SECURE AND DYNAMIC MULTI CATCHPHRASE SITUATED INVESTIGATE ENCODED CLOUD DATA

Akanksha Nayak[1], Puneeth B.R[2]
[1]MCA Student, NMAM Institute of Technology, Nitte
[2]Asst professor, NMAM Institute of Technology, Nitte

Abstract:

In the cloud computing concept, this project solves and describe the complexity of multi-catchphrase ranked seek over encrypted cloud data while preserving compact system wise privacy. In order to protect the privacy of sensitive data, the sensitive data should be encrypted before uploading the data to the cloud. Encryption of data is a value added data employment tune and is not an easy task. The user can confidently search the encrypted data through keywords by making use of some searchable encryption method. The user can carry out only Boolean search. This searching method does not meets the users expectation as there will be large number of data files and users located in cloud. Therefore there is a need to permit multiple catchphrases while searching for a file and to return the files with respect to keywords. By the Boolean search technique the user will get the unsorted result. So to overcome this problem multiple catchphrase search over encrypted cloud data has been introduced. When the data owner encrypts and stores the sensitive data to the cloud, this method establishes set of isolation for cloud data use during the splitting of cloud data and stores the portion of data in different servers. Even though there are number of techniques for multi catchphrase search, this method is chosen because of its "coordinate matching" search technique. Then the sorted results are created according to Top K Query method.

Key Terms: Searchable encryption; multi-keyword ranked search; dynamic update; cloud computing.

Introduction:

CLOUD computing is measured as the new emerging technology of enterprise IT communications, which assemble huge resources of computing, storage and applications. It also enables the user to have everywhere. Cloud computing is handy and on-demand access to a public team of configurable computing resources having great efficiency and with a minimal cost. So in order to supervise the data, both individual and enterprises outsource their data to the cloud as an alternative of purchasing software and hardware for themselves as they were attracted by the features of cloud computing. Even though cloud services provide many advantages, when we outsource some sensitive data to distant servers it may end up with some privacy issues as some users may access the information without permission. In order to keep the sensitive data safe we can encrypt the data before outsourcing. But when it comes to data usability, encrypting the data causes huge cost. On plaintext data we can make use of keyword-based information retrieval, which is an existing technique. But we cannot directly make use of the same technique on the encrypted data, as locally decrypting all the downloaded data from the cloud is unfeasible. In classify to overcome the problem, some researchers came up with the solutions with fully-homomorphic encryption or oblivious RAMs. The computational overhead of these methods were high for both cloud server and users. So these methods were not practical. Some solutions like searchable encryption (SE) schemes have made explicit contributions in terms of efficiency, functionality and security. Client can store the encrypted data to cloud and he was able to execute keyword search over cipher text by making use of SE scheme. So far many works have been proposed but when it comes to practical concept multi keyword ranked search achieves more concentration. Recently some significant works have been done in order to give the privilege to data owner to update their files which are in cloud server. In order to support insert and delete operation on files some dynamic schemes have been introduced.

Be that as it may, few of the dynamic plans bolster productive multi catchphrase positioned seek our commitments are condensed as takes after :

1. The searchable encryption scheme which we designed supports both the exact multi catchphrase ranked search and supple dynamic operation on documents.

2. The search difficulty of the projected system is basically kept to logarithmic as we introduced the unique arrangement of our tree-based index. By executing our “Greedy Depth-first search” algorithm, search efficiency of proposed system is kept high.

3. In order to lessen the time cost of search process we flexibly perform parallel search.

System construction:

User face:

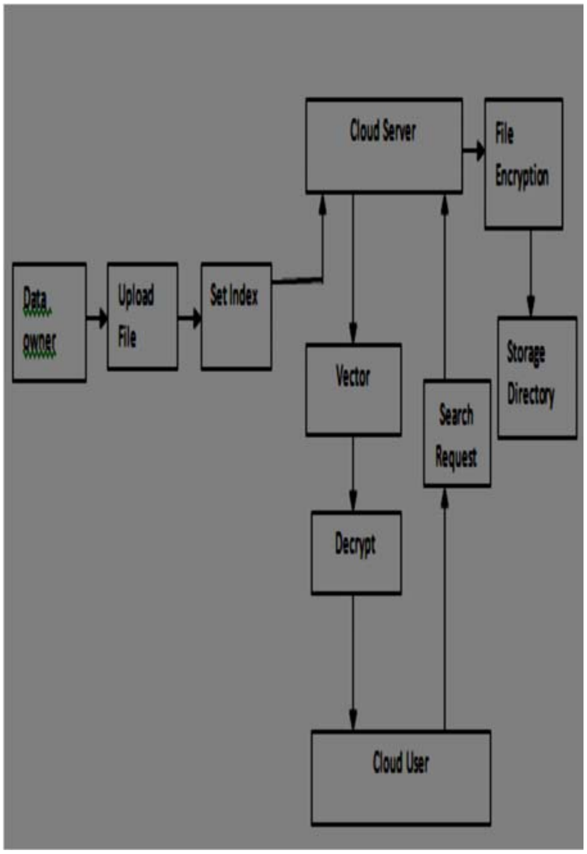
It searches for the required file from the cloud and sends the request to the Data owner for the access of the required file through multi keyword query request. Then the data owner sends the decrypt key to the user only if the user is authorized one and then the user can decrypt the file by using that key.

Data Owner Face:

The data owner encrypts the file before outsourcing it to the cloud. Data owner even outsources the secure index to the cloud servers. It constructs the tree in order to search the documents, before that the preprocessing is conducted over a set of documents.

Server side:

It stores the encrypted document which data owner has out sourced. Even it stores the encrypted searchable tree for data owner.



Reward:

- This system is more convenient for the user as it utilizes Ranking based search.

- Privacy, honesty and verifiability of client data against un- trusted cloud provider are the features provided by proposed cloud storage systems.

Module Description:

I. **Data Owner**

The processes maintained by Data Owner are:

- **Ensuring Network connection**

In order to check the network connection from cloud server and user data owner initializes server. In order to execute all the process the connection establishment should be done.

- **Document encryption**

In order to ensure the privacy of the sensitive data, Data owner will encrypt the data before outsourcing.

- **Storing encrypted document to cloud server**

Different types of encrypted document will be collected by the cloud server. The encrypted data which was outsourced by data owner will be stored to cloud server. Ranking is provided based on searching of documents in cloud by making use of some ranking criteria.

.

- **Mail decrypted key to user**

When user searches for some document and ask the owner for accessing that document, owner will check whether the user is authorized or not in order to send the decrypt key.

II. Cloud server

The processes maintained by the cloud server are:

- **Get back request from user**

When user request for some for the document to the data owner, Cloud server will help the owner to fetch the request done by user.

- **Search index/rank computation**

There will be large number of documents present in the cloud. So in order to have the efficient data fetching ranking technique is used. The ranking technique will return the most relevant data by eliminating unnecessary traffic in the network.

- **Answer to user**

The cloud server will help the user to search the document by providing the ranking to the documents and search index.

III. Data User

The processes maintained by the user are:

- **Ask for cloud server**

The user searches for the document and sends the request to data owner with the help of cloud server. The cloud server acts in an honest fashion.

- **Get back decrypted key from admin & document from cloud server**

The user will fetch the decrypt key sent by the owner in order to decrypt the encrypted document which user has requested. The user will fetch the document from the cloud server.

- **Decryption of file**

The file sent by the owner to the user will be in the encrypted format, so to read the file user needs to decrypt the file with the help of decrypt key.

Functionality:

- In order to protect the sensitive data before outsourcing to the cloud, Data owner needs to encrypt the data for the security of data. Before that the Data owner needs to register and login.
- Data Owner got the privilege to update their files which are in cloud server.
- Data owner can even check whether the user is authorized or not before sending the decryption key.
- Once the data user is registered and logged in, he can search for the required files
- Data users can even request the owners for decryption keys.
- By using decrypting key, User can download the files.

Calculation:

Step 1: Process of Authentication

- Verifying clients and respect them by classifying them into declaration proprietors and front page new clients.
- On the off chance that it is story client when specified offer affirmation to make a beat up showing with regards to its documents and oversee transferring records by all of file watchwords. In the event that it is word client prior permit to go to records as it were.

Step 2: Document Upload

- Information proprietor by all of number of documents (f1, f2….fn) will be validated by secret word.
- Making of minimal dark book (f1', f2'….fn') for each bungle document prior transferring.
- At that point, f and f' will be encoded.
- Transfer encoded f and f' to diminish server.

Step 3: Retrieval of File

- Users need to legally approve themselves by entering secret word.

- To look for particular claim the request in the constitute of watchwords (k) will be sent.

- Coordinating k with f1', f2'…..fn'.

- For agnate the varieties of looked catchphrases is thought about by the entire of the list documents.

- In light of this outcome (k~f') the rundown of documents (fm… fx) is sent to the client.

- The documents are orchestrated in rising request of their pertinence score.

- Higher made a beat up showing with regards to will be if and just if to the roughly downloading charge and this close will be refreshed as by download.

- Clients have the decision to choose document from fm….fx to download.

- At that point, at the heels of choice of case the feeling of obligation will be produced in any case particular charge for particular profession of augur and will be electronic mail to the addict, abaft wards entering this code already just the decoded detail of the had the law on is open to that client.

Encryption prepare: The encryption of the records will be finished by the office of SHA1 calculations as gives has a hop on security eventually for littler key timeframe contrasting with finish other calculation.

Estimated Results:

1. **Information Encryption and unscrambling Result**
   At the point when RSA calculation is connected on the information then we get scrambled information. Also, that encoded information is store on the cloud. Client can get to the information subsequent to downloading and unscrambling record. For encryption and decoding keys are given

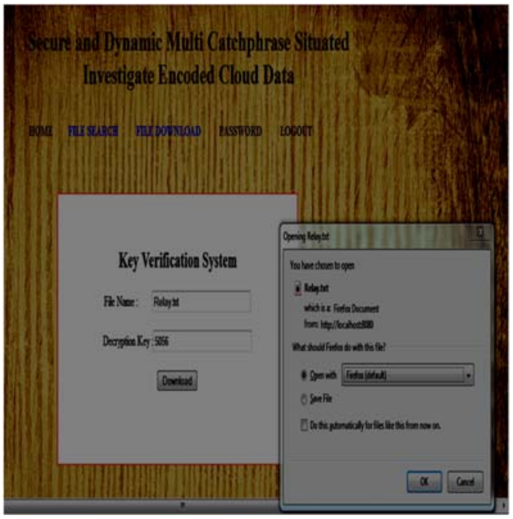
2. **Positioning Result**
   At the point when any User ask for the information then Ranking is done on asked for information utilizing k-closest neighbor calculation. For Ranking co-ordinate coordinating standard is utilized. Subsequent to positioning client gets the normal aftereffects of the question.

3. **Ready System Results**

   On the off chance that any unapproved User tries to get to or refreshing the information on cloud, then ready will be created as mail and messages. The ready lingerie the approved client.

Form to decrypt the encrypted file and to access the file:

In order to download the file the user needs to make use of decrypt key. After entering the decrypt key, if the entered key is correct then user can decrypt the encrypted file and can read it. Even the user can download the file



File Name : Relay.txt

Decryption Key : 5056

You have chosen to open

Relay.txt

which is a: Firefox Document

from: http://localhost:8080

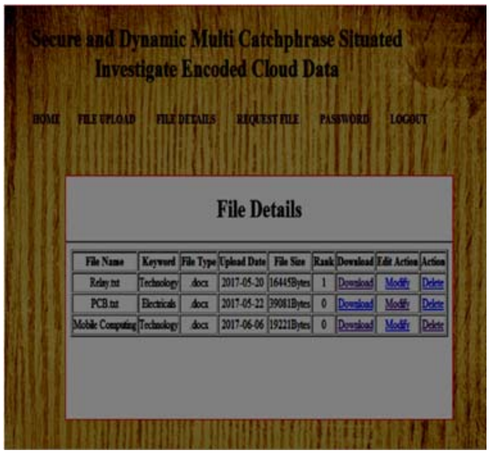
What should Firefox do with this file?

● Open with Firefox (default)

○ Save File

□ Do this automatically for files like this from now on.

Form which Determines Rank:


Secure and Dynamic Multi Catchphrase Situated
Investigate Encoded Cloud Data
HOME
FILE UPLOAD
FILE DETAILS
REQUEST FILE
PASSWORD
LOGOUT
File Details

File Name	Keyword	File Type	Upload Date	File Size	Rank	Download	Edit Action	Action
Relay.txt	Technology	docx	2017-05-20	16445Bytes	1	Download	Modify	Delete
PCB.txt	Electricals	docx	2017-05-22	39081Bytes	0	Download	Modify	Delete
Mobile Computing	Technology	docx	2017-06-06	19221Bytes	0	Download	Modify	Delete

When the user requests for some of the file or if the user downloads the file, then the rank of the file increases.

Conclusion:

- In the proposed system we projected a secure, efficient and dynamic scheme which supports both multi-keyword ranked search and dynamic deletion and insertion of documents.
- In order to get the better efficiency than linear search, we construct a special keyword balanced binary tree as the index, and propose a “Greedy Depth-first Search” algorithm.
- In order to reduce the time cost we carried out a parallel search process.
- By using kNN algorithm we gave the security to the scheme.

References:

[1] K. Ren, Cowing, Q.Wang *et al.*, “Security challenges for the publiccloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136– 149.

[3] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, “Software protection and simulation on oblivious rams,” *Journal of the ACM (JACM)*, vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in *Advances in Cryptology-Eurocrypt 2004*. Springer, 2004, pp. 506–522.

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III,“Public key encryption that allows pir queries,” in *Advances in Cryptology-CRYPTO 2007*. Springer, 2007, pp. 50–67.

[7]Xia, Zhihua, Xinhui Wang, Xingming Sun, and Qian Wang. "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, 2015.

[8] E.-J. Goh *et al.*, “Secure indexes.” *IACR Cryptology ePrint Archive*, vol. 2003, p. 216, 2003.

[9] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in *Proceedings of the Third international conference on Applied Cryptography and Network Security*. Springer-Verlag, 2005, pp. 442–455.

[10] 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.

[11] M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient similarity search over encrypted data,” in *Data Engineering (ICDE), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 1156–1167.

[12] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, “Achieving usable and privacy-assured similarity search over outsourced cloud data,” in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 451–459.