Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 139 – 145

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Efficient Keyword Search over Encrypted Cloud Data

Anuradha Meharwade[a], G. A. Patil[b]*

[a]*Student, M.E(CSE) II, D. Y. Patil College of Engineering and Technology , Kolhapur, 416006, India.*
[b]*Head and Associate Professor of Computer Science, D. Y. Patil College of Engineering and Technology , Kolhapur, 416006, India.*

Abstract

With the advent of cloud computing, most of the data owners are outsourcing their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But sensitive data has to be encrypted before outsourcing, for protecting data privacy. However data encryption makes effective data utilization a challenging task. Traditional data utilization based keyword search on encrypted data is a difficult task. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow keyword search request and return documents in the order of their relevance to these keyword. In this paper we proposed a system that supports multi-owner keyword ranked search over the encrypted cloud data with good key management scheme. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency.

Keywords: Encryption, Keyword Search, Searchable Index.

1. Introduction

Cloud computing is emerging as a promising pattern for data outsourcing and high-quality data services. As Cloud Computing becomes prevalent, more and more sensitive information are being outsourced to the cloud, such as emails, personal health records, company finance data, and government documents, etc. Since data owners and cloud server are no longer in the same trusted domain our outsourced unencrypted data may be at risk, such as the

* Anuradha Meharwade. Tel.: +91-758-883-6767.
*E-mail address:*anuradhameharwade@gmail.com.

doi:10.1016/j.procs.2016.02.023

cloud server may leak data information to unauthorized entities or even be hacked. So for data privacy and to prevent unauthorized user accesses, sensitive data has to be encrypted prior to outsourcing. Data encryption protects data to some extent, but at the cost of compromised efficiency.

In Cloud Computing, data owners may share their outsourced data with a large number of users, who might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways to do so is through keyword-based search. Such keyword search technique allows users to selectively retrieve files of interest. Related works on searchable encryption are based on frequency of occurrence of a keyword in the document. There may be files that contain more keyword related information with less frequency of occurrence of a keyword in the document. In this paper we presented a system that considers such documents while returning files in rank order to the requesting user.

2. Related Work

A number of different mechanisms have been proposed for security aspects in cloud computing. Ranked Searchable Symmetric Encryption (RSSE) technique[1], allow users to securely search over encrypted data through keywords. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. In this scheme complete file collection is scanned and a list of keywords is selected for building searchable index, which needs lots of computation for updating the searchable index when a user upload or delete a file. Ranking of files is based on number of times the keyword appear in the file, it does not consider files which have more word related data with low rank. Practical techniques for searches on encrypted data[2] describe different practical techniques for searching on remote encrypted data using an untrusted server with their advantages and disadvantages and provide proofs of security for the resulting crypto systems. Secure indexes[3] allows a user to check whether a document contains a keyword without having to decrypt the entire document, which is very useful for searching documents from large document collections. Fuzzy keyword search over encrypted data[4] greatly enhances system usability by returning the files that exactly match the users searching input predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails.

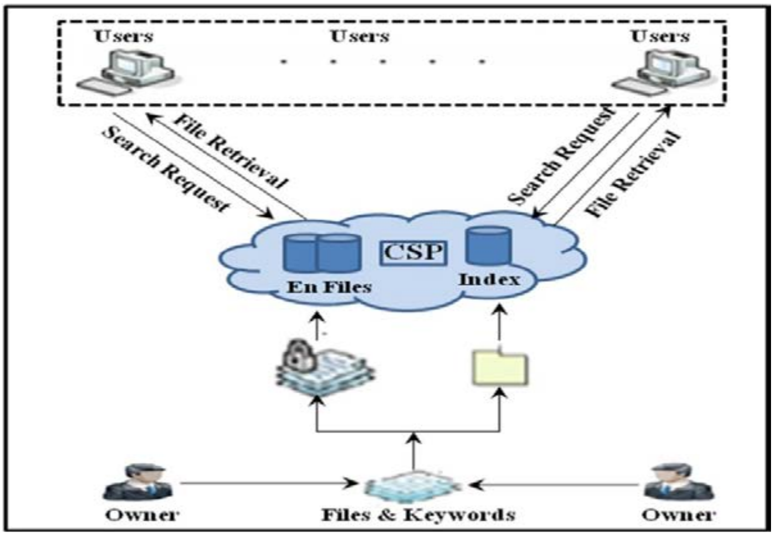

Figure 1. System Architecture.