# Accepted Manuscript


DIPOR: An IDA-based dynamic proof of retrievability scheme for cloud storage systems

Anmin Fu, Yuhan Li, Shui Yu, Yan Yu, Gongxuan Zhang

PII: S1084-8045(17)30403-4

DOI: 10.1016/j.jnca.2017.12.007

Reference: YJNCA 2027

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

Received Date: 10 July 2017

Revised Date: 24 November 2017

Accepted Date: 6 December 2017

Please cite this article as: Fu, A., Li, Y., Yu, S., Yu, Y., Zhang, G., DIPOR: An IDA-based dynamic proof of retrievability scheme for cloud storage systems, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2017.12.007.

# DIPOR: An IDA-based Dynamic Proof of Retrievability Scheme for Cloud Storage Systems[#]

Anmin Fu[a,b], Yuhan Li[a], Shui Yu[c], Yan Yu[a], and Gongxuan Zhang[a]

[a]School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China;

[b]Guizhou Provincial Key Laboratory of Public Big Data, GuiZhou University, Guiyang, 550025, China;

[c] School of Information Technology, Deakin University, Melbourne VIC 3125, Australia.

**Abstract**: As cloud storage has become more and more ubiquitous, there are a large number of consumers renting cloud storage services. However, as users lose direct control over the data, the integrity and availability of the outsourced data become a big concern for users. Accordingly, how to verify the integrity of stored data and retrieve the availability of the corrupted data has become an urgent problem. Moreover, in most cases, users' data is not always static, but needs to be updated. In this paper, we propose a dynamic proof of retrievability scheme for cloud storage system, named as DIPOR. The DIPOR not only can retrieve the original data of corrupted blocks by using partial healthy data stored in healthy servers, but also support for updating operations of data. Furthermore, the number of forks in our scheme is not fixed, which means we can always look for the optimal forks based on the number of data blocks. In addition, the security analysis indicates that our scheme is provably secure and the performance evaluations show the efficiency of the proposed scheme.

**Keywords:** Cloud Storage; Proof of Retrievability; Dynamic; IDA algorithm.

## 1 Introduction

In the era of big data, cloud storage system has become a focus as the continuous development of cloud computing. For big data, cloud storage system brings many benefits, such as reducing hardware cost, releasing local storage burden, supporting remote access. Nevertheless, cloud storage brings corresponding threats while providing users with conveniences. Highly centralized computing resources make the cloud storage face serious security challenges [1].

As users employing cloud storage system, the remote data may suffer peeping, modifying, or damaging by cloud computing providers or some other adversaries. In general, the confidentiality of data is ensured by data encryption, anonymous or other mechanisms. But when using cloud storage, users may not save any copies of remote data locally, which results in no guarantee for the security of stored data. Thus, how to assure the integrity and availability of outsourced data has become a key issue in cloud storage.

To solve that problem, a large number of methods have been proposed [2-29]. The research of cloud storage data integrity is mainly focused on Provable Data Possession (PDP) and Proof of Retrievability (POR), where the original models of these two researches are constructed by Ateniese *et al.* [2] and Juels *et al.* [3], respectively. PDP schemes [2, 4-21] can support for the data integrity checking, but not for the retrieving of corrupted data, which can be achieved in POR schemes [3, 22-29]. Although some of these schemes call as POR, we cannot find a definite solution for retrieving. Some of POR schemes only carry on privacy verification, which has a fault for public verification. Only a small part of POR

[#]This work is supported by National Science Foundation of China (61572255), the Six talent peaks project of Jiangsu Province China (XYDXXJS-032), the Open Project Program of the Guizhou Provincial Key Laboratory of Public Big Data (2017BDKFJJ031).