Instructions for Special Issue on Secure Smart World (S2World2020)

This special issue on Secure Smart World (S2World2020) is open by invitation to extended versions of high-quality papers presented at TrustCom 2020 held December 29, 2020 - January 1, 2021 in Guangzhou, China, SpaCCS 2020 held December 18-20, 2020 in Nanjing, China, and ICCCN 2020 held August 3- 6, 2020 in Honolulu, Hawaii, USA. This is also an open special issue where everyone is encouraged to submit papers.

The guest editors of the special issue are:

- Prof. Guojun Wang, Guangzhou University, China
- Prof. Qin Liu, Hunan University, China
- Prof. Prof. Richard Hill, University of Huddersfield, UK
- Prof. Jiankun Hu, The University of New South Wales, Australia

Scope

This smart world is set to be the next important stage in human history, where numerous smart things communicate and collaborate so that many tasks and processes could be simplified, more efficient, and enjoyable. As the cornerstone technologies enabling a smart world, Internet of things (IoT) and artificial intelligence (AI) have been interacting with each other to stitch everything smart towards smart life. However, a myriad of sensitive data is generated, processed, and exchanged through the IoT devices and AI technologies, one of the fundamental problems is how to organically integrate IoT and AI to provide intelligent services in smart world without compromising security and privacy. This special issue aims to bring together researchers and practitioners in IoT, AI, and network security to share their novel ideas and latest findings to show how IoT and AI can work together to enable a secure smart world.

This special issue will tackle the enabling technologies of a smart world. Original research articles are solicited, which include (but not limited to), the following topics:

- Novel IoT devices and infrastructure platforms in secure smart worlds
- Trust evaluation and management in smart worlds
- Secure smart city applications, including secure IoT/AI applications
- Authentication and access control in secure smart worlds
- Secure policies, models, and architectures for IoT and AI
- Novel cryptographic mechanisms for IoT and AI
- Threat intelligence for IoT and AI
- Intrusion detection theories and techniques for IoT and AI
- Secure experiments, testbeds, and prototyping systems for IoT and AI
- Software security for IoT and AI
- Secure communication technologies and their optimisation for IoT
- Secure multi-party computation techniques for ML
- Privacy-preserving ML
- Adaptive side-channel attacks
- Security and privacy in data mining and analytics
- Event alert and prediction in smart world
- Privacy and anonymity techniques for IoT and AI
- Security protocols for IoT and AI
- Privacy-preserving crowdsensing

- Biometrics security

Submissions must follow these guidelines:

- Please submit your paper to Manuscript Central as S2World2020 special issue.
- Submissions should be prepared for publication according to the Journal Submission Guidelines.
- Latex must be used with Wiley Template.
- The submitted papers must have at least 50% different material beyond any other previously published work.
- Manuscripts should not exceed 35 pages in length (inclusive of figures and tables)
- There is a limit of 15 papers plus an editorial in the special issue

Important dates:

- Submissions Deadline: September 1st, 2021
- First-round pass notification: October 17th, 2021
- Review result notification: January 1st, 2022
- Acceptance/rejection: April 3rd, 2022
- Estimated Publication: Q2 2022