Editorial

Yu Chen*

Department of Electrical and Computer Engineering,
Binghamton University, SUNY,
Binghamton, NY 13902, USA
E-mail: ychen@binghamton.edu
*Corresponding author

Wei-Shinn Ku

Department of Computer Science and Software Engineering,
Auburn University,
Auburn, AL 36849, USA
E-mail: weishinn@auburn.edu

Douglas H. Summerville

Department of Electrical and Computer Engineering,
Binghamton University, SUNY,
Binghamton, NY 13902, USA
E-mail: dsummer@binghamton.edu

Kai Hwang

Department of Electrical Engineering – Systems,
University of Southern California,
Los Angeles, CA 90089, USA
E-mail: kaihwang@usc.edu

Biographical notes: Yu Chen is an Associate Professor of Electrical and Computer Engineering at the Binghamton University - State University of New York. He received his PhD in Electrical Engineering from the University of Southern California (USC) in 2006. His research interest lies in trust, security and privacy in sustainable and survivable computing technologies. He has authored or co-authored over 90 research papers in refereed journals, conferences, and book chapters. His research has been funded by NSF, DoD, AFOSR, AFRL, and industrial partners. He has served as a reviewer for NSF panels and for international journals, and on the Technical Program Committee (TPC) of prestigious conferences. He is a member of ACM, IEEE, and SPIE.

Wei-Shinn Ku received his MS in Computer Science and also in Electrical Engineering from University of Southern California (USC) in 2003 and 2006, respectively. He also received his PhD in Computer Science from the USC in 2007. He is an Associate Professor with the Department of Computer Science and Software Engineering at Auburn University, Auburn, AL, USA. His current research interests include data management systems, data analytics, geographic information systems, and cyber security. He is a senior member of IEEE and a member of ACM.

Douglas H. Summerville is an Associate Professor in the Department of Electrical and Computer Engineering at Binghamton University – the State University of New York. He received his BE in Electrical Engineering in 1991 from the Cooper Union for the Advancement of Science and Art, and MS and PhD in Electrical Engineering from the State University of New York at Binghamton in 1994 and 1997, respectively. He has co-authored over 40 journal and conference papers and authored two textbooks on embedded systems design. He is a senior member of the IEEE and a member of the ASEE. He has received two State University of New York Chancellor's Awards for Excellence, in Faculty Service and in Teaching, the Binghamton University Council/Foundation Award for Service to the University, and several teaching awards. His research and teaching interests include microcontroller systems design, digital systems design, computer and network security, covert channels and tamper detection.

Kai Hwang is a world-renowned scholar in computer architecture, parallel computing, network security and Internet applications. He earned his PhD in EECS from U.C. Berkeley in 1972. Presently, he serves as a Professor of Electrical Engineering and Computer Science at the University of Southern California. He teaches computer architecture, wireless internet, cloud and pervasive computing courses at USC. He is also an EMC-endowed Visiting Chair Professor at Tsinghua University in China. An IEEE Life Fellow, he has served as the founding Editor-in-Chief of the *Journal of Parallel and Distributed Computing* (*JPDC*) for 28 years. He has received the Lifetime Achievement Award from IEEE CloudCom in 2012 for his pioneering contributions to parallel and distributed computing.

The cloud computing paradigm has been renovating the future of information technology (IT) industry because of many attractive features, including high elasticity, good scalability, support for pay-as-you-go service models, and capability of overcoming constraints in both software parallelism and hardware capacity. This paradigm not only enables users to enjoy convenient, versatile and efficient services, but also relieves the burden of maintenance. However, security remains the top concern to both users and service providers.

This special issue includes three papers that address security issues in cloud computing from different perspective. One is a survey paper, 'Cloud computing: a review of security issues and solutions'. Starting from an overview of the history, definition, and service models of cloud computing, this article illustrates the major security issues with cloud computing, including information confidentiality, integrity, availability and auditing. It then presents some countermeasures that can be implemented to tackle security breaches in the cloud. The editors hope this article will provide a current and thorough overview of this area to researchers.

While virtual machine (VM) checkpointing is useful for system administration, it can also increase the risk of exposing confidential user data. In 'Privacy-preserving virtual machine checkpointing mechanism', a security and privacy aware VM checkpointing mechanism called SPARC is introduced. SPARC enables users to selectively exclude a user's confidential data within a VM from being checkpointed. This paper details the design challenges in effectively tracking and excluding process-specific memory and disk contents from the checkpoint file for a VM running on a commodity Linux operating system. It also presents techniques to track process dependencies due to inter-process communication and to account for such dependencies in SPARC.

The performance and security of cognitive radio networks (CRN) is considerably constrained by its limited power, memory and computational capacity. In the paper 'Geolocation-aware resource management in cloud computing-based cognitive radio networks', the authors propose an approach to relieve this constraint using cloud. Distributed storage and computing resources in a cloud computing platform and geolocation of secondary users are leveraged to store spectrum occupancy information of heterogeneous wireless networks and facilitate the access of spectrum opportunities for secondary users (SU). This paper also proposes a scalable mapping method using storm, a real-time distributed processing model for a cloud computing platform to dynamically partition the geographical area according to the SU density.