IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 15-18
www.iosrjournals.org

Improved Indexing scheme for fast searching in encrypted cloud database

Rupali D. Korde[1] Dr. V.M. Thakare[2]
[1]*P.G Student, Dept. of Comp. Sci. & Engg., SGBAU, Amravati,* **rplkorde@gmail.com**
[2]*Head of Department, Dept. of Comp. Sci. & Engg., SGBAU, Amravati*, **vilthakare@yahoo.com**

Abstract: *Cloud computing with storage in cloud database is promising technology in near future. Data owner outsource their complex and sensitive data from local sites to commercial public cloud for economic saving and flexibility. But protecting data privacy and maintaining encrypted data is not an easy task. For easy access to encrypted data and fast processing service, it is essential that data must be stored in cloud database. This paper focused on five different techniques such as Efficient ranked searchable symmetric encryption (RSSE) scheme, Attribute based encryption providing data retrieval service, two-round searchable encryption (TRSE) scheme, multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework, Privacy preserving authenticated access control scheme. To improve this scheme the new method is proposed here that is Improved indexing scheme for fast searching in cloud database which improves the performance of cloud system.*

Keywords*— Cloud computing, indexing, encrypted data, keyword search.*

I. INTRODUCTION

Cloud computing is dreamed vision of computing where cloud customer can remotely stored their data into cloud database and take advantage of on-demand high quality service and application from shared pool of computing resources. For individuals and enterprise, it is easy to outsource their local data into cloud database as it provides great flexibility and economic saving. For protecting data privacy and unauthorized access to cloud data, it is necessary to store that data in encrypted form so that no one can easily access it. This encryption is done by data owner before this sensitive data is outsourced to public cloud. On the one hand, for effective data retrieval, large numbers of documents demanded by the cloud server to perform result relevance ranking, instead of returning undifferentiated documents. Such ranked search scheme enables data users to find the most relevant information easily, rather than sorting through every match in the collection.

This paper discusses five schemes which worked on encrypted cloud data and retrieval of data named Efficient ranked searchable symmetric encryption (RSSE) scheme, Attribute based encryption providing data retrieval service, two-round searchable encryption (TRSE) scheme, multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework, Privacy preserving authenticated access control scheme. All these schemes improved some part of data encryption and data retrieval. But these schemes also have some problem, So to overcome such problems, this paper proposes new scheme named "**Improved indexing scheme for fast searching in cloud database"** which improves the system performance and make data retrieval an easy task.

II. BACKGROUND

Many works have been done on cloud computing for privacy preserving and stored database. There are five different techniques has been studied in this paper which are as follows: Efficient ranked searchable symmetric encryption (RSSE) scheme is the scheme which is used for ranking the relevant result of user's query before displaying it [1]. Attribute based encryption (ABE) providing data retrieval service is worked on encrypted cloud data for search. In this scheme keywords are used as attribute which is served as index term for searching. It retrieves data efficiently and provides fine grain access control policy [2]. Two-round searchable encryption (TRSE) scheme worked on vector space model and homomorphic encryption. Using this scheme multi keyword searching is easily implemented [3]. Multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework has established set of strict privacy requirement for secure cloud data. It has worked on coordinate matching function as many matching documents are present in database [4]. Privacy preserving authenticated access control scheme supports anonymous authentication. Before storing data, this scheme verifies authenticity of series without knowing user identity. So it prevents replay attack [5].

This paper introduces five different schemes i.e. Efficient ranked searchable symmetric encryption (RSSE) scheme, Attribute based encryption providing data retrieval service, two-round searchable encryption (TRSE) scheme, multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework, Privacy preserving authenticated access control scheme. Paper is organized as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and comparisons between different schemes. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III. PREVIOUS WORK DONE

In last few years, many works have been done on cloud computing for its effectiveness. Cong wang et al. (2012) [1] has worked on Secure and Efficient Ranked Keyword Search and defines and solves the problem of secure ranked keyword search over encrypted cloud data. This method enhances system usability by enabling search result relevance ranking. This is the first work towards rank search in encrypted cloud data which enhances system usability. Dongyoung Koo et al. (2013) [2] have proposed scheme which is best suited for cloud storage systems with massive amount of data. This scheme provides rich expressiveness access control, fast search with simple comparisons of searching entities and also guarantees data security and user privacy during data retrieval process. Jiadi Yu et al. (2013) [3] has worked on multi-keyword retrieval technique and proposed two-round searchable encryption (TRSE) scheme which supports top-k multi keyword retrieval. TRSE employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking. When the cloud server receives a query from user consisting of multi-keywords, first it computes the score from the encrypted index stored in cloud database and returns the encrypted score of all files to the data user. Next, the data user decrypts the score and picks out the top k highest scoring files identifiers for request to the cloud server. The retrieval process takes a two round communication between the cloud server and the data user. The majority of computing work is done on the server side by operations only on cipher text. Ranking is done at the user side while scoring calculation is done at the server side. Ning cao et al. (2014) [4] has worked privacy preserving searching and solves the problem of multi-keyword ranked search over encrypted cloud data (MRSE). This scheme preserves strict system wise privacy in the cloud computing paradigm and provides a balance parameter for data users to satisfy their different requirements on precision and rank privacy. This scheme is based on coordinate matching function which meets different privacy requirement in two thread model. Sushmita Ruj et al. (2014) [5] has proposed Decentralized Access Control scheme for secure data storage in clouds which supports anonymous authentication. In this scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. It has added feature of access control in which only valid customers are able to decrypt the stored information. The Scheme prevents replay attacks and supports modification, creation, and reading data stored in the cloud database.

IV. EXISTING METHODOLOGIES

There are different scheme exists which worked on encrypted cloud data and retrieval of data named Efficient ranked searchable symmetric encryption (RSSE) scheme, Attribute based encryption providing data retrieval service, two-round searchable encryption (TRSE) scheme, multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework, Privacy preserving authenticated access control scheme.

Efficient ranked searchable symmetric encryption (RSSE) scheme is the scheme which is used for ranking the relevant result of user's query before displaying it. Ranked search enhances system usability because it shows us data relevant to query [1]. This scheme explores statistical measure approach. It creates secure index which is searchable and developed one to many order preserving mapping function to protect sensitive data.

Attribute based encryption (ABE) providing data retrieval service is worked on encrypted cloud data for search [2]. In this scheme keywords are used as attribute which is served as index term for searching. It retrieves data efficiently and provides fine grain access control policy. No one is able to identify the data owner's identity or identity of intended receiver.

Two-round searchable encryption (TRSE) scheme worked on vector space model and homomorphic encryption. Using this scheme multi keyword searching is easily implemented [3]. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on cipher text.

Multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework has established set of strict privacy requirement for secure cloud data [4]. It uses inner product similarity to evaluate similarity measure. As this scheme worked on coordinate matching, it is possible to search multi keyword searching.

Privacy preserving authenticated access control scheme supports anonymous authentication. Before storing data, this scheme verifies authenticity of series without knowing user identity [5]. So it prevents replay attack. In this scheme, when user creates file and stored it in cloud database it is securely stored. It worked on two protocols ABE and ABS. it supports modification, creation and reading data from cloud. This scheme has high data privacy and efficient for practical utilization.

V. ANALYSIS AND DISCUSSION

Ranked searchable symmetric encryption (RSSE) scheme shows that security guarantee of propose scheme is strong than previous searchable scheme. It enhances system usability by giving relevant result to query rather giving irrelevant data [1].

Attribute based encryption (ABE) providing data retrieval service is worked on encrypted cloud data for search. This scheme is best suit for massive amount cloud storage data and provides data security and privacy while retrieving data [2].

Two-round searchable encryption (TRSE) scheme worked on vector space model and homomorphic encryption. The majority of computing work is done on the server side by operations only on cipher text. Ranking is done at the user side while scoring calculation is done at the server side. Using this scheme multi keyword searching is easily implemented. The data owner encrypts the searchable index I to secure searchable index [3].

Multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework has established set of strict privacy requirement. It provides a balance parameter for data users to satisfy their different requirements on precision and rank privacy. It uses inner product similarity to evaluate similarity measure [4].

Privacy preserving authenticated access control scheme supports anonymous authentication and it verifies authenticity of series without knowing user identity. Using this it prevents replay attack and supports authentication, modification [5].

Encryption scheme	**Advantages**	**Disadvantages**
Ranked searchable symmetric encryption (RSSE) scheme	It enhances system usability by giving relevant result to query rather giving irrelevant data.	Cloud server has linearly traversed whole index of all the documents for each search request.
Attribute based encryption (ABE) scheme	This scheme is best suit for massive amount cloud storage data and provides data security and privacy while retrieving data.	Complicated retrieval operations for an environment where numerous receivers of cloud request frequently for huge amount of data.
Two-round searchable encryption (TRSE) scheme	Using this scheme multi keyword searching is easily implemented.	For security concerns, the vast majority of work should only be done by the data owner.
Multi-keyword ranked search over encrypted data in cloud computing (MRSE) framework	It provides a balance parameter for data users to satisfy their different requirements on precision and rank privacy.	It does not check integrity of rank order in query search result data.
Privacy preserving authenticated access control scheme	It supports anonymous authentication and it verifies authenticity of series without knowing user identity.	Cloud knows the access policy for each record stored in the cloud which is limitation of this scheme.

Table 1:- Comparison of different schemes

All this schemes are best at their levels but they also have some limitations and problems. This paper proposed new scheme where cloud system stored index of cloud data on virtual machine where it is executed and improves the performance of cloud.

VI. PROPOSED METHODOLOGY

Improved indexing scheme for fast searching in cloud database:-

Cloud system is consists of numbers of virtual machines (VM) and all are working simultaneously. Whenever any query is fired by user, it is processed by one of the VM in cloud. In encrypted cloud database whenever any keyword is requested by user, data owner encrypt that keyword and saved index of that keyword in its file for future queries. But when large number of data is stored in cloud database and large numbers of queries are requested by user, it degrades the performance of system.

This paper proposes new scheme where every virtual machine can stored index of encrypted keyword which is processed by that VM. So that whenever keyword is again requested by user, instead of going to the owner, VM searches the index it have and return result to user if that keyword is stored in it and saves time of searching the whole index of data owner. If that keyword is not present in VM's index file then that keyword is processed by VM and returns result to user. Dramatically this is shown as follows:

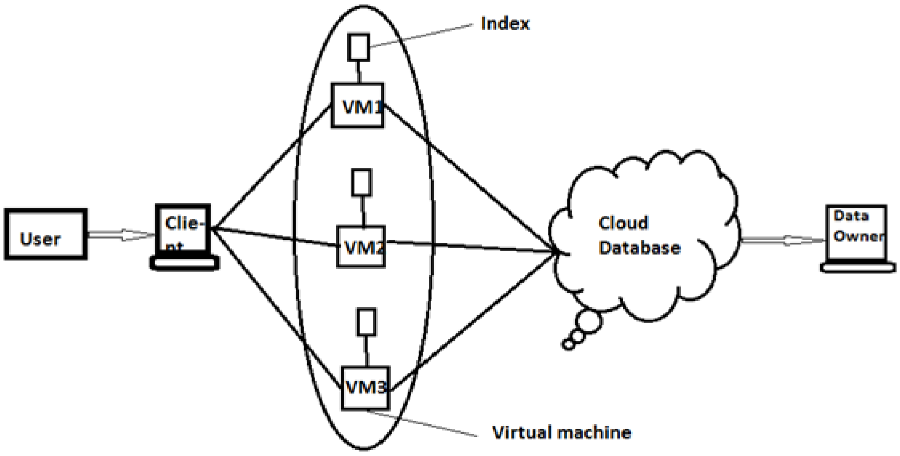

Fig 1:- Improved indexing scheme

VII. OUTCOME AND POSSIBLE RESULT

This paper proposed new scheme where every virtual machine in cloud stored index of encrypted keyword processed by it and improves the performance of overall cloud system. Each keyword is processed once and with the help of index, every time by showing it data is return to user and save time of processing it.

VIII. CONCLUSION

This paper focuses on study of five different searching schemes in encrypted cloud data. But they have some limitation which is improved by this paper. This paper proposes new scheme where index is stored on every virtual machine of cloud and make searching easy in huge amount of database. This scheme is best suit for large amount of encrypted cloud database.

IX. FUTURE SCOPE

Complications may occur if same keyword is encrypted by two different functions. To resolve this complication is the future work of this paper.

REFERENCES

[1]. Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou, “Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data,” *IEEE Transactions On Parallel And Distributed Systems, VOL. 23, NO. 8, pp. 1467-1479, August 2012.*

[2]. Dongyoung Koo, Junbeom Hur, Hyunsoo Yoon, “Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage,” *Computers and Electrical Engineering, 39, pp. 34–46, 2013.*

[3]. Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, and Minglu Li, “Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data,” *IEEE Transactions On Dependable And Secure Computing, VOL. 10, NO. 4, pp. 239-250, July/August 2013.*

[4]. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou,“Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data,” *IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 1, pp. 222-233, January 2014.*

[5]. Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, “Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,” *IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 2, pp. 384-394, February 2014.*