Privacy preserving cloud data auditing with efficient key update

Yannan Li, Yong Yu, Bo Yang, Geyong Min, Huai Wu

PII: S0167-739X(16)30298-9
DOI: http://dx.doi.org/10.1016/j.future.2016.09.003
Reference: FUTURE 3151

To appear in: *Future Generation Computer Systems*

Received date: 1 June 2016
Revised date: 3 September 2016
Accepted date: 7 September 2016

Privacy Preserving Cloud Data Auditing with Efficient Key Update*

Yannan Li[a], Yong Yu[a,b,*], Bo Yang[b], Geyong Min[a], Huai Wu[a]

[a] *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China.*
[b] *School of Computer Science, Shaanxi Normal University, Xi'an 710062, China.*

Abstract

Data integrity is extremely important for cloud based storage services, where cloud users no longer have physical possession of their outsourced files. A number of data auditing mechanisms have been proposed to solve this problem. However, how to efficiently update a cloud user's secret auditing key as well as the authenticators those keys are associated with when the digital certificate expires in the PKI system is a critical issue. In this paper, we propose a key-updating and authenticator-evolving mechanism with zero-knowledge privacy of the stored files for secure cloud data auditing, which incorporates zero knowledge proof systems, proxy re-signatures and homomorphic linear authenticators. We instantiate our proposal with the state-of-the-art Shacham-Waters auditing scheme. When the cloud user needs to update his key, instead of downloading the entire file and re-generating all the authenticators, the user can simply download one single file tag, work out a re-signing key with the new private key and upload the new file tag together with some verification information to the cloud server, in which the user undertakes the least amount of the workload in the updating phase. This approach dramatically reduces the communication and computation cost while maintaining the desirable security. We formalize the security model of zero knowledge data privacy for auditing schemes in the key-updating context and prove the soundness and zero-knowledge privacy of the proposed construction. Finally, we develop a prototype implementation of the protocol which demonstrates the practicality of the proposal.

Keywords: Cloud storage, Data integrity, Key update

1. Introduction

Cloud storage, which enables cloud users to move their data from local storage systems to the cloud, is an important service offered by cloud computing

[*] Corresponding author.
Email address: yuyong@uestc.edu.cn (Yong Yu)
*A short version of this paper appeared at ACISP2016[43].