Asymmetric Secure Storage Scheme for Big Data on Multiple Cloud Providers

Title	Asymmetric Secure Storage Scheme for Big Data on Multiple Cloud Providers
Publication Type	Conference Paper
Year of Publication	2018
Authors	Suwansrikham, P., She, K.
Conference Name	2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)
Date Published	may
Keywords	asymmetric secure storage scheme, asymmetric security concept, authorisation , Big Data, big data file, big data privacy, bit data center, cloud computing, Cloud Security, cloud service, cloud storage service, cryptography, data owner, data privacy, insider attack, local storage, meta data, metadata, multiple cloud providers, multiple cloud storage provider, pubcrawl, Servers, single cloud storage, storage management, store big data, users space

Abstract

Recently, cloud computing is an emerging technology along with big data. Both technologies come together. Due to the enormous size of data in big data, it is impossible to store them in local storage. Alternatively, even we want to store them locally, we have to spend much money to create bit data center. One way to save money is store big data in cloud storage service. Cloud storage service provides users space and security to store the file. However, relying on single cloud storage may cause trouble for the customer. CSP may stop its service anytime. It is too risky if data owner hosts his file only single CSP. Also, the CSP is the third party that user have to trust without verification. After deploying his file to CSP, the user does not know who access his file. Even CSP provides a security mechanism to prevent outsider attack. However, how user ensure that there is no insider attack to steal or corrupt the file. This research proposes the way to minimize the risk, ensure data privacy, also accessing control. The big data file is split into chunks and distributed to multiple cloud storage provider. Even there is insider attack; the attacker gets only part of the file. He cannot reconstruct the whole file. After splitting the file, metadata is generated. Metadata is a place to keep chunk information, includes, chunk locations, access path, username and password of data owner to connect each CSP. Asymmetric security concept is applied to this research. The metadata will be encrypted and transfer to the user who requests to access the file. The file accessing, monitoring, metadata transferring is functions of dew computing which is an intermediate server between the users and cloud service.

DOI 10.1109/BDS/HPSC/IDS18.2018.00036

Citation Key suwansrikham_asymmetric_2018

Cloud Computing data privacy Big Data pubcrawl Cryptography Servers authorisation storage management Cloud Security meta data big data privacy asymmetric secure storage scheme asymmetric security concept big data file bit data center cloud service cloud storage service data owner insider attack local storage metadata multiple cloud providers multiple cloud storage provider single cloud storage store big data users space