Abstract

Cloud is being used by different type of users to fulfil their storage needs and sharing requirements. Public cloud storage provides virtually unlimited capacity to its users for sharing encrypted data. The main challenge is to design the encryption scheme which is efficient in management of encryption keys. Numbers of keys are required in the sharing of group data scenario as well as it needs to distribute those keys in secure manner to the user and user has to store them securely again. Also user needs to create equally large number of trapdoors with keywords to access data. This project gives solution on this problem by providing a concrete scheme of key aggregate searchable encryption. In this, data owner needs to distribute a single key for sharing large number of documents and user required to submit a single trapdoor to the cloud for downloading multiple documents over the cloud. It also provides a solution for a situation where user searches for the documents shared by multiple owners and user needs to generate multiple trapdoors. In the proposed system, user needs to generate a single trapdoor for searching the files shared by multiple data owners.
References

1. Baojiang Cui, Zheli Liu and Lingyu Wang, “Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage”, IEEE transactions on computer vol. 65, No. 8, August 2016.

Index Terms

Computer Science Distributed Systems

Keywords

Cloud storage, Data privacy, Data sharing, Key aggregation, Searchable Encryption