Security and Communication Networks

Special Issue on

# Security and Privacy at the Edge: Threats and Challenges

WILEY | Hindawi

CALL FOR PAPERS

Recent approaches to Internet-of-Thing (IoT) applications are adopting new computing paradigms which distribute the decision-making tasks among edge devices such as smartphones, smart gateways or routers, and local PCs within the network instead of sending all the data to a centralized server. These have been coined edge/fog computing and tend to overcome inefficiencies of cloud computing when executing communication-intensive services and applications, which require higher reliability, real-time processing, mobility support, and context awareness like in healthcare, indoor navigation, or smart home/work/industrial/vehicular spaces.

In such decentralised scenarios, a certain degree of data treatment and processing power is therefore shifted from the cloud to the edge of the network to devices such as manufacturing robots, self-adjusting thermostats, and self-driving cars. This paradigm shift to the edge promises many benefits, including distributed processing, low latency, fault tolerance, better scalability, better security, and privacy. Looking at the latter, one could think that, since data is locally processed and filtrered a priori at the user device, movement of (encrypted or not) data from edge to server becomes simplified, protected from eavesdroppers. It can, however, intensify many security issues regarding data, virtualization, segregation, network, malware, and monitoring, to name a few.

Moreover, when creating compelling end-to-end IoT solutions, the public internet and public cloud architectures incur, unfortunately, performance and security vulnerabilities and the inclusion of intelligence at the edge might make them (what are also termed as Edge-of-Things–EoT–applications) suffer from many other threats. This special issue is aimed at fostering the latest developments in the design, implementation, and evaluation of architectures, protocols, services, and mechanisms in the field of secure and private IoT applications with edge compute capabilities. The major subjects cover methodologies, modeling, analysis, and newly introduced applications, all envisioned following a security/privacy-by-design approach. Besides the latest research achievements, this special issue also covers innovative services, systems, and applications of edge computing technology with comercial impact. The papers will be peer reviewed and selected on the basis of both their quality and their relevance to the theme of this special issue.

Potential topics include but are not limited to the following:

- Security and privacy models, architectures, frameworks, standards, and platforms in the EoT paradigm
- Design of secure EoT-based applications
- Secure and private data analytics and learning in EoT scenarios
- Cyberphysical security of edge devices
- Authentication, auditing, and accountability in EoT developments
- Access control mechanisms for EoT scenarios
- Sensor network security in EoT deployments
- Secure communications and networking protocols for EoT scenarios
- Embedded intelligence in EoT scenarios
- Trust management and reputation in EoT scenarios
- Simulation, emulation, and testbed support for secure EoT applications
- Secure mobile app development for emergent EoT scenarios such as indoor navigation, vehicular systems, healthcare systems, body sensors, and BYOD

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

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

**Lead Guest Editor**
Esther Palomar, Birmingham City University, Birmingham, UK
*esther.palomar@bcu.ac.uk*

**Guest Editors**
Ignacio Bravo, University of Alcala, Madrid, Spain
*ignacio.bravo@uah.es*

Karin Messer-Misak, FH JOANNEUM Gesellschaft mbH, Graz, Austria
*karin.messer-misak@fh-joanneum.at*

Zhiming Liu, Southwest University, Chongqing, China
*zhimingliu88@swu.edu.cn*

**Submission Deadline**
Friday, 26 October 2018

**Publication Date**
March 2019