Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 6872587, 2 pages
https://doi.org/10.1155/2018/6872587

*Editorial*

# Security and Privacy Protection of Social Networks in Big Data Era

**Lixiang Li**,[1] **Kaoru Ota**,[2] **Zonghua Zhang**,[3] **and Yuhong Liu**[4]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *Muroran Institute of Technology, Hokkaido, Japan*
[3] *Telecom Lille, Villeneuve d'Ascq, France*
[4] *Santa Clara University, Santa Clara, CA, USA*

Correspondence should be addressed to Lixiang Li; li_lixiang2006@163.com

Received 13 December 2017; Accepted 14 December 2017; Published 3 January 2018



Big Data draws the attention not only because of its great power but for the severe security and privacy challenges it brings. With the sources from various formats of user generated contents like digital video, blogging, forms, online social conversations, and so on, Big Data can be a strong tool to serve the users as well as attacking them. With the increasing applications of Big Data, profit-driven attacks are emerging rapidly, raising great challenges for data security, privacy, and trust. Hence, the recent research focus on Big Data Era has more emphasis on the protection of security and privacy. As the existence of the contradiction between large quantity of data with various formats and limited bandwidth and storage and computation power, the current defense solutions cannot resolve the problem entirely. So the conventional security mechanisms for small-scale or isomorphic data should be modified to adapt to the exponential increment of user generated data. It is important to develop new lightweight cryptographic algorithms (protocols), data mining, data organization and data optimization models, and performance evaluation methods to protect the security and the privacy of Big Data.

This special issue involves 14 original papers selected by the editors so as to present the most significant results in the above-mentioned topics. These papers are organized as follows.

Two papers on attribute-based encryption and revocation are as follows: "Modified Ciphertext-Policy Attribute-Based Encryption Scheme with Efficient Revocation for PHR System," by H. Zheng et al.; "Research on Ciphertext-Policy Attribute-Based Encryption with Attribute Level User Revocation in Cloud Storage," by G. Wang and J. Wang.

Five papers on user preference matching, classification model, and community discovery are as follows: "SHMF: Interest Prediction Model with Social Hub Matrix Factorization," by C. Cui et al.; "A Quick Negative Selection Algorithm for One-Class Classification in Big Data Era," by F. Zhu et al.; "Multiview Community Discovery Algorithm via Nonnegative Factorization Matrix in Heterogeneous Networks," by W. Tao and L. Yang; "A Stable-Matching-Based User Linking Method with User Preference Order," by X. Wang et al.; "New Collaborative Filtering Algorithms Based on SVD++ and Differential Privacy," by Z. Xian et al.

Five papers on attack and intrusion detection/handle are as follows: "Economic Levers for Mitigating Interest Flooding Attack in Named Data Networking," by L. Wang et al.; "A Universal High-Performance Correlation Analysis Detection Model and Algorithm for Network Intrusion Detection System," by H. Zhu et al.; "Games Based Study of Nonblind Confrontation," by Y. Yang et al.; "An Effective Conversation-Based Botnet Detection Method," by R. Chen et al.; "Identifying APT Malware Domain Based on Mobile DNS Logging," by W. Niu et al.

Two papers on data transmission are as follows: "Semitensor Product Compressive Sensing for Big Data Transmission in Wireless Sensor Networks," by H. Peng et al.; "Efficient Data Transmission Based on a Scalar Chaotic Drive-Response System," by A. Li and C. Wang.

## Acknowledgments

We would like to thank all authors who submitted their works for this special issue. Lixiang Li is supported by the National Key Research and Development Program of China (Grant no. 2016YFB0800602) and the National Natural Science Foundation of China (Grant no. 61573067).

*Lixiang Li*
*Kaoru Ota*
*Zonghua Zhang*
*Yuhong Liu*