Security and Communication Networks

Special Issue on

Theory and Engineering Practice for Security and Privacy of Edge Computing

CALL FOR PAPERS

With the development of the Internet of Things, increasing numbers of powerful devices are mediating our daily life. This will result in massive data generated by billions of sensors and devices. Meanwhile, the increasing demand for advanced services and applications, such as virtual reality, augmented reality, and infrastructure for smart cities has created considerable challenges in cloud computing. Edge computing has been proposed as a new computing paradigm where resources like computation and storage are placed closer to the data source. It enables a new class of latency and bandwidth-sensitive applications as data can be processed at the nearest edge. Without sending data to the cloud, edge computing, therefore, enhances security and privacy.

However, edge computing also brings new possibilities and challenges for research in the field of security and privacy, especially from the perspective of engineering, management, and practice. Edge nodes are close to the users, and as a result can potentially receive large amounts privacy-sensitive data. If the data from an edge node is leaked, the consequences can be serious. Furthermore, compared with cloud centers, edge nodes have limited resources, so they cannot support complex security mechanisms. Finally, due to the high mobility of the devices and users, the edge computing environment is always changing. Attackers can quickly join the group, and it is challenging to design security rules with multi-domain overlapping, such as device provider, data generator/user, etc.

The aim of this Special Issue is to collate original research and review articles addressing these key issues in security and privacy of edge computing.

Potential topics include but are not limited to the following:

- New threat models and attacks in edge computing
- Defenses and countermeasures
- Anonymity and privacy in edge computing
- Scalability issues and solutions
- Task scheduling of edge computing
- System and software security of edge nodes
- Lightweight cryptography, protocols, and standards in edge computing
- Trust management of edge system
- Formal method of specification, verification and testing to edge system
- Security and privacy management of edge system
- Security issues due to services and application deployment
- Security issues due to the overall architecture and cooperation
- Novel privacy, liability, and legal issues raised by edge computing
- Malware detection in edge application and system
- Secure service and application design

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=729975.

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

Lead Guest Editor
Honghao Gao, Shanghai University, Shanghai, China
gaohonghao@shu.edu.cn

Guest Editors
Zhiyuan Tan, Edinburgh Napier University, Edinburgh, UK
z.tan@napier.ac.uk

Wenbing Zhao, Cleveland State University, Ohio, USA
wenbing@ieee.org

Yuyu Yin, Hangzhou Dianzi University, Hangzhou, China
yinyuyu@hdu.edu.cn

Submission Deadline
Friday, 22 January 2021

Publication Date
June 2021