Review on Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing

Foundation of Computer Science (FCS), NY, USA

Volume 139

Number 2

Year of Publication: 2016

Authors:

R. Rakesh, Anoop S.

10.5120/ijca2016909101

Abstract

An efficient cryptographic approach for data sharing where data is shared among a group of users as Data sharing is an important functionality in cloud storage. How to securely and efficiently share a collection of data related to any subject areas with others in cloud storage. Development of new novel concept of Key- Aggregate Searchable Encryption (KASE). This concept is implemented through development of a concrete key-aggregate searchable encryption framework scheme. This scheme is described as where a data owner only needs to generate and distribute a single aggregate key to a data user for sharing a large number of documents and on the other side user only needs to submit a single aggregate trapdoor to the cloud server, so that he/she can query over the shared documents by the help of generated single aggregate trapdoor. This proposed scheme is perfectly more secure and practically efficient. It is an effective method which is considered as best solution to build a practical data sharing system based on public cloud storage. A detailed review of various methods used for data access controls and encryption is presented and a brief comparison among the discussed methods is given.
References


Keywords

Cloud Storage Provider, Outsourcing, Attribute based Encryption, Key-Aggregate Cryptosystem