International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | April-2016 www.irjet.net p-ISSN: 2395-0072

# *Dynamic multi-keyword rank scheme using Top key over encrypted cloud data*

M.Gomathi, M.E-II year
Department of CSE,
K.S. Rangasamy College of Technology,
Tiruchengode, Namakkal (DT).
m.gomath@gmail.com

Mr. D.Seenivasan, Assistant Professor,
Department of CSE,
K.S. Rangasamy College of Technology,
Tiruchengode, Namakkal (DT).

***Abstract-***Many data user are encouraged to outsource their data to cloud servers for great portable and reduced costs in data management which is increased popularity of cloud computing. However, sensitive data should be encrypted before outsourcing of data protection requirements, the use of data as keyword-based document obsoletes can be retrieved. It presents a secure multi-keyword search Place Scheme over encrypted cloud data that simultaneously supports dynamic update operations such as deleting and inserting documents. In particular, the vector space model and the widespread TF_IDF model aremigrated in the index evaluation and query generation. It construct a special tree-based index structure and propose a "Greedy search" code which is efficient multi-keyword search on the place and formed tree index structure. The safe kNN algorithm used to encrypt the index and query vectors, and evaluated calculation between encrypted index and query vectors for efficiency. To withstand statistical attacks are added Search results for Phantom dazzle with respect to the index vector. By using our special tree-based index structure, the proposed rule flexibly sublinear search time and deal with the deleting and inserting documents reach.

***Keyword-Multi keyword Retrieval, Cloud data, Data security***

## I. INTRODUCTION

Cloud Computing, a critical pattern for advanced data services, has to outsource a necessary feasibility for Data Users Data. Controversies on privacy, but were presented as outsourcing of sensitive information, including e-mail, medical records and personal photos unceasingly expands explosively. Reports of data loss and data breaches in cloud computing systems from time to time appear. The biggest threat to privacy roots when users outsource their private data to the cloud in the cloud itself. The cloud service providers capable of the data and the communication between the users and the cloud will, lawful or unlawful to control and monitor.

To ensure privacy, encrypt users usually the data before it brings to cloud outsourcing, the major challenges for effective data use. One of the most popular ways to do this is through keyword-based retrieval [1].Keyword-based retrieval is a typical data service and widely used in the text scenarios applied, where the users based on keywords retrieve relevant files in a file record. However, it turns out to be a difficult task in cipher text scenario, due to the limited operations on encrypted data [2] .besides to improve feasibility and save on costs in the cloud paradigm, it is preferable to the query result to obtained with the most important files in place of all the files that should point the interests of users that the files are selected in order of relevance by users' corresponding interest and only the files with the highest relevance are returned for users.

To date, efficient multi-keyword search on encrypted data remains a difficult problem. It suggests that efforts include the search on encrypted data not only information retrieval techniques such as advanced data structures used to represent the searchable index, [3] and efficient search algorithms, which lead through the corresponding data structure, but also the proper design of security protocols to ensure the safety and privacy of the entire system [4]. The blurring the keyword is detected by an innovative data structure and algorithmic design, without expanding the index and thus a high efficiency in terms the calculation and storage.

A general approach to protect the confidentiality of data is to encrypt the data prior to outsourcing. However, this is a huge cost in terms of data, the user experience lead [5].For example, the existing techniques for keyword-based information retrieval, which are often used on the plaintext data, cannot directly access the encrypted applied data. Download all data in the cloud and locally to decipher, is obviously impractical. To solve the above problem, researchers have some general purpose solutions with fully homomorphic encryption or blind Rams [11] constructed [6] .These methods are impractical due to their high computational difficulty for both the cloud Sever and users.

Flexible search sub linearly achieve by proposed scheme Search time and deal with the deleting and inserting of documents [ 7 ] .The secure kNN algorithm is used to encrypt the index and query vector , and in the meantime exact meaning score calculation between encrypted to ensure , index and query vectors [ 12 ] . To reflecting various attacks in different threat models we construct two secure search rules: dynamic Top -k Multi-keyword space search procedure in the known ciphertext model and the improved dynamic Top -k Multi- keyword space search procedure in the known background model.

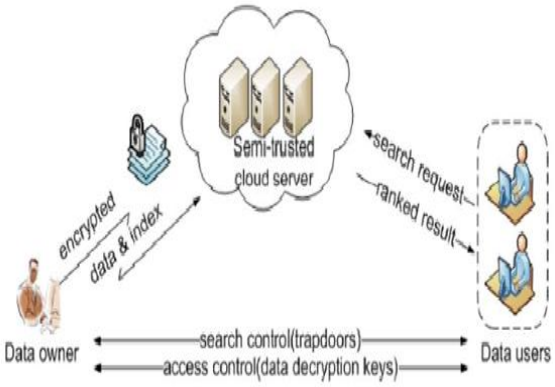


*Fig.1. Architecture diagram for Dynamic multi Keyword Ranking Search scheme*

## II PROPOSED SYSTEM

The first symmetrical searchable encryption (SSE) scheme and the search of the scheme is linear in the size of the data collection. Proposed formal security definitions for SSE and developed a system based on Bloom filter. It is proposed that two systems (SSE -1 and 2) that the optimal search time is reached. Your SSE 1 scheme is secure against attacks Chosen- Keyword (CKA1) and SSE -2 is secure against adaptive chosen- keyword attacks (CKA2). These early works are single keyword Boolean search schemes that are very simple in terms of functionality. After plenty of plants have been proposed under different threat models to search various search functions, such as single keyword search, similarity search more keyword Boolean search space and multi keyword search on place, etc. Multi - keyword Boolean search allows achieve the user to enter multiple query keywords to request appropriate documents.

Among these works, combining keyword search systems give only the documents that contain all of the query keywords. Disjunctive Keyword Schemes return all documents that contain keywords proposed [8] .Predicate search schemes a subset of the query, both connecting divisive to support search. All these schemes More Keyword retrieve search results based on the presence of keywords, which can provide not acceptable result ranking functionality [10].

Proposed guide can achieve sublinear search time flexible and deal with the deleting and inserting documents. The safe kNN algorithm used to encrypt the index and query vectors, in the meantime accurate relevancy score calculation between encrypted index and query vectors [9] .Ensure to withstand various attacks in different threat models, build two secure search systems: the dynamic top k multi- keyword search scheme selected in the known ciphertext model, and improved dynamic top k multi- keyword space search procedure in the known background model .Our contributions are summarized as follows:

1) We 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. And in practice, the proposed 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.

## III SYSTEM MODELS

Modules

Proposed system has been divided into 5 different modules. Each module has its own type of task and its implementation. 5 different modules are,

- Access Group key generation process
- User upload data Using Advanced Encryption Module
- Public Cloud Server implementation
- User Uploaded Data stored Split and store Tree Structure Module
- Data User Retrieve File to cloud Module

3.1 Access Group Key Generation Process Module

Access Key and Authentication is the process, in fact, to be determined. In private and public computer networks (the Internet), the authentication is often done through the use of logon passwords. Knowing the password is assumed to guarantee that the user is authentic. Each user initially registered (or registered by someone else), an assigned or self-declared with

password. On each subsequent use, the user must know and use the previously specified password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords are often stolen, accidentally revealed, or forgotten.

The process of authorizing an individual , usually based on a username and password in the security system which is the process of giving individuals access to system objects based on their identity authentication merely identifies that the individual is who he or she allowed to be , but says nothing about the access rights of the individual .

3.2 User Upload Data Using Advanced Encryption Module

After completing the registration phase the user wants the file to load it more files and choose to select upload option. Once the upload process can data owners to share their outsourced data with a number of users who could wish to retrieve the data files they are interested. One of the most popular ways to do this is through keyword -based Retrieval.

Keyword -based Retrieval is a one type of information service and widely used in the text scenarios applied, in which the user relevant files in a set of files to retrieve based on keywords. However, it is a difficult task in ciphertext to be scenario, by limited operations on encrypted data of the owner of the data is a collection of files n = C has {f1, f2, ..., fn} on the cloud server outsource in encrypted form, and expects the cloud server keyword retrieval service to ask yourself or other authorized users available to data subjects. To achieve this, the owner of the data has a searchable index I of a collection of l to build keywords drive W = extracted {w1, w2 ... wn} of C and outsource, then both the encrypted index I_ and encrypted files on the cloud server.

3.3 Public Cloud Server Implementation

The cloud server is considered honest in our work as "a model is used extensively by that the cloud server characterized honestly follow designed protocol hosted data and analyze the received requests to get additional information. When users their private data to outsource cloud, the cloud service providers capable of the data and the communication between the users and the cloud will, lawful or unlawful to control and monitor. Instances like the secret NSA program work, the recorded on the data to divide and should also create and splited data signatures are saved for all.

3.4 User Uploaded Data Stored Split and Store Tree Structure Module

Internet storage is a model of networked online storage, is stored in the data in virtualized storage pools that are hosted by a third party in general. Hosting companies operate large data centers, and people who need their data they host sale or lease be storage. The data center operators, in the background, virtualization resources in accordance with the requirements of the customer and using it as a storage pool to store the customers themselves, can share files or data objects. Physically, extend the resource across multiple servers. Internet storage or hosted storage that enables data storage Management solution that allows individuals or organizations to store their data on the Internet a data owner , either than storing the data locally on a physical disk , such as a hard disk or tape backup.

An increasing number of customers store their important data in remote servers in the cloud, without leaving a copy in their local computers. It can data dynamics Adapted easy to support. After uploaded files will be saved with the security in the cloud, the uploaded file. The guarantee shall be provided with combined encryption algorithm available.

3.5 Data User Retrieve File to Cloud Module

If the user wants to load the file device, you must check with the public verifiability process. To alleviate the computational load on the user side, raking should be on the server side, so we need to ensure an encryption scheme with the functioning and security at the same time on the server side. Advanced Encryption Scheme, certain types of calculations are performed on the corresponding ciphertext.

The result is performed on the clear text of the ciphertext of the result of operations. That is, advanced encryption scheme made light without knowing the calculation of ciphertext on the plaintext to obtain the proper encrypted result. Although it has such a beautiful property, originally fully advanced encryption scheme, the ideal lattice has over a polynomial ring is too difficult and not use for efficient manner. Therefore, we can reduce the original homomorphism in a complete form in a simplified form that only supports integer operations that does more efficiency than the full form allows.

## IVRESULTS AND DISCUSSION

The proposed scheme, data users can achieve different requirements on search precision of privacy by the standard deviation of adjustment that can be treated as a compensation parameter. The comparison of systems with a recent work that achieves high search efficiency. BDMRS scheme calls the search results by exact calculation of document vector and query vector. Thus, top- k search accuracy of BDMRS scheme is 100 %. But based and similarity Multi- keyword square search pattern, the basic scheme in suffering from loss of precision due to the accumulation of sub-vectors with the index construction . The test is repeated 16 times, and the average accuracy of 91 %. During the search, when the relevance of the node is greater than the minimum relevance in results Rlist, examines the cloud server, the children of the node; otherwise it returns. So many nodes not accessed during a real search. We denote the number of leaf nodes that contain one or more keywords in the query. It is generally greater than the number of documents required k, but far less than the cardinality of the document collection n. As a balanced binary tree, the height of the index n is log will be maintained, and the complexity of the calculation is ranked relevance O (m).

## V.CONCLUSION

Multi rank keyword search scheme is proposed, which not only supports true multi-keyword search on space, but also the dynamic deletion and insertion of documents. We build a special keyword balanced binary tree as the index. In addition, the search process may be performed in parallel to reduce the time, cost. The security of the system is protected against two threat models through secure top-k retrieval algorithm. The experimental results show the effectiveness of our proposed scheme. There are still many challenges problems in symmetric SE systems. In the proposed scheme the data owner is responsible for generating update information and sends it to the cloud server. Therefore, the owner of the data, the unencrypted to store index tree and the information that is necessary, in order to calculate the IDF values again. Such an active data owners for the cloud computing model may not be very suitable. It could be a useful but difficult.

## References

[1] Mark D. Ryan," Cloud computing security: the scientific challenge, and a survey of solutions" University of BirminghamJanuary 28, 2013

[2] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou," Secure Ranked Keyword Search over Encrypted Cloud Data" International Conference on Distributed Computing Systems, 2010

[3] Ming Li, Shushing Yu, Ming Caoand Wenjing Lou" Authorized Private Keyword Search over Encrypted Data in Cloud Computing", 31st International Conference on Distributed Computing Systems, 2011

[4] Jiadi Yu, Peng Lu, Yanmin Zhu, "Toward Secure Multikeyword Top-kRetrieval over Encrypted Cloud Data," IEEE member, IEEE Transactions on dependable and secure computing, vol. 10, no. 4, July/august 2013.

[5] Ming Cao, Cong Wang ,"Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, January 2014

[6] Yi Yang, Hongwei Li, Wenchao Liu, Haomiao Yao, Mi Wen," Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost", School of Computer Science and Engineering, University of Electronic Science and Technology of China, Globecom - Communication and Information System Security Symposium, 2014.

[7] Chi Chen, Xiaojie Zhu, "An Efficient Privacy-Preserving Ranked Keyword Search Method", Member, IEEE, IEEE DOI 10.1109/TPDS.2425407, IEEE Transactions on Parallel and Distributed Systems, 2015.

[8] Hongwei Li, Dongxiao Liu, Kun Jia, and Xiaodong Linss"Achieving Authorized and Ranked Multi-keywordSearch over Encrypted Cloud Data" School of Computer Science and Engineering, University of Electronic Science and Technology of China. IEEE ICC - Communication and Information Systems Security Symposium,2015

[9] Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun "Enabling Personalized Search over Encrypted OutsourcedData with Efficiency Improvement", DOI 10.1109/TPDS.2506573, IEEE Transactions on Parallel and Distributed System, 2015

[10] Wenhai Sun, Bing Wang, Ming Cao,"Privacy-preserving Multi-keyword Text Search in the Cloud SupportingSimilarity-based Ranking *"asia ccs'13,* May 8–10, Hangzhou, China. Copyright 2013 acm 978-1-4503-1767-2/13/05, 2013.

[11] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, "A Newer UserAuthentication, File encryption and Distributed Server Based Cloud Computing security architecture "Lecturer,Stamford University, Bangladesh, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[12] Chinua Xia, Xinhui Wang," A Secure and Dynamic Multi-keyword Ranked Search Scheme over EncryptedCloud Data", DOI 10.1109/TPDS. 2401003, IEEE Transactions on Parallel and Distributed Systems, 2015.