Accepted Manuscript

Title: Secure attribute-based data sharing for resource-limited users in cloud computing

Author: Jin Li, Yinghui Zhang, Xiaofeng Chen, Yang Xiang

PII: S0167-4048(17)30162-1
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2017.08.007
Reference: COSE 1187

To appear in: *Computers & Security*

Received date: 9-1-2017
Revised date: 25-7-2017
Accepted date: 14-8-2017

Please cite this article as: Jin Li, Yinghui Zhang, Xiaofeng Chen, Yang Xiang, Secure attribute-based data sharing for resource-limited users in cloud computing, *Computers & Security* (2017), http://dx.doi.org/doi: 10.1016/j.cose.2017.08.007.

Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing

Jin Li[a,*], Yinghui Zhang[b,c,d,*], Xiaofeng Chen[e], Yang Xiang[f]

[a]*School of Computer Science, Guangzhou University, Guangzhou, China*

[b]*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*

[c]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*

[d]*Westone Cryptologic Research Center, Beijing 100070, China*

[e]*State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, China*

[f]*School of Information Technology, Deakin University, Australia*

Abstract

Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing fine-grained data sharing, attribute-based encryption (ABE) has drawn wide attentions. However, most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieving fine-grainedness, high-efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. This paper addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing. The proposed scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public ciphertext test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate ciphertexts. For the sake of data security, a Chameleon hash function is used to generate an immediate ciphertext, which will be blinded by the offline ciphertexts to obtain the final online ciphertexts. The proposed scheme is proven secure against adaptively

*Corresponding authors.
Email addresses: lijin@gzhu.edu.cn (Jin Li), yhzhaang@163.com (Yinghui Zhang), xfchen@xidian.edu.cn (Xiaofeng Chen), yang@deakin.edu.au (Yang Xiang)