International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(4), pp.001-005
DOI: http://dx.doi.org/10.21172/1.84.01
e-ISSN:2278-621X

SECURE DYNAMIC MULTI KEY WORD RANKED SEARCH ON ENCRYPTED DATA

Umashree .E[1] and T.R. Muhibur Rahman[2]

Abstract: Multi keyword ranked search over encrypted cloud data defines the complexity in preserving definite System wise privacy in the cloud computing. Because of increasing use of the more and more data an owner are motivated to outsource their data to cloud servers to freedom from the complexity and minimizes the economic cost in data management. The data of the data owners should be encrypted before modifying the data by the data users for privacy requirements. The encrypted data can be utilized by using key-word based documents. A secure multi keyword ranked search supports the data owners to update the operations like inserting, deleting and modifying the existing documents. For the index construction and query generation vector space model and widely used TF_IDF model are used. This project constructs a special tree based index structure and proposes a "Greedy depth first search" algorithm to provide efficient multi keyword ranked search. The flexibility in adding and deleting the documents and sub linear search can be achieved by using special tree based index structure.

Key words: encryption, multi keyword, ranked search, cloud server, index construction, query generation, cloud computing.

I. INTRODUCTION

Cloud computing is a type of internet based computing that provides shared computer processing that provides shared computer processing resources and data to computers and other devices on demand. the resources are shared by other users. This enables on demand access to a shared pool of configurable computing resources. This reduces the management effort. Cloud computing provides data owners and data users with various capabilities to store and process their data in either privately owned or third party data centers that may be located far from the user, ranging the distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale. Many cloud platforms like Google drive, icloud, sky drive, Amazon s3, drop box and Microsoft azure provides storage services. Major challenges in cloud computing is security and privacy the virtualization of hardware and software resources in cloud nullifies the financial investment for owning the data warehouses and its maintenances.

The data owner and the data user may be located on different domain the outsourced data may be exposed to the vulnerabilities. Since before storing the data in the cloud, data need to be encrypted. Data encryption assures the data confidentiality and integrity. The encryption on the data is done by using searchable algorithms. Many researchers have been contributing to searching in encrypted data. The search techniques may be single keyword search or multi keyword search.

Searchable encryption focuses on single keyword search or Boolean keyword search and rarely sort the search results. The huge data base search may result in many documents to be matched with keywords. This may increases the difficulties for a cloud user to go through all documents and have most relevant documents. Raked search is another solution that can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data which is highly desirable in the pay-as- you use cloud paradigm. For privacy protection such ranking operation however should not leak any keyword related information.

II. LITERATURE SURVEY

[1] *Department of CSE BITM College, Ballari, Karnataka, India*
[2] *Department of CSE BITM College, Ballari, Karnataka, India*

cloud computing transforms the way information technology(IT) is expended and oversaw, promising enhanced expense efficiencies, quickened development, speedier time-to-market, and the capacity to scale applications on interest.[1]as per purva jain, proposes a special keyword balanced binary tree as the index, and intend a "Greedy Depth-first Search" algorithm to acquire preferable effectiveness over linear search. Likewise, the parallel search procedure can be completed to further lessen the time cost. The plan's security is ensured against two risk models by utilizing the safe kNN algorithm. Trial results display the efficiency of our proposed scheme. This paper proposes the information proprietor is in charge of producing overhauling data and sending them to the cloud server. Accordingly, the data owner needs to store the un-encrypted index tree and information that is required to recalculate the IDF values.

[2] As per Sudanagunta Bindu, describes the unencrypted dynamic multi-keyword ranked search (UDMRS) scheme which is constructed on the basis of vector space model and KBB tree. Based on the UDMRS scheme, two secure search schemes (BDMRS and EDMRS schemes) are constructed against two threat models, respectively. This also constructs a special keyword balanced binary tree as the index, and proposes 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.

[3] As per Vaibhavi Kulkarni, proposes AES algorithm for encrypting data files and GDFS. AES & GDFS increases the data security and improves privacy of data by its commutative nature. Using CRSA, data in a file can be updated dynamically without affecting the overall performance of searching on B-tree. In our proposed system, if encrypted data is modified, encrypting for the whole data is not required. This is a desirable feature as it reduces the computation time.

[4] As per Anita Chavan A protected, efficient and element inquiry plan is proposed, which bolsters the exact multi-essential word positioned hunt as well as the dynamic erasure and insertion of archives. We build an extraordinary decisive word adjusted parallel tree as the record, and propose an "Greedy Depth-first Search" calculation to acquire preferred efficiency over straight pursuit. Also, the parallel inquiry procedure can be completed to further diminish the time cost. The plan's security is ensured against two danger models by utilizing the protected kNN calculation. Trial results show the efficiency of our proposed plan. There are still numerous test issues in symmetric SE plans. In the proposed plan, the information proprietor is in charge of producing overhauling data and sending them to the cloud server. Therefore, the information proprietor needs to store the decoded record tree and the data that are important to recalculate the IDF values. Such a dynamic information proprietor may not be exceptionally suitable for the distributed computing model.

[5] As per Priya S, a safe, productive and dynamic pursuit plan is proposed, which bolsters not just the exact multicatchphrase positioned seek additionally the element cancellation and insertion of records. We build an exceptional catchphrase adjusted double tree as the list; what's more, propose a "Covetous Profundity first Inquiry" calculation to get preferable effectiveness over straight inquiry. Furthermore, the parallel pursuit procedure can be completed to promote diminish the time cost. The security of the plan is ensured against two danger models by utilizing the protected kNN calculation.

III. PROBLEM FORMULATION

Data owners can upload their encrypted data on the cloud. Searchable encryption algorithms maintain the confidentiality and privacy of owner's data by introducing searching keyword directly on encrypted data. Later the authorized users can perform private keyword search on encrypted data in cloud. Encrypted files include the multiple domains like cryptography, indexing storage etc. here are also involved in devising efficient security. To protect the data from the illegitimated user's confidentiality is to encrypt the data before outsourcing. after encrypting the data, data owners load their confidential data on the cloud server and data users retrieve the data from the cloud using keyword over the ciphertext. in the existing system to access the data from the cloud some functionalities need to be performed such as ranked search, single key word search, similarity search, multi keyword ranked search, multi keyword Boolean searched. Among these, multi keyword ranked search works more bitterly for its practical applications. The data stored on cloud will be retrieved by using keyword-based information on the plaintext; this cannot be directly applied on the cipher text since it requires downloading all the data from cloud. Existing system methods are not practical due to their high computational over head on the data server and user.

A. Existing System

To protect the data from the illegitimated user's confidentiality is to encrypt the data before outsourcing. after encrypting the data, data owners load their confidential data on the cloud server and data users retrieve the data from the cloud using keyword over the ciphertext.in the existing system to access the data from the cloud some functionalities need to be performed such as ranked search, single key word search, similarity search, multi keyword ranked search, multi keyword Boolean searched. Among these, multi keyword ranked search works more bitterly for its practical applications. The data stored on cloud will be retrieved by using keyword-based information on the plaintext; this cannot be directly applied on the cipher text since it requires downloading all the data from cloud. Existing system methods are not practical due to their high computational over head on the data server and user.

B. Proposed System

System architecture is the abstract design that defines the behavior and structure of a system. In architecture phase the basic structural framework of a system is recognized, major components of the system is are determined and communication between these components is defined.

Features of proposed system

- This project supports the multi keyword ranked search and dynamic operations can be performed on the document collection.
- The proposed system supports secure tree based search scheme over the encrypted cloud data. This can flexibly achieve sub linear search time and deal with the deletion and insertion of documents.
- To provide multi keyword ranked search on the cloud data specifically vector model and widely used term frequency and inverse document frequencies model are combined in the index construction and query generation.
- This also proposes "Greedy –Depth First Search" algorithm to obtain high search efficiency .and also proposes secure KNN algorithm which encrypts the index and query vectors, and also calculates the accurate relevance score between encrypted index and query vectors Proposed system.

1. System architecture

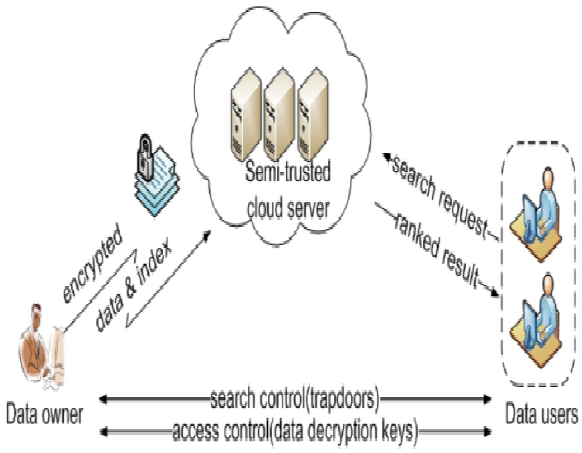

Fig.1. the architecture of ranked search over encrypted cloud data

Data owner

Data owner needs to login into the system with all his details, if he has collection of documents the he need to be outsourced on to the cloud server. To maintain security the data owner should encrypt the data before outsourcing to the users. Data owner uses the RSA algorithm to encrypt the collection of documents and then outsources the secure index and encrypted collection to the cloud server and then distributes the trap door generation and document decryption to the key information of authorized data user.

Data user

If any of the user needs to access the documents from the cloud server then initially data users should login into the system. If the registered user is authorized one then the user can access the documents of data owner by using query keywords. The data user can also generate trapdoor according to search control mechanisms to fetch encrypted document from the cloud server. Now he can decrypt the documents with the shared secret key.

Cloud server

Cloud server stores module used to store the encrypted documents of data owner. Soon after receiving trapdoor from the data use. Cloud server executes the search over the index tree and responses the corresponding collection of top-k ranked encrypted documents. It also updates the search index tree after receiving updating from the data owner.

Rank search

These module ensure the user to search the files that are searched frequently using rank search .this module allows the user to download the fie using his secret key to decrypt the downloaded data, this also 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 collection.

IV. MODULES

Index Construction of UDMRS Scheme

Amid the procedure of index development, we to begin with make a tree node for each document in the accumulation. These nodes are the leaf nodes of the index tree. By then, the internal tree nodes are made in view of these leaf nodes.

Search Process of UDMRS Scheme

The search procedure of the UDMRS scheme is a recursive methodology upon the tree, named as "Greedy Depth first Search (GDFS)" algorithm. We add to an outcome list meant as RList, whose components is described as ⟨RScore; FID⟩. Here, the RScore is the significance score of the archive fFID to the question. The RList stores the k got to reports with the biggest pertinence scores to the inquiry. The rundown's components are positioned in sliding request as indicated by the RScore, and will be upgraded opportune amid the search process.

BDMRS Scheme In view of the UDMRS scheme,

We build the essential element multi-keyword ranked search (BDMRS) scheme by utilizing the secure kNN algorithm. The BDMRS scheme is intended to accomplish the objective of privacy preserving in the known cipher text model. BDMRS scheme can secure the Index Confidentiality and Query Confidentiality in the known cipher text model.

DMRS Scheme

Cloud server has the capacity interface the same search requests by following way of visited nodes. The Cloud server recognizes a keyword as the standardized TF distribution of the keyword can be precisely acquired from the last computed relevance scores. A heuristic strategy to further enhance the security is to break such correct quality. Hence, we can acquaint some tunable haphazardness with exasperate the significance score estimation. Likewise, to suit diverse users' inclinations for higher exact positioned results or better protected keyword privacy, the arbitrariness are set movable.

Dynamic Update Operation of DMRS

After insertion or deletion of a record, we require updating synchronously the index. Since the index of DMRS scheme is planned as a balanced binary tree, the dynamic operation is done by redesigning hubs in the list tree. The report on record is just in view of archive recognizes, and no entrance to the substance of records is required

V. CONCLUSION

In this paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. We construct a special keyword balanced binary tree as the index, and propose 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 kNN algorithm. Experimental results demonstrate the efficiency of our proposed scheme.

REFERENCES

[1] Purva Jain, Dr. Abhijit Banubakode,” A Review Paper on Multi keyword Ranked Search on Encrypted Cloud Data”, IOSR Journal of Computer Engineering (IOSR-JCE) ,e-ISSN : 2278-0661, p-ISSN : 2278-8727 PP 28-32

[2]Sudanagunta Bindu, D. Kishore Babu, "Constructing A Tree-Based Index Structure For Efficient Multi Keyword Ranked Search" International Journal Of Scientific Engineering And Technology Research, Volume.05, Issueno.37, October-2016, Pages: 7643-7646

[3] Vaibhavi Kulkarni, Prof. Priya Pise," Secure Multi-keyword Ranked Search over Encrypted Cloud Data", IJARCCE, ISO 3297:2007 Certified Vol. 5, Issue 12, and December 2016.

[4] Anita Chavan, Supriya Gade, et.al,"Multi-Keyword Searching and Dynamic Operations on Encrypted cloud Data", International Journal of Research In Science & Engineering, Volume: 2 Issue: 3.

[5] Priya S , Ambika P R," A Multi-keyword Ranked Search Scheme that is Dynamic and Secure over Cloud Data", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Special Issue 10, May 2016.

[6] M. Li et al., 'Authorized Private Keyword Search over Encrypted Data in Cloud Computing,' 31st Int'l. Conf. Distributed Computing Systems, 2011, pp. 383–92.

.