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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Privacy-Preserving of Encrypted Cloud Data through Dynamic Multi-Keyword Search

Rahul Barate[1], Rohidas Chorghe[1], Pankaj Palaskar[1], Tukaram Sude[1], Prof Dhanshree Kulkarni[2]

Student, Department of Computer Engineering, Dr DY Patil College of Engineering, Ambi Talegaon Dabhade, Savitribai Phule Pune University, Pune, India[1]

Prof, Department of Computer Engineering, Dr DY Patil College of Engineering, Ambi Talegaon Dabhade, Savitribai Phule Pune University, Pune, India[2]

ABSTRACT: Recently, more and more individuals are intriguedto outsource their local data to public cloud servers for great comfortand reduced costs in data management and security. Be that as it may, in reality of thought security issues, sensitive data should be encrypted here before outsourcing, which obsoletes traditional data utilization like keyword-based document retrieval policy. Here, we introducea secure and efficient multi-keyword ranked search scheme over encrypted data, which supports dynamic update operations like deletion and insertion of documents and security supports. In particular, we buildan index tree based approach on vector space model to provide multi-keyword search, which then backings adaptable refresh operations.Here cosine similarity measure is utilized to support accurate ranking for search result. To enhanceeffectiveness of search efficiency, we propose a search algorithm based on "Greedy Depth-first Traverse Strategy". In addition, to ensure the search privacy, we propose a secure scheme of various privacy requirements in the known cipher text threat model mechanism. Here Experiments on the genuine word dataset demonstrate the adequacy and proficiency of proposed plan instrument.

KEYWORDS: Cloud computing, Encrypted data, Multi keyword search, Ranked Search, Similarity Matching, OTP.

I. INTRODUCTION

Now a days, cloud computing enjoys great reputation in data management due to its outstanding capability in computing, storage and various applications in the cloud era. Through cloud administrations, individuals could appreciate advantageous; on-request organizes access to a mutual pool of configurable registering assets with awesome productivity and insignificant monetary overhead with guaranteed security arrangement.Despite of the various advantages offered by cloud services, transfer of sensitive information (such as e-mails, company finance data, and government docs etc.) to semi-trusted cloud server brings concerns about privacy issues. For instance, the cloud server may spillunapproved substances or even be hacked, which puts the outsourced information at hazard. Traditionally, sensitive data regarding cloud should be encrypted by data owners before outsourcing, which, however, obsoletes traditional data utilization service like keyword-based information retrieval and its security policies.Here, we present a secure dynamic multi-keyword ranked search scheme over encrypted cloud data, which supports top-retrieval and dynamic updates on dataset regarding cloud view point. Specifically, we siphon the vector space model to provide multi-keyword queries, and cosine measure together with TF×IDF weight is utilized to achieve actual ranked results for improving efficiency. To correctedthe search efficiency, we build a tree-based index structure and propose a top-ranked search algorithm over this index which haslogarithmic search time. Besides, profit from the index tree structure, update on documents is available in our cloud scheme. The proposed dynamic multi-keyword ranked search scheme (DMRS) is secure under the known ciphertext model. Our contributions are summarized as given below:

1) Our proposed search scheme achieves multi-keyword ranked search over encrypted data with high efficiency and more search result accuracy.

2) We propose a secure DMRS scheme which converge privacy requirements in the known ciphertext model about cloud mechanism.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

3) Profit from tree-based index structure, our search scheme supports dynamic update operation (like deletion and insertion) on documents, which caters to real-world needs and is superior to most current static program.

Motivation

To motivated the ranked keyword search over encrypted data to achieve economies of scale for CloudComputing. In this section, we start from the review of existing searchable symmetric encryption (SSE) schemes and provide the definitions and framework for our proposed ranked searchable symmetric encryption (RSSE). Note that by following the same security guarantee of existing SSE, it would be very inefficient to support ranked search functionality over encrypted data, as demonstrated in our basic scheme. The discussion of its demerits will lead to our proposed scheme. we motivate and solve the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud Computing. We first give a basic scheme and show that by following the same existing searchable encryption framework, it is very inefficient to achieve ranked search. We then appropriately weaken the security guarantee, resort to the newly developed crypto primitive OPSE, and derive an efficient one-to-many order-preserving mapping function, which allows the effective RSSE to be designed. Through thorough security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of ranked keyword search.

Goal and Objective

1. It proposed schemes indeed introduce low overhead on computation and communication.
2. It uses ranked search mechanism to support more search semantics and dynamic data operations.
3. It is more secure and efficient.
4. **Secured Multi Keyword search:**
   Our technique allows the authorized user to specify sing and multiple keywords in the search query (i.e. filename, date of publish, owner id). MRSE provides accurate and relevant search result.
5. **Privacy Preserving:**
   Providing data privacy and search privacy is very difficult to provide but MRSE provides data privacy, keyword privacy and search privacy to the user.
6. **Efficiency:**
   By providing accurate and relevant searched ranked result to the user when and wherever required, it improves the searching efficiency and data efficiency.

II. LITERATURE SURVEY

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, [2] presented a break in the clouds: towards a cloud definition (2009).In cloud the data search appear only with the plain data. But it is essential to invoke search with the encrypted data also. The specialty of cloud data story age should allow abundant keywords in a solitary query and results the data documents in the relevance order.Authors focus on multi keyword search based on ranking over an encrypted cloud data (MRSE). The search uses the feature of similarity and inner r product similarity matching.

[2] S. Kamara and K. Lauter, proposed Cryptographic cloud storage, (2010). Authors tryto solve the problem of searching files through the huge amount of files securely and efficiently. The past techniques make the hunt non effective by methods for time and computational cost, yet the strategy examined in this paper makes the seeking extremely productive and secure.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, [6] presented Privacy-preserving multi-keyword ranked search over encrypted cloud data (2011).Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, author define and solve the challenging problem of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE). They set up an arrangement of strict protection prerequisites for such a safe cloud information usage framework. Among various multi keyword semantics, they choose the efficient similarity measure of “coordinate matching”, i.e., as many matches as possible, to capture the relevance of data documents to the search query. They further use “inner product similarity” to quantitatively evaluate such similarity measure. They first propose a basic idea for the MRSE based on secure inner

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models.

[4] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, [7]proposed Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking(2013).With the help of this paper we are taking idea of a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, author propose to build the search index based on termfrequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. To improve the search efficiency, they propose a tree-based index structure and various adaption methods for multi-dimensional (MD) algorithm so that the practical searchcapacity is much better than that of linear search.

[5] C. Orencik, M. Kantarcioglu, and E. Savas,[8] propose an efficient privacy-preserving search method over encrypted cloud datathat utilizes min hash functions(2013). One of the main advantages of this proposed method is the ability of multi-keyword search in a single query. The proposed technique is demonstrated to fulfill versatile semantic security definition.Authors also combine an effective ranking capability that is based on term frequency-inverse document frequency (tf-idf) values of keyword document pairs.

[6] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, [9] presented Secure ranked multi-keyword search for multiple data owners in cloud computing (2014).To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, authors systematically construct a novel secure search protocol. To rank the indexed lists and save the security of pertinence scores amongst catchphrases and records, they propose a novel Additive Order and Privacy Preserving Function family.

III. PROPOSED SYSTEM

Here, we define and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system wise privacy in the cloud computing scenarios. Various multi-keyword semantics, we choose the efficient similarity measure of “coordinate matching,” i.e., as many matches as possible, to capture the relevance of data documents to the search query. Specifically, here we use “inner product similarity”, i.e., the number of query keywords appearing in a document, to quantitatively evaluate similarity measure of that document to the search query. During the index construction, every document is associated with a binary vector as a sub-index where each bit represents whether corresponding keyword is contained in the document. The search query is described as a binary vector where each bit means whether corresponding keyword takein this search request, so the equality could be exactly measured by the inner product of the query vector with the data vector. However, here we directly outsourcing the data vector or the query vector will violate the index privacy or the search privacy. To achieve the test of supporting such multi key word semantic without privacy breaches, we propose a basic idea for the MRSE using secure inner yield computation, which is adjusted from a protected k-nearest neighbour (KNN) technique, and then give two fundamentally developed MRSE schemes in a step-by-step manner to achieve stringent privacy requirements in two threat models with increased attack capabilities.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Proposed system architecture

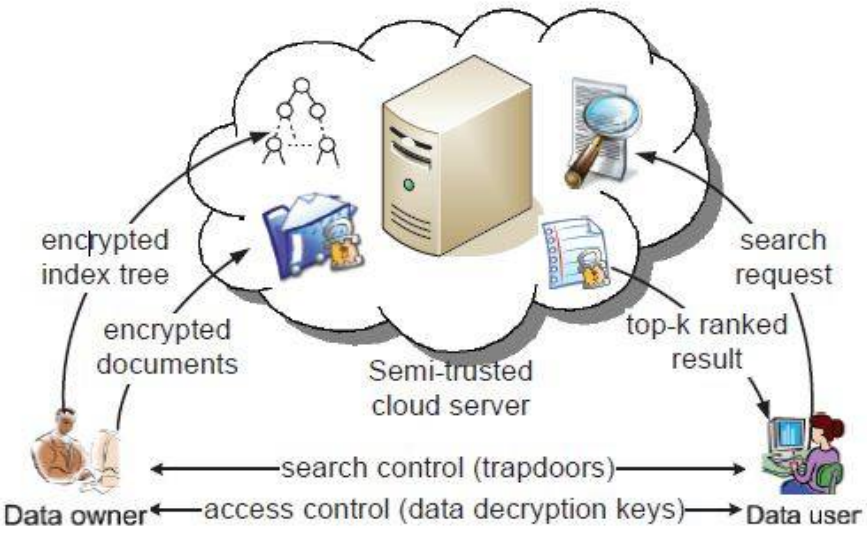

Figure 1: Architecture of ranked search over encrypted cloud data

Advantages:

1. It proposed schemes indeed introduce low overhead on computation and communication cost.
2. It uses ranked search mechanism to support extra search semantics and dynamic data operations.
3. It is more secure and efficient mechanism.

IV. EXPERIMENTAL SET UP

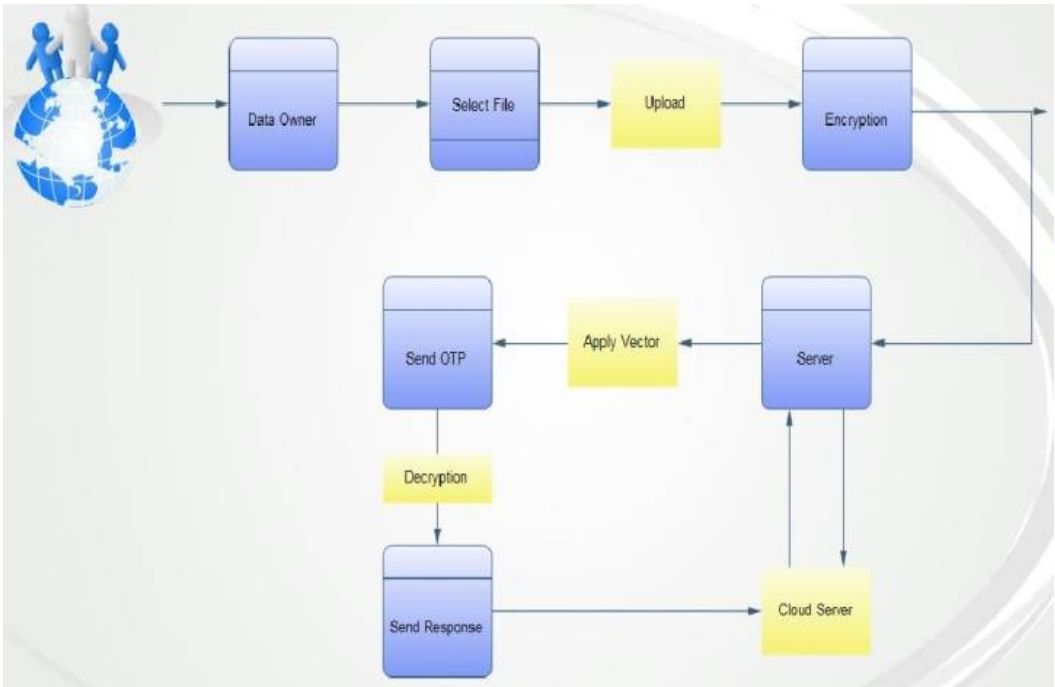

Figure 2: Experimental Diagram of proposed system

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

1. Data User Module
2. Data Owner Module
3. File Upload Module
4. Encryption
5. Rank Search Module
6. File Download Module
7. Decryption
8. View Uploaded and Downloaded File

Data User Module:
It includes the user registration login details.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.

Data Owner Module:
It helps the owner to register those details and also include login details.Data owner has a collection of documents F ={f1; f2; :::; 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. 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 (including keyword IDF values) 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.

Cloud Server Module:
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.

File Upload Module:
It help the owner to upload his file with encryption using ECC algorithm. This ensures the files to be protected from unauthorized user.

Rank Search Module:
It ensures the user to search the file that is searched frequently using rank search.

File Download Module:
It allows the user to download the file using his secret key to decrypt the downloaded data.

View Uploaded and Downloaded File:
It allows the Owner to view the uploaded files and downloaded files.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V. RESULT AND GRAPH

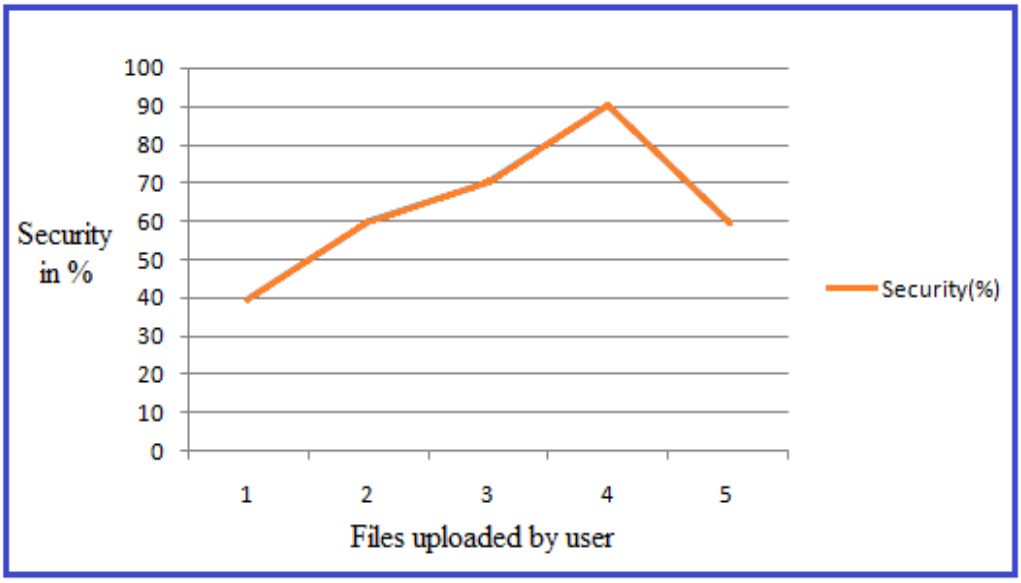

Figure 3: Performance of our framework in terms of security

The above result shows that our Privacy-Preserving of Encrypted Cloud Data through Dynamic Multi-Keyword Searchperformance in percentage (%). The X-axis represents the files which are uploaded by users and Y-axis represents how much security in percentage (%) is provided by our system to uploaded file. The above graph shows that's our system works efficiently and provides security to users data as compare to other systems.

TABLE 1
Performance of our framework in terms of security

Sr. No.	Files uploaded by users	Security in %
1	1	40
2	2	60
3	3	70
4	4	90
5	5	59

The above table shows that how much security is provides by our framework. Files are uploaded by users and we provide security to user's data (files) in percentage (%).

VI. CONCLUSION AND FUTURE WORK

Here, we propose an efficient multi-keyword ranked search scheme over encrypted cloud data, it supports dynamic update operations. Here various multi-keyword semantics, we choose the popular one, i.e., vector space model to

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

present the relevance between documents and keywords. Cosine similarity measure is used to quantitatively evaluate the similarity between outsourced documents and query keywords, and furthermore achieve accurate ranked search results. Search efficiency and update operations, we design a tree-based index and propose an efficient search algorithm. Moreover, in terms of privacy-preserving, Here we take a secure scheme in the known ciphertext threat model and successfully satisfy the privacy requirements. Lastly, experiments on the real-world dataset exhibit the effectiveness and efficiency of our DMRS scheme.Our future work will be to implement mechanism of reduction time cost for index tree construction. Here we will concentrate on designing more efficient search algorithm and secure scheme in enhanced threat model.

REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[2] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Compute. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009.
[3] E.-J. Gohet al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.
[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS. Springer, Heidelberg.
[6] 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.
[7] 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.
[8] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on. IEEE, 2013, pp. 390–397.
[9] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. IEEE, 2014, pp. 276–286.