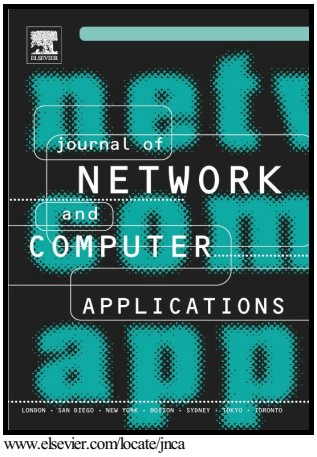
Blcokchain-Based Publicly Verifiable Data Deletion Scheme for Cloud Storage

Changsong Yang, Xiaofeng Chen, Yang Xiang



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30391-0
DOI: https://doi.org/10.1016/j.jnca.2017.11.011
Reference: YJNCA2014

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

Received date: 12 May 2017
Revised date: 31 August 2017
Accepted date: 28 November 2017

Cite this article as: Changsong Yang, Xiaofeng Chen and Yang Xiang, Blcokchain-Based Publicly Verifiable Data Deletion Scheme for Cloud Storage, *Journal of Network and Computer Applications,* https://doi.org/10.1016/j.jnca.2017.11.011

Blcokchain-Based Publicly Verifiable Data Deletion Scheme for Cloud Storage

Changsong Yang[a], Xiaofeng Chen[a,*], Yang Xiang[a,b]

[a] *State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, P.R. China*
[b] *Digital Research & Innovation Capability Platform, Swinburne University of Technology, Hawthorn, Australia*

Abstract

With the rapid development of cloud storage, more and more data owners store their data on the remote cloud, that can reduce data owners' overhead because the cloud server maintaining the data for them, e.g., storing, updating and deletion. However, that leads to data deletion becomes a security challenge because the cloud server may not delete the data honestly for financial incentives. Recently, plenty of research works have been done on secure data deletion. However, most of the existing methods can be summarized with the same protocol essentially, which called "one-bit-return" protocol: the storage server deletes the data and returns a one-bit result. The data owner has to believe the returned result because he cannot verify it. In this paper, we propose a novel blockchain-based data deletion scheme, which can make the deletion operation more transparent. In our scheme, the data owner can verify the deletion result no matter how malevolently the cloud server behaves. Besides, with the application of blockchain, the proposed scheme can achieve public verification without any trusted third party.

Keywords: Cloud Storage, Secure Deletion, Blockchain, Public Verification.

*Corresponding author
Email address: xfchen@xidian.edu.cn (Xiaofeng Chen)