J Ambient Intell Human Comput (2016) 7:607–609
DOI 10.1007/s12652-016-0390-3

EDITORIAL

Special issue on security and privacy techniques in mobile cloud computing

Ilsun You[1] · **Jin Li**[2]

Published online: 27 June 2016

Mobile cloud computing is the combination of cloud computing and mobile network which benefits the users, network operators, and cloud service providers. There are numerous challenges in the field of mobile cloud computing, including reliability, authenticity and privacy (Tunc and Hariri 2015; Vazquez et al. 2015). These challenges have become a barrier in the rapid growth of mobile cloud computing's subscriber. Without authenticity, any trust relationship could not be established in the mobile cloud computing system, and any attacker cloud can cheat through disguise; without reliability and privacy, mobile users would also increase the risk of outsourcing tasks to the cloud service providers.

Besides the security requirement (reliability, authenticity and privacy), efficiency is the other concern specific to the mobile cloud computing. Due to the constraint over the resources of mobile devices, it is always desired to offload the data and the computations to the cloud service providers; such that the local computations are minimized. This outsourcing paradigm raises a new challenge for carrying data inside the mobile devices as well as for the privacy of outsourced identities.

This special issue aims to bring together the researchers for the exchange of the state-of-art results in advancement of technologies towards the secure mobile cloud computing. Especially, it focuses on both the theoretical and the practical aspects of the security issues in mobile cloud computing. In this special issue, a total of ten papers were selected after a rigorous review process. These papers addressed the security and privacy issues in cloud computing and proposed efficient solutions for these problems.

The first paper entitled "Dynamic Proofs of Retrievability with Square-Root Oblivious RAM" by Xu et al. (2015) pointed out that the security challenges, such as efficient checking and proving of data integrity, need to be more considered for cloud storage. In this paper, the authors proposed dynamic proofs of retrievability via Square-Root Oblivious RAM. They first defined the notions in their scheme, followed by introducing the Square-Root ORAM protocol. It was shown from the security and efficiency analysis that the proposed scheme is efficient in supporting data dynamics with provable verification and retrievability.

The next paper entitled "Unidirectional IBPRE Scheme from Lattice for Cloud Computation" by Zhang et al. (2015a) proposed a property of backward collusion safety, which meant that the collusion between Alice and the proxy cannot extract secret key of Bob. The authors presented an IB-PRE scheme based on lattices with the highly desirable properties of anonymity, uni-directionality, multi-use and backward collusion safety. Besides this, the IND-PrID-CPA security proof of the proposed approach is given using the random oracle model based on the assumptions of the decisional learning with errors (LWE) hardness.

The particle swarm optimization (PSO) algorithm is a reasonable method for solving complex functions. However, this algorithm can easily fall into local minimum points and has a slow convergence speed. Using an established ontology model, the third paper entitled

✉ Ilsun You
isyou@sch.ac.kr

Jin Li
jinli71@gmail.com

[1] Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea

[2] Guangzhou University, Guangzhou, People's Republic of China

"Particle Swarm Optimization Algorithm Based on Ontology Model to Support Cloud Computing Applications" by Zhang et al. (2015b) proposed a framework and two novel PSO algorithms. The ontology model is introduced with various types of operators to the cooperation framework. In contrast with the traditional algorithms, the proposed algorithms include semantic roles and concepts to update crucial parameters based on the cooperation framework. Using function optimization problems as examples, the experiments show that the particle swarm algorithms within their framework are superior to other classical algorithms.

The fourth paper entitled "Multi-segment and Multi-stage Projected Tetrahedra" by Li and Liu (2015) presented an approach which partitions datasets into multiple segments in space, and divided the visualizing procedure into multiple stages in time. Multiple segments help sorting in parallel without write access violations, while multiple stages can satisfy different requirements and increase users' cognition. Cloud computing can help this process because the datasets are large and the sorting is complex.

The fifth paper entitled "Security Framework for RESTful mobile cloud computing Web Services" by Alshahwan et al. (2015) investigated the security aspects of a system for complex mobile Web service provisioning. The authors characterized the security requirements of the individual components, and presented a security framework which provides authentication and confidentiality between the clients and the mobile hosts. The proposed solution is based on the use of existing security protocols between the clients and the mobile hosts as well as a key management protocol between the individual mobile hosts. This is implemented using an out-of-band key exchange which is simple in practice, flexible and secure.

Currently, Vehicular cloud computing is a technological paradigm shift which takes advantage of cloud computing to provide vehicles with useful computational resources and services on the roads. The advancement in the smart vehicles and the information technologies motivate researchers and industries to pay attention to the combination of vehicular network with the cloud computing. For this, the sixth paper entitled "Pseudonymous Authentication for Secure V2I Services in Cloud-based Vehicular Networks" by Park et al. (2015) proposed an anonymous vehicle-to-infrastructure cloud access management system in which identity and location privacy of service requesting vehicles are prevented not only from a global eavesdropper but also from a single system management entity. The authors devised pseudonymous service access tokens for vehicles and RSU-local revocation mechanism to reduce the size of revocation list containing revoked pseudonyms.

The seventh paper entitled "Performance Analysis of Object Recognition and Tracking for The Use of Surveillance System" by Ahn and Lee (2015) presented a robust object recognition and tracking method, which uses an advanced feature matching in real time environment. Their algorithm recognizes an object using invariant features, and reduces the dimension of a feature descriptor to deal with the problems.

The eighth paper entitled "Public Key Encryption Secure Against Related-key Attacks and Key-leakage Attacks from Extractable Hash Proofs" by Hu et al. (2015) proposed a method to construct the public key encryption schemes which is secure against both weak key-leakage attacks and affine related-key attacks directly from extractable hash proof systems. Specifically, the authors first added Key Homomorphism and Fingerprinting properties to all-but-one (ABO) extractable hash proofs, and then, constructed a key encapsulation mechanism (KEM) scheme for security against related-key attacks. Thus, public key encryption scheme secures system against related-key attacks. Also, the authors proved that if the ABO-extractable hash proof with Key Homomorphism and Fingerprinting properties is weak leakage-resilient, then the key encapsulation mechanism scheme constructed from it is also weak leakage-resilient. Moreover, the authors proposed a public key encryption scheme to secure against affine related-key attacks based on the lattice.

The ninth paper entitled "A Secure Group-based Mobile Chat Protocol" by Chen et al. (2016) proposed a secure group-based mobile chat (SG-MC) scheme and presented its associated requirements. The scheme is implemented to provide mutual authentication, and prevents the password guessing attack and the undetectable on-line password guessing attack. The scheme could prevent the password-based authentication, and provide the password based key agreement (AKA) with easy to remember characteristics.

Finally, the tenth paper entitled "Automated Design, Verification and Testing of Secure Systems with Embedded Devices based on Elicitation of Expert Knowledge" by Desnitsky and Kotenko (2016) proposed an approach for the identification of an embedded security and its subsequent use in automated design, verification and testing tools for securing IoT systems. This paper encompasses the core elements of the proposed technique, namely, security component configuring, revelation of implicit conflicts, verification of network information flows, and abnormal data from sensors. The domain specific analysis of the embedded security is also described. Further, the authors presented the revealed expert knowledge which is used for configuration, verification, and testing of embedded devices.

We hope that the ten papers presented in this special issue will make a significant contribution to academic researchers, industry professionals, students, and all the interested readers of this subject, working to extend their

knowledge in the areas of security and privacy techniques in mobile cloud computing.

Finally, we would also like to express our sincere appreciation and thanks to all the authors for their valuable contributions. Our special thanks go to the editorial board for this special issue, journal staff and Professor Vincenzo Loia, editor-in-chief of the Journal of Ambient Intelligence and Humanized Computing, for this kind invitation to organize this issue and the great support provided by them throughout the entire publication processes.

References

Ahn H, Lee YH (2015) Performance analysis of object recognition and tracking for the use of surveillance system. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0325-4

AlShahwan F, Faisal M, Ansa G (2015) Security framework for RESTful mobile cloud computing web services. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0308-5

Chen HC, Mao CH, Lin YT, Kung TL, Weng CE (2016) A secure group-based mobile chat protocol. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-016-0368-1

Desnitsky V, Kotenko I (2016) Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-016-0371-6

Hu C, Liu P, Guo S (2015) Public key encryption secure against related-key attacks and key-leakage attacks from extractable hash proofs. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0329-0

Li X, Liu X (2015) Multi-segment and multi-stage projected tetrahedra. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0271-1

Park Y, Sur C, Rhee KH (2015) Pseudonymous authentication for secure V2I services in cloud-based vehicular networks. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0309-4

Tunc C, Hariri S (2015) CLaaS: cybersecurity lab as a service. J Internet Serv Inf Secur 5(4):41–59

Vazquez C, Krishnan R, John E (2015) Time series forecasting of cloud data center workloads for dynamic resource provisioning. J Wirel Mob Netw Ubiquitous Comput Dependable Appl 6(3):87–110

Xu J, Zhou F, Jiang Z, Xue R (2015) Dynamic proofs of retrievability with square-root oblivious RAM. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0258-y

Zhang M, Wu L, Wang XA, Yang X (2015a) Unidirectional IBPRE scheme from lattice for cloud computation. J Ambient Intell Humaniz Comput. doi: 10.1007/s12652-015-0260-4

Zhang C, Yang Y, Du Y, Ma C (2015b) Particle swarm optimization algorithm based on ontology model to support cloud computing applications. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-015-0262-2