International Journal of Computer Science and Engineering Communications,
Volume.4, Issue.2 (2016): Page. 1337-1342
www.scientistlink.com/ijcsec

Enhanced Dynamic Multi-Keyword Rank Scheme using top Key over Encrypted Cloud Data

[1]M.Gomathi and [2]D.Seenivasan
[1]PG Scholar, [2]Assistant Professor
[1,2]Department of Computer Science and Engineering,
[1,2]K.S. Rangasamy College of Technology, Tiruchengode, India
[1]m.gomath@gmail.com, [2]seenumoorthy@gmail.com

Abstract-*The cloud computing platform gives people the ability to share resources, services and information among people from all over the world. In the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data into cloud servers for great convenience and reduced costs in data management. The sensitive data should before the outsourcing of data protection requirements, data usage obsoletes such as keyword-based document retrieval is encrypted. Improved dynamic multi-keyword ranking search scheme with top key via encrypted cloud data that simultaneously supports dynamic update operations as deleting and inserting documents. Greedy depth first search algorithm is provided for efficiency multi keywords on place and index structure. The safe kNN algorithm is used to encrypt the index and query vectors and ensure precise meaning score calculation between encrypted index and query vectors. A secure multi-keyword search is controlled via encrypted cloud data that simultaneously supports dynamic update operations, such as deleting and inserting documents. Here, focus on the data security problems with extended searchable symmetric encryption. For the first time formulate the issue of privacy in terms of relevance and similarity scheme robustness. The observation of these server-side rankings inevitably leak based order-preserving encryption protection. In order to eliminate the leak, we propose to support the top-k Multi-full-text search. Thorough security and performance analysis show that the proposed scheme guarantees a high safety and practicality and dynamic update operations, such as deleting and inserting documents.*

Keyword- *Advanced Symmetric Encryption Certified Authority,Cloud data, Data security, Keyword Based Retrieval, Multi keyword Retrieval.*

I INTRODUCTION

Cloud Computing, a logical pattern for advanced data service is a necessary feasibility for data users, data was to outsource. Controversy over privacy, but outsourcing of sensitive information, including e-mail, medical records and personalphotos were explosively expanding [1] presented incessantly. Reports of data loss and privacy breaches in cloud computing systems appear from time to time. The biggest threat to privacy rooted in the cloud itself. When users outsource their private data on the cloud, control the cloud service provider capable of and monitor the data and communication between the users and it may be legally or illegally. To ensure privacy, typically user data before you, the major challenges for effective data use brings on outsourcing cloud encrypt [2]. However, even if the encrypted data use is possible, the user must still interact with the cloud, and allowing the cloud operates on the encrypted data, which causes leakage of potentially sensitive information. Further, in cloud computing, data owners can their outsourced data with a number of users who want to retrieve only the files you are interested in [9] share. One of the most popular ways to do this is through keyword-based retrieval,which is a typical data service and based on keywords widely used in plaintext scenarios where users retrieve applied relevant files in a file record. [8] However, it turns out to be difficult tasks in ciphertext scenario are due to the limited operations on encrypted data. In addition, to enhance the feasibility and save costs in the cloud paradigm, it is preferable to obtain the query results with the most important files that the interests of users, can instead display all files[3]. Preventing the cloud from those in the ranking and to have all the work for the user is a natural way to prevent data leaks. However, the limited computing power on the user side and the high computational effort includes information security. The issue of secure multi-keyword top-k retrieval via encrypted cloud data is thus how to during the process of recovery without the cloud more work information leaks. The concepts is similar relevance and scheme robustness to formulate the privacy issue into searchable encryption method, and then solve the insecurity problem

in that they are a two-round searchable encryption (TRSE) scheme. Novel technologies in cryptography community and information retrieval community employed including homomorphism encryption and vector space model. In the proposed scheme, the majority of the computational work on the cloud will be carried out while the user takes part in rankings, by using encrypted cloud data with high security and practicality and dynamic update operations, such as deleting and top-k Multi-full text search guarantees inserting documents.

1.1 Purpose

Three different devices are involved: cloud servers, data holders and data users. The cloud server hosts third-party data storage, and views [9]. Since data may contain sensitive information, the cloud server cannot be fully entrusted to the protection of data. For this reason, migrated files must be encrypted. Any kind of information leakage, which would affect the privacy, is considered unacceptable.

1.2 Scope of the Project

The concepts of similarity and relevance scheme robustness to formulate the privacy issue into searchable encryption method, and then solve the insecurity problem by a two round searchable encryption scheme [10]. New technologies in cryptography and information retrieval community are used, including homomorphic encryption and vector space model. In the proposed scheme, the cloud is performed while the user is in the rankings, the top k Multi- participates full text search over encrypted cloud data with high security and practicality guaranteed.

1.3 Overview of the project

A general approach to protect the confidentiality of data is to encrypt the data before outsourcing. However, this will result in an enormous cost in terms of data, ease of use. For example, the existing techniques for keyword-based information retrieval, which are widely used on the plaintext data, cannot be applied directly to the encrypted data. Download all data in the cloud and to decrypt locally is obviously impractical. To solve the above problem, researchers have some general purpose solutions with fully homomorphic encryption or blind RAMs [11] constructed. These methods are not practical due to their high computational cost for both the cloud Sever and users. Proposed scheme to achieve flexible search sub-linear search time and deal with the deletion and insertion of documents. The safe kNN algorithm is used to encrypt the index and query vectors, and in the meantime to ensure precise meaning score calculation between encrypted index and query vectors [12]. To various attacks reflected in different threat models we construct two secure search rules: the dynamic top-k multi-keyword space search procedure in the known cipher text model and the improved dynamic Top-k multi-keyword space search procedure in the known background model.

II RELATED WORK

Jiadi Yu, focus on data security problems with SSE. For the first time we formulate the privacy issue in terms of relevance and similarity scheme robustness. It notes that server -side rankings on the basis of order-preserving encryption (OPE) inevitably leak protection. To eliminate the leak, hit a Two round searchable encryption scheme, the top k Multi supports full-text search [4]. In this scheme,sufficient search accuracy has provided by the vector model and Homomorphic Encryption. Thorough security and performance analysis show that the proposed scheme guarantees a high safety and practicality.

Ning Cao, define and solve demanding problems of privacy-preserving more keyword rank over encrypted data in cloud computing (MRSE). This is the strict data protection requirements for such a secure cloud data usage System Posted. Among the various multi-keyword semantics, we will choose the efficient similarity measure of "coordinate adjustment". Here, use more "inner product similarity" to quantitatively evaluate how similarity measure [5]. The first beat hashed a basic idea for the MRSE via secure inner product, and then give two significantly improved MRSE systems to various privacy requirements in two different threat models to achieve [5]. The proposed regulations, in fact, low overhead introduce the computing and communications.

Yi Yang, use the secure k nearest neighbors to propose a secure dynamic searchable symmetric encryption methods .It can reach two important security functions [6]. (i.e.) forward and backward privacy. Very demanding in Dynamic searchable Symmetric encryption (DSSE) is around. The evaluation of the performance of this proposed scheme compared to other DSSE rules [6]. The comparison results show the effectiveness of the proposed regulation in relation to look at the storage and update complexity.

Chi Chen, has proposed a hierarchical clustering method to more search support semantics and the demand for fast passphrase -Search meet in a big data environment [7] .The proposed hierarchical approach clusters the documents on the basis of minimum relevance threshold , and then partitions The resulting hierarchical cluster is reached , the

restriction on the maximum size of the cluster [7] . In the search phase can achieve a linear computational complexity compared to an exponential increase in the size of document collection this approach. To verify the authenticity of the search results, a structure called minimum hash sub tree is designed in this paper. The proposed method has an advantage over the traditional method in the Rank Privacy as relevant documents.

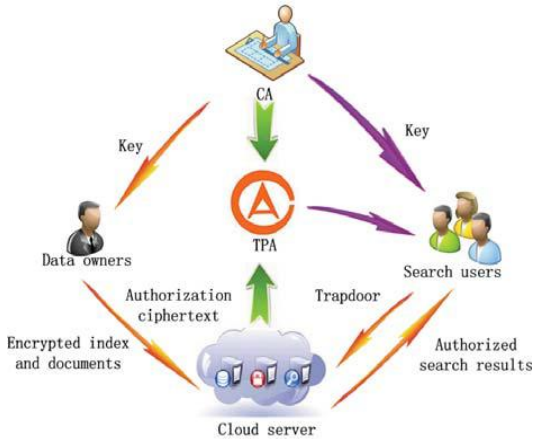

Fig.1.System Architecture

III PROPOSED SYSTEM

3.1 Modules

- 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

A Access Group key generation process Module

Access Key and Authentication is the process of determining, in fact. In private and public computer networks (including Internet), the authentication is often done through the use of login passwords. Knowledge of the password is assumed to ensure that the user is authentic [Fig.1].Each user first registered (or registered by someone else) with an assigned or self-proclaimed password. On each subsequent use, the user must know and use the previously declared password. The weakness of the system for transactions such as the exchange of moneyis that passwords are often stolen, accidentally revealed, or forgotten. The process of identifying an individual, usually on a username and password in security system-based authentication differs from approval, the people access objects which is identity authentication is only guaranteed the process of giving that the individual, people claims to be, but says nothing about the access rights of the individual. Internet business and many other transactions wants more stringent authentication process. The use of digital certificates from a certificate authority (CA) is issued as part of a Public Key Infrastructure and verified that the normal way to authenticate over the Internet are expected to perform.

B User upload data Using Advanced Encryption Module

The completion of the registration phase, when the user wants the file can choose multiple files and select upload option. Upon completion of the upload process can data owners their outsourced data with a number of users who want only the data files they are interested in. One of the most popular ways to retrieve this do to share is through keyword-based retrieval. Keyword-based retrieval is a typical data service and widespread in plaintext scenarios where users retrieve applied relevant files in a file set based on keywords. However, it gives a difficult task in ciphertext scenario due to the limited operations on encrypted data, the data owner has a collection of files n C = {f1, f2, ..., fn}, into the cloud server encrypted swap and expects the cloud server for full-text search service for data owner itself or other authorized users. To achieve this, the owner of the information to a searchable index I of a collection of l Construction Keywords W = {w1, w2... wl} extracted from C and store the encrypted index I_ and encrypted files on then the cloud server.

C Public Cloud Server implementation

The cloud server is honestly following the protocol developed to analyze the hosted data and the received queries to additional information about out. When users outsource their private data on the cloud, control the cloud service provider capable of and data and communication between the users and the Cloud Monitor at will, legally or illegally. Cases like the secret NSA program, which recorded about working to get the data to be shared and stored, and also to create a signature for all splited to ensure data to privacy, users typically the data before outsourcing it to Cloud, the major challenges for effective data sharing encrypt However even if the encrypted data usage is possible, the user must still communicate with the cloud and the cloud enabling works to the encrypted data that causes leakage of potentially sensitive information.

D User Uploaded Data stored Split and store Tree Structure Module

Internet storage is a model of networked online storage, stored in the data in virtualized storage pools that are typically hosted by third parties. To operate hosting companies large data centers and people who need their data to be hosted buy. The data center operators, pooling the resources according to the requirements of the customers and they put as storage pools that use the customer himself to save files or data objects. Physically, to span the resource across multiple servers which is enables the Internet storage or hosted storage, a data storage management solution that allows individuals or organizations to store their data on the Internet with a service provider, rather than locally storing the data on a physical disk, such as a disk or tape it's backup. To save a growing numbers of customers their important data in remote servers in the cloud, without a copy in their local computers. it can easily be adapted to support dynamic data. Thereafter, files uploaded, the uploaded file will be saved in cloud with the security. The guarantee shall be provided with combined encryption algorithm available.

E Data User Retrieve File to cloud Module

If the user wants to download the file with, you need to check with the public verifiability process. To alleviate the computational load on the user side, raking should be on the server side, so we have an encryption scheme to ensure the operability and safety at the same time on the server side. Advanced encryption scheme allows certain types of calculations are performed on the corresponding cipher text. The result is the cipher text of the results of operations performed on the clear text. That is, advanced encryption scheme allows calculation of the cipher text, without knowing the plaintext to obtain the proper encrypted result. Even though it has such a beautiful property, completely original enhanced encryption scheme, the grid employs over a polynomial ring is ideal, too complicated and inefficient for practical use.
Fortunately, as a result of using the vector space model to top-k retrieval, only addition and multiplication operations on integers are necessary to calculate the relevance scores from the encrypted searchable index. Therefore, we can use the original homomorphism in an overall shape to a simplified form of reducing allows only integer operations that does more efficiency than the full form.

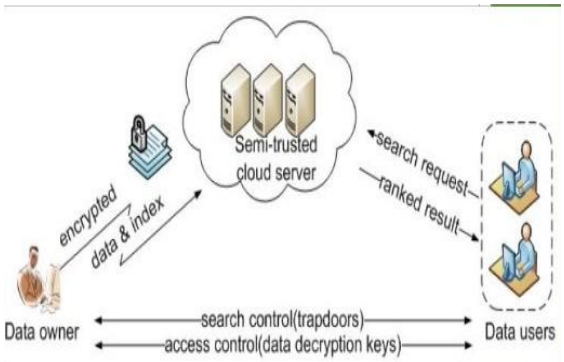

Fig.2. Architecture of the Search over Encrypted Cloud Data

3.2 Multi Keyword Ranking Search Algorithm

Setup: point or safety parameters as input, data are owner of a symmetric key as SK

Build index: Based on the amount of data that builds data owner a searchable index that is encrypted by the symmetric key SK and then outsourced to cloud server. After the index structure of the document collection can be independently encrypted and swapped.

Trapdoor: with keywords interest as input, this algorithm generates a corresponding trapdoor.

Query: As cloud servers a query request, it leads the ranking on the search index using the trapdoor and finally the rank ID list of top k documents sorted by their similarity returns.

3.3 Dynamic Searchable Encryption

Designing searchable encryption schemes, the structures obtained with sub- linear search time, In particular, dynamic search is simple, highly parallel and can easily handle updates. Specifically, for n documents on m keywords and with p cores (processors) indicated available and it supports complex queries and multi- client settings using SSE as a black box. To ensure that our data structures and related business activities which is support for dynamic databases and it support terabyte -Scale databases in this richer / complex encrypted search settings [12] .The dynamic expansion maintains the optimum index size and only basic size information.

IV PERFORMANCE ANALYSIS

In this environment, the entire model has an average of 5 seconds to execute all the steps. This hardware configuration is highest take 2 seconds to encrypt up to 10 KB file. This model is fast enough, and can be applied to current cloud computing environments. Working with the model at different times and with different user and his individual files in the size, the contents are different from each extension,etc. take different times for the implementation of the general model . Depending on file size varies program duration from person to person. Among the many users result, some of them are shown in the tables.

Table.1.Time measures supporting for dynamic Process

No of Persons	File Size (KB)	Time Required for Uploading files(in sec)By using Existing Algorithm	Time Required for downloading files(in sec) By using Existing Algorithm	Time Required for Uploading files(in sec)By using Proposed Algorithm	Time Required for downloading files(in sec) By using Proposed Algorithm
1	8.27	1	1.4	0.5	0.8
2	10.1	1.3	1.5	0.7	0.9
3	14.1	1.5	1.7	1	1.2
4	19.3	1.7	2	1.3	1.5
5	20	2	2.5	1.5	1.8

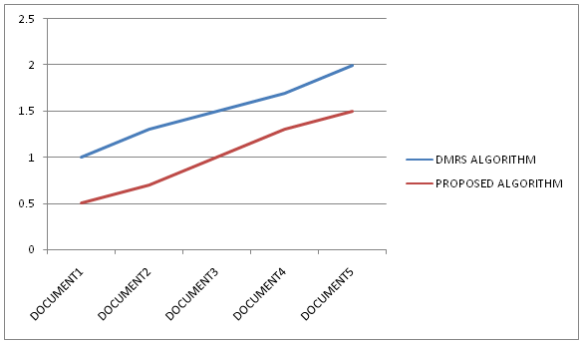

Fig.3.Time cost efficiency for uploading process.

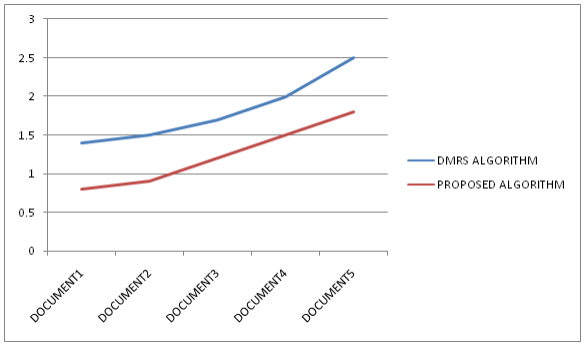

Fig.4.Time cost efficiency for downloading process

V. CONCLUSION

A first attempt, practical and effective multi keyword to obtain text search over encrypted data cloud. The beat system Improved dynamic multi keyword search Place Scheme over encrypted data cloud. Security analysis shows that the proposal document confidentiality, trapdoor unlink ability and strength to reach agreements. Extensive experiments show that the proposal to achieve better efficiency in terms of functionality and computational complexity as compared to the existing ones. Finally, in-depth analysis on the real world set of documents illustrating the performance of the dynamic search effectiveness, efficiency and privacy .The dynamic operation such as updating and deletion has to assume with privacy and security policies.

REFERENCES

[1] Mark D. Ryan," Cloud computing security: the scientific challenge, and a survey of solutions" University of Birmingham January 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 Outsourced Data 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 Supporting Similarity-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 User Authentication, 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 Encrypted Cloud Data", DOI 10.1109/TPDS. 2401003, IEEE Transactions on Parallel and Distributed Systems, 2015.