JOURNAL OF NETWORK AND SYSTEMS MANAGEMENT (SPRINGER)

SPECIAL ISSUE

Intelligent and Trustworthy Internet Edge

*** **Submissions due: December 31, 2019** ***

https://www.springer.com/?SGWID=0-102-2-1338221-0

[We encourage early submission, please check the open submission schedule policy below.]

The emerging and the ever-growing functionality of Internet edges, where physical and virtual things are connected to the network, are opening a wide set of new opportunities, both for novel services/applications and increased efficiency/scalability. These opportunities include locally sharing information, collaborating, and generating/consuming a huge amount of data, by involving a variety of entities, such as micro-data centers, end devices, and resource-sufficient networking nodes. While Fog/Edge Computing is usually expected to bring the resources, including storage and computation closer to users (in comparison to Cloud Computing), a significant effort is needed at the Internet edge to provide a trustworthy computation edge networking environment able to support new computation technologies. Indeed, distributed big data analytics, modern Machine Learning (ML) technology, Artificial Intelligence (AI), real-time data collection and processing, scalable and distributed security solutions such as blockchain, and distributed secure data processing, may play a significant role. Moreover, new networking technologies related to Information-Centric Networking (ICN), Software-Defined Networking (SDN), Network Function Virtualization (NFV), and network slicing have emerged as the novel paradigms for fast and efficient delivering and retrieving data. This triggers the convergence between the emerging networking concepts and the new computation technologies to reach the vision of an intelligent and trustworthy Internet edge.

In order to implement such trustworthy edge networks and services, several **operation and management challenges associated with intelligent and trustworthy Internet edge** need to be addressed. These challenges include: trustworthy connectivity and network resource management for heterogeneous networking (HetNet); security monitoring, measurement, and assessment to ensure networking and management functions to protect data; effective ML and computation models to consider different resources (storage, networking, and computing), security requirements, and real-time constraints; trustworthiness of data sources; in-network data processing and aggregation, intelligent planning and decision models to handle security and application requirements.

This special issue aims to bring together leading research on management infrastructure, applications and the most recent advances in Internet edge-based secure network management solutions. We hence encourage original paper submissions, which have not been published or submitted for publication elsewhere, from both academia and industry presenting novel research addressing the aforementioned challenges.

Topics of interest include, but are not limited to:

- Secure intelligent edge systems and networking architectures/protocols to integrate storage, computation, and networking;
- Secure intelligent coordination and networking between edge, fog, and cloud;
- Software architectures and toolkits for secure intelligent Internet edge;
- Trust management and networking among intelligent edges;
- Intelligent and secure service function/computation chaining;
- Secure NFV, SDN, and network slicing for distributed computations;
- Secure ICN with/for edge-enabled Internet;
- Secure in-network computation for future networks, inter-data center networking and 5G;
- Privacy management for intelligent Internet edge;
- Accountability, reliability, and resiliency for intelligent Internet edge;
- Quality of Service/Experience and energy efficiency for secure intelligent Internet edges;
- Distributed AI with/for secure edge networking;
- Distributed ML with enhanced data privacy, ownership, and obfuscation;
- Integrating Blockchain with distributed edges and Internet finance;
- Data mining and big data analytics for security management in edge networking;
- Trustworthy data collection and processing for big data at the edge;
- Privacy-preserving big data processing at the edge;
- Emerging applications for intelligent secure Internet edge, such as AR/VR, IoT, industrial IoT for Industry 4.0, 5G, cyber-physical systems, smart cities, vehicular systems, healthcare;
- Management framework for intelligent secure Internet edge;
- Security performance monitoring, measurements, modelling, and evaluations for intelligent Internet edge;
- SDN/NFV security architectures and applications for Internet edge;
- Security mechanisms in wireless SDN/NFV.

Planned Schedule

Open-submission schedule: in this special issue, we implement an "open" submission approach, where we do not have a submission time period. Interested authors can submit the paper any time before a fixed deadline, and the review process will be started right after the paper submission, i.e., in a first-in first-serve fashion. The detailed submission schedule is presented as follows:

- Manuscript due: December 31, 2019
- Revision notification: 2-month after the submission
- Revised paper due: 1.5-month after the revision notification
- Final notification: 1-month after the revised paper notification
- Expected Publication of the Special Issue: third-quarter of 2020 (early accepted papers will be accessible online before the deadline)

Submission Format and Review Guidelines

The submitted manuscripts must be written in English and describe original research not published nor currently under review by other journals or conferences. Parallel submissions will not be accepted. All submitted papers, if relevant to the theme and objectives of the special issue, will go through an external peer-review process. Submissions should (*i*) conform strictly to the *Instructions for Authors* available on the JNSM website and (*ii*) be submitted through the *Editorial Management* system available at http://www.editorialmanager.com/jons.

Guest Editors of the Special Issue:

- Dr. Dijiang Huang, Arizona State University, USA
  Email: dijiang.huang@asu.edu
- Dr. Jéferson Campos Nobre, Federal University of Rio Grande do Sul (UFRGS), Brazil
  Email: jcnobre@inf.ufrgs.br
- Dr. Ruidong Li, NICT, Japan
  Email: lrd@nict.go.jp
- Dr. Paolo Bellavista, DEIS, Università di Bologna, Italy
  Email: paolo.bellavista@unibo.it
- Dr. Abdelkader Lahmadi, University of Lorraine, France
  Email: abdelkader.lahmadi@loria.fr