IEEE INTERNET OF THINGS JOURNAL

CALL FOR PAPERS

IEEE Internet of Things Journal Special Issue on

Security, Privacy, and Trustworthiness in Intelligent Cyber-Physical Systems and Internet-of-Things

Recent advances in computation, communication, and control technologies have revolutionized the way that humans, smart things, and intelligent systems interact and exchange information. Intelligent Cyber-Physical Systems (ICPSs), characterized by the deep complex intertwining process among cyber components for computation and control with intelligent technologies (such as machine learning and deep learning) and the dynamic physical components that involve mechanical components, human activities and surrounding environment, will fuel this revolution. Examples of ICPS include intelligent automotive and transportation systems, intelligent avionics systems, smart home, building and community, smart grid, smart healthcare systems, intelligent wearable systems, intelligent energy systems, robotic systems, etc. Bringing machine/deep learning based intelligence techniques into CPSs can improve the performance in many aspects. However, this also imposes new security, privacy, and trust challenges, which highlights the need to develop novel methodologies to tackle these challenges.

This special issue will promote the state-of-the-art research covering all aspects of the security, privacy, and trust in intelligent CPSs. High quality contributions addressing related theoretical and practical aspects are expected. The topics of interest for this special issue include, but are not limited to

- Modelling, analysis, simulation, and verification of security, privacy, and trustworthiness for intelligent CPS and IoT
- Hardware and software co-design for intelligent CPS and IoT
- Detection, evaluation, and prevention of threats and attacks in intelligent CPS and IoT
- Data security, privacy, and trustworthiness in intelligent CPS and IoT
- Machine learning or deep learning based security solutions for intelligent CPS and IoT
- Secure and privacy-preserving CPS and IoT architectures
- Secure and trustworthy Cloud, fog, and edge computing for intelligent CPS and IoT
- Human-in-the-loop control and security for intelligent CPS and IoT
- Trustworthy smart systems and smart production systems
- Secure and intelligent design of smart grid CPS, mobile CPS, social CPS, medical CPS, and automotive CPS

Important dates:

Submission deadline: January 15, 2021	Second Reviews Due/Notification: June 15, 2021
First Review Due: March 31, 2021	Final Manuscript Due: June 30, 2021
Revision Due: May 15, 2021	Publication Date: 2021

Submission

All original manuscripts or revisions to the IEEE IoT Journal need to be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Author guidelines and submission information can be found at http://iot.ieee.org/journal. Each submitted manuscript will be sent to reviewers who will evaluate your work. The inquiries related to this special issue should be sent to S.Hu@soton.ac.uk.

Guest Editors

Shiyan Hu, University of Southampton, U.K., email: S.Hu@soton.ac.uk
Shui Yu, University of Technology Sydney, Australia, email: Shui.Yu@uts.edu.au
Helen Li, Duke University, USA, email: hai.li@duke.edu
Vincenzo Piuri, University of Milan, Italy, email: vincenzo.piuri@unimi.it