ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Efficient Secured Dynamic Searching Technique in Cloud Computing

G Shruthi[1], S S Lakshmi Lavanya M[2]

Assistant Professor, Sree Dattha College of Engineering and Science, Hyderabad, India [1, 2]

ABSTRACT: Due to the increasing the usage of networks, the maintains and storage of data is an open issue. An user always needs an efficient performance in searching for getting required data. Cloud computing is one the solution for the mentioned problem. Even though it performs well still it also suffers from satisfying the user searching data providing. Hence we proposed a secure dynamic searching technique which solves the user needs. When a data transforming over the networks security is also an issue can prevented by different encrypted algorithms. The issue now is applying searching on encrypted data in cloud in open issue. We made an attempt to give solutions for the given problem by developing an efficient secure dynamic searching technique. It also supports dynamic update operations like deletion and insertion of documents. In this paper we also adapted the concepts of a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient search. The secure kNN algorithm services taken to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. We conducted a sequence of experiments to demonstrate the efficiency of the proposed scheme which proves its efficiency.

KEYWORDS: Cloud computing, kNN algorithm, DFS, encrypted algorithms, security.

I. INTRODUCTION

Cloud computing, the new term for the long dreamed vision of computing as a utility, enables convenient, on-demand network access to a centralized pool of configurable computing resources (e.g., networks, applications, and services) that can be rapidly deployed with great efficiency and minimal management overhead.

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

DOI: 10.15680/IJIRCCE.2017. 0510014

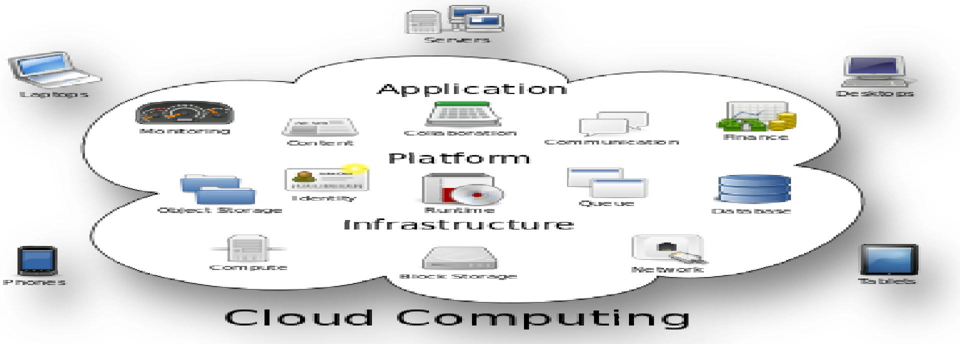


Fig.1.Structure of cloud computing

II. RELATED WORK

Traditional searchable encryption has been widely studied in the context of cryptography. Among those works, most are focused on efficiency improvements and security definition formalizations. The first construction of searchable encryption was proposed by Song et al. [12], in which each word in the document is encrypted independently under a special two-layered encryption construction. Goh [13] proposed to use Bloom filters to construct the indexes for the data _les. For each _le, a Bloom filter containing trapdoors of all unique words is built up and stored on the server. To search for a word, the user generates the search request by computing the trapdoor of the word and sends it to the server. Upon receiving the request, the server tests if any Bloom filter contains the trapdoor of the query word and returns the corresponding _le identifiers. To achieve more efficient search, Chang et al. [16] and Curtmola et al. [17] both proposed similar\index" approaches, where a single encrypted hash table index is built for the entire file collection. In the index table, each entry consists of the trapdoor of a keyword and an encrypted set of file identifiers whose corresponding data files contain the keyword. As a complementary approach, Boneh et al. [14] presented a public-key based searchable encryption scheme, with an analogous scenario to that of [12]. In their construction, anyone with the public key can write to the data stored on the server but only authorized users with the private key can search. As an attempt to enrich query predicates, conjunctive keyword search, subset query and range query over encrypted data have also been proposed in [18, 20]. Note that all these existing schemes support only exact keyword search, and thus are not suitable for cloud computing.

III. EXISTING WORK

A general approach to protect the data confidentiality is to encrypt the data before outsourcing. Searchable encryption schemes enable the client to store the encrypted data to the cloud and execute keyword search over ciphertext domain. So far, abundant works have been proposed under different threat models to achieve various search functionality, such as single keyword search, similarity search, multi-keyword boolean search, ranked search, multi-keyword ranked search, etc. Among them, multi-keyword ranked search achieves more and more attention for its practical applicability. Recently, some dynamic schemes have been proposed to 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.

Limitations: 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. Existing System methods not practical due to their high computational overhead for both the cloud sever and user.

IV. LITERATURE SURVEY

Security challenges for the public cloud, K. Ren, C.Wang, Q.Wang et al.Cloud computing represents today's most exciting computing paradigm shift in information technology. However, security and privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

A fully homomorphic encryption scheme, C. Gentry propose the first fully homomorphic encryption scheme, solving an old open problem. Fully homomorphic encryption has numerous applications. For example, it enables encrypted search engine queries—i.e., a search engine can give you a succinct encrypted answer to your (boolean) query without even knowing what your query was.

Public key encryption with keyword search, D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano given searching on data that is encrypted using a public key. Practical techniques for searches on encrypted data, D. X. Song, D. Wagner, and A. Perrig, explained data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality.

Ravindra Changala at, Data Mining Techniques for Cloud Technology, given few of cloud computing technologies in the view of data mining.

Ravindra Changala at, Data Mining Challenges with Big Data, explained few issues with searching and accessing issues in cloud data.

V. PROPOSED WORKS

This paper proposes 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, we construct a tree-based index structure and propose a "Greedy Depth-first Search" algorithm based on this index tree.

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, we construct two secure search schemes: the basic dynamic multi-keyword ranked search (BDMRS) scheme in the known ciphertext model, and the enhanced dynamic multi-keyword ranked search (EDMRS) scheme in the known background model.

The purpose of the k Nearest Neighbours (kNN) algorithm is to use a database in which the data points are separated into several separate classes to predict the classification of a new sample point. This sort of situation is best motivated through examples.

Suppose each sample in our data set has n attributes which we combine to form an n-dimensional vector: x = (x1, x2, . . . , xn). These n attributes are considered to be the independent variables. Each sample also has another attribute, denoted by y (the dependent variable), whose value depends on the other n attributes x. We assume that y is a categoric variable, and there is a scalar function, f, which assigns a class, y = f(x) to every such vectors.

The algorithm described and can be summarized as:

1. A positive integer k is specified, along with a new sample

2. We select the k entries in our database which are closest to the new sample

3. We find the most common classification of these entries

4. This is the classification we give to the new sample

VI. SCOPE OF THE SYSTEM

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

VII.. DESCRIPTION OF THE WORK AND RESULTS

The system is equipped the following details and contains, Data Owner Module, Data User Module, Cloud server and Encryption Module and Rank Search Module

Data Owner: This module helps the owner to register those details and also include login details. This module helps the owner to upload his file with encryption using RSA algorithm. This ensures the files to be protected from unauthorized user. Data owner has a collection of documents *F ={f*1*; f*2*; :::; fn}* that he wants to outsource to the cloud server in encrypted form while still keeping the capability to search on them for effective utilization.

SYSTEM ARCHITECTURE:

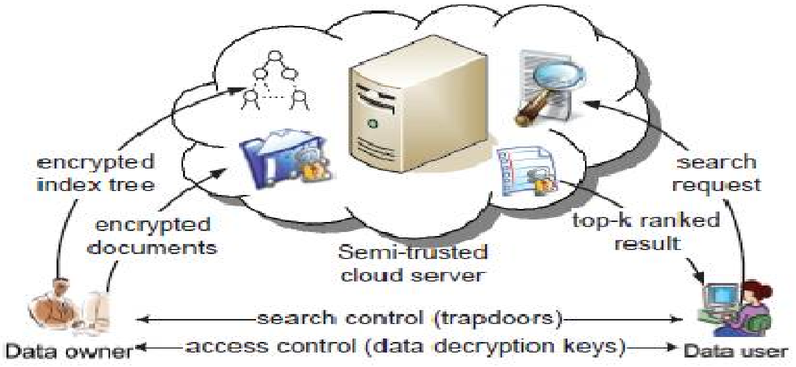
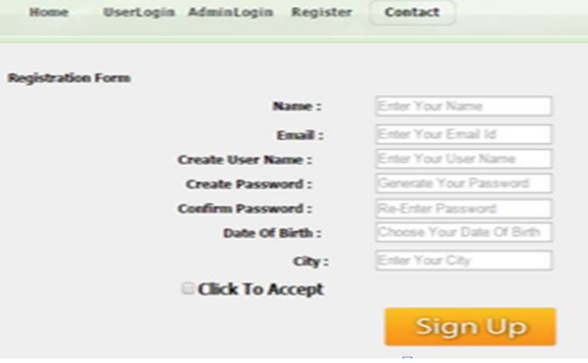


Fig.1. Proposed system model

In our scheme, the data owner firstly builds a secure searchable tree index *I* from document collection *F*, and then generates an encrypted document collection *C* for *F*. Afterwards, the data owner outsources the encrypted collection *C* and the secure index *I* to the cloud server, and securely distributes the key information of trapdoor generation and document decryption to the authorized data users. Besides, the data owner is responsible for the update operation of his documents stored in the cloud server. While updating, the data owner generates the update information locally and sends it to the server.



Registration Form

Name : Enter Your Name

Email : Enter Your Email Id

Create User Name : Enter Your User Name

Create Password : Generate Your Password

Confirm Password : Re-Enter Password

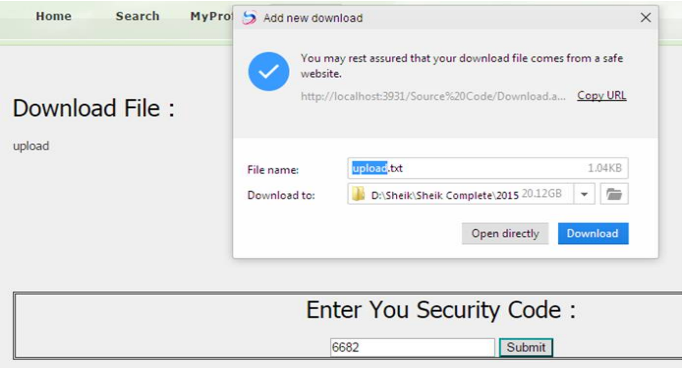
Date Of Birth : Choose Your Date Of Birth

City : Enter Your City

□ Click To Accept

Fig.2. User login

Data User: This module includes the user registration login details. This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail email before enter the activation code. After user can download the Zip file and extract that file. Data users are authorized ones to access the documents of data owner. With *t* query keywords, the authorized user can generate a trapdoor *TD* according to search control mechanisms to fetch *k* encrypted documents from cloud server. Then, the data user can decrypt the documents with the shared secret key.



Download File :

upload

Add new download

You may rest assured that your download file comes from a safe website.

http://localhost:3931/Source%20Code/Download.a...

File name: upload.txt 1.04KB

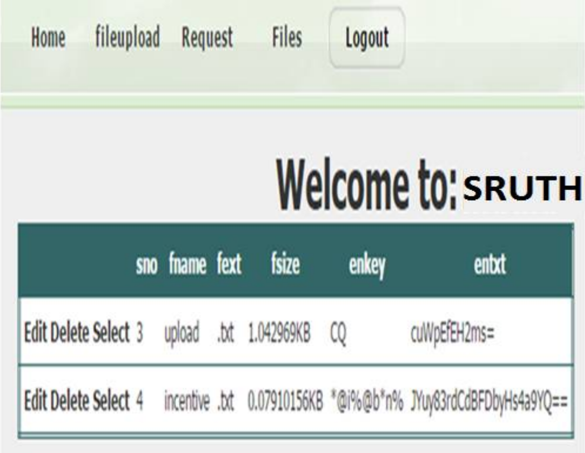
Download to: D:\Sheik\Sheik Complete\2015 20.12GB

Enter You Security Code :

6682

Fig.3. working of searching

Cloud Server and Encryption: This module is used to help the server to encrypt the document using RSA Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download. Cloud server stores the encrypted document collection *C* and the encrypted searchable tree index *I* for data owner. Upon receiving the trapdoor *TD* from the data user, the cloud server executes search over the index tree *I*, and finally returns the corresponding collection of top- *k* ranked encrypted documents. Besides, upon receiving the update information from the data owner, the server needs to update the index *I* and document collection *C* according to the received information. The cloud server in the proposed scheme is considered as “honest-but-curious”, which is employed by lots of works on secure cloud data search.



Welcome to: SRUTHI

	sno	fname	fext	fsize	enkey	entxt
Edit Delete Select	3	upload	.txt	1.042969KB	CQ	cuWpEfEH2ms=
Edit Delete Select	4	incentive	.txt	0.07910156KB	*@i%@b*n%	JYuy83rdCdBFDbyHs4a9YQ==

Fig.4. List of files searched

Rank Search: These modules ensure the user to search the files that are searched frequently using rank search. This module allows the user to download the file using his secret key to decrypt the downloaded data. This module allows the Owner to view the uploaded files and downloaded files. The proposed scheme is designed to provide not only multi-keyword query and accurate result ranking, but also dynamic update on document collections. The scheme is designed to prevent the cloud server from learning additional information about the document collection, the index tree, and the query.

VIII. CONCLUSION

In this paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate searching but also the dynamic deletion and insertion of documents. We used the concepts of "Greedy Depth-first Search" algorithm for improving the better efficiency in search. The security can be managed with kNN algorithm. The data owner is responsible for all activities regard data in the cloud. Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful but difficult future work to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only. We fixed main issues still there few works left for the future scope as trapdoor generation, identification of users integrity. Any how our work has given better results comparatively.

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. Ravindra Changala, Automated Health Care Management System Using Big Data Technology, Journal of Network Communications and Emerging Technologies (JNCET), Volume 6, Issue 4, April (2016), ISSN: 2395-5317,EverScience Publications pp-37-40.
3. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.
4. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.
5. Ravindra Changala, Annapurna Gummadi, Knowledge Discovery Process: The Next Step for Knowledge Search, International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 3, Issue 5, May 2015, ISSN (Online): 2320-9801 ISSN (Print): 2320-9798.s
6. 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. 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.
7. Ravindra Changala, Annapurna Gummadi, A Generalized Association Rule Mining Framework for Pattern Discovery, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (4) , 2014,Pages- 5659-5662, ISSN: 0975-9646.
8. 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.
9. Ravindra Changala, A Survey on Development of Pattern Evolving Model for Discovery of Patterns in Text Mining Using Data Mining Techniques, Journal of Theoretical and Applied Information Technology (JATIT), Vol.95. No.16, ISSN: 1992-8645,pp-3974-3981.

10. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in IEEE INFOCOM, April 2011, pp. 829–837.
11. Ravindra Changala, Data Mining Techniques for Cloud Technology, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015, ISSN (Print) 2319 5940.
12. Ravindra Changala, Data Mining Challenges With Big Data, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 3 Issue VI, June 2015, ISSN: 2321-9653.
13. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "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.

BIOGRAPHY

Ms. S S Lakshmi Lavanya M received Master Degree in Computer Science and Engineering (CSE) form Jawaharlal Nehru Technological University, Hyderabad (JNTUH). Her research interest includes Big Data and Data Mining. Presently working as Assistant Professor in CSE Department, Sree Dattha College of engineering and science, Hyderabad., India.

Ms. G Sruthi received Master Degree in Computer Science and Engineering (CSE) form Jawaharlal Nehru Technological University, Hyderabad (JNTUH). Her research interest includes Cloud Computing and Network Security. Presently working as Assistant Professor in CSE Department, Sree Dattha College of engineering and science, Hyderabad., India.