Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Secure Computation on 4G/5G Enabled Internet-of-Things

CALL FOR PAPERS

The rapid development of Internet-of-Things (IoT) techniques in 4G/5G deployments is witnessing the generation of massive amounts of data which are collected, stored, processed, and presented in an easily interpretable form. Analysis of IoT data helps provide smart services such as smart homes, smart energy, smart health, and smart environments through 4G and 5G technologies. At the same time, the threat of the cyberattacks and issues with mobile internet security is becoming increasingly severe, which introduces new challenges for the security of IoT systems and applications and the privacy of individuals thereby. Protecting IoT data privacy while enabling data availability is an urgent but difficult task.

Data privacy in a distributed environment like IoT can be attained through secure multiparty computation. An emerging area of potential applications for secure computation is to address privacy concerns in data aggregation and analysis to match the explosive growth of the amount of IoT data. However, the inherent complexity of IoT systems really complicates the design and deployment of efficient, interoperable, and scalable secure computation mechanisms. As a result, there is an increasing demand for the development of new secure computation methods and tools which can fill in the gap between security and practical usage in IoT.

This featured topic will benefit the research community by identifying challenges and disseminating the latest methodologies and solutions to secure computation on 4G and 5G enabled IoT data. Its objective is to publish high-quality articles presenting open issues, algorithms, protocols, policies, frameworks, standards, and solutions for secure computation techniques related to IoT. All received submissions will be sent out for peer review by at least two experts in the field and evaluated with respect to relevance to the special issue, level of innovation, depth of contributions, and quality of presentation. Reviews and case studies, which address state-of-art research and state-of-practice industry experiences, are also welcomed. Guest Editors will make an initial determination of the suitability and scope of all submissions. Papers that either lack originality and clarity in presentation or fall outside the scope of the special issue will not be sent for review and the authors will be promptly informed in such cases. Submitted papers must not be under consideration by any other journal or publication.

Potential topics include but are not limited to the following:

- Secure multiparty computation in cellular IoT
- Security and privacy for cellular IoT networks
- Secure computation outsourcing in cellular IoT
- Large-scale secure computation for IoT-sensor networks
- Security for mobile-IoT services and applications in 4G/5G environemnts
- Efficient secret sharing techinques for smart cellular IoT networks
- Mobile user authentication and authorization
- Privacy-preserving data mining in cellular IoT
- Searchable encryption in cellular IoT databases
- Digital forensics for vulnerability identification of cellular IoT devices
- Privacy and trust for smart Mobile IoT
- Privacy-preserving machine learning in IoT
- Cellular IoT protocols security
- Cybercrime detections in IoT devices

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

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

Lead Guest Editor
Karl Andersson, Luleå University of Technology, Luleå, Sweden
karl.andersson@ltu.se

Guest Editors
Ilsun You, Soonchunhyang University, Asan, Republic of Korea
ilsunu@gmail.com

Rahim Rahmani, Stockholm University, Stockholm, Sweden
rahim@dsv.su.se

Vishal Sharma, Soonchunhyang University, Asan, Republic of Korea
vishal_sharma2012@hotmail.com

Submission Deadline
Friday, 18 January 2019

Publication Date
June 2019