World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:07, 2014

Searchable Encryption in Cloud Storage

Authors : Ren Junn Hwang, Chung-Chien Lu, Jain-Shing Wu

Abstract : Cloud outsource storage is one of important services in cloud computing. Cloud users upload data to cloud servers to reduce the cost of managing data and maintaining hardware and software. To ensure data confidentiality, users can encrypt their files before uploading them to a cloud system. However, retrieving the target file from the encrypted files exactly is difficult for cloud server. This study proposes a protocol for performing multikeyword searches for encrypted cloud data by applying k-nearest neighbor technology. The protocol ranks the relevance scores of encrypted files and keywords, and prevents cloud servers from learning search keywords submitted by a cloud user. To reduce the costs of file transfer communication, the cloud server returns encrypted files in order of relevance. Moreover, when a cloud user inputs an incorrect keyword and the number of wrong alphabet does not exceed a given threshold; the user still can retrieve the target files from cloud server. In addition, the proposed scheme satisfies security requirements for outsourced data storage.

Keywords : fault-tolerance search, multi-keywords search, outsource storage, ranked search, searchable encryption
Conference Title : ICICS 2014 : International Conference on Information and Computer Security
Conference Location : Singapore, Singapore
Conference Dates : July 05-06, 2014