Mathematical Problems in Engineering

Special Issue on
Security and Privacy Protection of Social Networks in Big Data Era

CALL FOR PAPERS

As ubiquitous computing dramatically changes the way people think, work, and interact, it has become more convenient for individual users to proactively generate, share, and exchange digital contents through online social media, such as online social networks (e.g., Facebook and Twitter), review/rating websites (e.g., Amazon and Yelp rating systems), online crowd sourcing platforms (e.g. Amazon Mechanical Turk), and knowledge gathering and sharing platforms (e.g., Stack Overflow and Wikipedia). These user generated contents (UGC), which take various format as digital video, blogging, forums, online social conversations, mobile phone photography, and so on, have experienced exponential increase recently and become an essential source of Big Data.

However, profit-driven attacks are emerging rapidly, raising great challenges for data security, privacy, and trust. On one hand, malicious attackers can easily manipulate such contents to conduct unethical promotions, to spread rumors, and to mislead public's decision makings. On the other hand, people carelessly posting their personal information on social media can easily have their privacy breached. In particular, the sheer amount and diverse format of user generated contents have led to emerging security and privacy issues that cannot be resolved by current defense solutions. Traditional security mechanisms and models, which are tailored to securing small-scale or isomorphic data, are inadequate to solve this challenge in Big Data era due to limited bandwidth, storage, and computation power, and so forth. Therefore, how to develop new lightweight cryptographic algorithms/protocols, data mining/organization/optimization models, and performance evaluation methods, to solve the big security challenges, becomes crucial for the success of Big Data.

The purpose of this special issue is to publish high-quality research papers as well as review articles covering the most recent research results that address the mathematical model and algorithms on security, privacy, and trust challenges in Big Data era. Original, high quality contributions that are not yet published or that are not currently under review by other journals or peer-reviewed conferences are sought.

Potential topics include but are not limited to the following:

- Access control models and anonymization algorithms in Big Data
- Authentication/authorization algorithms/protocols in Big Data
- Big Data privacy model in social networks
- Cryptography in Big Data
- Data protection and integrity in Big Data
- Data mining and provenance in Big Data
- Encrypted searching in Big Data
- Large-scale data collection and filtering problem
- New trust mechanism in social networks
- Privacy and security preserving protocol for social networking
- Secure outsourcing computing in Big Data
- Sparse data modeling, compressing, and sensing
- System designs for secure data storage in Big Data

Authors can submit their manuscripts through the Manuscript Tracking System at http://mts.hindawi.com/submit/journals/mpe/spps/.

Lead Guest Editor
Lixiang Li, Beijing University of Posts and Telecommunications, Beijing, China
li_lixiang2006@163.com

Guest Editors
Zonghua Zhang, TELECOM Lille, Villeneuve d'Ascq, France
zonghua.zhang@telecom-lille.fr

Kaoru Ota, Muroran Institute of Technology, Hokkaido, Japan
ota@mmm.muroran-it.ac.jp

Liu Yuhong, Santa Clara University, Santa Clara, USA
yhliu@scu.edu

Manuscript Due
Friday, 17 February 2017

First Round of Reviews
Friday, 12 May 2017

Publication Date
Friday, 7 July 2017