A SURVEY ON SECURED OUTSOURCED ENCRYPTED DATA WITH INDEX AND RANKING TECHNIQUES

Prajna M1 and Prabhakara B.K2

1,2Department of Computer Science Engg,Sahyadri College of Engg&Management

Abstract- Cloud computing is encouraging data owner to outsource the document to the cloud server. But the data user is taking the advantages of cloud only when there is security for the document. For that purpose before outsourcing the document to cloud it need to be encrypted. Encryption is done using symmetric encryption rather than asymmetric encryption. Considering, large number of data user and document in cloud, it is challenge to provide the search services for encrypted document. To meet this challenge multikeyword search technique is used. For the purpose of effective data retrieval ranking techniques is used. This system will define and provide solution to the problem of privacy by establishing strict privacy for secured cloud documents.

Keywords- Cloud computing, multikeyword, Searchable encryption.

I. INTRODUCTION

The cloud customer is storing the data in the cloud in order to get better services and high quality resources. Features of cloud such as extensibility and cost-effectiveness are encouraging organization and single user to outsource the complex data onto the cloud. To protect the data from the access of unauthorized user encryption is required before outsourcing to cloud. Later retrieving all the data from cloud and then decrypting at the restricted area is impractical, due to large bandwidth cost of cloud. Storing the data in cloud rather than storing it locally in storage management is useless unless there is efficient usage of resources and effective searching process. Considering the large number of user and outsourced document, it is a challenge to meet the requirements of usability of a system, performance of system, system scalability.

Ranking technique is provided to speed up the search process. But all documents are assigned the same priorities so that the third party and the service provider in cloud will not know the information of document and thus privacy is provided to the document. Ranked search will allow removing the unwanted network traffic by sending only the relevant data back to the user. For protecting the privacy such as ranking search, should not release any keyword related to the documents. To improve the Searching experience of the user and also to increase the accuracy of search result it is necessary to support ranking technique with multikeyword search. The user may provide multiple keywords in order to extract the relevant data. Actual privacy is provided only when the user identity is unexposed from the third party and the service provider of the cloud.

In this paper the section 2 explains the different methods that are used for security and the techniques used for extracting the data are cloud server and then conclude the paper.

II. LITERATURE SURVEY

C. Wang, N. Cao [1] proposed that in cloud the document is usually outsourced from the local storage to the cloud. To provide security to the document the data is encrypted and stored. It is important to invoke the searching process for the encrypted data. The searching process is done using multiple keywords. On receiving the request from user and the relevant document are extracted and send back to the user in relevant order. Data user is provided with keyword sets instead of single keyword. Each keyword helps in retrieving the data. “Coordinate matching” is implemented to extract the data that is relevant to the query. “Inner product similarity” The query keywords totally appearing in a data document is quantitatively calculating identical measures of data document from
the query is used in multikeyword technique. The limitation of using this method is that the User identity is not hidden. Any user who is outsourcing the data is known to the Service Provider of that cloud. A security issue arises so it is risky to store and maintain the confidential data.

D. Song [2] proposed an efficient technique that is desirable for storing data in cloud server. If user request to retrieve the document that consist of particular words and those words are not previously known then how the documents are searched by the cloud server without leaking the private data. For this purpose Cryptographic schemes with basic primitives are used such as generator, permutation, function. For searching probabilistic search techniques is used. Advantages of using this technique is only authorized user are allowed to read data from server. The schemes implemented are efficient because the algorithm used during implementation is simple. The cons arises are Security issues during search process.

C. Wang Cloud [3] described an approach where user has no knowledge of encrypted data stored on the cloud, and performing the post processing on the every document to find the matching data from the requested once. If we go on extracting all the documents that contains the query keyword, this leads to the unwanted traffic issues in the networks. Searching process takes place on the file based on the order of ranking. This will provide privacy to the file in cloud server. The ranking scheme proves to return efficient an relevant document which is requested by cloud user. The Objectives of using this scheme is to enhance the security for the document in the cloud.

S. Kamara and K. Lauter [4] described the main advantages of using cloud are to provide security and reduce the risk while storing confidential data. But there are many issues arise based on security. To overcome this problem cryptographic system for storage is used in cloud. The legal problems from customer and service provider will be reduced. The services of cloud build on the layer above the cryptographic services for storage purpose will be securely exchanging the data, provide backup facilities, records related to the hospitals is also explained in details.

N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou [5] proposed a method in which data when outsourced to cloud it will be in encrypted form for security purpose. Encrypting the document before outsourcing is done on the sensitive data to provide effective utilization of the resources present in the cloud. Filtering, verification method is used. Index is implemented to provide the information related to data graph that are encrypted and then select the keyword and use it to perform filtering. To select a keyword and perform computation product schemes is used inorder to meet the privacy issues. In filtering input is taken as data graphs from many possible dataset and output produced in the set of candidate subgraph. In verification each subgraph is checked by subgraph isomorphism. Set of subgraph is smaller when compared with the dataset. Such technique requires limited subgraph isomorphism which increases the performance of the system. When data graph is in encrypted form and stored on to cloud the filtering technique is eliminated which is mainly related to the data in plaintext form. Inorder to reduce the size of the index on the required subgraph that are frequently used and those subgraph are different from one another are indexed.

J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, [6] proposed a method for secured searching. The cloud user are increasing day by day and the amount of sensitive data stored on the cloud is also increasing. For security purpose the document are in encrypted form and then stored on cloud. Earlier schemes provided secure searching method based on the keyword and retrieved only those document that user has requested. Techniques allowed extracting only the exact keyword. This technique produced the problem such as low efficiency, usability of the system was reduced, and complexity of searching method is increased. To overcome this problem fuzzy keyword searching scheme is used. In this method keyword match is not foundor failed in matching the similar keyword then the closest match of the document based on the requested keyword is retrieved. This reduces the overheads of the document representation and storage space.

C. Wang, Q. Wang, K. Ren, and W. Lou, [7] proposed an efficient method for storing data in which user does not have physical control over large set of outsourced files and providing security will also be a challenging task. User outsources the files to cloud in order to reduce the burden of data storage and its maintenance. Providing auditability for data storage in cloud is a difficult task.
because the user can request independent audit party to verify the security of data stored in cloud. To select the independent party auditor they need to meet the basic requirements. The first requirement is third party auditor should audit the data stored on cloud effectively without pressuring for the copy of the locally stored data and should not provide the online responsibility on the cloud server. Second requirement is the data stored on cloud will be processed by the independent audit party but it should not add new burden to the sensitive data the user. The public key is combined uniquely based on random masking with the homomorphism authenticator to provide privacy for auditing system in cloud. Bilinear aggregation signature is a technique used to handle efficiently many auditing job. This techniques is highly secured and also efficient.

Eu-Jin Goh[8] Proposed a secured method for index. Anindexes given for each document will help to retrieve the document containing the keyword in a specific amount of time. Only the trapdoor which is valid will be accepted and the specific document is released. Proposed model for indexing is semantic security (IND-CKA). In this method the document that is encrypted need to be of the same size and we provide indexes to those document. The drawback is some information about the document other than the keyword was leaked. To overcome this problem advanced method was used IND2-CKA. In this method two document are provided index with different keywords that cannot be differentiated. On the other side No of keywords present in the document cannot be reduced from the size of document that is encrypted. Later Z-IDX techniques is used with the two methods bloom filters and pseudo-random function. The time required for searching each document is O(1).

III. PROPOSED METHODOLOGY

In order to extract the data from the cloud server we make use of multikeyword instead of single keywords so that only the relevant data is being extracted from the cloud and also the network traffic problem is reduced by stopping unwanted data from being extracted. Before outsourcing data need to be encrypted by making use of symmetric encryption method and also to provide indexing for each data. While extracting only the op k data is extracted even ranking technique is being used.

IV. CONCLUSION

This paper, describes large number of techniques that are used to provide security for the cloud data which is in encrypted form. Different method are used to provide index for the cloud document that is stored on cloud server and thendifferencing techniques are used to search the related document based on the index and then retrieving those document will be easy and fast. To retrieve the data we used ranking technic so that only the matched data was retrieved. If matched data was not found closely matched data will be extracted and given to the user. Ranking technic will also reduce the network problem related to unnecessary traffic.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure Ranked-Keyword Search over Encrypted Cloud Data,” Proc. IEEE 30th Int’l Conf. Distributed Computing Systems (ICDCS ’10), 2010.
[2] D. Song, D. Wagner, and A. Perrig, “Practical Techniques for Searches on Encrypted Data,” Proc. IEEE Symp. Security and Privacy, 2000.
[3] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467-1479, Aug. 2012.
[4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, Jan. 2010.
[5] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, “Privacy-preserving Query over Encrypted Graph-Structured Data in Cloud Computing,” Proc. Distributed Computing Systems (ICDCS), pp. 393-402, June, 2011.
[6] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy-Keyword Search Over Encrypted Data in the Cloud computing,” Proc. IEEE INFOCOM, Mar. 2010.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, 2010.
[8] Eu-Jin Goh, “Secured indexes”, eujin@cs.stanford.edu, 2004.