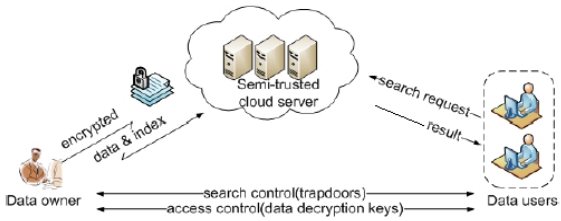
encryption techniques. The schemes designed to support the encryption which is searchable allows the client to save the information which is encrypted into the cloud and allows us to execute a required keyword search. [2][4]

Till now, lots of works have been suggested under separate models to accomplish various search functionalities, such as search for single keyword, search for similarity, Boolean search multi-keyword, ranked search of multi-keywords, etc. [7]



Disadvantages of Existing System

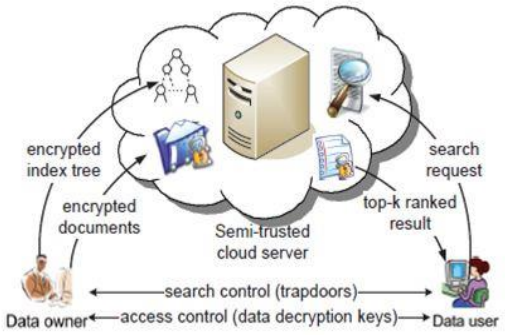
- Vast cost in terms of information usability. For example, some of the existing techniques on retrieval of information, cannot be implemented and applied on the text which has been encrypted. It is undoubtedly impractical to consider the downloading of the data and then followed by the decryption of it locally. [3]
- Existing System methods are not practical because of their mammoth time complexity not only for the cloud sever but also user. [11]

Our Implementation

In this particular paper, we have created a binary tree which is balanced also known as the index, and present a “Greedy Depth-First Search” type of algorithm so as to achieve much better capability than the currently existing linear search. The kNN secure algorithm is used for Ranked search scheme for encrypted data. It also supports operations such as deleting and inserting in a dynamic manner. These works are symbolic as it is highly possible that the data owners require updating their data on the cloud server.

Advantages of Proposed System

- It is more efficient algorithm ranking the datasets in the cloud.
- It provides support for dynamic operations on the documents.
- More securely stored data in the cloud.



Project Modules

- Provider of Cloud Service
- Data owner Module
- Data user Module
- Ranking System

Provider of Cloud Service

In this particular module, we have been developing a module for service providing. This allows the provision of storage of data in the cloud which is considered public. [4]

This S-CSP has to provision of redistributing of services and also saves the required data on account of the users.

To dampen and ultimately curtail the cost of storage, this S-CSP eradicates the saving of the data which is repeating via the extermination of duplicate data so as to keep only the proper and exclusive data.

In this particular paper, there is an imperative assumption that the S-CSP is something which is always on the line and the capacity of storage which is mammoth, and also has a greater power of computation.

Data owner Module

An owner can be described as someone who has the privilege of having abundant amount of storage space and also has the authority to grant it to the required user for the purpose of storage of data at any particular time. [8][11]

Considering a system of storage which supports deduplication of data, the person who owns the storage space allows the user who wants the storage space to upload the data in his granted space, which can be leased to other users.

Data user Module

A user can be considered as an individual who wishes to redistribute the storage of the required data to that corresponding S-CSP and also has the privilege to access that particular information whenever the individual wishes. [5]

Considering a storage system which rapports the deduplication of data, the data being uploaded by the user is unique, but not something which is duplicate, this is so as to save bandwidth, irrespective of the owner.

Consider the deduplication system which supports authorization, every particular user is subjected to a set of allowances in the composition of the arrangement. [9][10] Every file is guarded by using the corresponding key which is encrypted, after this, the allowance keys have to be used so as to remove the deduplication with privileges which are differential.

Ranking System

In data deduplication ranking system done through enhanced dynamic ranked search of multi-keywords.

The search keywords are predicted and shown in the search results according to the ranking.

If a user is involved in keyword search, the enhanced dynamic ranked search of multi-keywords will analyze the keyword and manage to show a result according to the ranking system created by the user. Hence the top ranked search results will be shown first. And the less priority search results will be on the below.

Conclusion and Future Work

This particular paper presents a search scheme which is immune, very efficient and which also supports dynamic operations in a productive manner. [12] Additionally, this scheme is very unique as it not only supports definite ranked search which consists of multiple keywords, but also supports operations such as deleting and inserting in a dynamic manner. In this paper, we create a binary tree which is balanced also known as the index, and present an algorithm of the type "Greedy Depth-First Search" so as to achieve much better capability than the currently existing linear search. [9][10] Moreover, the time cost can be reduced significantly by utilizing the process of parallel search. The security of this particular design is guarded against the two threat models by employing kNN secure algorithm.

The future work of this scheme seems ambitious and arduous, this is because the operation can only be done by the cloud server only. Moreover, keeping the ability of the system to support ranked search of multi-keywords. On top of this, because of the fact that almost all the work is about searchable encryption, this particular scheme acknowledges the difficult of the cloud server.

References

[1] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou, "Privacy-Preserving Ranked search of multi-keywords over Encrypted Cloud Data," *IEEE Parallel and Distributed Systems*, vol. 25, no. 1, 2014.

[2] K. Ren, C. Wang, Q. Wang *et al.*, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

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

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D.dissertation, Stanford University, 2009.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public

key encryption with keyword search," in *Advances in CryptologyEurocrypt 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] E.-J. Goh *et al.*, "Secure indexes." *IACR Cryptology ePrint Archive*, vol. 2003, p. 216, 2003.

[8] 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.

[9] 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.

[10] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–5.

[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.