IEEE Internet of Things Journal Special Issue on
Privacy and Security in Distributed Edge Computing and Evolving IoT

Recent advances in artificial intelligence, edge computing, and big data, have enabled extensive reasoning capabilities at the edge of the network. Edge servers are now capable of extracting meaningful analytics from IoT nodes, which give insights about unprecedented changes of data-driven economy that finds applications in diverse sectors ranging from smart manufacturing and smart transportation to predictive maintenance and precision healthcare. Despite this ongoing advancement, there are growing concerns regarding the privacy of data providers when they grant edge applications direct access to their embedded sensors.

Data mining on genuine data could be harmful to data privacy. For example, data mining on time-series data taken from motion sensors, microphones, and GPS sensors could reveal users' activities, demographics, attributes and daily interactions. This could potentially lead to security/privacy concerns in many participatory and opportunistic crowd-sensing applications, where a large group of individuals having mobile devices capable of sensing and computing collectively share data and extract information to measure, map, analyze, estimate or infer any processes of common interest. While privacy preserving has not been the initial focus of traditional data analytics on edge servers, when used in domains such as cyber security, there are incentivized, malicious adversaries present in the system willing to game and exploit edge processing vulnerabilities.

This special issue focuses on solutions that leverage techniques and insights from the domains of artificial intelligence, edge computing, and big data to resolve privacy and security challenges in distributed edge computing and evolving IoT applications. Topics of interest for this special issue include, but are not limited to

- Optimization of the utility-privacy tradeoffs
- Privacy-preserving data aggregation
- Privacy-preserving data mining
- Privacy protection in edge computing assisted with evolving IoT
- Privacy preserving solutions for crowdsensing
- Privacy preserving in presence of advanced persistent threats
- Privacy-enhancing cryptographic techniques
- Multiparty access control in edge computing assisted with evolving IoT
- Middleware for privacy protection in IoT applications
- Future perspectives of privacy issues in IoT applications

Important Dates:
Submissions Deadline: July 1, 2019
First Reviews Due: September 15, 2019
Revision Due: October 15, 2019
Second Reviews Due/Notification: November 15, 2019
Final Manuscript Due: December 15, 2019
Publication Date: 2020

Submission:
All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Solicited original submissions must not be currently under consideration for publication in other venues. Author guidelines and submission information can be found at http://iot.ieee.org/journal.

Guest Editors: Dr. Alireza Jolfaei, Federation University, Australia (a.jolfaei@federation.edu.au)
Dr. Pouya Ostovari, San Jose State University, USA (pouya.ostovari@sjsu.edu)
A/Professor Mamoun Alazab, Charles Darwin University, Australia (mamoun.alazab@cdu.edu.au)
Professor Iqbal Gondal, Federation University, Australia (iqbal.gondal@federation.edu.au)
Professor Krishna Kant, Temple University, USA (kkant@temple.edu)