

# Special Issue Proposal for Concurrency and Computation: Practice and Experience

## --- Special Issue on Security and Privacy Issues in Fog Computing

Fog computing, a paradigm that extends cloud computing and services to the edge of the network, meets enhanced requirements by locating data, computation power, and networking capabilities closer to end nodes. Fog computing is distinguished by its accessibility to end users, particularly its support for mobility. Fog nodes are geographically distributed, and are deployed near wireless access points in areas with a significant usage. Fog devices may take the form of stand-alone servers or network devices with on-board computing capabilities. Services are hosted at the network edge or even within end-user devices, such as set-top boxes or access points. This reduces service latency, improves quality of service and provides a superior experience for the user. Fog computing supports emerging Internet of Things (IoT) applications that demand real-time or predictable latency, such as industrial automation, transportation, and networks of sensors and actuators. Due to the capability to support a wide geographical distribution, fog computing is well positioned for real-time big data analytics. Fog supports densely distributed data collection points, adding a fourth axis to the often-mentioned big data dimensions (volume, variety, and velocity).

Issues of security and privacy are in fog computing, but this remains an understudied particularly in the design and implementation of fog computing, such solutions may not suit fog computing devices that are at the edges of networks. In such environments, fog computing devices face threats that do not arise in a well-managed cloud environment.

### Topics

The aim of the proposed Special Issue of CCPE is to promote research and reflect the most recent advances of security and privacy issues in Fog computing, with emphasis on the following aspects, but certainly not limited to:

- Authentication in Fog
- Auditing and accountability in Fog
- Dependability in Fog
- Access control mechanism in Fog
- Security model in Fog applications
- Key management in Fog
- Privacy preserving in Fog computing
- Location privacy in Fog computing
- Privacy enhanced technologies for Fog applications
- Data confidentiality in Fog devices
- Security in Internet of Things (IoT)
- Secure outsourcing computation of Fog device
- Cyber physical security of Fog devices

### Paper Solicitation

This issue is an open special issue where everyone is encouraged to submit papers. We will solicit papers through two ways: conference and open call-for-papers.

1. **Selected Papers from the 9<sup>th</sup> International Symposium on Cyberspace safety and Security (CSS 2017)**

CSS 2017 covers research on all theoretical and practical aspects related to network and system security. The aim of CSS 2017 is to provide a leading edge forum to foster interaction between researchers and developers with the network and system security communities, and to give attendees an opportunity to interact with experts in academia, industry, and governments. The conference website is

<http://anslab.org/events/CSS17/index.html>

We plan to select the papers relevant to privacy preserving issues from the accepted papers based on the reviews (comments and scores) and the presentations during the conferences. Each selected paper must be substantially extended, with at least 30% difference from its conference version.

## 2. Open Call-For-Papers

We also plan to publicize an open call-for-papers (CFP) by listing the CFP in major academic announcement mailing lists/websites and by sending the CFP to researchers in the areas around the world. We estimate there will be a number of submissions via the open call-for-papers. Then we plan to select another a few papers from the submissions.

Each paper (including the selected papers from the conference) will go through a rigorous peer-review process by at least three international researchers. In total, we plan to include 8-12 papers in this special issue. The acceptance rate will be fairly low, but we regard quality as our top priority. The anticipated readers of this Special Issue include both academic and industrial researchers working in relevant areas of security and privacy preserving.

## Important Dates

<b>Submission Due</b>	December 31, 2017
<b>1<sup>st</sup> Round Notification</b>	March 1, 2018
<b>Final Notification</b>	April 1, 2018
<b>Publication</b>	Fall 2018

## Proposed Guest Editors

**Dr. Sheng Wen**, E-mail: [sheng.wen@deakin.edu.au](mailto:sheng.wen@deakin.edu.au)  
Deakin University, Australia

**Dr. Aniello Castiglione**, E-mail: [castiglione@ieee.org](mailto:castiglione@ieee.org)  
Salerno and University of Naples, Italy

**Dr. Tian Wang**, E-mail: [wangtian@hqu.edu.cn](mailto:wangtian@hqu.edu.cn)  
Xiamen Huaqiao University, P.R. China

**Dr. Md Zakirul Alam Bhuiyan**, E-mail: [zakirulalam@gmail.com](mailto:zakirulalam@gmail.com)  
Fordham University, USA

## Brief Biography of Guest Editors

**Dr. Sheng Wen** received two Ph.D. degrees from Central South University, China in February 2013 and Deakin University, Melbourne, in October 2014, respectively. He has been working full-time as a research fellow at Deakin University after he submitted his doctoral

thesis in April 2014. From January 2015, he has been a Lecturer in Computer Science in the School of Information Technology in Deakin University. He also joined the Centre of Cyber Security Research as a core research member. Dr. Wen manages several small research projects that are considered as seed funding for national projects. For example, he is in charge of three Central Research Grants Schemes (CRGS) in Deakin University. He also manages industrial funding for start-up companies, such as Industry Engagement and Incentive Scheme in Deakin University. Since late 2014, Dr. Wen has received 5 small projects from both academia and industries. Dr. Wen is also leading a small research group. This small team includes Dr. Wen, 3 Ph.D. students in Deakin and one external senior researcher as a collaborator (Dr. Mohammad S. Haghighi in University of Teheran). The small team focuses on the research of social network analysis and cyber-physical security. In the last four years, as an excellent early career researcher, Dr. Wen has published more than 40 high-quality papers, including 25 journal papers (e.g. IEEE TPDS, TDSC, TIFS, TC, ACM TOSN) and 15 conference articles in the fields of information security, epidemic modeling and source identification. Dr. Wen has also been actively providing services to the research community. For example, he is on the editorial board of Journals: 1) Ad Hoc & Sensor Wireless Networks (Elsevier, IF=0.487), 2) International Journal of Computer and Applications (Flayer, IF=0.22). He has been invited to be Chair Committee member for WMNC 2015, CSS 2015, IEEE BigDataService 2015, and GPC 2015. He also served as PC member for a number of International Conferences, such as Trustcom 2014, NSS 2014, SmartComp 2014, Trustcom 2015, ACISP 2016, AICCSA 2015, CSS 2012, DependSys 2015, HPCC 2015, ICA3PP 2015, ICA3PP 2011, ISICA 2015, NSS 2015, SNAMS 2015, SocialSec 2015, SocialSec 2016, DependSys 2016, TrustCom 2016, IEEE ICC 2016, IEEE GlobalCom 2016.

**Dr. Aniello Castiglione** was born in Civitavecchia (Rome) and actually lives in Ischia, a small island in the bay of Naples. He received the Laurea degree in Computer Science from the University of Salerno. From February 2006 he joins the Staff of the Dipartimento di Informatica ed Applicazioni "Renato M. Capocelli" as Network and Security manager. In November 2007 he took the Ph.D. in Computer Science from the University of Salerno under the supervision of Professor Alfredo De Santis.

He is a Member of IEEE (Institute of Electrical and Electronics Engineers), of ACM (Association for Computing Machinery), of IEEE Computer Society, of IEEE Communications Society, and of GRIN (Gruppo di Informatica). He is a Fellow of FSF (Free Software Foundation), of FFII (Foundation for a Free Information Infrastructure) and of FSFE (Free Software Foundation Europe). In November 2005 he joined the drafting process of the GPLv3 (GNU Public License version 3). On June 29, 2007, the final version of the GPLv3 has been released. For many years he has been involved in forensic investigations as consultant for several Law Enforcement Agencies. He has spent much in the open-source community and is a co-founder of the LuG-Ischia, the Linux User Group in Ischia. His research interests include Data Security, Wireless Communication Networks, Protocols and Forensics.

**Prof. Tian Wang** received the B.Sc. and M.Sc. degrees in computer science from the Central South University, Changsha, China, in 2004 and 2007, respectively, and the Ph.D. degree in computer science from the City University of Hong Kong, Kowloon, Hong Kong, SAR, in 2011. He was a research assistant in the City University of Hong Kong from 2006-2008. He is currently an Associate Professor at the College of Computer Science and Technology, Huaqiao

University, Xiamen, China. His research interests include wireless sensor networks, cloud computing, and fog computing. Dr. Wang manages several research projects such as the National Natural Science Foundation of China (NSFC).

He has 2 patents and more than 70 technical publications in international conferences and journals in the areas of wireless sensor networks, cloud computing, and mobile computing. His papers have appeared in the prestigious journals/conferences in the domain, including IEEE TMC, IEEE TVT, ACM TOSN, Information Sciences, Computer networks, ACM Mobihoc, IEEE RTSS, IEEE MASS, IEEE ICC, and so on. He has served as publicity chair and program committee member of numerous international conferences.

He serves as a publicity chair for IEEE DependSys 2016, session chair for SpaCCS 2016, track co-chair for IEEE CSS 2017, and program committee member of numerous international conferences (3PGCIC 2014, APSCC 2014, HPCC 2015, CoCoNet'15, ICA3PP 2015, WASA 2015, HPCC 2016, DependSys 2015, DependSys 2016). He is on the editorial board of International Journal of High-Performance Computing and Networking (IJHPCN).

**Dr. Md Zakirul Alam Bhuiyan** is currently an Assistant Professor of Computer and Information Sciences at the Fordham University. Before that, he worked for Temple University USA. He also worked as a Postdoctoral Research Fellow in the School of Information Science and Engineering and the School of Software at Central South University, China. He received the Ph.D. degree and the MEng degree in Computer Science and Technology from Central South University (CSU), China, in 2013 and 2009 respectively. He received the BSc degree in Computer Science and Engineering from International Islamic University Chittagong, Bangladesh, in 2005. He is a key member of the Trusted Computing Institute of CSU, where his research interests lie in cyber-physical systems (CPS), wireless sensor network applications, fault-tolerance and reliability, and sensor-cloud computing.

He was a Research Assistant at the Hong Kong Polytechnic University in 2010-2011 and a Software Engineer at international software companies. He was a recipient of a "Youth Scientific Fund 2015-2017" from NSF of China, "2012 Top-notch Ph.D. Student Award" from CSU, "2012 Hunan Province Innovative Engineering Research Fund Award", and a recipient of the "Outstanding Master Degree Dissertation Award" at both the provincial and the university levels. His papers have appeared in the prestigious journals/conferences in the domain, including ACM TOSN, IEEE TC, IEEE TPDS, IEEE SECON, IEEE/IFIP DSN, IEEE SRDS, IEEE DCOSS, and so on. He won the "Best Paper Award" at the IEEE ISPA 2013, Melbourne, Australia, and the "Best Academic Paper Award 2012". He was invited to serve as a Guest Editor, Workshop Chair, Publicity Chair, Program Co-Chair, TPC, and reviewer for international journal/conference proceedings. He is a member of IEEE and a member of ACM.

## Potential Reviewers

Potential reviewers are the experts in the research areas all over the world, who will be mainly selected from IEEE CSS 2017 program committees.