Data Sharing and Self-Destruction Scheme in Cloud

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 178

Number 4

Year of Publication: 2017

Authors:
Mohammadi Kamlee, Babruvan Solunke

10.5120/ijca2017915817

Abstract

There is a huge use of cloud services in our day today life e.g. Google Drive, Dropbox, SharePoint etc. Sharing data within friends might consist of sensitive/personal information. It’s always the users responsibility to safeguard own data while sharing and avoid misuse of it. It becomes a challenge for user to protect self-data on cloud network, to overcome this scenario it is important to design and allocate self-destruct period assigned by the user and access control to the data until the expiry period. The shared data should be self-destructed after the user-defined expiration time. With the help of KPABE (Key-policy ABE) and where can apply time interval to each attribute in the form of decryption attributes. In the KP-TSABE scheme, every cipher text is labeled with a time interval while private key is associated with a time instant. Deletion of data in a secure way is the task of deleting data irrecoverably from a physical storage medium. In this digital world, data is not securely deleted by default; instead, many approaches add secure deletion to existing physical medium interfaces.

References
13. L. Zeng, S. Chen, Q. Wei, and D. Feng, “Sedas: A selfdestructing data system based on active storage framework,” 2168-7161 (c) 2013 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

Index Terms
Keywords

ABE, KP-ABE, CP-ABE, TSE, TRE, DTI, KP-STABE, Proxy Re-encryption, RBAC.