Preface

Fatos Xhafa

Department of Computer Science,
Technical University of Catalonia,
Campus Nord, Ed. Omega,
C/Jordi Girona 1-3, 08034 Barcelona, Spain
Fax: +34-93-413-7833
Email: fatos@cs.upc.edu

Biographical notes: Fatos Xhafa received his PhD in Computer Science in 1998, from the Department of Computer Science of the Technical University of Catalonia (UPC), Spain. Currently, he holds a Permanent Position of Professor Titular (Hab. Full Professor) at the UPC. He was a Visiting Professor at the University of London, UK, 2009–2010, and Research Associate at Drexel University, USA, 2004–2005. He has published in international journals, conferences/workshops, chapters, books and proceedings. He is the Editor-in-Chief of *IJGUC* and *IJSSC*, Inderscience, of the Elsevier Book Series *Intelligent Data-Centric Systems* and of *Lecture Notes on Data Engineering and Communication Technologies*. His research interests include parallel and distributed algorithms, massive data processing and collective intelligence, optimisation, networking, P2P, cloud computing, security and trustworthy computing, among others.

There is taking place a fast adoption of cloud computing platforms and data outsourcing to cloud data centres by companies, businesses, organisations, etc. In this process, security and privacy remain among the most important issues for researchers, developers, users, and stakeholders. These are challenging issues due to the complexity of handling them at various system parts and levels, such as access, authentication, privacy, etc., which require reliable and secure algorithms. Additionally, due to the ever-increasing growth in data size, such algorithms should be efficient and scalable by taking advantage of data locality.

This special issue aims to report and disseminate latest research findings and developments in the field of security and privacy and efficiency for massive cloud data storage, new algorithms and techniques in the field, with special emphasis on efforts related to the foundational theory, but also to practical real-life applications. The special issue accepted five papers based on their quality and suitability to the special issue.

The first paper 'A study of the internet financial interest rate risk evaluation index system in cloud computing' by Mu et al. the authors tackle some challenging issues to risks in internet finance (ITFIN risk in China), which integrates online transaction data generated in various social networks. One such issue in ITFN is that one person can play many identities in the network. This phenomenon posed a severe challenge to ITFIN network security and has largely intensified the risks, including the operational risk, market selection risk and network and information security risk. The authors conducted theoretical and empirical analysis, and then constructed an assessment model against China's ITFIN risk. The empirical research results indicate that the model can effectively

reduce redundant data information with rough set theory. Overall, the model is shown to have good generalisation and learning ability.

The second paper 'Novel implementation of defence strategy of relay attack based on cloud in RFID systems' by Xu et al. consider cloud based RFID, which can be used can be used for cash-less payment, physical access control, temporary rights and identification in cloud environment. When an RFID card is used, there is a wireless transaction between the card and its reader, which could be attacked by several methods, including a relay attack. In recent years, researchers have proposed solutions using second channels to resist relay attack, such as using environmental measurements including noise, light and temperature. The authors presented some research finding on the defence techniques for relay attacks in cloud-based RFID systems.

Yang et al. in the third paper 'Reconfigurable design and implementation of nonlinear Boolean function for cloud computing security platform', propose a hardware structure of reconfigurable nonlinear Boolean function. This structure can realise the number of variables and AND terms less than 80 arbitrary nonlinear Boolean function in stream cipher algorithms. The entire architecture is verified on the FPGA platform, the result proves that the design is propitious to carry out the most nonlinear Boolean functions in stream ciphers, compared with other designs, the structure can achieve relatively high flexibility, and it has an obvious advantage in the area of circuits and processing speed.

In the fourth paper 'Network optimisation for improving security and safety level of dangerous goods transportation based on cloud computing', Wang et al. deal with network optimisation for improving security and safety level of dangerous goods transportation, which is an important part of dangerous goods logistics security monitoring system. Cloud storage is one of the core technologies of the system to ensure the system security and stability based on data backup and disaster technology. An improved risk analysis is devised to achieve the purpose of balancing the security and the cost for the route. Based on cloud computing task scheduling, a detailed design of the simulated annealing algorithm is presented. An example is analysed to demonstrate that the improved algorithms are efficient and feasible.

Finally, the fifth paper 'Proofs of retrievability from linearly homomorphic structure-preserving signatures', Zhang et al. investigate some issues on proofs of retrievability (PoR), which enables clients to outsource huge amount of data to cloud servers, and provides an efficient audit protocol. The authors present a generic construction of PoR from linearly homomorphic structure-preserving signature (LHSPS), which makes public verification possible. Authenticity and retrievability of our PoR scheme are guaranteed by the unforgeability of LHSPS. Results are further extended to dynamic PoR and a publicly verifiable (dynamic) PoR scheme is derived. The security is based on standard assumptions and proved in the standard model.

As we conclude this preface, we give special thanks to honorary Editor-in-Chief of *IJICS* journal Professor Eldon Y. Li for giving us the opportunity to edit the special issue. We would like to thank all the authors for submitting their papers and the reviewers for their volunteer work and time to make it possible to publish this special issue. The support from journal manager is appreciated.