CALL FOR PAPERS
IEEE Internet of Things Journal Special Issue on
Recent Advances of Security, Privacy, and Trust in Mobile Crowdsourcing

With the rapid advances of mobile and communication technologies, mobile devices are equipped with powerful processors, various sensors, large memories, and fast wireless communication modules. By taking advantage of powerful mobile devices and human intelligence, mobile crowdsourcing is an emerging paradigm that enables users to outsource tasks (usually difficult to accomplish individually) to a group of people (workers) at an affordable price. Specifically, human mobility offers unprecedented opportunities to sense the surroundings wherever their holders arrive, and human capabilities also offer intelligent human-assisted computation with their devices, e.g., human perception, intelligence, cognition, knowledge, visual recognition, and experiences.

Due to human involvement and crowdsourcing, critical concerns are raised toward security, privacy and trust in mobile crowdsourcing, e.g., location leakage in sensed data, false data injection by malicious workers. However, it is challenging to protect security and privacy, especially in the IoT era, due to human mobility, device diversity, dynamic topology, and data heterogeneity. To address these challenges, this special issue solicits the latest research outcomes and developments on security, privacy, and trust in mobile crowdsourcing. Topics of interest include, but are not limited to:

- Authentication of mobile crowdsourcing devices
- Key management in mobile crowdsourcing
- Access control of task contents and results
- Trust-aware and privacy-preserving task matching and recommendation
- Privacy-preserving truth discovery in mobile crowdsensing
- Privacy-preserving data processing and analytics in the cloud, fog and IoT
- Secure and privacy-preserving federated learning and machine learning
- Trust management of crowdsourcing workers
- Trust-aware incentive mechanisms
- Blockchain-assisted crowdsourcing
- Security and privacy in fog/edge-assisted mobile crowdsourcing
- Secure and privacy-preserving mobile crowdsourcing in smart city applications

Important Dates:

Submission Deadline: June 15, 2023
First Review Due: August 31, 2023
Revision Due: October 15, 2023

Sec. Reviews Due/Notification: Nov 15, 2023
Final Manuscript Due: Nov 30, 2023
Publication Date: 2023

Submission:

The original manuscripts to be submitted need to follow the guidelines described at: http://ieeeiotj.org/guidelinesfor-authors/, which should not be concurrently submitted for publication in other venues. Authors should submit their manuscripts through the IEEE Manuscript Central at: https://mc.manuscriptcentral.com/iot. The authors must select as "SI: Recent Advances of Security, Privacy and Trust in Mobile Crowdsourcing" when they reach the "Article Type" step in the submission process.

Guest Editors:

- Kan Yang, University of Memphis, USA, email: kan.yang@memphis.edu
- Rongxing Lu, University of New Brunswick, Canada, email: RLU1@unb.ca
- Mohamed Mahmoud, Tennessee Technological University, USA, email: mmahmoud@tntech.edu
- Xiaohua Jia, City University of Hong Kong, China, email: csjia@cityu.edu.hk