Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Security and Privacy Challenges for Internet-of-Things and Fog Computing

CALL FOR PAPERS

Internet-of-Things (IoT) has profound impacts on our daily life by offering advanced connectivity of devices, systems, and services that go beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. Billions of IoT devices (embedded with electronics, software, sensors, actuators, and network connectivity) collect data through wireless technology and are able to interoperate within the existing Internet infrastructure. Traditional cloud computing framework stores and processes these massive amounts of data, which requires vast amounts of bandwidth, storage, and computation resources. Unfortunately, it leaves near-user fog devices (such as smart meters, smart traffic lights) as dumb portals and negatively impacts the performance of the cloud-centric system. The new fog/edge computing paradigm allows data storing and processing being implemented at the network edge or anywhere along the cloud-to-endpoint continuum, rather than completely in a relatively small number of clouds, which can meet users' requirements to a maximum. It also overcomes IoT devices' limited processing and storage capabilities and battery life and network bandwidth constraints and allows us to design a far more capable architecture. However, this new IoT-Fog paradigm brings many security and privacy issues such as information confidentiality, authentication and authorization, and secure communication. With nearly unlimited computation and storage resources, the traditional cloud-based platform can even use heavyweight lattice-based cryptosystem to enhance the system security, which cannot be performed by the resource constrained edge devices. Moreover, different from the tradition IoT-cloud architectures, millions of smart fog devices are wildly distributed and located in different areas, which can be easily compromised by some malicious parties. These compromised fog devices may temper the data collected by smart health IoT devices, and these fake data may mislead the data user or even threat people's lives. To address these arising challenges and opportunities different from traditional cloud based architecture, this special issue is interested in inviting and gathering recent advanced security and privacy techniques relevant to the convergence of Internet-of-Things with fog computing.

Potential topics include but are not limited to the following:

- Authentication in crowdsourcing of IoT and fog computing
- Lightweight data protection scheme for smart IoT devices
- Secure machine learning technique on edge devices for IoT data analysis
- Hardware security and privacy issues for IoT and edge devices
- Secure data integrity and validation techniques for smart IoT devices
- Privacy computation and processing protocols on edge-cloud platform
- Secure M2M communication for smart IoT and edge devices
- Formal security model for cryptographic protocols for fog computing
- Future and smart fog-based vulnerability assessment interfaces
- Design and tune intrusion detection systems for distributed IoT and fog devices
- Secure programming models and toolkits for fog computing in IoT
- Virtualization security and management for mobile and fog computing
- Experiment prototype for secure and trusted IoT-Fog framework
- Blockchains and smart contracts for IoT and fog computing
- New privacy challenges in IoT and fog-cloud computing

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

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

Lead Guest Editor
Ximeng Liu, Singapore Management University, Singapore
snbnix@gmail.com

Guest Editors
Yang Yang, Fuzhou University, Fuzhou, China
yang.yang.research@gmail.com

Raymond Kim-Kwang Choo, The University of Texas at San Antonio, San Antonio, USA
raymond.choo@fulbrightmail.org

Huaqun Wang, Nanjing University of Posts and Telecommunications, Nanjing, China
wanghuaqun@aliyun.com

Submission Deadline
Friday, 9 March 2018

Publication Date
July 2018