Accepted Manuscript

Remote data possession checking with privacy-preserving authenticators for cloud storage

Wenting Shen, Guangyang Yang, Jia Yu, Hanlin Zhang, Fanyu Kong, Rong Hao

PII: S0167-739X(16)30493-9
DOI: http://dx.doi.org/10.1016/j.future.2017.04.029
Reference: FUTURE 3431

To appear in: *Future Generation Computer Systems*

Received date: 30 October 2016
Revised date: 15 March 2017
Accepted date: 15 April 2017

Please cite this article as: W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, R. Hao, Remote data possession checking with privacy-preserving authenticators for cloud storage, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.04.029

Remote Data Possession Checking with Privacy-Preserving Authenticators for Cloud Storage

Wenting Shen[1], Guangyang Yang[1], Jia Yu*[1,2,3], Hanlin Zhang[1], Fanyu Kong[4], and Rong Hao[1]

[1]College of Computer Science and Technology, Qingdao University, 266071 Qingdao, China

[2]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093

[3]School of Computer and Software, Nanjing University of Information Science & Technology, 210044 Nanjing, China

[4] Institute of Network Security, Shandong University, 250100 Jinan, China

Abstract. As a convenient and economical data storage solution, cloud storage has been widely adopted in recent years. For cloud storage users, how to guarantee data integrity is one of the biggest concerns. Remote data possession checking schemes are proposed to address this problem. Nonetheless, the existing approaches do not consider the privacy of authenticators, which sometimes may bring financial loss to users. In this paper, we propose a new paradigm named remote data possession checking with privacy-preserving authenticators for cloud storage. In this new paradigm, both cloud service provider and the public verifier do not have access to the real authenticators (signatures) for cloud data. Meanwhile, the integrity of cloud data is still able to be efficiently checked. It is potentially useful in some special situations where electronic checks and contracts are outsourced. To securely protect the privacy of the authenticator, we design a new authenticator called Homomorphic Invisible Authenticator (HIA), which protects the privacy of authenticator and supports the blockless verification. Based on HIA, we construct the first remote data possession checking scheme with privacy-preserving authenticators for cloud storage. To evaluate the security and efficiency of our proposed scheme, we conduct both theoretical analysis and simulation experiments. The results show that our proposed paradigm is secure and efficient.

Keywords: Cloud Storage; Data Possession Checking; Privacy Preserving; Homomorphic Invisible Authenticator

1. Introduction

Cloud storage has greatly changed the way people deploy their data storage in recent years. Unlike traditional storing solutions, the cloud provides enormous storage as service, which benefits users tremendously [1, 2]. By using the cloud, users can outsource their data into the cloud without concerning the data storage and maintenance. Organizations and individuals are inclined to employ the cloud storage service and take advantage of the efficient and economical nature of the cloud. Meanwhile, users can still efficiently complete data search over encrypted cloud data by symmetric searchable encryption

Users, however, no longer physically possess these data once they store their data into the cloud. Data corruption incidents indicate that even the most powerful cloud service providers are not absolutely reliable [3, 4, 5]. This brings data security concerns to cloud users. To efficiently check the data possession, researchers have come up with several solutions, such as Provable Data Possession (PDP) [6] and Proof of Retrievability (PoR) [7]. In the existing data possession checking schemes, an outsourced data file needs to be preprocessed in the form of blocks, and

* Corresponding author: qduyujia@gmail.com