Accepted Manuscript

Secure data deduplication using secret sharing schemes over cloud

Priyanka Singh, Nishant Agarwal, Balasubramanian Raman

PII: S0167-739X(17)32747-4
DOI: https://doi.org/10.1016/j.future.2018.04.097
Reference: FUTURE 4197

To appear in: *Future Generation Computer Systems*

Received date : 27 November 2017
Revised date : 12 March 2018
Accepted date : 29 April 2018

Please cite this article as: P. Singh, N. Agarwal, B. Raman, Secure data deduplication using secret sharing schemes over cloud, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.04.097

Secure data deduplication using secret sharing schemes over cloud

Priyanka Singh[a], *Nishant Agarwal*[b], *Balasubramanian Raman*[c]

[a]*Department of Computer Science, Dartmouth College, New Hampshire, USA*
[b]*Department of Computer Science, Viterbi School of Engineering, University of Southern California, USA*
[c]*Department of Computer Science and Engineering, Indian Institute of Technology at Roorkee, Uttarakhand, INDIA*

Abstract

Data deduplication has become an integral part of managing repositories of outsourced data to the cloud data centers. However, centralized data centers face issues of data loss and accessibility if something goes faulty as deduplication maintains just a unique copy of the content. Secure data deduplication exploits convergent encryption to perform data deduplication in encrypted domain. However, managing convergent keys provides a single point of vulnerability and overhead problems. Towards this end, we propose a secure data deduplication scheme that formally addresses the problems of fault tolerance, efficient and reliable key management, data confidentiality by obfuscation of outsourced information and integrity check at the user's end prior to downloading via computation of authentication codes. Data is distributed into random looking shares based on Permutation ordered binary (POB) number system at multiple servers and is further made secure via the notion of proof of ownership (PoW) concept. Also, key overhead is minimized using Chinese Remainder Theorem (CRT) based secret sharing. The efficacy of the proposed scheme has been demonstrated by the experimental results and security analysis validates its suitability with respect to various attacks in real time scenarios.

Keywords: Data deduplication, Permutation ordered binary (POB) number system, Chinese Remainder Theorem (CRT)