

CALL FOR PAPERS
IEEE Internet of Things Journal Special Issue on
Big Security Challenges in Big Data Era

The “Internet of Things” (IoT) and “Big Data” are two of the most-talked-about technology topics in recent years. The IoT and Big Data are clearly intimately connected: billions of internet-connected “things” will, by definition, generate massive amounts of data. Big Data, as it is regarded as a key basis of future competition and innovation, has attracted considerable attention from both the industry and academia in recent years. Nevertheless, business and IT executives are also gradually learning through harsh experience that Big Data inevitably brings big security headaches. One example is the crowdsourcing, in which it is essential to aggregate data from a crowd of users to get true facts or consensus opinions. In the scenario, the attacks could be launched by internal and external adversaries. As a result, the crowdsourced data could be suffered from the ubiquitous message injection/modification attacks. Furthermore, along with data getting “Big Data”, it is significantly challenging to identify true and valuable data from the large-scale and heterogeneous ones. It is undeniable that the security issues in the crowdsourcing are magnified by “Big Data”. Traditional security mechanisms, which are tailored to securing small-scale or isomorphic data, are inadequate to solve the big security challenges in Big Data era. Therefore, how to develop new tools to solve the big security challenges become crucial for the success of Big Data.

This special issue covers the most recent research results that address the big security challenges in Big Data era. We solicit papers covering various topics of interest that include, but not limited to the following:

- Encrypted search in Big Data
- Secure outsourcing computing in Big Data
- Secure data storage in Big Data
- Access control and anonymization in Big Data
- Authentication and authorization in Big Data
- Data provenance in Big Data
- Integrity verification in Big Data
- Real-time security monitoring in Big Data
- Useable security in Big Data
- Implementation and testbed for secure Big Data

Important DatesSubmissions Deadline: **February 15, 2016**

Revision Due: May 15, 2016

Final Manuscript Due: July 30, 2016

First Reviews Due: April 15, 2016

Second Reviews Due/Notification: June 30, 2016

Publication Date: October 2016

Submission

We seek submission of papers presenting novel and original results and findings concerning secure Big Data. Submissions must not be currently under consideration for publication in other venues. Author guidelines and submission information can be found at <http://iot.ieee.org/journal>. All manuscripts should be submitted through Manuscript Central, <http://mc.manuscriptcentral.com/iot>.

Guest Editors

Hongwei Li (Corresponding Guest Editor)
University of Electronic Science and Technology
of China, China
E-mail: hongweili@uestc.edu.cn

Rongxin Lu
Nanyang Technological University,
Singapore
E-mail: rclu@ntu.edu.sg

Jelena Mistic
Ryerson University, Canada
E-mail: jmistic@scs.ryerson.ca