International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 1, January 2019 |

An Efficient Search with Multi-Keyword Top-K Ranked Search Scheme and Dynamic Updates Over Encrypted Cloud Data

Snehal A. Kulkarni

M.E. II year Student, Department of Computer Engineering, SKNCOE, Pune, Maharashtra, India

ABSTRACT*:* With the growing popularity and benefits of cloud computing, the data owners prefer to outsource their documents over cloud servers. Outsourcing data over cloud reduces management cost and provides great convenience and ease of access. This causes the issue of privacy which can be overcomed by encrypting the sensitive data before outsourcing. But this obsoletes data utilization like keyword based document retrieval. In this paper, we present efficient search scheme named as multi-keyword top-k ranked search scheme over encrypted cloud data. It is very necessary to get the required document among thousands of encrypted documents over cloud in short time. The proposed system provides efficient and fast search over encrypted cloud data. The sensitive data over the cloud is protected from the unauthorized access using revoke to user. Only data owner have authority to provide access to documents and update or delete the content or document. In this way system provides relevant data in a short time by ensuring the security for sensitive data over cloud.

KEYWORDS*:* Cloud Computing, Dynamic Update, Multi-keyword Ranked Search, Searchable Encryption, Secure Search, AES algorithm, DSS algorithm, DFS .

I. INTRODUCTION

Cloud Computing is considered as a new model to provide convenient,ubiquitous and on demand network access to a shared pool of computing resources (storage,application,services etc.) that can be rapidly provisioned and released with minimal economic overhead and minimal management effort of service providers interaction. These appealing features attracted both individuals and enterprises to outsource their data to cloud rather than purchasing software and hardware and managing by their own.

Despite of providing various benefits of cloud services,it brings the privacy concerns to the critical and sensitive data outsourced over remote servers.The users private data can be accessed by the cloud service providers without authorization.The data is protected in this case by encrypting it beforeoutsourcing to cloud.However,this increases the cost of data utilization.

In cloud computing,the outsourced documents,who may want to access only particular data files they are interested in during specific session.Generally,keyword-based information retrieval is used to do so but is applicable for only plaintext data while not on encrypted data.Later on searchable encryption schemes have made major contributions in terms of security,functionality and efficiency.Searchable encryption allows client to store encrypted data and to execute keyword search over them. Researches are conducted under different threat models to achieve various search functionality.Multi-keyword ranked search achieves more attention among all for its practical applicability.Recently, some dynamic schemes have also been proposed to support inserting and deleting operations on document collection.

In proposed system the access to sensitive document is provided to only authorize user. To achieve efficient keyword searching the documents are stored based on keywords over cloud. To get required document we are using relevance score and accordingly user can request for the file. Only owner can update or delete the document. Cloud server manages unauthorized access by revocation. AES algorithm is used for data encryption and decryption over cloud.

II. RELATED WORK

The authors Wei Zhang,Yapping Lin and Sheng Xiao [1] introduced different MRSE schemes to improve search result and privacy.In this paper they have defined and solved the challenging problem of privacy preserving multi-keyword ranked search over encrypted data in cloud computing. In the search request, it is necessary to allow multiple keywords and return documents in the order of their relevance by considering the large number of documents and data users in cloud.

In the paper[2],authors proposed a model called secure computation on an encrypted database.The model captures execution and security requirements.Paper discusses the general problem of secure computation on encrypted database and the problem of k-nearest neighbor computation on an encrypted database.They developed a new asymmetric scalar product preserving encryption (ASPE) and is used to construct two secure schemes that support kNN computation on encrypted data.The authors song, Wagner and Perring in their paper[3] presented described cryptographic schemes for the problem of searching on encrypted data over cloud.Usually it is seen that user have to compromise functionality for security.Authors have mainly worked over provable secrecy.The schemes used also provide query isolation,controlled searching and supports hidden queries.

In the paper[4],authors proposed a secure and privacy pre-serving keyword searching scheme.The scheme allows CSP to return the only files containing certain keywords specified by the user and also to participate in decryption.The scheme reduces both the communication and computational overhead in decryption for users.It also satisfies the user data privacy and user querying privacy.

To improve the search efficiency, in the paper[5] authors proposed tree based index structure methods for multidimensional algorithm.They used multi-keyword text search scheme over the cloud supporting similarity based ranking.They have proposed two secure index schemes under strong threat models to meet the privacy requirements.In this paper[6] the aim of the authors is to find the solution of multikeyword ranked search over encrypted cloud data by preserving the system wise privacy in cloud comput-ing paradigm.Authors used similarity measure of coordinate matching semantics among the different available multikey-word semantics.They used relevancy to the search query is used to capture the data documents.To quantitatively evaluate similarity measure of a document to the search query in MRSE algorithm,inner product similarity is used.

The paper[7] provides solution to a problem in which user wants to store files on remote file servers in encrypted form and later the user wants to retrieve efficiently,the encrypted files containing specific keywords by keeping these keywords secret without keeping the security of remotely stord files in danger.In this paper authors provided some schemes in which the well defined security requirements are offered and are efficient as no public-key cryptosystem is involved.The proposed approach is independent of the encryption method chosen for remote files.The main theme of paper is storing data remotely on server and retrieving that data from anywhere using thin clien devices like mobiles,laptops etc.The approach is incremental in which user can store the new files which are secure against previous queries and searchable among the future queries.

Ranked search improves system usability by matching files in ranked order regarding certain relevance criteria.It also eliminates the unnecessary traffic over network.The authors of the paper[8] for the first time solved the challenging problem of privacy preserving multi-keyword ranked search (MRSE) over encryptedcloud data.They designed a secure cloud data utilization system to become a reality.The proposed ranking methods are efficient to return the most relevant documents corresponding to the submitted search keywords.

Orencik et.al [10].proposed a secure multikeyword search method over encrypted cloud data. System uses minhash based privacy preserving multikeyword search, which provides the high precision rates. They also used the term frequency and inverse document frequency of keywords for ranking. Cao et al.[11] worked over privacy preserving techniques for multi-keyword ranked search. To capture the data relevance to the search query they used coordinate match-ing.For quantitative similarity measure they used inner product similarity.But the scheme does ont consider the importance of different keywords. The Sun et.al.[12] constructed a searchable index tree to provide the ranking result.Authors used vector space model and adopted cosine measure together for satisfy-ing the purpose.But the scheme results in precision loss.

Zhang et al.[13] proposed a secure multikeyword ranked search scheme in multi-owner model.In this scheme different data owner uses different secret keys to encrypt their keywords and documents.The authorized users can fire the search query without knowing the encryption key for the document of these different data owners.To retrieve the most relevant search results authors proposed Additive Order Preserving Func-tion.The scheme doesnt support for dynamic data operations.

In such a technologically developed age ,data owner practically may need to dynamically update the documents multiple times after uploading them over the cloud.In the paper [14] authors considered each document as a sequence of fixed length words and are indexed individually.The scheme sup-ports the update operations but having the low efficiency of up-dation.The scheme supports only straightforward updates.Goh [15] proposed a new bloom filter scheme,in which a sub index is generated for every document based on keywords. In this case updates are very easy.While updating the bloom filter is updated along with the corresponding document.The scheme has linear search time but suffers from false positives.

III.IMPLEMENTATION STATUS

Modules:
1. User Module
2. Data Owner or Admin Module
3. Cloud Server Module

I.User Module:
1. Every user needs to register for searching and getting access permission to required document.
2. User can access the account using id and password created during registration and can update the details.
3. User can search data using multi-keywords, request for key to owner and can download.

II.Owner Module:
1. Owner uploads the encrypted data saved using keywords.
2. Responsible for sending decryption key of document to user.
3. They can check for the request for decryption keys from users.
4. They can check for document contents and flexibly updates data.

III.Cloud Server Module:
1. Responsible for managing the cloud documents.
2. Server have privileges to revoke user from accessing the account.
3. Can view the user and file details but cannot read or update data.

IV .PROPOSED SYSTEM ARCHITECTURE

The system provides efficient document search over encrypted cloud data without affecting the confidentiality of document. The system is able to provide multi-keyword ranked search and provides the effective or relevant results for search query over encrypted cloud data. To secure the confidentiality, the document is encrypted using AES algorithm before sending over cloud. The document is saved using indexes of keywords. During searching the search is made over keywords and relevant ranked results are provided. Unwanted users are revoked to get the account access. The access key or data decryption key is provided by admin to user on email of user. Cloud server can only view the encrypted documents thus pursuing confidentiality.DSS Algorithm is used to send key to user over email and DFS is used for relevancy search through indexes. If there is no file which the user is searching for the error is generated, if it is searched for more than three times then null file is allowed to download.

The system is basically consists of three modules, viz. user module, Admin or data owner module and cloud server module. Each module is having its own functionality. User can access account, search for the document, request the decryption key, download the document etc. Admin can view the file contents, update file contents, encrypts data, view key requests and send keys. Cloud Server can view encrypted file details, user details, and have authority to revoke unwanted users.

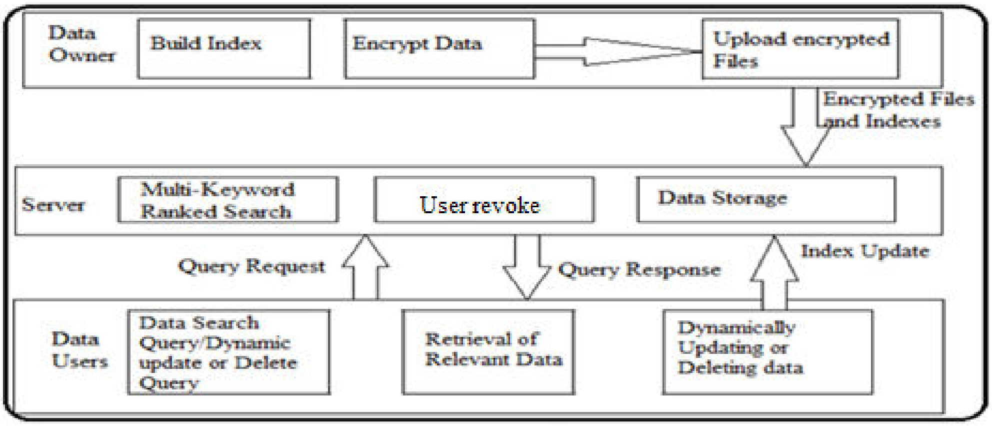
Data Owner
Build Index
Encrypt Data
Upload encrypted Files
Encrypted Files and Indexes
Server
Multi-Keyword Ranked Search
User revoke
Data Storage
Query Request
Query Response
Index Update
Data Users
Data Search Query/Dynamic update or Delete Query
Retrieval of Relevant Data
Dynamically Updating or Deleting data

Fig.1.Proposed System Architecture

Algorithms:

I. SecureKey Distribution Algorithm DSS(Digital Signature Standard And Mail method):

Generating Random pre message value k where k<0<q. Calculate r=(gk mod q) mod q, q=N-bit prime number. If unlike case that r=0 and start again different random k .Calculate s=k-1 (H (m)+xr) mod q, x=choose secret key, s=public key.

If unlike uncase s= then again start with different random k . Sign(r,k).

II.AES Algorithm

```
1) Cipher(byte in[16],byte out[16],key-array round_key[(Nr+1)]
2) Begin
3) byte state[16];
4) State=in;
5) AddRoundKey(state,round key[0]);
6) for round = 1step 1 to Nr-1
SubBytes(state);
    ShiftRows(state);
    MixColumns(state);
7) AddRoundKey(state, round_key[i]);
8) end for
   SubBytes(state);
   ShiftRows(state);
   AddRoundKey(state, round_key[Nr])
   out = state
9) end
```

III. Depth First Search Algorithm

```
1) DFS(G,v);(v is the vertex where the search starts)
2) Stack S := {};   ( start with an empty stack)
3) for each vertex u,
4)  set visited[u] := false;
5)  push S, v;
6)  while (S is not empty) do
7)     u := pop S;
8) if (not visited[u]) then
9)    visited[u] := true;
```

IV.PERFORMANCE MEASURES AND RESULT EVALUATION

Table 1 gives the comparison between the existing system and the proposed systems.

Parameter	Exiting System	Proposed System
Search Efficiency	Low	High
Search Security	Less	High
Dynamic Updates	No	Yes
Search Time	More	Less
Upload/Download Time	More	Less
Document Confidentiality	Sometimes Violated	Mostly Preserved
User Revocation	No	Yes
Access Control	Less	More

Table 1.Result evaluation.

V.CONCLUSION

The system is designed for secure and dynamic multikey-word top-k ranked search over encrypted cloud data. The system provides the accurate result ranking with the dynamic update on encrypted cloud documents. The system provides search efficiency due to the use of tree based index and efficient search algorithm.The scheme is privacy preserving and provides Index confidentiality,query confidentiality.The system is able to provide keyword privacy and trapdoor unlinkability.The system provides data security from unau-thorized access.The proposed system supports revocation. For future work there are many callenges in symmetric searchable encryption scheme.As it is assumed that all the data users are trustworthy .But in practical,the dishonest data user may distribute his secure keys to unauthorized users.

REFERENCES

[1] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou ”Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data ”, IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, IEEE 2014.

[2] Wong,Cheung,Kao,MamoulisSecurekNN computation on encrypted databases, SIMOD,09July-July2,2009 Providence,Rhode Island,USA.

[3] Dawn Xuedong Song ,David Wagner ,Adrian Perrig.Practical Techniques for Searches on Encrypted Data2000.

[4] Liu,Wang,Wu Secure and privacy preserving keyword searching for cloud storage services., 2003, pp. 131145.

[5] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Hou, Y.T., Hui Li,”Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking ”, IEEE Transactions on Parallel and Distributed Systems, IEEE 2014.

[6] Ankatha Samuyelu Raja Vasanthi , Secured Multi keyword Ranked Search over Encrypted Cloud Data, 2012.

[7] Y.-C. Chang and M. Mitzenmacher, Privacy Preserving Keyword Searches on Remote Encrypted Data, In Proc. Third Intl Conf. Applied Cryptog-raphy and Network Security, 2005. .

[8] Y. Prasanna, Ramesh . Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data, 2012.

[9] Z.Xia,X.Wang,X.Sun and Q.WangSecure and Dynamic multi-keyword ranked search scheme over encrypted cloud data IEEE trans.on parallel and distributed systems,vol 27,2016.

[10] C. Orencik, M. Kantarcioglu, and E. Savas, A practical and secure multi-keyword search method over encrypted cloud data, in Proc. IEEE 6th Int. Conf. Cloud Comput., 2013, pp. 390397.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Privacy-preserving multi-keyword ranked search over encrypted cloud data, in Proc. IEEE INFOCOM, Apr. 2011, pp. 829837.

[12] 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 Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. secur., 2013, pp. 7182.

[13] 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 Syst. Networks (DSN), IEEE 44th Annu. IEEE/IFIP Int. Conf., 2014, pp. 276286.Ca.

[14] D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, in Proc. IEEE Symp. Secur. Privacy, 2000, pp. 4455.

[15] E.-J. Goh, Secure indexes, IACR Cryptol. ePrint Archive, vol. 2003, p. 216, 2003.

[16] (2014). Request for comments. [Online]. Available: http://www. rfc-editor.org/index.html