International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Apr 2019. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-04

Title: EFFICIENT SEARCHABLE ENCRYPTION WITH MULTI-KEYWORD RANKED SCHEME OVER ENCRYPTED CLOUD DATA

Volume 08, Issue 04, Pages: 145–149.

Paper Authors

P.GANGADHARA RAO, Mrs.K.UDAYASRI
NRI INSTITUTE OF TECHNOLOGY, A.P., India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

EFFICIENT SEARCHABLE ENCRYPTION WITH MULTI-KEYWORD RANKED SCHEME OVER ENCRYPTED CLOUD DATA

P.GANGADHARA RAO[1], Mrs.K.UDAYASRI[2]

[1]Student, NRI INSTITUTE OF TECHNOLOGY, A.P., India.

[2]Assistant Professor & HOD, Dept. Of Department of Master of Computer Applications, NRI INSTITUTE OF TECHNOLOGY, A.P., India.

Abstract —The public cloud server like Amazon, Microsoft Azure, Google Drive, etc. With the help of data outsourcing, the organizations can provide reliable data services to their users without any concerns for the data management overhead. . Normally, CSPs (Cloud Service Providers) take care of the data and its privacy, but there are some of the factors because of which the data privacy and user identity may be violated like an apostate employee, etc. Therefore, data owners should encrypt their respective sensitive data before outsourcing it to the public cloud server. Because the data is getting encrypted before outsourcing which may affect the performance of some important data accessing operations like searching of a document, etc. Searchable encryption is a cryptographic method to provide security. In literature many researchers have been working on developing efficient searchable encryption schemes. , we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. So we propose Encryption Module. This entity is considered to be a trusted third party which is responsible for the generation and management of the decryption Data. So we by considering this we can reduce the data owner work load.

Keywords — Cloud Storage, multi Ranked-Search, Encrypted-Data Search, secure cloud.

INTRODUCTION

Security and privacy concerns have been the major challenges in cloud computing. The hardware and software security mechanisms like firewalls etc. have been used by cloud provider. These solutions are not sufficient to protect data in cloud from unauthorized users because of low degree of transparency [4]. Since the cloud user and the cloud provider are in the different trusted domain, the outsourced data may be exposed to the vulnerabilities [5]. Thus, before storing the valuable data in cloud, the data needs to be encrypted [2]. Data encryption assures the data confidentiality and integrity. To preserve the data privacy we need to design a searchable algorithm that works on encrypted data [13]. Many researchers have been contributing to searching on encrypted data. The search techniques may be single keyword search or multi keyword search [11]. In huge database the search may result in many documents to be matched with

keywords. This causes difficulty for a cloud user to go through all documents and have most relevant documents. Search based on ranking is another solution, wherein the documents are ranked based on their relevancy to the keywords [3]. Economical searchable encryption techniques help the cloud users especially in pay-as-you use model. The researchers combined the rank of documents with multiple keyword search to come up with efficient economically viable searchable encryption techniques. In searchable encryption related literature, computation time and computation overhead are the two most frequently used parameters by the researchers in the domain for analysing the performance of their schemes. Computation time (also called "running time") is the length of time required to perform a computational process for example searching a keyword, generating trapdoor etc.

PROPOSED SYSTEM

Encryption Module: By using CRSA, data in a file can be updated dynamically without affecting the overall performance of searching on B-tree. If the encrypted indexed data is modified, re-indexing for the whole data is not needed. Similarly there is no need of re-encrypting the files in the database whenever the file is modified. This is a desirable feature as it reduces the computation time

Commutative Encryption (CRSA): The RSA cryptosystem is one of the optimum public key cryptography approaches. However, its overall robustness gets limited due to one way encryption and majority of existing RSA schemes suffer from reorder issues. Therefore, in order to make this system least complicated and more efficient, an approach called Commutative RSA has been proposed. In this scheme, the order in which encryption has been done would not affect the decryption if it is done in the same order. Encryption is the standard method for making a communication private. With the many cryptographic approaches, our system follows the commutative RSA algorithm. The mathematical scheme for performing this encryption is described by a pseudo algorithm presented below. Let us consider two prime numbers and initialized amongst all the group members. Let and represent the group members required to communicate over the documents. To compute the encryption keys and decryption key pairs of the commutative RSA algorithm the parameters and are computed using the following From the above equations it is clear that and for and . The encryption key pair of and are represented as (and is to be obtained. The is obtained by randomly selecting numbers such that it is a co-prime of or in other terms Where represents the greatest common divisor function between two variables and . The decryption key pair of and is represented by and and the parameter is computed based on the following equation Let represent the encrypted data . The encryption operation is defined as follows The commutative RSA decryption operation on the encrypted data is defined B- Tree: A B-tree is a data structure as shown in Figure 2. The tree contains index nodes and leaf nodes. All leaf

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

nodes are at the same level (same depth). Each index nodes contain keywords and pointers. Each node except root node in a B-tree with order n must contain keys between n to 2n keys. Each node also contains (number of keys + 1) pointers to its child nodes. If the root node is an index node then it must have at least 2 children. The insertion, deletion, search operations takes only logarithmic time.

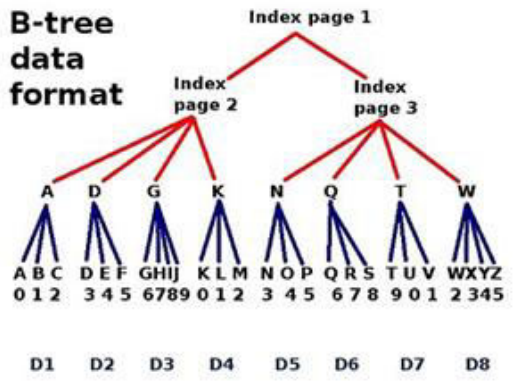

Figure 1: B tree data format.

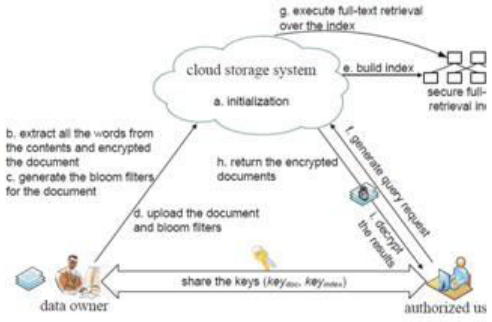

Figure 2: Architecture of searchable encryption scheme for multi-user databases.

LITERATURE SURVEY

1. Privacy-preserving Multi-keyword Text Search: Wenhai Sun [1] proposed this search that provides similarity based search result ranking, keyword privacy, Index and Query confidentiality and Query Unlink ability. The encrypted file is built by vector space model supporting consolidated and distinctive file search. The searchable index is built using Multidimensional B tree. Owner creates encrypted query vector $\bar{Q}$ for file keyword set. User gets the respective encrypted query vector of W from owner which is given to CS. Now CS searches index by Merkle–Damgård construction algorithm and compares cosine measure of file and query vector and returns top k encrypted files to user. Limitation: -The similarity rank score of the document vector fully depends on the type of the document.

2. A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data: This proposed method [2] suggest a secure tree-based search scheme over the encrypted cloud storage, which supports multi keyword ranked search along with dynamic operation on document collection available at server. The vector space model and term frequency (TF) × inverse document frequency (IDF) model are combinly used in the construction of index and generation of query to provide multi keyword ranked search output. To obtain high search efficiency results, author construct a tree-based index structure and proposed a Greedy Depth-first Search algorithm based on this index tree. Because of this special structure of tree-based index, the proposed search scheme can flexibly achieve sub linear search time and can effectively deal with the deletion and insertion of documents. The kNN algorithm is applied to encrypt the index and query vectors, and till then ensure accurate

relevance score calculation between encrypted index and query vectors.

3. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data: This proposed method has defined and solved the problem of effective but safe and sound rank keyword search over Encrypted cloud data [3]. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain important criteria (e.g. keyword frequency) thus making one step closer towards sensible consumption of secure data hosting services in Cloud Computing. These papers has defined and solved the challenging problem of privacy preserving and efficient multi keyword ranked search over encrypted cloud data storage (MRSE), and establish a set of strict privacy requirements for such a protected cloud data utilization system to become a reality. The proposed ranking method proves to be efficient to go back extremely relevant documents corresponding to submitted search terms. The idea of proposed ranking method is used in our future system in order to enhance the security of information on Cloud Service Provider. Limitation: - Dynamic updating and deletion of the document from the cloud is not possible.

4. Privacy Preserving Multi-Keyword Ranked Search (MRSE): Ning [4] proposed this search for known cipher text model and background model over encrypted data providing low computation and communication overhead. The coordinate matching is chosen for multi-keyword search. They used inner product similarity to quantitatively evaluate similarity for ranking files. The drawback is that MRSE have small standard deviation σ which weakens keyword privacy. Limitation: - Multi-keyword ranked search (MRSE) for known cipher text model may produce two different trapdoor which vague the privacy leakage problem of trapdoor unlink ability which may weaken the keyword privacy. MRSE has small standard deviation σ which in turn weakens the keyword privacy. The integrity of the rank order is not checked in MRSE.

CONCLUSION AND FUTURE WORK

The paper , 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.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, re-encrypting for the whole data is not needed. This is a desirable feature as it reduces the computation time.

1. Such an active data owner may not be very suitable forthe cloud computing model. It could be a meaningfulbut difficult future work to design a dynamic searchableencryption scheme whose updating operation can becompleted by cloud server only, meanwhile reservingthe

ability to support multi-keyword ranked search.

2. Inaddition, as the most of works about searchable encryption,our scheme mainly considers the challenge from thecloud server. Actually, there are many secure challengesin a multi-user scheme. Firstly, all the users usuallykeep the same secure key for trapdoor generation in asymmetric SE scheme.

REFERENCES

[1] Qin Liuy, Guojun Wangyz, and Jie Wuz, ”Secure and privacy preserving keyword searching for cloud storage services”, ELSEVIER Journal of Network and computer Applications, March 2011.

[2] Cong Wang et al., ”Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE Transactions on parallel and distributed systems, vol. 23, no. 8, August 2012.

[3] International Journal of Computer Applications (0975 – 8887) Volume 126 – No.14, September 2015.

[4] Wenhai Sun et al., "Privacy-Preserving Multikeyword Text Search in the Cloud Supporting Similarity-based Ranking", the 8th ACM Symposium on Information, Computer and Communications Security, Hangzhou, China, May 2013.

[5] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, Member, IEEE Computer Society, and Minglu Li,”Toward Secure Multikeyword Top k Retrieval over Encrypted Cloud Data”, IEEE Journal of Theoretical and Applied Information Technology 10th August 2014. Vol. 66 No.1 © 2005 - 2014 JATIT & LLS. All rights reserved. ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195 64 Transactions on dependable and secure computing, vol. 10, no. 4, July/August 2013.

[6] Ning Cao et al.,” Privacy-Preserving MultiKeyword Ranked Search over Encrypted Cloud Data”, IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, jan 2014.

[7] Wenhai Sun et al., "Protecting Your Right: Attributebased Keyword Search with Finegrained Ownerenforced Search Authorization in the Cloud", IEEE INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014 [10]Secure Ranked Keyword Search over Encrypted Cloud Data, IEEE PAPER, 2010. [8]Zhihua Xia, “A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL: PP NO: 99 YEAR 2015.