International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - I **ISSN (Online): 2454- 1966**

SECURE MULTI-KEYWORD TOP KEY RANKED SEARCH SCHEME OVER ENCRYPTED CLOUD DATA

Dr.B.Kalaavathi, SM.Keerthana, N.Renugadevi

Professor, Assistant professor, PGScholar
Department of Computer Science and Engineering
KSR Institute for Engineering and Technology
Kalabhuvanesh@gmail.com, Keerthi.sm18@gmail.com, renuzaa246@gmail.com

March – 2016

www.istpublications.com

SECURE MULTI-KEYWORD TOP KEY RANKED SEARCH SCHEME OVER ENCRYPTED CLOUD DATA

Dr.B.Kalaavathi, SM.Keerthana, N.Renugadevi

Professor, Assistant professor, PG Scholar
Department of Computer Science and Engineering
KSR Institute for Engineering and Technology
Kalabhuvanesh@gmail.com, Keerthi.sm18@gmail.com, renuzaa246@gmail.com

ABSTRACT

Nowadays, more and more people are motivated to outsource their local data to public cloud servers for great convenience and reduced costs in data management. Sensitive data should be encrypted before outsourcing, which obsoletes traditional data utilization like keyword-based document retrieval a secure and efficient multi-keyword ranked search scheme over encrypted data, which additionally supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used "term frequency (TF) and inverse document frequency (IDF)" model are combined in the index construction and query generation. to construct a special tree-based index structure and proposed a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. Moreover, to protect the search privacy and proposed scheme There are still many challenge problems in symmetric SE schemes. Try to improve the SE scheme to handle these challenge problems.

Keywords: *searchable encryption, encrypted cloud data, multi-keyword ranked search dynamic update.*

I. INTRODUCTION

Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications, and enable users to enjoy ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead. Attracted by these appealing features, both individuals and enterprises are motivated to outsource their data to the cloud, instead of purchasing software and hardware to manage the data themselves. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt the data before outsourcing. However, this will cause a huge cost in terms of data usability. For example, the existing techniques on keyword-based information retrieval, which are widely used on the plaintext data,cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is obviously impractical. In order to address the above problem, researchers have designed some general-purpose solutions with fully-homomorphic encryption or oblivious RAMs However, these methods are not practical due to their high computational overhead for both the cloud sever and user.

On the contrary, more practical special purpose solutions, such as searchable encryption (SE) schemes have made specific contributions in terms of efficiency, functionality and security. Searchable encryption schemes enable the client to store the encrypted data to the cloud and execute keyword search over cipher text domain. Under threat models to achieve search Functionality in multi-keyword ranked search,. Among them, multi-keyword ranked search achieves

more and more attention for its practical applicability. Recently, some dynamic schemes support inserting and deleting operations on document collection.

These are significant works as it is highly possible that the data owners need to update their data on the cloud server. But few of the dynamic schemes support efficient multi keyword ranked search. A secure tree-based search scheme. Over the encrypted cloud data, which supports multi keyword ranked search and dynamic operation on the document collection. Specifically, the vector space model and the widely-used "term frequency (TF) × inverse document frequency (IDF)" model are combined in the index construction and query generation to provide multi keyword ranked search. In order to obtain high search efficiency, construct a tree-based index structure "Greedy Depth-first Search" algorithm based on this index tree. Due to the special structure of our tree-based index, the proposed search scheme can flexibly achieve sub-linear search time and deal with the deletion and insertion of documents. 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. To resist different attacks in different threat models, construct two secure search schemes: the basic dynamic multi-keyword ranked search (BDMRS) scheme in the known cipher text model, and the enhanced dynamic multi-keyword ranked search (EDMRS) scheme in the known background model. Our contributions are summarized as follows:

1) Design a searchable encryption scheme that supports both the accurate multi-keyword ranked search and flexible dynamic operation on document collection.

2) Due to the special structure of our tree-based index, the search complexity of the proposed scheme is fundamentally kept to logarithmic. This scheme can achieve higher search efficiency by executing our "Greedy Depth-first Search" algorithm. Moreover, parallel search can be flexibly performed to further reduce the time cost of search process. There are still many challenge problems in symmetric SE schemes.to improve the SE scheme to handle these challenge problems.

II. RELATED WORK

Sun.W (2013) [5] proposed this search that provides similarity based search result ranking, keyword privacy, Index and Query confidentiality and Query Unlinkability. The encrypted file is built by vector space model supporting conjunctive and disjunctive file search. The searchable index is built using Multidimensional B tree. Owner creates encrypted query vector $\bar{Q}$ for file keyword set. User gets encrypted query vector of W from owner which is given to CS. Now CS searches index by MD algorithm and compares cosine measure of file and query vector and returns top k encrypted files to user.

Jiadi Yu (2013) [6] proposed a searching technique that uses Two- round searchable encryption (TRSE). In the first round, users submit an encrypted query to achieve privacy .The encrypted query may contain single or multiple keywords. A trapdoor is created for this query and this query is sent to the cloud server. The cloud server contains the encrypted documents and the index file. It computes the scores of documents from this index file and then returns the encrypted score result vector to user. In the second round, user decrypts the score with secret key and calculates the scores of files and then requests files with top-k scores. In this method the ranking is done on user side and computing

score is done on server side. The TRSE utilizes vector space model and homomorphic encryption. The vector space model provides sufficient search accuracy, and the homomorphic encryption allows users to participate in the ranking. The majority of computing work is done on the server side .As a result, information leakage can be eliminated and data security is ensured. The user takes part in ranking, which guarantees top-k multi-keyword retrieval over encrypted cloud data with high security and practical efficiency. This method finds a solution to the problem of secure multi-keyword top-k retrieval over encrypted cloud data. But this method suffers from high communication overhead if the encrypted trapdoor size is too large.

Wenhai Sun et al (2014) [7] proposed Verifiable Privacy-Preserving Multi-keyword Text Search search that provides multi-keyword search by similarity search based result ranking. Owner outsources encrypted document Ď using vector space model and authenticated secure index tree built using Multidimensional B- tree encrypted using RSA and SHA-1 . User submits W to owner and receives encrypted query vector Q̄ for W. The query Q̄ along with search parameter k is given to CS. Now CS searches Q̄ using MD algorithm and compares cosine measure of Ď and Q̄ and returns top k encrypted files to user. Then user searches this minimum tree using the same search algorithm as CS and verifies the query results.

Lou.w et al (2014) [8] In order to make data retrieval more effective, it is necessary to allow multiple keywords in the search request. Also to solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data, this method (MRSE) establishes a set of strict privacy requirements. Coordinate matching is used to capture the similarity between search query and documents. This method consists of Setup, Build Index, Trapdoor, Query. Setup phase uses Key Generation algorithm for generating public/private key. Build Index algorithm is used to generate index file which contains keywords from file. Both the encrypted file collection and index file is outsourced to cloud. When a user submits a query, based on some known parameters, a trap-door is generated. After receiving the trapdoor, cloud server performs a search on the index file and then finally returns the ranked list, sorted by their relevance with the user's keyword. This method chooses the efficient similarity measure of "coordinate matching" for capturing the relevance of outsourced documents with the query keywords and uses "inner product similarity" to quantitatively evaluate the similarity measure. This method proposes a basic idea of MRSE which uses secure inner product computation to support multi-keyword searching over the encrypted data.

III. EXISTING SYSTEM

Multi rank keyword search scheme is existing technique, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents and construct a special keyword balanced binary tree as the index, and existing technique was a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be carried out to further reduce the time cost. The security of the scheme is protected against two threat models by using the secure top k retrieval algorithm. Experimental results demonstrate the efficiency of our existing technique. There are still many challenge problems in symmetric SE schemes. In the existing scheme, the data owner is responsible for generating updating information and sending them to the cloud

server. Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful but difficult.

A. DISADVANTAGE

- Many challenge problems in Symmetric SE schemes.
- All the data users usually keep the same secure key.
- Revocation of the user is big challenge.
- Dishonest data user may search the documents and distribute to the unauthorized ones.

IV PROPOSED SYSTEM

Proposed scheme to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search. In addition, as the most of works about searchable encryption, our scheme mainly considers the challenge from the cloud server. Actually, there are many secure challenges in a multi-user scheme. Firstly, all the users usually keep the same secure key for trapdoor generation in a symmetric SE scheme. In this case, the revocation of the user is big challenge. If it is needed to revoke a user in this scheme, need to rebuild the index and distribute the new secure keys to all the authorized users. Secondly, symmetric SE schemes usually assume that all the data users are trustworthy. It is not practical and a dishonest data user will lead to many secure problems. For example, a dishonest data user may search the documents and distribute the decrypted documents to the unauthorized ones. Even more, a dishonest data user may distribute his/her secure keys to the unauthorized ones. Proposed scheme to improve the SE scheme to handled these challenge problems.

A ADVANTAGES

- Rebuild the index and distribute the new secure keys to all the authorized users
- Revoke of the user in this scheme
- Proposed scheme try to improve the SE scheme to handle these challenge problems.

V CONCLUSION

In this paper Searchable encryption scheme that supports both the accurate multi-keyword ranked search and flexible dynamic operation on document collection A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data. “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search Scheme. there are still many challenge problems in symmetric SE schemes. try to improve the SE scheme to handle these challenge problems. Proposed SE scheme to improve the SE scheme to handle these challenge problems. in future work to designing a more efficient search algorithm and secure scheme in enhanced threat model.

VI REFERENCES

1. Boneh.D et al, “Public key encryption with keyword search,” in *PROC. OF EUROCRYP’04, VOLUME 3027 OF LNCS*. Springer, 2004.

2. Cong Wang et al "Secure and efficient ranked keyword search over outsourced cloud data".Proc. *IEEE TRANSACTION. PARALLEL DISTRIBUTED SYSTEMS*, 23: 1467-1479,2012.
3. Jin Li et al., "Fuzzy keyword search over encrypted data in cloud computing," *in Proc. OF IEEE INFOCOM'10 MINI-CONFERENCE*, San Diego, CA, USA, 2010.
4. Jiadi Yu et al., "Toward secure multikeyword top-k retrieval over encrypted cloud ata," *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, vol. 10, 2013.
5. Lou.W et al., "Privacy-preserving multi-keyword ranked search over encrypted cloud data*," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, 2014.
6. Perrig.A et al, "Practical techniques for searches on encrypted data," in *Proc. of IEEE SYMPOSIUM ON SECURITY AND PRIVACY'00*, 2000.
7. Sun.W and Wang.B,"Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th *ACM SIGSAC SYMPOSIUM ON INFORMATION, COMPUTER AND COMMUNICATIONS SECURITY*. ACM, 2013, pp. 71–82,2013.
8. Wenhai Sun et al.,"Verifiable Privacy- Preserving Multi-keyword Text Search in the Cloud Supporting Similarity-based Ranking", Accepted for *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS (TPDS)*,2014.
9. Wang.B, S., and Hou Y. T., "Privacy-preserving multi key word fuzzy search over encrypted data in the cloud," *in IEEE INFOCOM*, 2014.
10. Wang.B, and Lou.W, "Privacy-preserving multi key word fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014.