

Security, Privacy and Forensics in the Critical Infrastructure: Advances and Future Directions

Cyber security and privacy is an essential need for modern society where information technology and services pervade every aspect of our lives. Specially, security, privacy and forensics of critical infrastructure (a nation's strategic national assets, i.e. banking and finance, communications, emergency services, energy, food chain, health, water, mass gatherings, transport, etc) which is an essential part of our daily life to access different systems, services and applications is a serious issue, today. However, it is challenging to achieve, as technology is changing at rapid speed and our systems turn into ever more complex. Moreover, cyber space is considered as fifth battle-field after land, air, water and space. The explosion of big data has created unprecedented opportunities and fundamental security challenges as they are not just big in volume, but also unstructured and multi-modal.

The aim of this special issue is to provide a premier international platform for wide range of professions including scholars, researchers, academicians and Industry people to discuss and present the most recent security and privacy challenges and developments in "big data in critical infrastructure" from the perspective of providing security awareness and its best practices for the real world.

In addition, extended version of the best papers selected from the 2nd *International Workshop on Future Information Security, Privacy and Forensics for Complex Systems (FISP-2016)* in conjunction with 11th *International Conference on Future Networks and Communications (FNC-2016)* during August 15-18, 2016 in Montreal, Quebec, Canada and from the 1st *EAI International Conference on Security and Privacy in New Computing Environments (SPNCE-2016)* during December 15-16, 2016 in Guangzhou, China will also be invited to submit in the present special issue. This special issue is open to submit novel and high quality research contributions in the field of Big Data security and privacy. We anticipate that this special issue will open new entrance for further research and technology improvements in this important area.

The scope of the issue encompasses, but is not restricted to, the following areas:

- Security and privacy of big data in banking systems
- Security and privacy of big data in telecommunication systems
- Security and privacy of big data in finance systems
- Security and privacy of big data in communication systems
- Security and privacy of big data in eCommerce
- Security and privacy of big data in emergency services, energy, food chain
- Security, privacy and forensics of big data in critical infrastructure
- Security and privacy of big data in mobile cloud computing
- Security and privacy management of big data in Cloud Computing
- Security and privacy of Industrial control systems
- Security, privacy and forensics of big data in stock trade
- Mobile cloud computing intrusion detection systems
- Cryptography, authentication, authorisation and usage control for big data in cloud
- Security and privacy of multimedia big data in smartphone devices
- Security of Mobile, peer-to-peer and pervasive services in clouds
- Security of big data in Mobile commerce and mobile internet of things
- Security and privacy of multimedia big data in sensor networks
- Big data-enabling social networks on Clouds
- Resource management for multimedia big data on Clouds
- Cryptography, authentication, authorisation and usage control for big data in mobile devices
- Multi-modal information retrieval for big data on Clouds
- Security and privacy of big data in social applications and networks
- Security and privacy of big Data in Web service

Guest Editors

- ▶ **B. B. Gupta**, National Institute of Technology Kurukshetra, *India*
- ▶ **Dharma P. Agrawal**, University of Cincinnati, *USA*
- ▶ **Shingo Yamaguchi**, Yamaguchi University, *Japan*
- ▶ **Nalin A. G. Arachchilage**, University of New South Wales, *Australia*
- ▶ **Suresh Veluru**, United Technologies Research Centre, *Ireland*

Paper Submission

Papers must be written in English and describe original research not published or currently under review by other journals or conferences. The length of the article file should not exceed 35,000 characters including spaces (i.e., around 5,500 words). The manuscripts that are outside the expected length are likely to be rejected. All relevant papers submitted will go through an external review process. Submissions should be sent according to the instructions available at:

<http://annalsoftelecommunications.wp.mines-telecom.fr/how-to-publish/>

Proposed schedule

- | | |
|---|---------------------|
| • Manuscript submission deadline | January 15, 2017 |
| • Peer Review due | March 30, 2017 |
| • Revision due | June 15, 2017 |
| • Final manuscripts due | July 15, 2017 |
| • Online with DOI | As soon as accepted |
| • Printed issue | Early 2018 |