Privacy Preserving Ranked Multi Keyword Search for Multiple Data Owners

Rajan Kumar[#], Anurag Roy[#], R. Yamini[*]

[#] Student, Dept. of CSE, SRM University, Kattankulathur
[*]Assistant Professor, Dept. of CSE, SRM University, Kattankulathur

***Abstract*—As we know, most cloud server do not serve single user, they give service to multiple user at the same time. This project consist of functions in which user can search multiple file and send the file to multiple user at the same time. It has ranking search technique in which most frequent searches are shown. A dynamic secret key is generated which prevent others for stealing data.**

Keywords: Cloud computing, ranking search, multiple data owners, dynamic secret key

I. INTRODUCTION

Cloud computing becomes popular and has important role in our lives. Cloud computing gives many benefits such as data storage, running websites into the cloud. Users can upload many documents like financial details, government details etc. All these information can be access by the user. To protect the data privacy in cloud, the data has to be encrypted first by the user before uploading on the cloud and after that the data is decrypted by the key and download data on the local system.

II. LITERATURE SURVEY

EXISTING SYSTEM:

In the Existing System, the data owner share file to a single user and the user who is authorized can download the shared files by giving the decryption key. This system was not secured and takes more time to share files to user. The Existing System does not have any searching technique of the data files in cloud.

PROPOSED SYSTEM:

In this paper, we proposes scheme which enables users for searching files by giving the keyword. This project consist of protocols in which users uses different keys to encrypt and decrypt files. This paper consist of secure search protocol in which user can search files by giving the short or full data files names. To prevent the attackers from eavesdropping, a dynamic secret key is generating.

- *ADVANTAGE OF PROPSED SYSTEM*

A. It allow searches over encrypted files.
B. Decryption key should be send via a secure channel like Gmail.
C. Data files are encrypted on the cloud server.

III. PROBLEM FORMULATION

A. PROBLEM DEFINATION

This project is used to search multiple keywords and share files to multiple users. This project consist of searchable technique which gives the facility to search over cloud.

B. ARCHITECTURE MODEL

The proposed system contain data users, the cloud server and the administration server. When the users have right to access in the server from their local system, they select the file which have to upload on the cloud. This selected files is saved on the location where all the users files are saved (Because there is not only single user, there are multiple user which cannot interact directly). Now from that location, the user uploads the data file on the cloud. When the data is uploaded, if the user wants to share that uploaded files, he/she can share with the registered users along with the private key. When the data files are uploaded on the cloud, the server can't know the contents of data files because the data files are encrypted. When the shared users wants to access the file, he/she requests the decryption key. Then the decryption key is sent to their registered mail account. By using that decryption key, the contents of the data file gets decrypted and the users can download the data file.

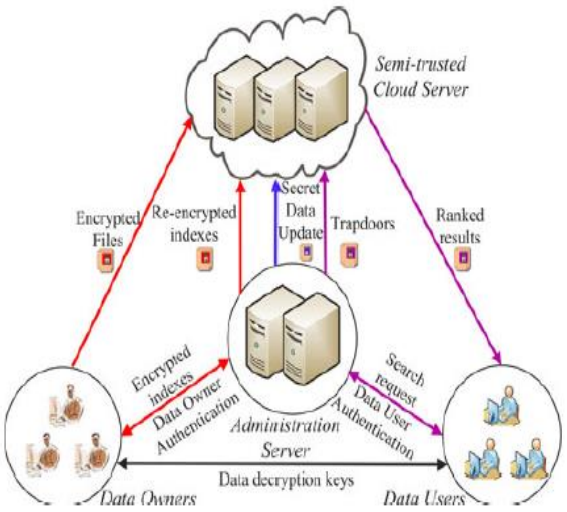
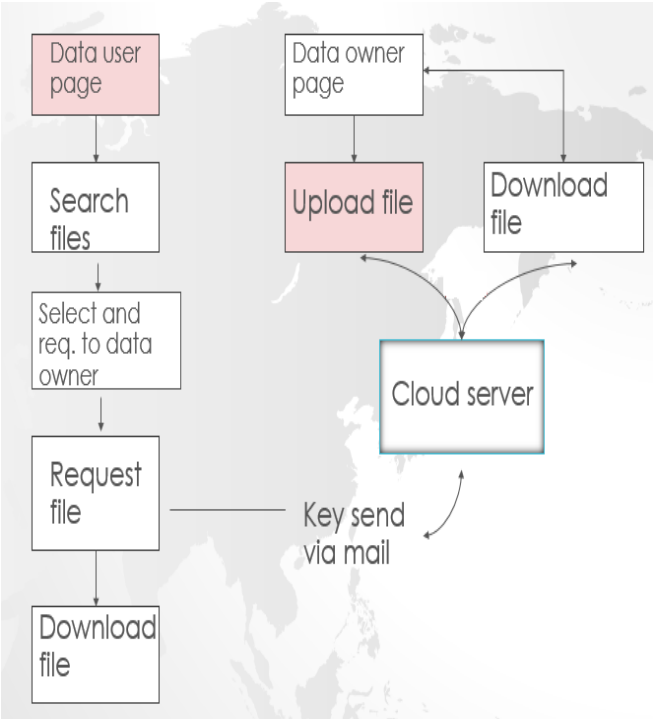


Fig. 1. Architecture of privacy preserving keyword search in a multi-owner and multi-user cloud model.

If any attackers can access the cloud server then he/she cannot get the contents of the actual data files. The cloud server is only responsible for storage of data files.



Flow Diagram

C. SECURITY GOALS

In this paper, we proposes scheme in which function design satisfy security goals.

- **Multi keyword Search over Multiple data owner:** This paper allow multiple search over encrypted data files. This allows the server to ranked the searched result among different users and return the most frequent results.

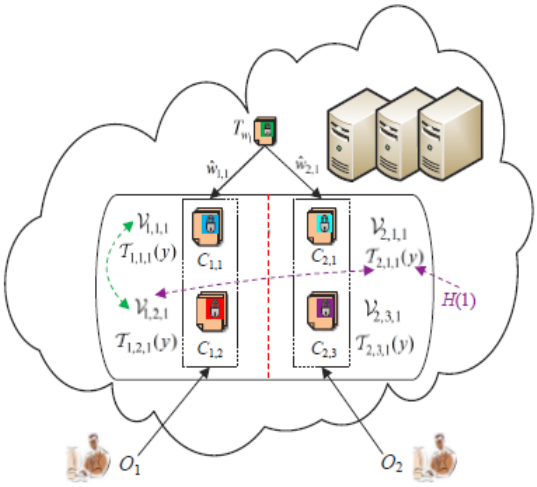


Fig. 5: Example of ranking search results

- **User scalability:** This paper allow new data users to register and login to this system without disturbing other users.
- **User revocation:** This paper allow that only registered data users can perform right search.
- **Security Process:** This paper prevent attacker from eavesdropping. When the files is shared which is in the encrypted form, another users wants the keywords to decrypt the data files.

D. *MULTIPLE KEYWORDS SEARCH*

In this paper, user can search multiple file names. This proposed system also search the fuzzy keyword which means if the data file name is abcd.txt and the user search ab then it shows all the data files that contain the letter ab simultaneously.

IV. SYSTEM MODULE

1) Authentication and Authorization

In this module, the data user register with their user-id, Password, email-Id, mobile number and gender then user can access the database. After registration completed, user access the database by giving the user-id and their password.

2) Uploading and Downloading

In this module, Files are uploaded to the server after file is encrypted by the encryption method. This encryption is done by AES (Advanced Encryption Standard) Algorithm and generate key. This Encrypted Data is in the form of Binary and stored in Cloud. User needs decryption key to download the data files.

3) File Sharing

In this module, the uploaded files are shared to the multiple users. In this system, the Private Key of the Data which is shared will be send via a secure channel called Gmail. This decryption key is used by the user at the time of download the files.

4) **Key Generation**

In this module, when the user wants to access the data files then the server send the decryption key. Through this decryption key, the user who wants to access the data file, uses this decryption key to decrypt the files with the help of private key sent at the time of file sharing.

5) ADMIN MODULE

In this module, admin can view the details of all the registered users. Admin can see the status of the shared files among multiple users.

V. ALGORITHM USED

There are two types of algorithm used in this project.

1. Encryption:

This is used to encrypt the data files. This convert the plain text into the cipher text. This uses the AES (Advanced Encryption Standard) algorithm.

2. Decryption:

This is used to decrypt the data files. This convert the cipher text into the plain text. This uses the ADS (Advanced Decryption Standard) algorithm.

VI. SECURITY ANALYSIS

A. KEYWORD

In this proposed system, keywords are known only for the registered user. If the unknown users gives the keyword for searching the data files, it does not search and shows that the data file is not found.

B. ENCRYPTION and DECRYPTION Key

In this proposed system, when the user shares a particular data file, the private key is sent to all the shared users. When a user wants to decrypt the data file then he/she request the decryption key. Then the server sends the decryption key to the authenticated user to their registered mail Id. By using this decryption key, the user decrypts the data files and then he/she can download the file.

VII. CONCLUSION AND FUTURE WORK

In this paper, we solve the problem of secure multi keyword search for multiple data owners in the cloud computing. We introduced a secret key generation protocol and a new data user authentication protocol which is used to protect the system from attackers and authenticate only the registered users.

In our future work, we work on the secure fuzzy keyword search in multiple data owner and we are planning to implement on the commercial cloud.

REFERENCES

[1] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE,Jie Wu, Fellow, IEEE, and Siwang Zhou," Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing".

[2] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in *Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014)*. Atlanta, USA: IEEE, jun 2014, pp. 276–286.

[3] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[4] T. Jung, X. Y. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proc. IEEE INFOCOM'13, Turin, Italy, Apr. 2013, pp. 2625–2633.

[5] W. Sun and et al., "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in *Proceedings of ACM SIGSAC*, 2013.

[6] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *Computers, IEEE Transactions on*, vol. 62, no. 11, pp. 2266–2277, 2013.

[7] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in *Proc. IEEE INFOCOM'12*, Orlando, FL, Mar. 2012, pp. 451–459.

[8] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in *Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014)*. Atlanta, USA: IEEE, jun 2014, pp. 276–286.

[9] 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. IEEE ASIACCS'13*, Hangzhou, China, May 2013, pp. 71–81.

[10] Y. Yi, R. Li, F. Chen, A. X. Liu, and Y. Lin, "A digital watermarking approach to secure and precise range query processing in sensor networks," in *Proc. IEEE INFOCOM'13*, Turin, Italy, Apr. 2013, pp. 1950–1958.