Editorial

Fatos Xhafa*

Department of Computer Science,
Technical University of Catalonia,
Campus Nord, Ed. Omega,
C/Jordi Girona 1-3, 08034 Barcelona, Spain
Email: fatos@cs.upc.edu
*Corresponding author

Xu An Wang

Key Laboratory of Cryptography and Information Security,
Engineering University of Chinese Armed Police Force,
Wujing Road No. 1, Sanqiao Town, Xi'an City,
Shaanxi Province, 710086, Xi'an, China
Email: wangxazjd@163.com

Biographical notes: Fatos Xhafa received his PhD in Computer Science from the Technical University of Catalonia (UPC), Barcelona, Spain, where he holds the permanent position of a Professor Titular d'Universitat. He was a Visiting Professor at the University of London, UK (2009/2010) and Research Associate at the Drexel University, Philadelphia, USA (2004/2005). He has widely published in peer reviewed international journals, conferences/workshops, book chapters and edited books and proceedings in the field. He is the Editor-in-Chief of the *International Journal of Space-based and Situated Computing*, and *International Journal of Grid and Utility Computing*, Inderscience. He is actively participating in the organisation of several international conferences. His research interests include parallel and distributed algorithms, combinatorial optimisation, networking, cloud, grid and P2P computing.

Xu An Wang received his BS and MS in Computer Science and Cryptography from the Engineering University of Chinese Armed Police Force, and PhD in Cryptography from the Xidian University. He is currently an Associate Professor in the Engineering University of Chinese Armed Police Force. His research interests are public key cryptography, cloud security, provable security and information security. He has published more than 60 research papers at referred national and international journals, conference proceedings. He has served as the Program co-Chair or programme committee member in several international conferences.

We are now in an era of cloud computing and big data, more and more large and very large datasets are generated everyday/everywhere. How to deal with these massive datasets efficiently and in a scalable way is a very difficult problem. Moreover, how to solve security issues around data centres and cloud computing platforms becomes more and more challenging. Middleware, cryptographic schemes, high performance computing (HPC) techniques and big data handling method can all be used to handle these issues.

This special issue on 'Middleware and schemes for secure authentication and access to data centres and cloud computing platforms' brings some new advanced techniques on these aspects, such as public cloud storage auditing scheme, new architecture of cloud platform, secure access and associate deleting technique, round-optimal key agreement protocol, low-connectivity essential proteins discovering method, efficient method for the quasilinear elliptic problems and flow isolation mechanism. It comprises seven papers carefully selected from the contributions of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2015) and other excellent submissions directly for this special issue. They are the following:

In Shen et al.'s paper titled as 'A public cloud storage auditing scheme for resource-constrained clients', the authors propose a public cloud storage auditing scheme with lightweight authenticator generation. They design a new framework of public cloud storage auditing, in which an authenticators generation centre (AGC) is in charge of generating authenticators for users. In their proposed scheme, the AGC does not know the real cloud data of users because it only generates the authenticators for blinded cloud data. To reduce the computation burden at user side, the cloud can verify whether the authenticators generated by the AGC are correct or not. As a result, the users only consume very little computation for public authenticator generation and verification. The security analysis and the performance analysis show the proposed scheme is secure and efficient.

In Deng et al.'s paper titled as 'Architecture of cloud platform for CAE simulation in supercomputing environment', the authors present the three novel layers for architecture of cloud platform, including user interaction layer, middleware layer, and HPC resource layer. The platform adopts a series of security technology solutions in each layer. A technology called CAE application packaging template (CAEAPT) is proposed for integrating heterogeneous CAE softwares to make full use of the computing resources of 'Tianhe No. 1'. The platform has been implemented using the Java language, Tuscany, Struts, Hibernate, Spring and other open source softwares. The user interaction layer of the platform uses the Struts-Spring-Hibernate (SSH) framework. The middleware layer uses the Tuscany, Hibernate and Spring as the combination. The CAEAPT technology uses the template files for job instructions and configuration files, and automatically generates the job scripts for parallel computing to CAE simulation, then executes parallel job for CAE simulation through the file transfer channel and the command channel. According to the architecture, the design ideas and the key technologies in this paper, the second prototype of the platform has been completed, and the part applications in the platform have been demonstrated.

In Xiong et al.'s paper titled as 'A secure access and associate deleting scheme for multi-replica in multi-cloud environment', the authors propose a secure access and associate deleting scheme for multi-replica (MADS) in multi-cloud environment, which is based on symmetric encryption algorithm, attribute-based encryption and replica location technology. We construct a novel multi-layered key structure, called multi-way search key tree (MSKT), that ensures no key material will be revealed, yet the data owner is able to control the master key and manage other keys by performing some tree operations. They also propose a data replica associated model, which is able to associate all the data replicas in multi-cloud environment. Comprehensive comparison and security analysis demonstrate that the proposed MADS scheme is effective and secure.

In Li et al.'s paper titled as 'Round-optimal ID-based dynamic authenticated group key agreement', an identity-based dynamic authenticated group key agreement (DAGKA) protocol is presented. It is round-optimal, since:

1 in setup and join algorithms, only one round of communication is required

2 in leave algorithm, there is no message exchange among group members.

Joining members cannot compute previous session keys and leaving members cannot compute subsequent session keys. The protocol is provably secure. Its AKE-security is proved under decisional bilinear Diffie-Hellman (DBDH) assumption. In addition, the protocol resists key control attack and achieves forward security.

In Zhao et al.'s paper titled as 'Efficient expanded mixed finite element method for the quasilinear elliptic problems', an expanded mixed finite element method is introduced to solve the quasilinear elliptic problems. This method expands the traditional mixed finite element method in the sense that three variables are explicitly treated simultaneously. Existence and uniqueness of the discrete approximation are demonstrated. L^2-error estimates for three variables are presented. Numerical examples are carried out to validate the theoretical analysis. Considering the rapid development of computing power, advanced modelling and numerical simulation technology has become a useful and powerful tool, thus this result can be useful for many engineering large projects.

In Dong's paper titled as 'Discovering low-connectivity essential proteins based on protein-protein interaction network', they present three indexes to measure biological features of low-connectivity essential proteins. And they also propose a centrality measure interaction-complex-function centrality (ICFC) to predict low-connectivity essential proteins, which combines topological structure information of the PPI network with the distinguishable biological properties of essential proteins. The experimental results demonstrate that the predicted precision of ICFC outperforms ten exiting centrality measures. The improvements of ICFC over the ten exiting centrality measures are up to 1.08 3.31 times. Their method can be used to handle massive biological datum in the approaching big data era.

In the last paper titled as 'On flow isolation mechanism for different applications in NFV controller', Gao et al. propose a historical overhead-based flow isolation mechanism (HOB-FIM) to ensure that each control plane occupies a fixed amount of bandwidth resources. It can determine the scheduling priority of control plane by calculating the historical overhead of each control plane. Their experimental results prove that their proposed mechanism has superiority over FIFO algorithm in terms of the fairness of shared link bandwidth in NFV controller. It also can provide support for the delay-sensitive control plane in VNFs.

Acknowledgements

The guest editors would like to thank Prof. Nadia Nedjah (Editor-in-Chief of *IJHPSA*) for providing us the opportunity to edit this special issue. We would like to thank Inderscience Journal Manager, Ms. Liz Harris, for carefully editing this special issue. Finally, we thanks all authors, reviewers and editorial members for their invaluable contribution to this special issue.