to attain the business continuity. ii) Reliability, unlike the regular IoT that operates in domestic areas, Industrial IoT systems operate in hazardous areas with safety implications that may threaten lives. iii) Scalability is needed to, dynamically and remotely, add and revoke sensor nodes efficiently. iv) Power consumption is very important factor to be carefully considered especially with ambient power and battery-driven devices. v) Security is a serious issue for all sensory applications; however, industrial usages need more robust and reliable procedures due to their safety implications. All these constrains must be considered during the security protocols design process. As encryption is the cornerstone of information security, authenticated encryption has been getting a lot of attention in the IIoT context to attain integrity and confidentiality. Fast and lightweight encryption plays a great role in achieving the adapted security and privacy for IIoT; however, lightweight encryption still needs to study new techniques, which must be formally verified over the modern cryptography. On the other hand, key management in terms of authenticated key agreement with key confirmation (AKC) protocols need to be obtainable in a new customization for the IIoT context to consider fast rekeying and nodes addition and revocation.

This Special Section aims to attract pioneer and novel work of Security, Privacy, and Trust for the Industrial Internet of Things including novel and innovative security mechanisms that are resilient to the current Industrial IoT cyberattacks.

Topics include, but are not limited to, the following research topics and technologies:

Lightweight encryption protocols for IIoT
Key management protocols for IIoT
Mutual authentication protocols for IIoT
Privacy and security protocols for IIoT
Cyberattacks detection and prevention for IIoT
Threat models and attack scenarios for IIoT
Security solutions complexity for IIoT
Authorization, authentication, and access control in IIoT
Secure M2M communications in IIoT
Operational technologies (OT) security and privacy in the IIoT context
Secure smart grids in the IIoT context
Applied cryptographic solution for the IIoT context
Crypto analysis and enhancement for current IIoT security solutions
Malware and intrusion detection for IIoT
Hardware and embedded security for IIoT
SCADA-security

Manuscript Preparation and Submission

Follow the guidelines in "Information for Authors" in the IEEE- IES website: 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, Privacy, and Trust for Industrial Internet of Things**.

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 31, 2018 (Extended to Jan. 31, 2019)**
	Expected publication date (tentative)	**August 2019**

Editor-in-Chief: Prof. Dr.-Ing; Ren C. Luo tii@ira.ee.ntu.edu.tw
http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics

IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Guest Editors:

Prof. Mikael Gidlund, Mid Sweden University, Sweden, *mikael.gidlund@miun.se*
Dr. Gerhard. P. Hancke, City University of Hong Kong, Hong Kong, *gp.hancke@cityu.edu.hk*
Dr. Mohamed Eldefrawy, Mid Sweden University, Sweden, *Mohamed.eldefrawy@miun.se*
Dr. Nuno Pereira, Polytechnic Institute of Porto, Portugal, *nap@isep.ipp.pt*
Dr. Johan Åkerberg, ABB Corporate Research, Västerås, Sweden, *johan.akerberg@se.abb.com*