5G-enabled Intelligent Applications for Distributed Industrial Internet-of-Thing System

**Theme:** As a novel network infrastructure that realizes the interconnection of humans, machines, and things, 5G enables a large number of devices with communication and sensing capabilities to securely, quickly, and reliably connect to the Internet and facilitates IIoT (Industrial Internet of Things) applications such as smart cities, smart homes, and smart grids. 5G-enabled drones have potential applications in various military and civilian settings such as Radar anomaly detection, UAV (Unmanned Aerial Vehicles) data storage sharing, and traffic data analysis. 5G-enabled IIoT deployments will generate diverse traffic, reliability, bit rates, energy consumption, and security and privacy. Specifically, there are underlying privacy considerations associated with the data collection, handling, storage, and analysis in this distributed network, including high overhead and privacy leakages. Blockchain is a decentralized distributed database technology. Its decentralization, immutability, and transparency characteristics can ensure the security of data in a distributed network. Although the combination of 5G-enabled intelligent applications and blockchain has a bright future and can promote the development of distributed IIoT systems, it also brings a series of severe challenges, including poor scalability, low efficiency, and privacy leakages. Thus, it is challenging to apply 5G-enabled intelligent applications for the distributed IIoT system. In this special issue, we aim to collect the latest developments in using 5G and blockchain technology for designing and developing privacy-preserving solutions.

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

- Trust manage, computing or evaluation in 5G-enabled IIoT
- Blockchain based access control designs for shared data in 5G-enabled IIoT
- Public data auditing in 5G-enabled IIoT
- Encrypted textual data search in 5G-enabled IIoT
- Verifiability of search results in 5G-enabled IIoT
- Data deduplication over encrypted cloud data in 5G-enabled IIoT
- Encrypted image search in the 5G-enabled IIoT applications
- Attacks on searchable encryption schemes in 5G-enabled IIoT
- Different types of encrypted data search in 5G-enabled IIoT
- Threat model and risk assessment in 5G-enabled IIoT
- Secure data computation in 5G-enabled IIoT
- Machine learning algorithms for 5G-enabled IIoT
- Novel security architectures in 5G-enabled IIoT data mining
- Privacy preservation in data mining in 5G-enabled IIoT
- Defense countermeasures of data mining in 5G-enabled IIoT
- Federated learning architecture in 5G-enabled IIoT
- Trust discovery architecture in 5G-enabled 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](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](https://mc.manuscriptcentral.com/tii). On the submitting page #1 in popup menu of manuscript type, select: SS on 5G-enabled Intelligent Applications for Distributed Industrial Internet-of-Thing System

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: February 25, 2021
- Expected publication date (tentative): October 2021

**Guest Editors:**

- Prof. Ximeng Liu, Fuzhou University, China, x@fzu.edu.cn
- Prof. Robert Deng, Singapore Management University, Singapore, robertdeng@smu.edu.sg
- Dr. Yinbin Miao, Xidian University, China, ybmiao@xidian.edu.cn
- Prof. Athanasios V. Vasilakos, Lulea University of Technology, Sweden, athanasios.vasilakos@ltu.se

---

**Editor-in-Chief:** Prof. Dr.-Ing. Ren C. Luo

tii@ira.ee.ntu.edu.tw