Call for Paper for the Special Session (IJCNN-SS-36)

Artificial Intelligence for Cyber Security of IoT Systems (AICSIoT)

Aim and Scope

Cybersecurity and Artificial Intelligence (AI) are currently two hot topics in the field of computer science and important drivers for the future development of many aspects of the upcoming digital society. The Internet of Things (IoT) creates new value by connecting people, processes and data. However, IoT systems create a large cyberspace and could be threatened by various cyberattacks, crimes, and terrorism. Security automation is a future trend to ensure the safety of the cyber world. AI is the key to implement security automation. Therefore, the special session provides a cross-fertilisation venue where researchers working in relevant fields are invited to present their innovative research on cybersecurity of IoT systems, covering the cybersecurity of all network stack layers, from physical, data link, network, transport, to application layers, with AI technology (e.g., deep learning) for cyber-attack detection or in-depth investigation of AI algorithm security, promote the AI applications in cyber security, and enhance collaboration between theoretical researchers and industrial practitioners.

List of Topics

The goal of AICSIoT is to invite all researchers working on the application of artificial intelligence to cybersecurity of IoT systems to share innovative research results on the above topics. We welcome contributions that address cybersecurity of all network layers, from the physical layer, data link, network, transport, to application layers for IoT systems, using AI technologies, especially state-of-the-art machine learning techniques (e.g., Deep Learning). We also welcome contributions on security automation, in particular adaptive and autonomous security architectures. We expect a variety of contributions on different topics and beyond. We look forward to meeting colleagues from relevant fields. The special session is primarily, but not exclusively, for researchers from the following areas:

1) Machine learning for cyber-attack, intrusion and spam detections
2) Computer and Network Security
3) Wireless and mobile security for data protection and authentication.
4) Cybersecurity of industrial control systems.
5) Cybersecurity of autonomous systems, embedded systems and edge devices
6) Secure human-machine interactions
7) Socio-technical modelling & simulation for cybersecurity
8) Co-design of safety and security of IoT systems
9) Resilient and secure AI algorithms
10) Resilient architectures of cyber-physical systems.

Important Dates

- Paper Submission: *31 January, 2022*
- Notification of Acceptance: *26 April, 2022*
- Final Paper Submission: *23 May, 2022*
- IEEE WCCI 2022, Padua, Italy. *18-23 July 2012*

Submissions

Please submit your manuscript through the conference main website by following the instructions provided in **THIS LINK**

Organisers (* primary contact)

*Mary H. He, Eerke Boiten, Richard Smith
De Montfort University, UK
Emails: mary.he@dmu.ac.uk, eerke.boiten@dmu.ac.uk, rgs@dmu.ac.uk

Watson, Jeremy Daniel McKendrick, Ani, Uchenna
University College London (UCL), UK
Emails: jeremy.watson@ucl.ac.uk, u.ani@ucl.ac.uk

Riccardo Pecori
University of Sannio, Benevento, Italy
Email riccardo.pecori@gmail.com

Marta Cimitile
University of Rome Unitelma Sapienza, Italy
Email: marta.cimitile@unitelmasapienza.it

Gillian Dobbie
The University of Auckland, New Zealand
Email: g.dobbie@auckland.ac.nz