Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on
Privacy Preserving IoT Environments

CALL FOR PAPERS

The Internet of Things (IoT) promises to enable a plethora of smart services in almost every aspect of our daily interactions to improve the quality of life. The resulting IoT ecosystems will enable billions of smart devices in our surroundings to interconnect and communicate information about themselves and their physical environments including data the people deem private. With the growing widespread adoption of IoT and increasing fine-grained data acquisition from private domains, significant challenges on user privacy and system security arise. Users develop growing concerns to lose control of how their data is collected and shared with others. Hence, data and user privacy become a primary impediment to the realization of the IoT vision. Classical privacy and security mechanisms fall short in IoT environments due to resource limitations and the unique IoT characteristics. Although the community has recently paid special attention to these topics, there are no solid solutions yet to address both user and data privacy in open IoT environments.

This special issue intends to gather cutting-edge results on privacy issues in IoT deployments. The objective is to promote research efforts and accelerate and recent advances of technologies on privacy preserving in IoT scenarios in including applications related to smart cities, healthcare, transportation, law enforcements, emergency response, and disaster relieves.

Potential topics include but are not limited to the following:

- Privacy-preserving techniques
- Data and anonymization and summarization techniques
- Authentication and access control in dynamic environments
- Critical infrastructures privacy and security issues
- Security techniques for privacy-preserving environments
- Security and privacy risk analysis in IoT scenarios
- Lightweight security solution of resource-contained environments
- Privacy-preserving machine learning
- Privacy-preserving data mining techniques
- Privacy-aware data collection approaches
- Digital forgetting mechanisms
- Trust establishment models in IoT applications
- Privacy-preserving system design principles

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/wcmc/ppie/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Khalid Elgazzar, University of Ontario, Oshawa, Canada
elgazzar@cs.queensu.ca

Guest Editors
Tamer Nadeem, Virginia Commonwealth University, Virginia, USA
tnadeem@vcu.edu

Ali Ebnenasir, Michigan Technological University, Michigan, USA
aebnenas@mtu.edu

Submission Deadline
Friday, 22 February 2019

Publication Date
July 2019