IEEE Internet of Things

Special Issue on
Robustness and Efficiency in the Convergence of Artificial Intelligence and IoT

Today, the Internet of Things (IoT) is increasingly flourishing with establishing ubiquitous connections between smart devices and objects, and by 2020 there will be a total of 30 billion connected things reported by IDC. The unprecedented data explosion provides immense opportunities for valuable information mining while it also floods the infrastructure with tremendous values it necessarily handles and proposes high challenges to traditional data storing or processing techniques. On the other hand, Artificial Intelligence (AI) has become a key component for many applications that deeply change our lives. Machine learning, especially Deep Learning (DL) technologies, are largely improving the traditional computer science and networking technologies. The convergence of AI and IoT enables data to be quickly explored and turned into significant decisions. In particular for companies and enterprises, AI enhances the speed and accuracy of data processing in order for instant market strategies.

However, DL techniques are also facing the serious issue that the meticulously trained DL models are very sensitive to the tiny perturbations in the input data called Adversarial Examples (AEs). This issue brings many attacks to mislead the DL models by generating AEs maliciously or the “messy” objects in the physical world will challenge the robustness of DL models. On the other hand, deploying AI methods on IoT systems must consider the efficiency issues. Therefore, in this special issue, we aim to focus the research on the robustness and efficiency of the AI techniques in current IoT Systems. Firstly, the special issue will include the novel research on robust issues such as AE-based attacks and defense on the IoT systems. Then, we also would like to pay close attention to efficiency issues of the convergence AI solutions with the IoT systems.

Topics include, but are not limited to the following:

- Privacy and Security Issues in the Convergence of AI and IoT
- Novel Theories, Concepts, and Paradigms of the Convergence of AI and IoT
- ML/DL Enabled Attacks and Defense in Hardware Level IoT Systems
- ML/DL Enabled Attack and Defense in Cloud Computing Systems
- Performance Assessment Metrics and Evaluation Criteria for AI-enabled IoT Systems
- New Approaches for Generating Adversarial Examples with IoT Systems
- Software Level Acceleration for DL models in IoT Systems
- Hardware Level Acceleration for DL models in IoT Systems
- Adversarial Examples Attacks and Defense in IoT Systems

Important Dates:

Submission Deadline: May 15, 2020
First Review Due: August 1, 2020
Revision Due: September 15, 2020
Sec. Reviews Due/Notification: October 15, 2020
Final Manuscript Due: November 1, 2020
Publication Date: 2020

Submission Guidelines:

Authors need to follow the manuscript format and an allowable number of pages described at http://ieeeiotj.org/guidelines-for-authors/. To submit a manuscript for consideration for the special issue, please visit the journal submission website at https://mc.manuscriptcentral.com/iot.

Guest Editors:

Prof. Meikang Qiu, Columbia University, USA, qiumeikang@yahoo.com (lead guest editor)
Prof. Bhavani Thuraisingham, University of Texas at Dallas, USA, bhavani.thuraisingham@utdallas.edu
Prof. Mahmoud Daneshmand, Stevens Institute of Technology, USA, mdaneshm@stevens.edu
Prof. Huansheng Ning, University of Science and Technology Beijing, China, ninghuansheng@ustb.edu.cn
Prof. Payam Barnaghi, University of Surrey, UK, p.barnaghi@surrey.ac.uk