Security and Communication Networks

Special Issue on

Security and Privacy for Edge-Assisted Internet of Things

CALL FOR PAPERS

With the booming of embedded computing, various smart and embedded devices (e.g., smart cameras, smart electronic devices and smartwatches) have been integrated into our lives and form the Internet of Things (IoT). It is estimated that there are about 25 billion connected devices worldwide. IoT is revolutionizing the way we live, which enables us to collect information from the physical environment. Whilst operating, it can affect the physical environment. We have witnessed a dramatic increase in the application of IoT (e.g., smart homes, smart buildings, smart health and smart transportation). Cloud infrastructure has been deployed to process the fast-growing data volume in IoT.

However, cloud computing cannot support ultra-fast computing. It cannot provide the required real-time and reliable services, which are essential for mission-critical systems. Fortunately, edge computing can provide flexible and on-demand processing power, as well as provisioning of a variety of services using fifth-generation technology (5G). The large-scale nature of IoT can be effectively and efficiently supported and assisted by edge systems. This is referred to as edge-assisted IoT. Even if the coupling of edge computing and IoT bring a new level of convenience to our lives, they are much more vulnerable to many new and unknown attacks from traditional computing domains. For example, IoT often collects sensitive and private information about the physical environment. Therefore, edge-assisted IoT has become an ideal target for various security and privacy threats in the IoT ecosystems.

The aim of this Special Issue is to bring together researchers to exchange the state-of-art research results addressing the privacy and security protection issues in edge-assisted IoT. Both original research articles and review articles are solicited to explore the challenges in the field.

Potential topics include but are not limited to the following:

- New attacks on edge-assisted IoT
- Threat models and defensive mechanisms for edge-assisted IoT
- Authentication techniques for edge-assisted IoT
- Physical security for edge-assisted IoT
- Data privacy for edge-assisted IoT
- Data outsourcing for edge-assisted IoT
- Secure access to outsourced data
- Computation outsourcing for edge-assisted IoT
- Privacy-aware location-based services
- System and software security for edge-assisted IoT
- Cryptographic techniques for securing edge-assisted IoT

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=549047.

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

Lead Guest Editor
Ding Wang, Nankai University, Tianjin, China
wangding@nankai.edu.cn

Guest Editors
Qi Jiang, Xidian University, Xi'an, China
jiangqixdu@xidian.edu.cn

Shi-feng Sun, Monash University, Melbourne, Australia
shifeng.sun@monash.edu

Chunhua Su, University of Aizu, Aizuwakamatsu, Japan
chsu@u-aizu.ac.jp

Submission Deadline
Friday, 17 September 2021

Publication Date
February 2022