Accepted Manuscript

Two-factor authentication for trusted third party free dispersed storage

Ertem Esiner, Anwitaman Datta

PII: S0167-739X(17)32285-9
DOI: https://doi.org/10.1016/j.future.2018.08.001
Reference: FUTURE 4385

To appear in: *Future Generation Computer Systems*

Received date : 6 October 2017
Revised date : 2 April 2018
Accepted date : 1 August 2018

Please cite this article as: E. Esiner, A. Datta, Two-factor authentication for trusted third party free dispersed storage, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.08.001

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.

ACCEPTED MANUSCRIPT

Two-factor authentication for trusted third party free dispersed storage

Ertem Esiner, Anwitaman Datta

Nanyang Technological University, 50 Nanyang Ave, 639798

Singapore

Abstract

We propose a trusted third party free protocol for secure (in terms of content access, manipulation, and confidentiality) data storage and multi-user collaboration over an infrastructure of untrusted storage servers. It is achieved by the application of data dispersal, encryption as well as two-factor (knowledge and possession) based authentication and access control techniques so that unauthorized parties (attackers) or a small set of colluding servers cannot gain access to the stored data. The protocol design takes into account usability issues as opposed to the closest prior work [1]. We explore the security implications of the proposed model with event tree analysis and report on experiment results to demonstrate the practicality of the approach concerning computational overheads. Given that the protocol does not rely on any trusted third party, and most operations including actual collaboration do not require users to be online simultaneously, it is suitable not only for traditional multi-cloud setups but also for edge/fog computing environments.

Keywords: Layered security, two-factor access control, data out-sourcing, edge computing, user controlled encryption, erasure codes

2017 MSC: 00-01, 99-00

Email addresses: ertem001@ntu.edu.sg (Ertem Esiner), anwitaman@ntu.edu.sg (Anwitaman Datta)

ACCEPTED MANUSCRIPT

Download English Version:

https://daneshyari.com/en/article/11002394

Download Persian Version:

https://daneshyari.com/article/11002394

Daneshyari.com