Special Issue Proposal

CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE

1. Proposed title for the Special Issue

Special Issue on Cyber Security and Privacy: ATIS 2017

2. Rationale

With the surge of data collected from billions of devices, data analytics techniques provide the potential to reveal new insights with the potential to transform business and society. However, most data analytics involves the fully or partial transfer of data ownership, and if not done properly, this may lead to information abuse. literatures have shown information abuse examples such as continual observation of recommendations to customers with some background information makes it possible to infer the individual's rating or even transaction history. In the context of cyberspace, information abuse can be referred to the willful or negligent analysis activity that reveals the private information of users, or the trade secret of businesses. This is particularly vital for systems involving highly sensitive information, such as in accounting and financing context.

Without a proper security and privacy protection in all aspects of cyberspace including communication, analytics environment, information abuse will pose severe threats on the individuals. Moreover, as the access, storage, management, sharing, and analytics of such massive data are often outsourced to various partners, traditional security solutions confined within a well-defined security perimeter fail to be applied in such open and sharing environments. As such, there is a need to investigate the information abuse prevention techniques in the cyberspace by examining the cyberspace infrastructure, platforms, security and privacy, and data analytics in detail hence for the call for this special issue.

We believe the special issue is very timely and there is a body of significant research that will be captured in the special issue of the journal, for the following reasons:

- Advanced research work in security and privacy in cyberspace will result in safer collaboration and trusted information sharing, especially for cyber space involving highly sensitive big data.
- While there are various papers and special issues on information security and data privacy in different domains, limited resources can be identified on information abuse from a unified perspective. This forms the timely need of developing advanced, formal and general methodologies and techniques for information abuse prevention.

- The special issue is well aligned with *Concurrency and Computation: Practice and Experience*'s themes of "Information and Knowledge Grids, Data-mining, Knowledge Discovery", as well as "Dependability and security issues, adaptable and mobile grids."

3. International Conference on Applications and Techniques for Information Security (ATIS 2017)

In 2017, the proposed guest editors have organized the 8th International Conference on Applications and Techniques for Information Security (ATIS 2017), in Auckland, New Zealand. The conference website is available at:

- http://atis.massey.ac.nz/
- http://www.atis.conferences.academy

This conference solicits research contributions from related domains, and will offer a timely forum for researchers and industry partners to present and discuss latest advances in abuse preventive data mining. In this year's ATIS conference, a high number of papers have been presented in the area of , and this sets a solid basis for soliciting high quality papers into this special issue.

4. Topics to be Covered

This proposed special issue will include but not limited to the following topics:

- Cyberspace Vulnerabilities
    - Digital Forensics
    - Intrusion Detection
    - Malicious software
- Curbing Cyber Crimes
    - Cyber-Gossip Spread Models
    - Identity authentication
    - Datasets for cyber-gossips detection
    - Collusive crime/piracy detection
- Data Privacy in Cyberspace
    - Privacy Preserving Intelligent Systems
    - Privacy Preserving Data Publishing
    - Privacy in Information Sharing

- Data Security in Cyberspace
    - Data Permission Abuse
    - Electronic Commerce Security
    - Data Protection in Outsourcing

5. The process to solicit articles

There are around 4-5 top papers on the proposed theme in ATIS 2017, and we will also solicit articles through the following methods:

(1) Where to collect the high-quality papers?

- Open public call for papers.
- Invite leading researchers in the field to contribute highest quality of papers

(2) Who will be the reviewers?

- Identify the appropriate reviewers for each manuscript
- Selected program committee members from related conferences and workshops
- Key researchers in the relevant areas of data mining, privacy preserving and data security, etc.

(3) How to guarantee the paper quality?

- Round 1 Review: All submissions will be rigidly peer reviewed by at least three reviewers discussed in the Guest Editor team, and Guest Editors will provide independent review of all papers by providing comments too;
- Round 2 Review: Guest Editors will review the review reports for each paper, and consolidate Rounds 1 review comments into an initial decision list
- EIC checking: decisions from Round 2 will be sent to the EIC for comments before sending out the notifications
- Revision 1: Selected papers from the EIC Checking will be asked for revision by addressing reviewer, GE and EIC's comments
- Round 3 Review: Revised papers will be reviewed by invited reviewers, and then by the GEs, decisions will be made for authors to further improve it, unsatisfactory papers will be rejected
- Final checking: the final submissions will be checked by GEs, EIC

6. Tentative Timetable

Upon the review results, the proposed special issue expects to **accept 5 to 7 high-quality papers**. Because this special issue is based on the ATIS-2017 conference, a faster procedure can be expected, and the tentative time schedule is as below:

Submission of manuscript: Dec. 1st, 2017

Author Notification: Mar. 15th, 2018

Revision Due: May. 15th, 2018

Final Notification: Jun. 1st, 2018

Camera Ready to the Journal: Jun. 1st, 2018

7. Proposed guest editors

- A/Prof. Gang Li, Deakin University, Australia,
  - URL: http://www.deakin.edu.au/about-deakin/people/gang-li
  - Email: gang.li@deakin.edu.au
- Prof. Lynn Patten, Deakin University, Australia
- Dr DongSeong Kim, University of Canterbury, New Zealand
- Dr Xuyun Zhang, University of Auckland, New Zealand

Brief CV of leading guest editor

- Gang Li, IEEE senior member, an associate professor in the school of IT, Deakin University (Australia).

  He serves on the IEEE Data Mining and Big Data Analytics Technical Committee (Vice-Chair 2017), IEEE Enterprise Information Systems Technical Committee, IEEE Enterprise Architecture and Engineering Technical Committee. He is an associate editor for Decision Support Systems (Elsevier), IEEE Access (IEEE) and Information Discovery & Delivery (Emerald). He has co-authored six papers that won best paper prizes, including the IEEE Trustcom 2016 best student paper, IFITT 2016 Journal Paper of the Year (3rd award), PAKDD2014 best student paper, ACM/IEEE ASONAM2012 best paper award, the 2007 Nightingale Prize by Springer journal Medical and Biological Engineering and Computing. He served on the Program Committee for over 120 international conferences in artificial intelligence, information abuse prevention, data privacy, tourism and hospitality management.