Multikeyword Retrieval over Encrypted Data

Balamurugan P, Ramya G

Abstract—The main aim of project is data owners are motivated to outsource their complex data management systems from local sites to the cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted data search service is of paramount importance. Considering the large number of data users and documents in the cloud or server, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and sort the search results. In this process, define and solve the challenging problem of privacy preserving Multi-keyword ranked search over encrypted data. Among various multi keyword semantics, choose the efficient similarity measure of coordinate matching, as many matches as possible, to capture the relevance of data documents to the search query. Provide the data to the users in a secure manner.

Index Terms – Two round searchable encryption, searchable symmetric encryption, order preserving encryption, multi keyword search.

I. INTRODUCTION

To define and solve the problem of effective secure ranked keyword search over encrypted data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency). It makes practical deployment of privacy-preserving data hosting services in servers. The construction of ranked keyword search under the Searchable Symmetric Encryption (SSE) security definition, and demonstrate its inefficiency. The proposed solution for ranked searchable symmetric encryption provides an efficient design and performance. Thorough analysis shows that new proposed solution guarantee more security compared to previous SSE schemes. Extensive experimental result demonstrates the efficiency of the proposed solution. Web Server enables customers to store their data into the server to access the on-demand high quality applications and services from a shared pool of configurable computing resources. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria. It makes one step closer towards practical deployment of privacy-preserving data hosting services in the context of data access from server. Specifically, we explore the relevance score of each file during the establishment of searchable index before outsourcing the encrypted file collection. As directly outsourcing relevance scores will leak lots of sensitive frequency information against the keyword privacy. We then integrate a recent cryptography primitive order preserving symmetric encryption and properly modify it for our purpose to protect those sensitive information, while providing efficient ranked search functionalities.

II. PROBLEM DEFINITION

There is a difficult to encrypt all the data which are stored in server. The data can be retrieved by searchable encryption focus on single keyword search. The searchable symmetric encryption focuses on single keyword search or boolean keyword search, and rarely differentiates the search results. The problem is search without ranking in the server side and the data leaks from the server during searching. To overcome this problem the two round searchable encryption provides the multi keyword retrieval over encrypted data.

III. PROPOSED SYSTEM

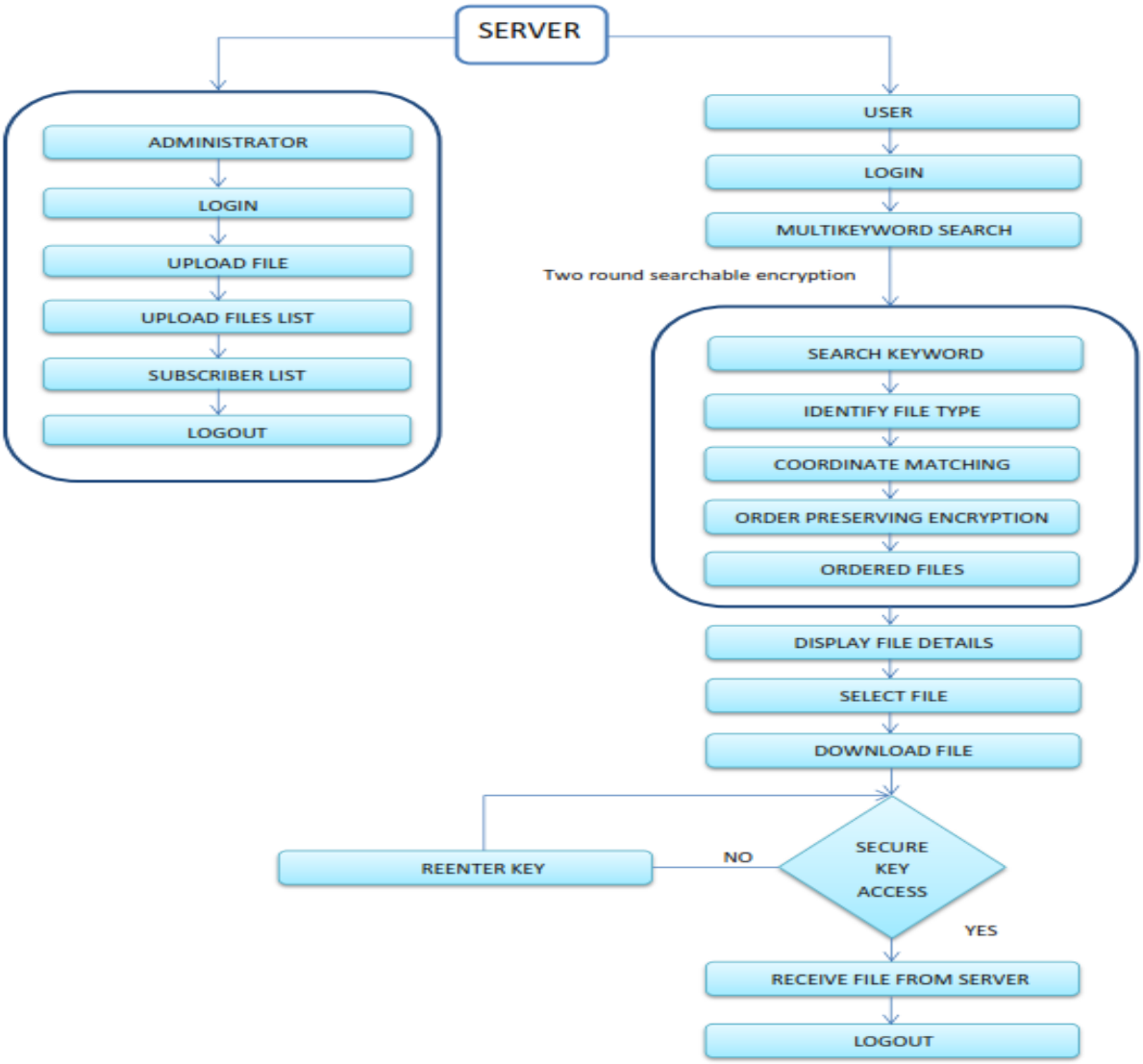
Searchable symmetric encryption allows retrieval of encrypted data over server. In this process, we focus on addressing data privacy issues using searchable symmetric encryption .We propose a two-round searchable encryption (TRSE) scheme, which fulfills the secure multi-keyword retrieval over encrypted data. Specifically, for the first time we employ relevance score to support multi-keyword retrieval. We propose server side ranking based on order-preserving encryption (OPE) inevitably violates data privacy. It purpose to retrieve overall data order wise from server. Searchable symmetric encryption schemes have been proposed to enable search on cipher text. Traditional SSE schemes enable users to securely retrieve the cipher text, but these schemes support only Boolean keyword. Thorough analysis investigating privacy and efficiency guarantees of the proposed schemes is given, and experiments on the real-world dataset further show the proposed schemes indeed introduce low overhead on computation and communication.

Manuscript Received on March 2015.

Balamurugan P, School of Information Technology and Engineering (SITE), Vellore Institute of Technology University, Vellore – 632014, Tamilnadu, India.

Ramya G, School of Information Technology and Engineering (SITE), Vellore Institute of Technology University, Vellore – 632014, Tamilnadu, India.

IV. SYSTEM ARCHITECTURE



A. Multimedia File Uploading on the Server:

In chapter number IV system architecture, the multimedia file contains all type of files. The multimedia files are uploaded to the server by the administrator. While the file is being uploaded, the browser asks periodically the server for the progress status using two tier markets. Finally when the form has been completely sent, the admin response is written in the frame, instead of the main document. It is possible to clear the file while it is being transferred. The uploaded file list can be maintained by administrator. Once the file is uploaded, it is encrypted into cipher text. It can be accessed by others in a secure manner.

B. Secure authentication service:

The user need to login or register before accessing the data from the server. The user details are stored in a database. The data which can be accessed by all type of users. But they can access the necessary information based on their user type. It is based on two-round searchable encryption scheme, which fulfills the secure multi-keyword retrieval over encrypted data. So user details are stored in secure manner. The subscriber's details are also stored in same database. It purposes is to download the packet using SSE.

C. Multi code word Process:

The two round searchable encryption supports multi keyword retrieval over encrypted data. The keywords are useful to find the file easily and quick access to the files. Among various multi keyword semantics, we choose the efficient similarity measure of coordinate matching, as many matches as possible, to capture the relevance of data documents to the search query. The TRSE also separate the files depend on the format in which the files are stored in the database.

D. Downloads files by the users:

The user request the data to server, at that time once the user selects a file the browser asks the server, and download the file. The server provides file to the user and continuous downloads with the process information.

When you download something from the server, you can keep an eye on its download progress in the download icon. When the file is done downloading, just click its button to open it. All the files you have downloaded are listed on the files.

V. SSE ALGORITHM

Searchable symmetric encryption allows retrieval of encrypted data over cloud. In this process, we focus on addressing data privacy issues using searchable symmetric encryption. Data encryption protects data security effectively. Client can upload additional "encrypted" data structures to help search. Client has a collection of documents that consists of a set of words encrypts document collection together with additional data structure sends everything to server.

VI. OBSERVATION

The data stored in the server are in encrypted form to reduce security issues. If a client wants to retrieve a document with certain search keyword, it was not sure that data will obtain by the client without any loss of data confidentiality [1]. The technique of secrecy provide for encryption, the untrusted server not know about the conversion from plaintext to cipher text. If the technique provides a controlled search, then the untrusted server won't search without user's authentication. Data owners outsource their data to third party user storage. While outsourcing the users need to trust service providers. Data stored in server can be hacked by outside attackers. But the encryption technology reduce the data from outside attackers [2].It is difficult to provide the retrieval data with single keyword query to large no of users. The search will rarely sort results to users. The solution to this problem is defining new encryption algorithm with most secure and effective access of data, that is multi keyword searchable encryption. The concept of buffer controller [3] provides a quick search of data and security. Searchable symmetric encryption allows data retrieval from server. To provide privacy and data leakage, two round searchable encryption provide multi keyword retrieval along with log file generation [5]. The homomorphic encryption provides ranking of retrieval data in server side, so the data will be secured and there is no information leakage.

VII. CONCLUSION

We define and solved the problem occurs during the retrieval of encrypted data from server. The feasibility increased by achieving quick search results by two round searchable encryption. The data can be securely retrieved to user by searchable symmetric encryption. The access of data made effective and efficient by two round searchable encryption. The order preserving encryption useful in ordering the data. According to proposed scheme the data retrieval from server is made secure in a practical proficiency.

REFERENCES

1. D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.
2. Sharad Mehrotra & Bijit Hore," A Middleware Approach for Managing Privacy of Outsourced Personal Data".
3. Suman M, B. Chempavathy, "An Approach for Efficient and Secure Retrieval of Encrypted Cloud Data Based On Top-K Multikeywords",2014.
4. Dan Boneh, Giovanni Di Crescenzo, "Public Key Encryption with Keyword Search".
5. Mrs. P. Shanmuga Priya M.E(Ph.d), Preethi.D, Priya.J, shanthini.B, "Retrieval of Encrypted Data Using Multi Keyword Top –K Algorithm",April 2014.
6. Jiadi Yu, Peng Lu, Yanmin Zhu," Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data",Aug2013.