HPCC'2020

Special Session: Security, Trust and Privacy for AI-based High-Performance Applications in Mobile Edge Computing

In recent years, many artificial intelligence (AI) applications have been developed successfully, which often demand low latency and quick responses, e.g., smart health, driverless cars, smart home, etc. Fortunately, as a supplement of traditional cloud computing technology, mobile edge computing (MEC) has been considered as a promising computing paradigm that offers end-users with low latency in their access to high-performance applications deployed at the edge of the cloud. Therefore, the integration of AI and MEC brings more opportunities in people's daily lives.

Unlike the centralized cloud computing paradigm, the various computing resources in MEC environment are often provided and managed in a decentralized or distributed manner. Accordingly, the AI applications for MEC are also deployed in a decentralized manner. However, there is a lack of security, trust and privacy solutions specifically designed for the devices and servers operating in the MEC environment. This further challenges the security, trust and privacy issues in AI-based high-performance applications, e.g., data privacy disclosure, adversarial attacks, confidentiality attacks, etc.

This Special Session aims to share and discuss the recent advances and future trends of Security Trust, Privacy for AI-based High-Performance Applications in Mobile Edge Computing, and to bring academic researchers and industry developers together.

This is a special session of the 22nd IEEE International Conference on High Performance Computing and Communications (http://cse.stfx.ca/~hpcc/2020/index.html). Please submit your paper via the submission site (http://edas.info/N27662) and select the special session of "Special Session 1: Security, Trust and Privacy for AI-based High-Performance Applications in Mobile Edge Computing".

Potential topics include but are not limited to the following:

- Advanced AI algorithms for MEC security
- AI-based privacy preservation in MEC
- Intelligent data preprocess, communications and integration in MEC
- Attacks and Countermeasures for high-performance applications in MEC
- AI-based energy efficient networking techniques for MEC
- Smart sensor networks and IoT devices
- AI-based network resource allocation in MEC
- AI-enabled hardware aspects in high-performance MEC applications
- Distributed signal processing via AI algorithms
- Trust, reliability and dependability in MEC
- Encryption, Signature and Forensics for MEC applications

Submission Deadline: 1 September 2020

Organizers:

- **Lianyong Qi, Qufu Normal University, China**
  (email: lianyongqi@qfnu.edu.cn)

- **Mohammad R. Khosravi, Persian Gulf University, Iran**
  (email: m.khosravi@mehr.pgu.ac.ir)
- **Varun Menon, SCMS School of Engineering & Technology, India**
  (email: varunmenon@scmsgroup.org)
- **Dr. Dharavath Ramesh, Indian Institute of Technology (ISM), India.**
  (email: ramesh.d.in@ieee.org)

Contact: lianyongqi@qfnu.edu.cn.