Volume 6, Issue 9, September 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Secure and Encrypted Cloud Data with Multi-keyword Rank Search and Revocation of User

Jeniphar Francis, Ruchika Bansod, Chetna Getme, Priyanka Bagde

RTMNU, Nagpur Maharashtra India

Abstract— Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF×IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme. Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF×IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme

Keywords— Cloud computing, Encryption, Single Keyword Search, Multi-keyword search, ranking, Trapdoor, User Revocation

I. INTRODUCTION

Cloud computing is the long dream vision of computing of sources which deliver a service over a network. It also build a new resources in IT infrastructure. Various advantages of cloud services, such as e-mail, personal information, government documents, and finance data can store in cloud. Cloud basically used for storing user's data A major characteristic of cloud service is that data is usually store remotely on cloud which is not access by user. The cloud service provider(CSP)that store the data of user which is access sensitive information without authorization. To secure user data is to encrypt the data before accessing. In cloud computing, data owner can store their data in cloud which number of user's can retrieve interested data in given session on the basis of keyword-based search. Such type of keyword-based search allows user to access the files on the basis of needs which is widely used in plaintext scenario. To address above issue researchers invent some new technique to solve over encryption. Searchable encryption is used to store the encrypted data on cloud and search on basis of keyword search. To achieve various search functionality such as single keyword search ,similarity search , multi-keyword Boolean search multi-keyword ranked search.. Multi keyword ranked search is more efficient than other functionality. Recently there is use of insertion and deletion technique on cloud store data through ranked search scheme .Data owner need to update their data which is stored in cloud. To support this dynamic scheme on collection of data through multi keyword ranked search scheme which is based on tree based structure. To execute dynamic scheme vector space model and "term -frequency * inverse document frequency "models are combine together to form an index. Index is based on "Greedy Depth first Search" algorithm. In cloud system the revocation process is to be done here because when there are no longer user to access file on cloud then owner discard his authentication but the unauthorized user can trapdoor the key and used another files to solve this problem owner can rebuild the indexes of data files.

II. RELATED WORK

The proposed system concentrates over the encrypted cloud information as well as utilizes the tree-based search.

System also supports to dynamic operation and multi keyword ranked search over list of the files. The Term Frequency (TF) Inverse Document Frequency (IDF) model are combined for the query generation and index generation to provide multi keyword ranked search. This system is flexibly allows the insertion as well as deletion of files due to specific structure of tree-based index. This system consist three various entities:

1. Cloud Server
2. Data Owner
3. Data User

Data Owner has a list of files to be encrypted and stored over the cloud. User is allowed to search over this encrypted information. Data owner has responsibility of key distribution to the authorized users that is needed for file decryption. On the basis of query request for specific document from user, cloud server executes searching over the index tree and the list of encrypted top k ranked outcomes is given to user. At the end, user can decrypt the obtained files through utilizing secret key provided by owner of data.Our system gives capability such as user revocation to the data owners.

III. PROPOSED SYSTEM

1. Client

This module contains user registration as well as login with Database, Client and Server with socket programming and encrypted data by AES Encryption and transferred to client side. In Client side it is decrypted along with GUI.

2. MPPI Index creation algorithm

MPPI algorithm is implemented to generate index of every private server. Index indicates the detail explanation of data stored at private server.

3. Index combining and Upload on Cloud

Observing system has responsibility for index mixture of every private server and uploads this last merge index file over public cloud.

4. Input Query and response from public Cloud

User uploads a query to cloud server for obtaining specific information from private server and in response public cloud gives merged index.

5. User Authentication and token generation

After more obtaining index, user has to connect to private server to access the outcomes. First, user will login to the server and after accomplishing successful authentication, private server create and disperse the token to user as well as KDC.

6. Key distribution and file decryption

On the basis of authentication of tokens, KDC give the key to user and this key is used for decryption of outcomes that is collected from private server.

7. TF IDF ranking results

After authentication, user will collect the outcomes from private server is in encrypted manner. These encrypted outcomes are decrypted by implementing key received from KDC. At the end, the ranking of outcomes are created by implementing TF IDF.

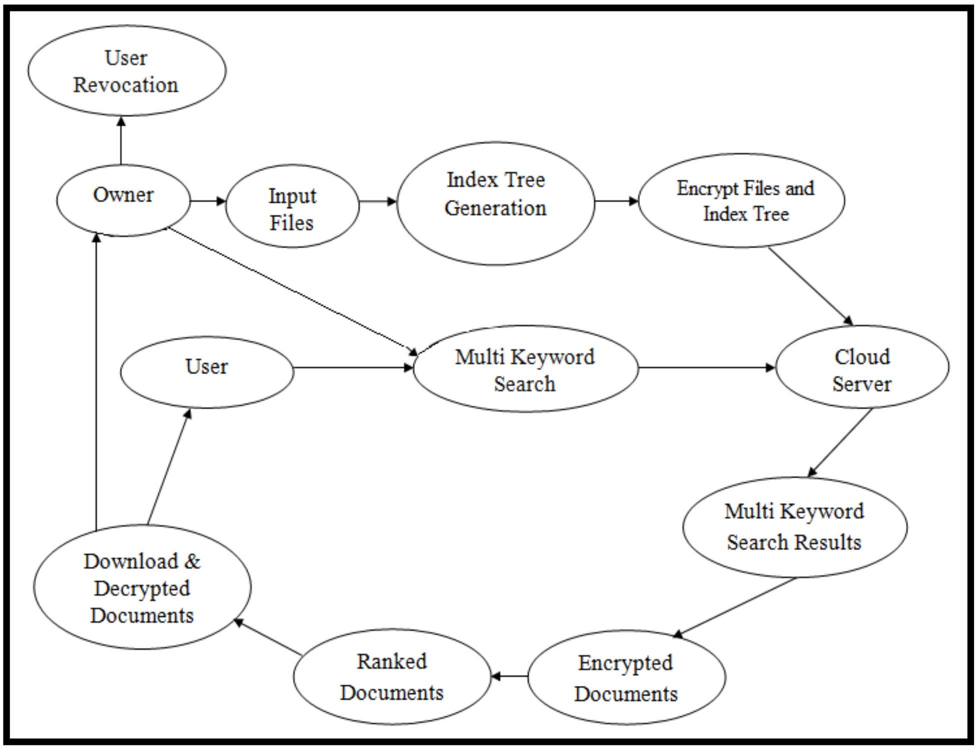

Figure 1:- Architecture of A Secure and Encrypted Cloud Data with Multi-keyword Rank Search and Revocation of User.

We analyze the BDMRS scheme according to the three predefined privacy requirements in the design goals:

1) Index Confidentiality and Query Confidentiality: In the proposed BDMRS scheme, Iu and TD are obfuscated vectors, which means the cloud server cannot infer the original vectors Du and Q without the secret key set SK. The secret keys M1 and M2 are Gaussian random matrices. According to [38], the attacker (cloud server) of COA cannot calculate the matrices merely with cipher text. Thus, the BDMRS scheme is resilient against cipher text only attack (COA) and the index confidentiality and the query confidentiality are well protected.

2) Query Unlinkability: The trapdoor of query vector is generated from a random splitting operation, which means that the same search requests will be transformed into different query trapdoors, and thus the query unlinkability is protected. However, the cloud server is able to link the same search requests according to the same visited path and the same relevance scores.

3) Keyword Privacy: In this scheme, the confidentiality of the index and query are well protected that the original vectors are kept from the cloud server. And the search process merely introduces inner product computing of encrypted vectors, which leaks no information about any specific keyword. Thus, the keyword privacy is protected in the known cipher text model. But in the known background model, the cloud server is supposed to have more knowledge, such as the term frequency statistics of keywords.

4) Revocation: It is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing.

IV. CONCLUSION

In this paper which not only support multi keyword rank search but also revocation of user and insertion and deletion file There is adequate initialization of remotely stored encrypted data in cloud computing. We build a keyword balanced binary tree as the index, and propose a “Greedy Depth-first Search” algorithm to obtain better effective linear search. The actual multi-keyword ranked search challenge, all the data is store in cloud is in encrypted format for this trapdoor generation scheme is allow to access the data. In this stage , the revocation of user is difficult. In our system it is possible in such way as the data owner have to rebuild all index of files store in cloud and provide a new secure key to all required authorized user .In our system is provide an improve secure scheme.

REFERENCES

[1] K. Ren, C. Wang, Q. Wang et al., “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[3] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, “Software protection and simulation on oblivious rams,” Journal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advance in Cryptology Eurocrypt 2004.Springer,2004 pp. 506–522.

[6] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted scloud data,” in IEEE INFOCOM, April 2011, pp. 829–837.