IMPLEMENTATION AND REVIEW PAPER OF SECURE AND DYNAMIC MULTI KEYWORD SEARCH IN CLOUD

Savitri Domanal[1] ,Kiran.B.Patil[2]

[1]M.Tech Student, Department of Computer Science and Engineering,BLDEA's Dr.P.G.Halakatti College of Engineering & Technology Vijayapur, Karnataka, India
[2] Assistant Professor, Department of Computer Science and Engineering, BLDEA's Dr.P.G.Halakatti College of Engineering & Technology Vijayapur, Karnataka, India

---***---

Abstract – *A Dynamic and secure Multi-keyword or implementation of secure Ranked search that user can change the encrypted data into decrypted one using secret key ,many data owners want to outsource their data into cloud for the great use by user and user friendly connectivity .However, more sensitive data should be in the encrypt user form or before delivering for privacy requirements, which gives great savings or to put to use of data documents . In this paper ,we will implementing multikeyword search or at a time we can search two files from cloud using encrypted cloud data, which alternatively supports dynamic update operations like deletion and insertion of documents. Intially , the vector space model and the widely-used TFIDF model are combined in the index construction of tree structure and query generation. To construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search.*

Key Words**: Keyword Search, PEKS, Secure Cloud Storage, Encryption ,Decryption, TFIDF,TPA,MAC.**

1. INTRODUCTION

In order to avoid the above problem, researchers have designed some general-purpose solutions with fully-matches the result of operation matched to decoded data or oblivious hardware like RAMs. However, these methods are impractical due to their high computational overhead for both the cloud sever and user. On the bases of cloud more practical special purpose solutions, such as searchable encryption (SE) schemes have make specific contributions in terms of efficiency, user friendly and security. A, more sensitive data should be in the encrypt user form or before delivering for privacy requirements, which gives great savings or to put to use of data documents .in order to save data confidentiality from third party or hackers is to encrypt data before delivering data to the user, at that owner will send request to trapdoor to generate S_K and send it the user for decryption, in user model it will register for search for file it will help to avoid data duplication then if that file present in the cloud it will send request to trapdoor to generate private key to dewcrypt the particular file then trapdoor will send the private key to the user mail id this will completes process .

2. RELATED WORK

In this section we first see related works addressing security of dynamic cloud. Main Issue of security is very important in cloud there are many more techniques available here is review of all these. Data security from unauthorized users is the main challenge in the cloud computing as user's data will store in the servers which are remotely switched situated and far away from the end-users. These data may include very confidential data , personal information which may be enclosed to competitors or publicly. So security emerges as the main priority issue [2]. In [3] Third party auditor for verification, they include three network entities i.e. client which is user, cloud storage server which is handled by cloud service provider and Third Party or mediator Auditor which is verifier. Third party administrator not having private key, it is only having public key, it deals with only trusted server, they are not concentrate on data privacy and search. This Third party administrator algorithm is able to detect which encrypted delivered or outsourced document has a specific keyword without letting other parties such as cloud service provider and unauthorized users to learn anything during search and retrieving process.

In [4] it defines both basic schemes. Scheme 1 : User computes the media access control of every file block. Transfers the file blocks & codes to cloud and shares the key with TPA or third party administrator. During the second or Audit phase, the TPA requests from the cloud server a number of randomly selected blocks and their corresponding media access control ort MACs to verify the correctness of the data file.

Main disadvatage of this scheme is TPA algorithm can see cloud data. Scheme 2: In Setup phase, User uses s keys and computes the media access control for blocks and user shares the keys and media acesss with TPA algorithm. During Audit, TPA gives a key to cloud service provider and requests MACs for the blocks. TPA compares with the media access controls at the TPA. Improvisation from Scheme 1: TPA doesn't consider the data, gives privacy. Drawback: a key can be used once, Schemes 1 & 2 are good for static data .

In paper [5] they discuss main challenges for achieving cloud computing services, this problem focuses on accountability in cloud computing. Accountability means verification of access control policies. We describe a working implementation of a variant of Gentry's fully homomorphism encryption scheme STOC in year 2009, similar to the variant used in an earlier implementation effort by Smart and Vercauteren PKC in year 2010.

4. EXISTING SYSTEM

Instead of being free from secret key giving to others, PEKS schemes to bear from an not secure regarding the trapdoor keyword privacy. The main event leading to such a security appering as if it is that anyone who knows receiver's public key can generate the PEKS ciphertext of switched to keywords. Specifically, given a trapdoor, the server can choose a imaginig keyword from the keyword space and then use the keyword to generate a PEKS ciphertext. The server then can test whether the idea of keyword is the one considering it as main in the trapdoor. This imagining-then-testing procedure can be repeated until the correct keyword is found. Such aidea of guessing attack has also been considered in many password-based systems. However, the attack can be launched more efficiently against PEKS schemes since the keyword space is difficulty to the same as a simple dictionary for example it must contain meaningful high level english words, which has a tiny size than a password dictionary for example it ust contain 6 alpanumeric words, only secret key holders can generate the keyword ciphertext and hence the adversarial server is not able to launch the inside KGA[6]. As the keyword always indicates the privacy of the user data, it is therefore of practical importance to overcome this security threat for secure searchable encrypted data outsourcing.

3. PROPOSED SYSTEM

This paper initiates a secure tree-based search scheme over the encrypted cloud data, which supports multi keyword ranked search and dynamic operation on the document or file collection. Specifically, the vector space model and the widely-used "term frequency (TF) × inverse document frequency (IDF)" model are combined to provide the index construction and query generation to provide multi-keyword ranked search as shown in Fig.1. In order to obtain high search efficiency, we build a tree-based index structure and propose a "Greedy Depth-first Search" algorithm based on this index tree. The secure K nearest neighbour(kNN) algorithm is utilized to encrypt the file index and queries, and meanwhile ensure accurate relevance to score calculation between encrypted index and query vectors. To withstand various attacks in different threat models, using PEKS algorithm we construct tree based model to search multikeyword that will sent from owner to user using trapdoor as mediator to transfer the files.

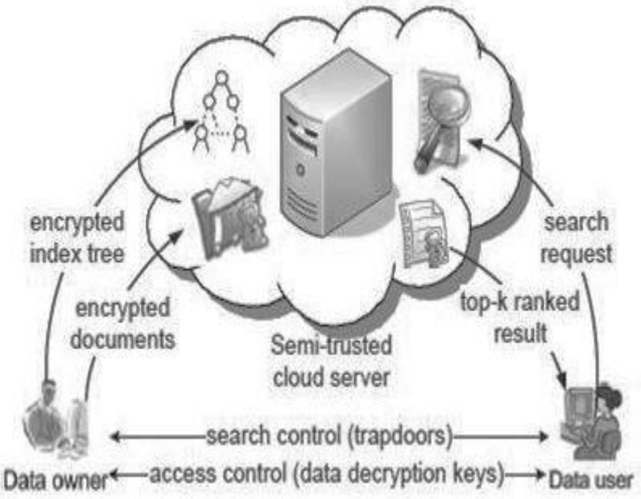


Fig 1. The architecture of ranked search over encrypted cloud data. Advantages of Proposed System:

1)Assigned to the important structure of our tree-based index, the proposed search scheme can flexibly achieve sub-linear search time and it will do with the deletion and insertion of documents or files.

2)we must construct a searchable encryption scheme that supports both the accurate multi-keyword ranked search and more flexible dynamic operation on document or file collection.

3)Because of the special tree based structure of our tree-based index, the search complexity of the proposed scheme is basically kept to logarithmic. And in practice, the proposed scheme can achieve higher search efficiency by executing our "Greedy Depth-first Search" algorithm. Moreover, simultanious search can be dynamically performed to further reduce the time cost of search process.

TFIDF algorithm

"TF(t) = (Number of times term t appears in a document) / (Total number of terms in the document).

IDF(t) = log_e(Total number of documents / Number of documents with term t in it)."[1]

Greedy depth first search

"Pseudocode

Input: A graph *G* and a vertex *v* of G

Output: All vertices reachable from *v* labeled as discovered

A recursive implementation of DFS:[5]

```
procedure DFS(G,v):
  label v as discovered
  for all edges from v to w in G.adjacentEdges(v) do
    if vertex w is not labeled as discovered then
      recursively call DFS(G,w)
```

A non-recursive implementation of DFS:[6]

```
procedure DFS-iterative(G,v):
  let S be a stack
  S.push(v)
  while S is not empty
    v = S.pop()
    if v is not labeled as discovered:
      label v as discovered
      for all edges from v to w in G.adjacentEdges(v) do
        S.push(w)"[1]
```

Advantages of Proposed System:

1)because of the special structure of tree-based index, the new search scheme can dynamically achieve sub-linear search time and deal with the deletion and insertion of documents or file.

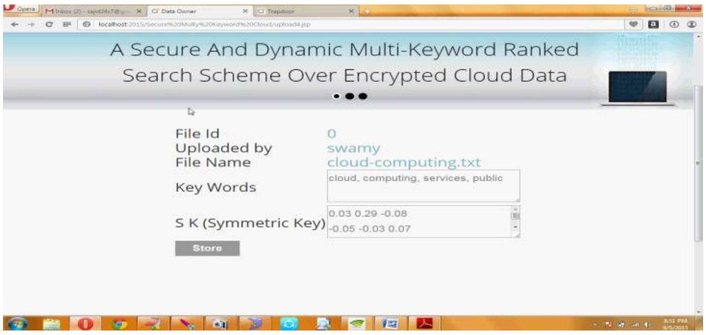
2) We design a searchable encryption method or scheme that supports both the accurate multi-keyword ranked search and dynamic operation on document collection.

3)Due to the special structure of our tree-based index, the search complexity of the proposed scheme is fundamentally kept to logarithmic. And in practice, the proposed scheme can achieve higher search efficiency by executing our "Greedy Depth-first Search" algorithm. Moreover, parallel search can be flexibly performed to further reduce the time cost of search process.

1. Data Owner: Register with cloud server and login (username must be unique). Send request to the admin. Browsing file file and generate keywords for the fill and then request it will done by trapdoor content key to encrypt the data, Upload data to cloud server. These keywords will be ssent to the user.
2. Data User : Register with data user and login (username must be unique). Send request to the trapdoor admin. Login and search by entering users choice keyword. This user id will be sent to email .
3. Trapdoor:Trapdoor model helps to generate secreate key ,this will act as mediator between user and owner will send the encrypted file to trapdoor to genetrate S_K and it will send it into user to decypt using RSA algorithm.
4. Search: In this module, the user will search that which file he want so for that he will give only keywords that may be multikeywords related to that keyword file will decrypted with help of trapdoor so using trapdoor user will decrypt file and download,so that S_K will sent ur user id.

5. RESULTS

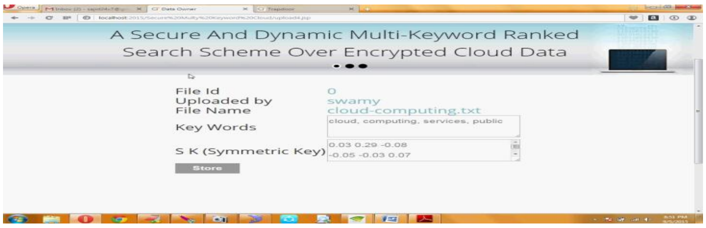
Below shown figures represents the results of proposed system.



A Secure And Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data

File Id 0
Uploaded by swamy
File Name cloud-computing.txt
Key Words cloud, computing, services, public
S K (Symmetric Key) 0.03 0.29 -0.08 -0.05 -0.03 0.07

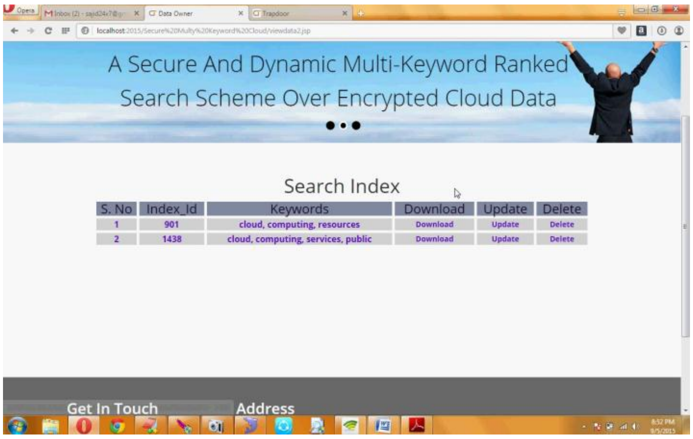
Fig-2: Keywords generation and File encryption by Data owner



A Secure And Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data

File Id 0
Uploaded by swamy
File Name cloud-computing.txt
Key Words cloud, computing, services, public
S K (Symmetric Key) 0.03 0.29 -0.08 -0.05 -0.03 0.07

Fig-2: Keywords generation and File encryption by Data user

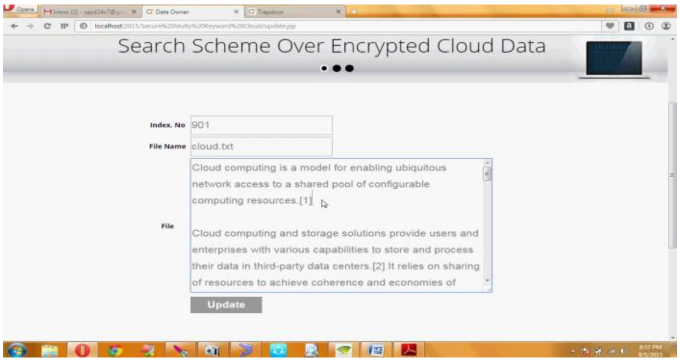


A Secure And Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data

Search Index

S. No	Index_Id	Keywords	Download	Update	Delete
1	901	cloud, computing, resources	Download	Update	Delete
2	1438	cloud, computing, services, public	Download	Update	Delete

Fig-3: Search in the cloud storage by data user



Search Scheme Over Encrypted Cloud Data

Index. No 901

File Name cloud.txt

File Cloud computing is a model for enabling ubiquitous network access to a shared pool of configurable computing resources.[1]

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers.[2] It relies on sharing of resources to achieve coherence and economies of

Fig-4 : File uploaded by owner

6. CONCLUSION

A dynamic search, and secure efficient search scheme is proposed, which will support not only the correct multikeyword ranked search but also the dynamically delete or insert of document or files. The security purpose of the scheme is protect against two threat models by There are still many difficult challenge problems in symmetric encryption S_K schemes. In already exists system. To design a more accurate character or keyword balanced binary tree based as the index, and propose a Greedy Depth-first Search algorithm to obtain better impact than linear search. In addition, the simultanious search process can be run out to further reduce the cost. The security of the scheme is protected against two threat models by using the secure kNN(k nearest neighbour) algorithm. In the proposed or new scheme, the data owner is responsible for generating updating information or file and sending them to the cloud server. Thus, the data owner needs to store the unencrypted file or index tree.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[3] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245.

[4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22,no. 5, pp. 847-859, 2011.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[6] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine,vol. 24, no. 4, pp. 19-24, July/Aug. 2010.