Editorial

Xiaofeng Chen*

The State Key Laboratory of Integrated Service Networks (ISN),
Xidian University,
Yanta District, Xi'an, 710071, China
Email: xfchen@xidian.edu.cn
*Corresponding author

Xinyi Huang

School of Mathematics and Computer Science,
Fujian Normal University,
Fuzhou, Fujian, 350117, China
Email: xyhuang81@gmail.com

Joseph K. Liu

Faculty of Information Technology,
25 Exhibition Walk, Clayton Campus, Monash University,
VIC 3800, Australia
Email: ksliu9@gmail.com

Biographical notes: Xiaofeng Chen received his PhD in Cryptography from Xidian University in 2003. Currently, he works at Xidian University as a Professor. His research interests include applied cryptography and cloud computing security. He has published over 100 research papers in refereed international conferences and journals. His work has been cited more than 3,000 times at Google Scholar. He is in the editorial board of *Computing and Informatics*, *International Journal of Grid and Utility Computing*, *International Journal of Embedded Systems*, etc. He has served as the Program/General Chair or program committee member in over 30 international conferences.

Xinyi Huang received his PhD degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia. He is currently a Professor at the School of Mathematics and Computer Science, Fujian Normal University. His research interests include applied cryptography and network security. He has published over 100 research papers in refereed international conferences and journals. He is an Associate Editor of *IEEE Transactions on Dependable and Secure Computing*, in the editorial board of *International Journal of Information Security* and has served as the Program/General Chair or program committee member in over 60 international conferences.

Joseph K. Liu received his PhD in Information Engineering from the Chinese University of Hong Kong in 2004, specialising in cryptographic protocols for securing wireless networks, privacy, authentication and provable security. He is now a Senior Lecturer at the Faculty of Information Technology, Monash University, Australia. His current technical focus is particularly lightweight cryptography, wireless security, security in smart grid system and cloud computing environment.

1 Introduction

Cloud computing, based on utility and consumption of computing resources, involves deploying groups of remote servers and software networks that allow centralised data storage and online access to computing services or resources. It is competent to provide clients who are resource constrained or financially restricted with flexible and convenient services in the pay-per-use manner. Despite the tremendous benefits, cloud computing also inevitably suffers from some new security challenges. For instance, malicious entities may jeopardise data confidentiality and integrity by compromising keys or relevant ID information of the legitimate users. Also, service availability may also be out of order due to the attackers. To cope with these threats, plenty of researchers come up with many efficient schemes and protocols which can be successfully deployed on the cloud infrastructure.

This special issue on 'Advances in cloud computing security' attempts to highlight some of the latest research addressing those challenges. It consists of nine papers selected from the contributions of the 8th International

Conference on Network and System Security (NSS 2014). More specifically:

- The paper of Xiang and Tang, titled 'Securely verifiable outsourcing schemes of matrix calculation', proposes three new and secure outsourcing schemes of matrix calculation by using a trusted cloud server, which are superior in efficiency due to the reduction of user cost.
- The paper of Yao, Xu and Huang, titled 'Batch public auditing for distributed mobile cloud computing', proposes an efficient data encryption protocol for distributed mobile systems, which contains several desirable properties, including batch public audit, collusion preventing, and open channel transmission.
- The paper of Song, Zhou, Luo and Deng, titled 'The B^+-tree-based method for nearest neighbour queries in traffic simulation systems', proposes a B^+-tree-based methods to improve the efficiency of NN queries by borrowing ideas from methods used in databases. Meanwhile, they create a linked local B^+-tree, called LLB^+-tree, which is a variation of the original B^+-tree, to maintain the index of neighbours of each vehicle. They also build a mathematical model to optimise the parameter setting of the LLB^+-tree according to multiple parameters for lanes and vehicles.
- The paper of Wang, Zheng and Yang, titled 'New identity-based key-encapsulation mechanism and its applications in cloud computing', proposes a new identity-based key-encapsulation mechanism in the generic levelled multilinear map setting and prove its security under multilinear decisional Diffie-Hellman assumption in the selective-ID model.
- The paper of Zhang, Liu, Tang and Tian, titled 'A lattice-based designated verifier signature for cloud computing', proposes a lattice based designated verifier signature scheme with a set of new mechanisms for efficiently managing parameter boundaries of lattice based schemes, which are among the major obstacles to the deployment of designated verifier signature schemes in the future.
- The paper of Li, Mao, Chen, Li and Chen, titled 'Rating cloud storage service by collaborative remote data checking', proposes a new rating algorithm to assess the credibility of cloud service providers (CSPs) which is based on technical evidences. To ensure the fairness of the assessment and detect the dishonest clients, this paper introduces a robust reputation model based on the clients' behaviour during the collaborate verification process.
- The paper of Wang, Susilo, Li and Xu, titled 'File sharing in cloud computing using win-stay-lose-shift strategy', incorporates win stay lose shift (WSLS) strategy into file sharing and simulates it compared with tit-for-tat (TFT) strategy in clouds. Simulation results show that WSLS is an optimal strategy for users to share their files in clouds.
- The paper of Zhao, Wang, Xu and Wang, titled 'Cloud data integrity checking protocol from lattice', proposes a cloud data integrity checking protocol from lattice, which achieves privacy-preserving public verifiability and remains secure against quantum computer attacks.
- The paper of Zhang and Qin, titled 'Lattice-based threshold cryptography and its applications in distributed cloud computing', proposes an efficient lattice-based secret sharing algorithm without interactivity among sharers, which is the key technology of the first multi-authority identity-based encryption scheme from lattices employing threshold decryption.

Finally, we appreciate all authors, reviewers and editorial members for their invaluable contribution, without which this special issue cannot be reality.