

Accepted Manuscript

A Fair Data Access Control towards Rational Users in Cloud Storage

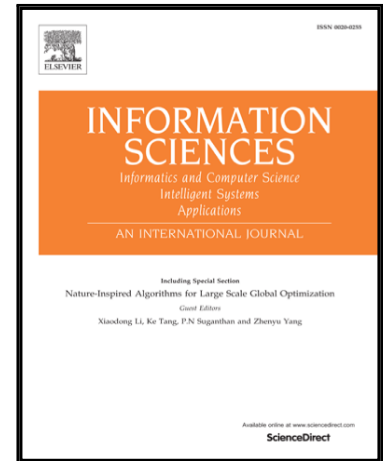
Hai Liu, Xinghua Li, Mengfan Xu, Ruo Mo, Jianfeng Ma

PII: S0020-0255(17)30289-X
DOI: [10.1016/j.ins.2017.07.023](https://doi.org/10.1016/j.ins.2017.07.023)
Reference: INS 12989

To appear in: *Information Sciences*

Received date: 23 January 2017
Revised date: 21 June 2017
Accepted date: 14 July 2017

Please cite this article as: Hai Liu, Xinghua Li, Mengfan Xu, Ruo Mo, Jianfeng Ma, A Fair Data Access Control towards Rational Users in Cloud Storage, *Information Sciences* (2017), doi: [10.1016/j.ins.2017.07.023](https://doi.org/10.1016/j.ins.2017.07.023)



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

A Fair Data Access Control towards Rational Users in Cloud Storage

Hai Liu^{a,b}, Xinghua Li^{a,b,*}, Mengfan Xu^{a,b}, Ruo Mo^{a,b}, Jianfeng Ma^{a,b}

^aState Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China

^bSchool of Cyber Engineering, Xidian University, Xi'an, 710071, China

Abstract

In cloud storage, many encrypted data are inaccessible unless several users are simultaneously present. However, when directly adopting the existing rational secret sharing schemes, it is difficult to achieve a fair key reconstruction, which leads that none of the users sends their shares and no one can access the shared data. To address this problem, this paper introduces an incentive exchange mechanism into rational secret sharing, and proposes a fair data access control scheme for cloud storage. In the proposed scheme, a large number of fake keys are generated to obfuscate the decryption key of the shared data. During the exchange of shares, a user is required to first send his/her shares when he/she deviates from the prescribed scheme. This punishes the users' selfish behaviors and incentivizes them to access the shared data together. Theoretical analysis shows that, in the proposed scheme, the Nash equilibrium is that all the users always send their shares, enabling them to reconstruct the decryption key fairly. Additionally, extensive experiments demonstrate that the proposal can control data access policies efficiently.

Keywords: cloud storage, data sharing, access control, rational users, fairness

1. Introduction

Because cloud storage services not only provide cheaper and on-demand storage resources but also require less hands-on management, increasing num-

*corresponding author

Email address: xhli1@mail.xidian.edu.cn (Xinghua Li)

Download English Version:

<https://daneshyari.com/en/article/4944219>

Download Persian Version:

<https://daneshyari.com/article/4944219>

[Daneshyari.com](https://daneshyari.com)