IEEE Internet of Things

Special Issue on

Data Management and Security in Resource-constrained Intelligent IoT Systems

In recent years, various IoT devices today also are deployed with Artificial Intelligence (AI) algorithms or Deep Learning (DL) models for complex tasks such as face recognition, autonomous intelligent systems, intelligent robotics, etc. In order to realize an intelligent IoT system, various resource-constrained IoT devices today should play a role in not only data collection systems (e.g. sensor networks) but also data processing systems. However, rapidly increasing data is collected, transmitted, and processed by today's IoT devices which leads to two novel challenges as follows. First, many IoT devices are resource-constrained including limited data storage and processing ability or limited energy consumption requirements which needs novel solutions to efficiently manage the data to support the intelligent tasks of these IoT systems. Second, the novel data protection requirements appear since constrained resources like computation power or energy of IoT devices cannot support classic data protection methods like encryption algorithms.

In this special issue, we aim to seek novel solutions from hardware level to algorithm level for the above two challenges to realize intelligent IoT systems. For data management, we expect novel theories, concepts, and paradigms for data compression, storage, communication, etc. for efficiently and effectively managing the big data for resource-constrained intelligent IoT systems. For data security, we expect novel threats and protection schemes that can outperform classic methods for resource-constrained intelligent IoT systems.

Topics include, but are not limited to the following:

- Novel Data-centric Security Techniques in Intelligent IoT Systems
- Novel Task-oriented Data Compression Methods in Intelligent IoT Systems
- Novel Theories, Concepts, and Paradigms of the Data Management Solutions in IoT
- Access Control and Policies for Data Security in Intelligent IoT Systems
- Semantic Communications in the Intelligent IoT Systems
- Lightweight Hardware Verification in Intelligent IoT Systems
- Privacy-enhancing Technologies in Intelligent IoT Systems
- Novel Adversarial Attacks in Intelligent IoT Systems
- Emerging Data Bias Security Issues in Intelligent IoT Systems
- Big Data Assessment Metrics and Evaluation Criteria in Intelligent IoT Systems

Important Dates:

Submission Deadline: Feb. 1st, 2024
Final Manuscript Due: Jun. 15th, 2024
Publication Date: July 2024

Submission Guidelines:

Authors need to follow the manuscript format and an allowable number of pages described at http://ieeeiotj.org/guidelines-for-authors/. To submit a manuscript for consideration for the special issue, please visit the journal submission website at https://mc.manuscriptcentral.com/iot.

Guest Editors:

Prof. Meikang Qiu, Dakota State University, USA, qiumeikang@yahoo.com (lead guest editor)
Prof. Sun-Yuan Kung, Princeton University, USA, Email: kung@princeton.edu
Prof. Cheng Zhang, Ibaraki University, Japan, cheng.zhang.abbott@vc.ibaraki.ac.jp
Prof. Han Qiu, Tsinghua University, China, qiuhan@tsinghua.edu.cn