

BigSecurity 2014

with IEEE INFOCOM 2014

April 27 - May 2, 2014
Toronto, Canada

Call for Papers

The Second International Workshop on Security and Privacy in Big Data

(BigSecurity 2014, in conjunction with IEEE INFOCOM 2014)

<http://www.nsp.org.au/confs/bigsecurity2014/>

Scope and Topics of Interest

As we are deep into the Information Age, we also witness the explosive growth of data available on the Internet. For example, human beings create about 2.5 quintillion bytes of data every day in 2012, which come from sensors, individual archives, social networks, Internet of Things, enterprise and Internet in all scales and formats. We face one of the most challenging issues, i.e., how to effectively manage such a large amount of data and identify new ways to analyze large amounts of data and unlock information. The issue is also known as Big Data, which has been emerging as a hot topic in Information and Communication Technologies (ICT) research.

Security and privacy issue is critical for Big Data. Many works have been carried out focusing on business, application and information processing level from big data, such as data mining and analysis. However, security and privacy issues in Big Data are seldom mentioned to date. Due to its extraordinary scale, security and privacy in Big Data faces many challenges, such as efficient encryption and decryption algorithms, encrypted information retrieval, attribute based encryption, attacks on availability, reliability and integrity of Big Data.

The purpose of this workshop is to offer a timely venue for researchers and industry partners to present and discuss their latest results in security and privacy related work of Big Data.

The topics of interest include, **but are not limited to:**

- Threat and Vulnerability Analysis in Big Data
- Architecture for Security and Privacy in Big Data
- Encrypted Information Retrieval in Big Data
- Cryptanalysis and Applications in Big Data
- Lightweight Cryptographic Algorithms in Big Data
- Trust in Big Data
- Network Security, Privacy in Big Data
- Network Forensics in Big Data
- Anonymous Communication in Big Data

- Physical Layer Security in Big Data
- Privacy and Security in Cloud Data
- Privacy and Security in Data Center Networks
- Application Level Security and Privacy in Big Data
- Attacks and Counter Measures in Big Data
- Information Forensics in Big Data
- Secure Cross-layer Design in Big Data
- Identity Management and Key Management in Big Data
- Intrusion Detection and Response in Big Data
- Security and Privacy in Complex Networks
- Malware and Virus Detection in Big Data
- Biometric Security and Forensics in Big Data
- Reliability and Availability in Big Data
- Network Security in Big Data
- Network Privacy in Big Data
- Security and Privacy Theories in Big Data
- Security, Privacy, and Trust in Cloud
- Security, Privacy, and Trust in Large Scale Systems

General Co-chairs

Professor Ivan Stojmenovic, University of Ottawa, Canada

Professor Hsiao-Hwa Chen, National Cheng Kung University, Taiwan

Technical Program Co-chairs

Dr Shui Yu, Deakin University, Australia

Professor Xiaodong Lin, University of Ontario Institute of Technology, Canada

Submission Instruction

For instructions on the manuscript layout, please visit http://www.ieee-infocom.org/Author_C4P_MP.html. Submission through <http://edas.info/N16167>.

Important Dates

Submission Deadline: December 31, 2013 (extended)

Authors Notification: February 07, 2014

Final Manuscript Due: February 28, 2014

Enquiries should be submitted to Dr Shui Yu (syu AT deakin.edu.au) or Dr Xiaodong Lin (xiaodong.lin AT uoit.ca)