J Ambient Intell Human Comput (2015) 6:531–532
DOI 10.1007/s12652-015-0324-5

EDITORIAL

Editorial preface for the special issue "Advances in security, privacy and trust technologies"

Fatos Xhafa[1] · Xiaofeng Chen[2] · Leonard Barolli[3]

Published online: 26 September 2015

With the fast development of Internet technologies, the information and communication systems are continuously facing new security, trust and privacy challenges. Indeed, the potentially invasive nature of the information has implications on privacy of the users and their online activity such as transactions. Likewise, the implicit reliance on technology to make decisions on one's behalf makes essential to study new mechanisms for expressing and reasoning about trust.

This special issue brings together research articles covering diverse aspects of security, privacy and trust in computer and networked-based information systems, including privacy concerns, tools to help secure information, methods for development and assessment of trustworthy systems, analysis of vulnerabilities and attacks, trends and new developments, secure operating systems and applications, security issues in wireless networks and pervasive systems, design and test strategies for secure and survivable systems, and cryptology, among others.

The papers of the special issue are selected based on strict review results, where papers went through three rounds of review and revision. As a result, nine papers were selected and are arranged in the special issue as follows.

Xiong et al. in the first paper "The finite volume element method for a parameter identification problem" use finite volume element method to solve a parameter identification problem of parabolic equations with over-specified data. The authors provide the numerical scheme of the unknown function and control parameters and obtain the error estimates of approximate solution. The proposed method is experimentally evaluated and compared with the exact solution to confirm the good accuracy of the presented scheme.

The second paper by Chen et al. "An Opinion Mining Framework For Cantonese Reviews", analyze opinion mining for Cantonese language. The authors motivate the need to construct a particular lexical database for Cantonese and explore some Cantonese special written-tradition rules and incorporate them into the feature-based opinion summarization system framework. The experimental results show that the proposed framework significantly outperforms the traditional Mandarin sentiment analysis method using ICTCLAS.

In the third paper "A Secure Remote Data Integrity Checking Cloud Storage System from Threshold Encryption", Yao et al. study the confidentiality and integrity issues in cloud storage system. The authors address the privacy issue of decentralized cloud storage system using threshold cryptography. The threshold encryption scheme is therefore integrated with a secure decentralized erasure code to form a secure cloud storage system.

Zhang et al. in the fourth paper "How to build a faster private information retrieval protocol", propose a secure multi-bit homomorphic encryption scheme based on Learning With Errors over Rings (RLWE) assumption. The authors use canonical embedding to transform ring

✉ Fatos Xhafa
fatos@cs.upc.edu

Xiaofeng Chen
xfchen@xidian.edu.cn

Leonard Barolli
barolli@fit.ac.jp

[1] Universitat Politècnica de Catalunya, Barcelona, Spain

[2] Xidian University, Xi'an, China

[3] Fukuoka Institute of Technology, Fukuoka, Japan

elements into vectors over Zq, and thus decrease encryption and decryption cost. Then, an efficient private information retrieval protocol that employs this scheme is presented.

The fifth paper "Dual-kernel Based 2D Linear Discriminant Analysis for Face Recognition" by Liu and Ye, present a new image feature extraction method for face recognition by integrating multiple kernel discriminant analysis with existing two dimensional linear discriminant analysis method. The experimental results on the ORL and UMIST face databases show the effectiveness of the proposed method.

The sixth paper by Li et al. "Image encryption algorithm with compound chaotic maps" propose a novel image encryption scheme based on two even-symmetric chaotic maps and a skew tent chaotic map, consisting of a permutation process and a diffusion process. The performance and security of the proposed method are evaluated thoroughly histogram, correlation of adjacent pixels, information entropy and sensitivity analysis. Results suggest that the scheme is reliable to be adopted for the secure image communication application.

Wang et al. in the seventh paper "Multiobjective optimization algorithm with objective-wise learning for continuous multiobjective problems" propose a single objective guided multi-objective optimization framework to solve continuous multi-objective optimization problems (MOPs). In their framework, a solution is selected from archive, and then objective-wise learning strategy is developed to promote the evolution of each objective of the selected solution. A specific instantiation of their framework is implemented and compared with several state-of-the-art multi-objective evolutionary algorithms.

In the eighth paper "A fault-tolerant architecture for ROIA in cloud", Liu addresses the needs for highly robust and efficient architecture for supporting real-time online interactive application (ROIA) beyond the C/S or P2P mode. The proposed approach takes advantage of the cloud computing technologies to achieve higher scalability and resource utilization. A new fault-tolerant architecture for ROIA in the Cloud platform, is therefore presented, which is based on cell overlapping technique. This new architecture provides redundancy to enhance the robustness and the scalability of ROIA.

Finally, Chen and Yu in the last paper, present a new adaptive method to estimate blind minimum mean square error (MMSE) equalizer with arbitrary delay of single-input-multiple-output (SIMO) channel. By using a recursive least square (RLS)-similar algorithm to recursively update a correlation matrix and its pseudo-inverse, the proposed algorithm ensures convergence and is not sensitive to the initialization of its parameters. The method is evaluated and compared with other batch-type approaches to demonstrate the performance of the proposed method.

We would like to thank all the authors for their valuable contributions and the reviewers for their time and constructive feedback during several rounds of review and revision.

Fatos Xhafa's work has been partially supported by funds from the Spanish Ministry for Economy and Competitiveness (MINECO) and the European Union (FEDER funds) under grant COMMAS (ref. TIN2013-46181-C2-1-R).