International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 11 3650 - 3653

Efficient Multi - Keyword Ranked Search over Encrypted Cloud Computing

Miss.Snehal M.Shewale
Padmabhooshan Vasantdada Patil Institute of Technology
Computer Engineering Department
Pune,India
e-mail:snehalshewale2008@gmail.com

Prof.Y.B.Gurav
Padmabhooshan Vasantdada Patil Institute of Technology
Computer Engineering Department
Pune,India
e-mail: ybgurav@gmail.com

***Abstract*—** Cloud computing allow customer to store their data on remote site so it reduce burden on local complex data storing. But before storing sensitive data it can encrypted and this can overcome plaintext keyword search.AS large number of user and data on cloud and for search on that data allow multi keyword search also provide result similarity ranking for effective retrieval of data. From number of multi-keyword semantics to identify similarity between search query and data highly efficient rule of coordinate matching, i.e., as many matches as possible, and then use inner data similarity for quantitatively similarity measure. In this system, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE),and establish a set of strict privacy requirements for such a secure cloud data utilization system to be implemented in real. We first propose basic idea of different privacy preserving multi-keyword search technique along with search on data that store on cloud in encrypted form and maintaining the integrity of rank order in search result and the cloud server is untrusted. .By hiding the user's identity, the confidentiality of user's data is maintained

Keywords-*Cloud Computing ,Privacy Preseving,multikeyword,Ranked Saerch,Encryption*

*****

I. INTRODUCTION

The Cloud Computing can provide dynamically scalable resources provisioned as a service over the cyberspace. It transfers stored data as well as service for demand users. Due to rapid expansion of data, data owner tends to store data into cloud to release the burden of data storage and maintenance [1]. Cloud provides more flexibility and economic savings for both individuals and enterprises to outsource their local complex data management system into the cloud. Large amount of data can store in cloud. Cloud provider encrypts the confidential data and stores it in the cloud so that only the authenticated users can access the data. Thus the keyword privacy is maintained. To provide privacy of sensitive data such as email, hospitals records, tax documents, photo album etc. encrypted by data owners before outsourcing to the commercial public cloud; this however violates the traditional data utilization service based on plaintext keyword search. In Cloud Computing, to protect data privacy and combat unasked accesses, sensitive data has to be encrypted before outsourcing [4] so as to give data confidentiality assurance in the cloud.

Huge number of on-demand data users and large amount of outsourced data documents in the cloud, so it is difficult to meet the requirements of performance, system usability, and scalability. To maintaining privacy of data ,document ranking is provided for fast search, but the priorities of all the data documents is kept same so that the cloud service provider and third party remains unaware of the important documents.

Large amount of documents demands the cloud server instead of returning undifferentiated result only relevant document can retrieve using ranking .Ranking can also eliminate unwanted network traffic .For protection purpose the information related to keyword should not be leak while use the ranking scheme. To enhance the accuracy of ranking system it supports multiple keyword search along with single keyword search. As a common practice indicated by today's web search engines (e.g., Google search), data users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data[5].In multi-keyword ranked (MRSE)search require privacy in terms of data privacy, index privacy, keyword privacy.

II. LITURATURE SURVY

Data is stored as public or private so different searching strategies are available for both types of data. The confidential data are stored in the cloud using encryption technique [2,3]. So only the authenticated members who know the key can access the data. Accessing data from encrypted storage is very difficult. A different type of searching technique is used to search for encrypted data [6] such as Fuzzy keyword search, search using conjunction of keyword etc.

A. Secured Multi-keyword Ranked Search over Encrypted cloud data

In cloud computing complex data management system of local site can outsource to commercial public cloud for economic savings and providing flexibility to data access. To provide security to stored data, it is must to encrypt before storing data. In main aim is to find the solution of multi-

keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise privacy in the cloud computing paradigm[15]. Among various multi-keyword semantics, the efficient similarity measure is "coordinate matching", (as many matches are possible) to effectively capture the relevance of outsourced documents to the query keywords, and use "inner product similarity" to quantitatively evaluate such similarity measure of that document to the search query is used in MRSE algorithm[5].

B. Crptographic cloud storage.

When public cloud is used for outsource the data ,it introduces security and privacy risck.It seems that cloud storage concern about the data integrity and confidentiality. In [7], an overview of the benefits of a cryptographic storage service, for example, reducing the legal exposure of both customers and cloud providers, and achieving regulatory compliance is provided. Besides this, cloud services that could be built on top of a cryptographic storage service such as secure backups, archival, health record systems, secure data exchange and e-discovery is stated briefly.

C. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data

As data of commercial local site is stored on public cloud in the encrypted format then user does not know about the encrypted data, have to process every retrieval file by finding their matching interest. But user query contains multiple keywords and matching so it incurs unnecessary network traffic. This paper has defined and solved the problem of effective yet secure ranked keyword search over encrypted cloud data [8].In Ranked search enhance the process of returning matching files in ranked order by using some relevance criteria.Mehod of secure rank is efficient to return highly relevant document corresponding to user entered query or search. This idea of ranking method is used in our proposed system to enhance the security of encrypted cloud data.

D. Enabling Efficient Fuzzy Keyword Search over Encrypted Data in Cloud Computing

In this paper, main idea is to formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy [9]. This basic idea is taken but it is for multi-keyword raked search (MRSE scheme) in our proposed system. In [10], design of secure cloud storage service which addresses the reliability issue with near optimal overall performance is proposed.

E. . Privacy Preserving Keyword Searches on Remote Encrypted Data

Consider a problem when User A want to store his file in encrypted format on remote file server S. Later the user A wants to efficiently retrieve some of the encrypted files containing specific keywords, keeping the keywords themselves secret and not to endanger the security of the remotely stored files. In [11], solutions for this problem under Well-defined security requirements are offered.

This method is efficient as no public key cryptography is used. In that, user A can submit new files which are secure against previous queries but still searchable against future queries. By this method storing data remotely on other server and retrieving that data from anywhere such as mobile, laptop etc.

F. Providing Privacy Preserving in Cloud Computing

Privacy is very important for cloud computing in terms of legal compliance and user trust and needs to be considered at every phase of design. The [12] paper tells the importance of protecting individual's privacy in cloud computing and provides some privacy preserving technologies used in cloud computing services. This paper suggests that while designing the cloud system privacy is also take into account. This paper describes about privacy of data but doesn't allow indexed search . Thus these drawbacks are overcome in our proposed system.

G. Achiving ,fine-grained data access in cloud compuing

Achieving secure scalable access to cloud data and maintain confidentiality to access data problems remain unresolved. The paper [13] addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents.

III. PROPOSED SYSTEM

In cloud data store consider three main entities the data owner, the data user and the cloud server. We consider three roles coherent with previous works [5, 14].Data owner, who is the actual owner of the database. The data owner collects and/or generates the information in the database and lacks the means (or is unwilling) to maintain/operate the database, Users are the members in a group who are entitled to access part of the information of the database, Server, is a professional entity such as cloud to offer information services to authorized users. It is often required that the server is oblivious to content of the database it maintains, the search terms in queries and

 ISSN: 2321-8169
3650 - 3653

documents retrieved. The Cloud computing entities are arranged in system of search as show in "Fig.1"below

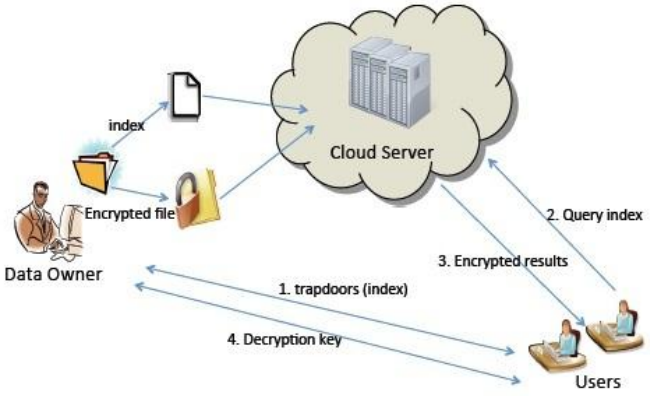

Figure1: Architecture of Search Method

Data owner has a collection of data documents D ={$d1$, d 2 , ..., d m } .A set of distinct keywords W = {$w1$, $w2$, ..., wn } is extracted from the data collection D . The data owner will firstly built an encrypted searchable index I from the data collection D. All files in D are encrypted and form a new file collection, C. After the encryption of, the data owner upload both the encrypted index I and the encrypted data collection C to the cloud server. Data user provides K keywords to the cloud server. A corresponding trapdoor X through search control mechanisms is generated. This is used for authorization between data owner and data user. Cloud server received X from the authorized user. Then, the cloud server calculates and returns to the corresponding set of encrypted documents to data user. In addition to that to reduce the communication cost, the data user may send an optional number N along with the trapdoor so that the cloud server only sends back top- N files that are most relevant to the search query.

This system is design by considering security aspect. The system is expected to give the following security and performance guarantees as follows.

- Multi-keyword Ranked Search: To design search method that allow multi-keyword query and provide result that is relevant to user query ranking for effective data retrieval, instead of returning undifferentiated results
- Privacy-Preserving: To prevent the cloud server and third party from learning additional information from the data and the index stored in cloud , and to meet the basic privacy requirements
- Efficiency: Ranked search can provide privacy and also low communication and computation overhead

Our main purpose of the system is among different multi-keyword semantics we choose efficiently similarity measure as many possible to capture the relevance of documents stored on cloud to the query keywords ,and use "inner product similarity" to quantitatively evaluate such similarity measure To meet challenge of multi keyword semantic without violating privacy the basic idea of MRSE using secure inner product computation. We enhance the of ranked search mechanism, including supporting more search semantics, i.e., TF _IDF, and dynamic data operations. Also performs the provision of maintaining the integrity of rank order in search result and the cloud server is untrusted.Beacouse of providing the integrity to rank order the quality of search is enhanced or improved .User save the time to get relevance document to their search query. In order to improve the document retrieval accuracy, the search result should be ranked by the cloud server according to ranking criteria as coordinate matching in order to make the data on cloud more secure. To reduce the cost of communication data user can provide N number along with the trapdoor so that cloud server return only top-N document which having are relevance to user query.

TABLE I. REVIEW SUMMARY

Sr.No	Papers	
	Paper title	***Objective***
1	Secured Multi-keyword Ranked Search over Encrypted Cloud Data[15]	Main Objective of this paper is to provide solution to multi-keyword Search in cloud computing environment
2	Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data[8]	This paper has defined and solved the problem of effective yet secure ranked keyword search over encrypted cloud data.
3	Enabling Efficient Fuzzy Keyword Search over Encrypted Data in Cloud Computing[9]	Main idea is to formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy.
4	Privacy Preserving Keyword Searches on Remote Encrypted Data[11]	Main objective is to to get the access to user's data which is stored remotely from anywhere according to user's convenience
5	Providing Privacy Preserving in Cloud Computing[12]	The main idea is protecting individuals' privacy in cloud computing and provides some privacy preserving technologies used in cloud computing services.

IV. CONCLUSION

The previous work [15] mainly focused on providing privacy to the data on cloud in which using multi-keyword ranked search was provided over encrypted cloud data . The previous work [8] also proposed a basic idea of MRSE using secure ranking by measuring similarity between user query and data. There was a need to provide more real privacy which is proposed in this paper. This system can reduces the cost of communication. It reduces communication cost by returning only top N result to the user and N is provided by user along with the trapdoor. By hiding the user's identity, the confidentiality of user's data is maintained. The user ID is kept hidden from the cloud service provider as well as the third party user in order to protect the user's data

REFERENCES

[1] M.Armbrust, "A view of cloud computing",Communications of the ACM,vol.53, no. 4, **(2010)**,pp. 50-58.

[2] D.X.Song,D. Wagner and A.Perrig,"Practical techniques for searches on encrypted data. in Security and Privacy", 2000. S&P 2000,Proceedings 2000 IEEE Symposium,IEEE, **(2000)**

[3] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive- subset keywords search", Journal of Network and Computer Application s, vol. 34, no. 1, (2011)

[4] M.Belare, A.Boldyreva, and A.O'Neil, "Deterministic and efficiently searchable encryption," in Proceedings of rypto 2007, volume 4622 of LNCS. Springer- Verlag, 2007.

[5] N. Cao,"Privacy-preserving multi-keyword ranked search over encrypted cloud data",INFOCOM, 2011 Proceedings IEEE,IEEE, **(2011)**.

[6] S. Ji, G. Li, C. Li, and J. Feng. Efficient interactive fuzzy keyword search. In Proc. of 18th International World Wide Web Conference(WWW'09), Madrid, Spain. ACM, April 2009

[7] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Proc.*14th Int'l Conf. Financial Cryptograpy and Data Security, Jan.2010.

[8] Y. Prasanna, Ramesh . "Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data", 2012.

[9] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," *Proc.*IEEE INFOCOM, Mar. 2010.

[10] .N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," *Proc. IEEEINFOCOM,* pp. 693-701, 2012.

[11] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," *Proc. Third Int'l Conf.*Applied Cryptography and Network Security, 2005.

[12] Jain Wang, Yan Zhao , Shuo Jaing, and Jaijin Le, "Providing Privacy Preserving in Cloud Computing",2010.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing," *Proc.*IEEE INFOCOM, 2010.

[14] P. Wang, H. Wang, and J. Pieprzyk. An e_cient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data. In Information Security Applications, Lecture Notes in Computer Science, pages 145{159. Springer, 2009.

[15] Ankatha Samuyelu Raja Vasanthi ," Secured Multi keyword Ranked Search over Encrypted Cloud Data", 2012