IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
www.ijiset.com
ISSN 2348 – 7968

# Privacy-Preserving Of Encrypted Cloud Data Through Dynamic Multi-Keyword Search.

**Miss. Suvarna Dandekar[1], Miss. Sunita Khamkar[2], Miss. Snehal kurumkar[3] and Miss. Vrushali Pandit[4]**

[1] Computer Engineering, Savitribai Phule Pune University
Shrigonda, Maharashtra, India

[2] Computer Engineering, Savitribai Phule Pune University
Shrigonda, Maharashtra, India

[3] Computer Engineering, Savitribai Phule Pune University
Shrigonda, Maharashtra, India

[4] Computer Engineering, Savitribai Phule Pune University
Shrigonda, Maharashtra, India

**Abstract**

Recently, more and more people are interested to outsource their local data to public cloud servers for great convenience and reduced costs in data management and security. But in fact of consideration privacy issues, sensitive data should be encrypted here before outsourcing, which obsoletes traditional data utilization like keyword-based document retrieval policy. Here, we present a 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. Specifically, we construct an index tree based approach on vector space model to provide multi-keyword search, which meanwhile supports flexible update operations. Here cosine similarity measure is utilized to support accurate ranking for search result. To improve effectiveness of search efficiency, we propose a search algorithm based on "Greedy Depth-first Traverse Strategy". Moreover, to protect the search privacy, we propose a secure scheme of various privacy requirements in the known cipher text threat model

***Keywords:***

*Cloud computing, Encrypted data, Multi keyword search, Ranked Search, Similarity Matching, OTP*

## 1. 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 services, people could enjoy convenient, on-demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead [1] with assured security policy. 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 leak information to unauthorized entities or even be hacked, which puts the outsourced data at risk. 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 propose a secure dynamic multi-keyword ranked search scheme over encrypted cloud data, which supports top-retrieval and dynamic updates on dataset regarding cloud perspective. Specifically, we adopt the vector space model to provide multi-keyword queries, and cosine measure together with TF×IDF weight is utilized to achieve accurate ranked results for improving efficiency. To improve the search efficiency, we construct a tree-based index structure and propose a top-ranked search algorithm over this index which has logarithmic search time. Besides, benefiting 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 cipher text 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 meets privacy requirements in the known cipher text model regarding cloud mechanism.

3) Benefiting from tree-based index structure, our search scheme During the index construction, every document is

ISSN 2348 – 7968

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 appears in this search request, so the similarity 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 challenge of supporting such multi-keyword semantic without privacy breaches, we propose a basic idea for the MRSE using secure inner product computation, which is adapted from a secure k-nearest neighbor (k-NN) technique, and then give two significantly improved MRSE schemes in a step-by-step manner to achieve stringent privacy requirements in two threat models with increased attack capabilities.

### Advantages of proposed System:

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
4. dynamic update operation (like deletion and insertion) on documents, which caters to real-world needs and is superior to most current static schemes

### Disadvantages of Existing System:

1. It still not adequate to provide users with acceptable result ranking functionality.
2. It cannot accommodate such high service-level requirements like system usability, user searching experience, and easy information discovery.
3. Shared data will not be secure in traditional mechanism.

## 2. Proposed System Mechanism:

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.

## 3. Our System Scope:

1. Search result should be ranked by the cloud server according to ranking criteria.
2. To minimize the communication cost.

## 4. System Architecture:

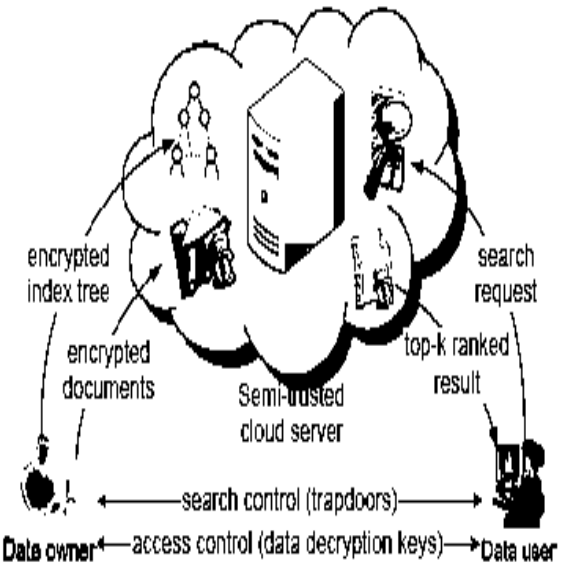

Fig. 1. The architecture of ranked search over encrypted cloud data

4.1System Architecture Flow:

Explanation:
In the Proposed work, we will explore checking the integrity of the rank order in the search result assuming the cloud server is un-trusted mechanism. To Develop OTP (one Time Password) as our future work. This OTP used to see data in cloud and it can be used once only in a time, when you search a file and tend to see the file the OTP will send to email and you get the OTP and apply to see the file which is excellent mechanism.

ISSN 2348 – 7968

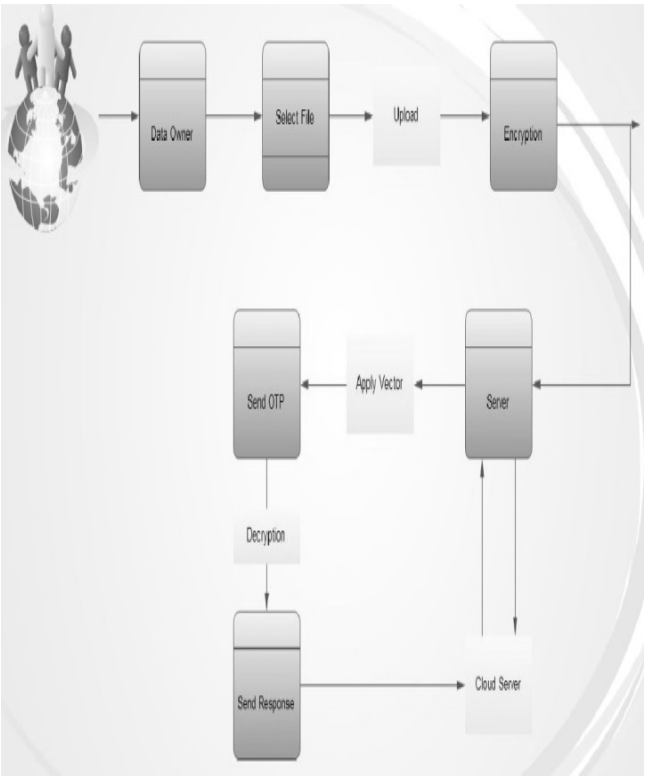


Figure 2 System Architecture Flow 1 System architecture flow

4.2 Experimental Set up :

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

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

4.2.2 Data Owner Module**:**
It helps the owner to register those details and also include login details.

4.2.3 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.

4.2.4 Encryption:
In that encrypte fil using encryption algorithm.

It ensures the user to search the file that is searched frequently using rank search.

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

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

4.2.7 Decryption:
In that decrypt the data by using decryption key.

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

## 5. Conclusion:

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 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 adopt a secure scheme in the known cipher text threat model and successfully satisfy the privacy requirements. Eventually, experiments on the real-world dataset demonstrate the effectiveness and efficiency of our DMRS scheme.

## 6. Future Scope:

1. Reduce the time cost for index tree construction.
2. Here we will concentrate on designing more efficient search algorithm and secure scheme in enhanced thread model.

ISSN 2348 – 7968

## 7. References:

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS. Springer, Heidelberg.

[3] Singhal, "Modern information retrieval: A brief overview," IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2001.

[4] H. Witten, A. Moffat, and T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images," Morgan Kaufmann Publishing, San Francisco, May 1999.

[5] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.

[6] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[7] R. Curtmola, J.A. Garay, S. Kamara, and R.Ostrovsky, "Searchable Symmetric Encryption: ImprovedDefinitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),2006.