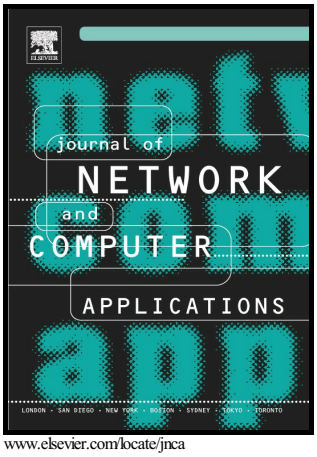
Light-Weight and Privacy-Preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium

Wenting Shen, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu, Rong Hao



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30021-8
DOI: http://dx.doi.org/10.1016/j.jnca.2017.01.015
Reference: YJNCA1831

To appear in: *Journal of Network and Computer Applications*

Received date: 27 July 2016
Revised date: 18 December 2016
Accepted date: 15 January 2017

Cite this article as: Wenting Shen, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu and Rong Hao, Light-Weight and Privacy-Preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2017.01.015

Light-Weight and Privacy-Preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium

Wenting Shen[1], Jia Yu[1,2*], Hui Xia[1], Hanlin Zhang[1], Xiuqing Lu[1] and Rong Hao[1]

[1]College of Computer Science & Technology, Qingdao University

Qingdao, 266071, China

[2]School of Computer and Software, Nanjing University of Information Science & Technology,

210044 Nanjing, China

[e-mail: qduyujia@gmail.com]

Abstract. To verify the integrity of cloud data, many cloud storage auditing schemes have been proposed. However, most of them incur a lot of computation overhead for users when data authenticators are generated or the data integrity is verified, which inevitably brings in heavy burdens to resource-constrained users. To overcome this problem, we propose a cloud storage auditing scheme for group users, which greatly reduces the computation burden on the user side. In our scheme, we introduce a Third Party Medium (TPM) to perform time-consuming operations on behalf of users. The TPM is in charge of generating authenticators for users and verifying data integrity on behalf of users. In order to protect the data privacy against the TPM, we blind data using simple operations in the phase of data uploading and data auditing. The user does not need to perform time-consuming decryption operations when using cloud data. We set an expiration time of the authorization to make sure only the TPM who possesses the authorization within valid period is able to upload data to the cloud and challenge the cloud data. The security proof and the performance analysis show that our proposed scheme is secure and efficient.

Keywords: Cloud storage; Cloud storage auditing; Privacy preserving; Data security

1. Introduction

The cloud computing incurs some new security issues, for example, integrity checking for cloud data [1, 2], the keyword search over encrypted cloud data [3-5], etc. Cloud storage auditing is used to verify the integrity of cloud data. This periodic cloud storage auditing task can be performed by users, but it incurs a lot of computation overhead for the resource-constrained users. In order to ensure the integrity of cloud data and save users' computation resources, the Third Party Auditor (TPA) which has better expertise and capability than users is introduced. The TPA can help the user to verify the integrity of cloud data, which is referred to as public cloud storage auditing.

Recently, a number of public cloud storage auditing schemes [6-21] have been proposed. These schemes mainly focus on several different aspects of cloud storage auditing. In the process of public cloud storage auditing, if the TPA is malicious or pretended, it may be arbitrarily challenge cloud data without the user's permission, which might cause the cloud spending a lot of computation resources in responding to these auditing challenges. To

* Corresponding author: qduyujia@gmail.com