Computer Standards & Interfaces 54 (2017) 1–2

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Editorial

Cloud computing security and privacy: Standards and regulations

ABSTRACT

Cloud computing is a distributed computation model over a large pool of shared and virtualized computing resources, such as storage, processing power, applications and services. It has received considerable attention from the research communities and the industry due to its practicality This kind of new computing represents a vision of providing computing services as public utilities like water and electricity. Cloud computing provides a number of benefits, including reduced IT costs, flexibility, increased collaboration, etc. However, the advent of cloud computing has posed a variety of new challenges for both cloud users and cloud service providers. Taking data privacy as an example, encryption is becoming a standard practice for both cloud users and cloud service providers, as a mechanism against unauthorized surveillance as well as malware. However, the introduction of encryption to cloud also leads to new problems such as key management, as well as the inability of cloud to provide some utilities such as data manipulation. Providing cloud as utilities is an active research area of interest, which includes how these encrypted data can be searched, shared or used as input for computation directly.

1. This Special Issue

We are pleased to present 8 technical papers dealing with cutting-edge research and technology related to this topic. These papers were selected out of the significantly extended versions of the 60 submissions from 23 countries in the 9th International Conference on Provable Security (ProvSec., 2015) and 39 open submissions. These papers have been rigorously reviewed and only the best papers were selected.

In the first paper entitled "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment [1]", Odelu et al. presented a novel ciphertext-policy attribute-based encryption (CP-ABE) scheme, which is designed to be sufficiently light-weight for deployment in a mobile cloud environment. Specifically, the scheme offers both constant size ciphertexts and secret keys with an expressive AND gate access structure. The authors also proved the security of the scheme against chosen-ciphertext adversary in the selective security model. Potential future research directions such as extending the scheme to other access structures, and evaluating the scheme in a real-world environment were also outlined by the authors.

In the second paper, "Identity-Based Provable Data Possession Revisited: Security Analysis and Generic Construction [2]", Liu et al. showed that an existing ID-DPDP is flawed since it fails to achieve the property of soundness. The authors then fix the flaw by presenting a generic construction of identity-based PDP (ID-PDP) protocol, derived from identity-based signatures (IBS) and traditional PDP protocols. The authors proved that the soundness of the generic ID-PDP construction depends on the security of the underlying PDP protocols and the IBS. The authors provided a concrete ID-PDP protocol as well as an instance of the generic construction to a state-of-the-art PDP protocol due to Shacham and Waters.

In the third paper, "Characterizing the Semantics of Passwords: The Role of Pinyin for Chinese Netizens [3]," Han et al. explore the semantics of passwords for Chinese netizens. They first presented a comprehensive statistical analysis on a large scale real passwords used on several leading Chinese websites. Then they managed to characterize the Pinyin semantics of the passwords. Their findings show that over 76% passwords can be covered by the patterns of pure numeric and concatenation of Pinyin and digits. The authors make an interesting step towards aiding discovery of interesting semantic patterns in user choice by analyzing Pinyin structures in passwords. Since the cloud (accessible from anywhere in the world) has to deal with password-based user identities, understanding semantic patterns in passwords can help us to better inform usable password policies and password creation guidelines.

Similarly designed for mobile cloud computing, the forth paper entitled "SeGoAC: A tree-based model for self-defined, proxy-enabled and group oriented access control in mobile cloud computing [4]" by Ren et al. described a lightweight tree-based model. The model allows self-defined, proxy-enabled and group-oriented access control for file storage access control in a mobile cloud computing deployment.

In the fifth paper, "Verifiable delegated quantum computation with χ-type entangled states [5]," Tan et al. present a delegated quantum computation protocol without a trusted center that includes four participants. The authors pointed that the other two particles can collapse into a certain Bell state if the first two particles are measured in four-particle χ-type entangled states. Alice only needs to be capable of getting access to quantum channels, perform Pauli operations and also has a memory of two graph states, but she does not need to prepare any quantum state. They not only verify the correctness of measurement outcomes, but also give blind analysis and proof rigorously.

In the sixth paper, "A Two-party Privacy Preserving Set Intersection Protocol Against Malicious Users in Cloud Computing [6]", Cao et al. propose a two-party privacy preserving set intersection protocol based on a novel and light-weight combination of commutative encryption and hash-based commitments. The scheme

http://dx.doi.org/10.1016/j.csi.2017.03.005
0920-5489/

determines the intersected elements between two datasets while keeping the privacy of each dataset to its owner. Compared to the state-of-art research, the scheme can prevent cheating participants; the completeness of the integration is guaranteed even if the dataset owners misbehave. The scheme is useful for datasets where no secure infrastructure is established.

In the seventh paper, "Provable Data Transfer from Provable Data Possession and Deletion in Cloud Storage [7]," Xue et al. proposed a provable data transfer protocol based on provable data possession and deletion for secure cloud storage. The scheme achieves the desirable features of supporting both plaintext and ciphertext operations. The data owner can transfer the outsourced data from one cloud to another, without retrieving the entire data from the old cloud, and checking the data integrity in the new cloud. The user does not need to worry about the deletion of the removed data in the original cloud for the cloud can generate the deletion evidence on the cloud data. Thus, users can ensure the data are transferred successfully and indeed deleted in the original cloud.

In the eighth paper, "A Secure and Privacy-Preserving Mobile Wallet with Outsourced Verification in Cloud Computing [8]," Qin et al. first identified practical threat and unique design requirements in terms of security and privacy protection for mobile wallet. Then the authors presented a novel authentication approach to secure the mobile wallet and protect the privacy of the mobile user by incorporating the digital signature and pseudo-identity techniques. Further, the computation task on the client side, which is usually featured with limited computation resources, is outsourced to the untrusted cloud server securely. The performance evaluation and security analysis of Qin et al.'s approach demonstrate that their approach can achieve desirable efficiency and security properties of mobile wallet.

We sincerely hope that you will enjoy reading these papers in this special issue. We thank all the international reviewers for their professional services. We deeply thank Professor Rory O'Connor, the Editor-in-Chief, for providing this opportunity to publish this special issue. We thank the journal manager, Dhanalakshmi Thilakraj and publishing content specialist, Qian Jiao for their time and effort on this special issue. With these continuous support, encouragement and guidance throughout this publishing project, this special issue has been very successful.

References

[1] V. Odelu, A. Kumar Das, Y.S. Rao, S. Kumari, M. Khurram Khan and K. Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment", CSI-D-16-00004.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[2] H. Liu, Y. Mu, J. Zhao, C. Xu, H. Wang, L. Chen and Y. Yu, "Identity-Based Provable Data Possession Revisited: Security Analysis and Generic Construction", CSI-D-16-00014.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[3] G. Han, Y. Yu, X. Li, K. Chen and H. Li, "Characterizing the semantics of passwords: The role of Pinyin for Chinese Netizens", CSI-D-16-00046.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[4] W. Ren, R. Liu, M. Lei and K. Choo, "SeGoAC: A tree-based model for self-defined, proxy-enabled and group-oriented access control in mobile cloud computing", CSI-D-16-00047.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[5] X. Tan, X. Zhang and T. Song, "Verifiable delegated quantum computation with χ -type entangled states", CSI-D-16-00054.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[6] X. Cao, H. Li, L. Dang and Y. Lin, "A Two-Party Privacy Preserving Set Intersection Protocol against Malicious Users in Cloud Computing", CSI-D-16-00066.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[7] L. Xue, J. Ni, Y. Li and J. Shen, "Provable data transfer from provable data possession and deletion in cloud storage", CSI-D-16-00071.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.
[8] Z. Qin, J. Sun, A. Wahaballa, W. Zheng, H. Xiong and Z. Qin, "A Secure and Privacy-Preserving Mobile Wallet with Outsourced Verification in Cloud Computing", CSI-D-16-00052.R1. Computer Standards and Interfaces [this issue]. Special Issue Paper: Publisher—Please put full reference here in proofs.

Yong Yu
School of Computer Science, Shaanxi Normal University, Xi'an 710062, China
E-mail address: yyucd2012@gmail.com

Atsuko Miyaji
Department of Electrical Engineering, Graduate School of Engineering, Osaka University, Japan
E-mail address: miyaji@comm.eng.osaka-u.ac.jp

Man Ho Au
Department of Computing, The Hong Kong Polytechnic University, Hong Kong
E-mail address: csallen@comp.polyu.edu.hk

Willy Susilo
School of Computing and Information Technology, University of Wollongong, Australia
E-mail address: wsusilo@uow.edu.au