International Journal of Trend in Innovative Research (IJTIIR)
www.ijtiir.com | Volume- 2 | Issue- 3

A Review on: Multi-Agent System for Multi-Keyword Search and Blind Storage

[1]Nirali Borad, [2]Rupal Shilu
[1,2]Attmiya University, Kalawad Road, Rajkot

Abstract-- As keyword searching is one bottleneck as well as service in this era. As there many research works using numerous approaches is there in current system. File system keyword search is one of them. Continuous improvement is going in this area since long ago, to match exact part with efficiency from huge amount of storage is challenge that need to address. Among various methods Multi -Agent system concept is proposed to address this challenge. Performance of time would be measurable parameter here, while security of data using AES approach for encryption and decryption is also there. Integration of security of data as well efficient searching of keywords of file which are located in cloud environment is focused here.

Keywords-- *Searchable encryption; searchable public key encryption; searchable symmetric encryption; decentralized.*

I. INTRODUCTION

Cloud computing and cloud storage have gained popularity as the most convenient way of transferring information and providing functional tools on the Internet. Like public, private, community hybrid cloud. These four types of cloud are best way to transfer the information via cloud. The idea of "cloud computing" is to combine multiple computers and servers into a single environment designed to solve certain kinds of problems, such as scientific problems or complex calculations. In mobile cloud computing, mobile data need to be outsourcing to external cloud server for scalable data storage. The outsourced data need to be encrypted due to the privacy and confidentiality concern of their owner. Previous proposals, however, fails to offer construction of full functioned searchable encryption. So, difficulties arise on the accurate search over the encrypted cloud data. Searchable encryption technique developed for multi-keyword search over the storage data. Also they used Blind storage schemes, which allows a client to store a set of files on remote server in such a way that server does not learn how many files are stored, or length of the individual files, server learn about existence of retrieved files, but file's name and content are not revealed. In proposed approach we are using multi-agent system. By applying multi-agent system we can overcome the problem of searching each and every keyword individually. In which each agent is assigned to each keyword, so parallel searching will help to improve the search time and search mechanism. A multi-agent system (MAS) is a collection of multiple interacting agents. Multi-agent system can be used to solve problem that are difficult for individual agent to solve. Main focus is to improve efficiency in terms of search functionality and search time compared to existing system by using multi-agent system for multi-keyword search.

II. MULTI-AGENT SYSTEM

A multi-agent system (MAS) is a collection of multiple interacting intelligent agents. Multi-agent system can be used to solve problems that are difficult for an individual agent to solve. The main characteristics of multi-agent system include autonomy, local views and decentralization etc[12],[13]. To summarize this, multi-agent system represent another distributed computing paradigm based on multiple interacting agent that are capable of intelligent behavior. In existing system there is facility of multi-keyword search but fast response was not possible. In this paper we introduce multi-keyword search with multi-agent system. The reason behind multi-agent system is to reduce response time and improve the search efficiency. If multi-agent system is used for multi-keyword search then it will search each keyword parallel by creating thread for each keyword so it will help to improve the search efficiency

III. RELATED WORK

Numerous research works has been done in the field of searching the keywords. The searching of huge amount of data has attracted many researchers to searching multi-keyword in parallel way.

This section contains limitations, benefits, comparisonof different methods/algorithm/techniques etc. From literature survey we can identify different problems of existing system and understand how it works. With some modification in existing system we can define new system. In this paper we identified multi-keyword search using multi-agent system with the help of literature survey. Working of that paper, motivation for proposal of that algorithm, advantage and their limitations are briefly describe here. They are as follows:

The main problem in keyword search on outsourced data on cloud is traditional searchable encryption technique. In this technique Boolean search is only possibility and are not yet sufficient to meet effective data utilization need that is demanded by large number of users [3]. Solution of this limitation is ranked search. Another problem of outsourcing data is privacy concerns. To mitigate the concerns, it is desirable to outsource sensitive data in encrypted form [11]. Next problem is identified in literature survey is similarity-based ranking [5]. Privacy-preserving

multi-keyword text search (MTS) scheme is solution of the problem. To build dynamic symmetric searchable encryption (SSE) scheme, blind storage is introduce. Which allows a client to store a dynamic collection of encrypted documents with a server, and later quickly carry out keyword search [9].Difficulty is the accurate search over the encrypted data. The solution is multi-keyword search over encrypted data [10]. Multi-agent system is the main aim of this paper. Multi-agent system helps to improve the search efficiency and search time ofmulti-keyword search.

IV. SEARCHABLE SYMMETRIC ENCRYPTION (SSE)

Searchable symmetric encryption (SSE) allows a client to encrypt its data in such a way that this data can still be searched. The most immediate application of SSE is to cloud storage, where it enables a client to securely outsource its data to an untrusted cloud provider without sacrificing the ability to search over it. SSE has been the focus of active research and a multitude of schemes that achieve various levels of security and efficiency have been proposed. Any practical SSE scheme, however, should satisfy the following properties: sublinear search time, security against adaptive chosen-keyword attacks, compact indexes and the ability to add and delete files efficiently. SSE constructions achieve all these properties at the same time.As an additional contribution, multi-userSSE scheme also considered. All prior work on SSE studied the setting where only the owner of the data is capable of submitting search queries [21]. Then the natural extension considered, where an arbitrary group of parties other than the owner can submit search queries. They define SSE in the multi-user setting, and present an efficient construction that achieves better performance than simply using access control mechanisms.

V. BLIND STORAGE

SSE scheme is based on Blind Storage. A Blind Storage scheme allows a client to store a set of files on a remote server in such a way that the server does not learn how many files are stored, or the lengths of the individual files; as each file is retrieved, the server learns about its existence (and can notice the same file being downloaded subsequently), but the file's name and contents are not revealed. Blind Storage scheme also supports adding new files and updating or deleting existing files. Further, though not needed for the Dynamic SSE construction, Blind Storage scheme can be used so that the actual operation whether it is reading, writing, deleting or updating is hidden from the server. Blind Storage system would have direct applications in itself, rather than as a tool in constructing flexible and efficient Dynamic SSE schemes. Blind Storage scheme does not make requirements on the server other than storage, it can be used with commodity storage systems such as Drop box.

VI. PROPOSED ALGORITHM

This section divided into three sub-sections. The first sub-section explains existing work then problem observed with current work is explained in second sub-section and at the end of this section introduces proposed algorithm to overcome the problem.

A. EMRS System Model[10]

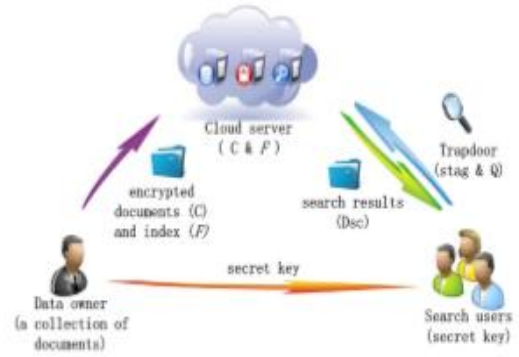

Figure 1: EMRS system model

As shown in Fig., the system model in the EMRS consists of three entities: data owner, search users and cloud server. The data owner keeps a large collection of documents D to be outsourced to a cloud server in an encrypted form C. In the system, the data owner sets a keyword dictionary W which contains d keywords. To enable search users to query over the encrypted documents, the data owner builds the encrypted index z. Both the encrypted documents C and encrypted index z are stored on the cloud server through blind storage system. When a search user wants to search over the encrypted documents, she first receives the secret key from the data owner. Then she chooses a conjunctive keywords which. Finally, the search user sends stag, Q, and an optional number k to the cloud server to request the most k relevant results. Upon receiving stag, Q, and k from the search user, the cloud server uses the stag to access the index z in the blind storage and computes the relevance scores with the encrypted query vector Q. Then, the cloud server sends back descriptors (Dsc) of the top-k documents that are most relevant to the searched keywords. Moreover, since the EMRS aims to eliminate the risk of sharing the key that is used to encrypt the documents with all search users.

B. Problem with Current System Model

Problem with current system i.e, efficient multi-keyword ranked search is observed when they use single-agent to search multiple keywords on encrypted data through blind storage. Due to this, it requires more search time and search efficiency and it needs to process entire algorithm for each keyword, when a request is made. Hence the bottleneck lies within it and response time and search time is increase.

C. Proposed Algorithm

The main aim of our system is to create multi-agent system in cloud to enabling more efficient multi-keyword search for each and every keyword. Multi-agent systems are often used to solve problems by using a decentralized approach where several agents contribute to the solution by co-operating one each other. Several agents that can run on a parallel or distributed computer to keep execution time low. Multi-Agent system create agent for each & every keyword. By creating agent for each keyword, parallel searching is possible and they help to improve search efficiency and also search time.

Step 1: Read the string from user

Step 2: Each keyword are separated by special character

Step 3: Encrypt the each keyword

Step 4: Encrypted keywords are given to the agent

Step 5: Agent checked that whether keyword is matched?

1. If yes,
   a) Match found
   b) Decrypt the result
   c) Merge the result
2. If No,
   a) Match not found

Step 6: Display result to user

CONCLUSION

Lots of technique, methods and algorithm are used to improve the efficiency of searching in cloud computing. So many applications are used by many of people on single click. So the burden on cloud is increased. To remove this type of complexity of cloud and for faster response we can use any of the technique as per the application use. Both the techniques are having its own pros and cons. So any of this can be used.And for better performance we can use multi-agent system with searchable encryption and blind storage.

ACKNOWLEDGMENT

Thanks to all the experts who already researched this kind of good topic of cloud computing. With the help of that researched work this paper is completed with very sharp ideas and well knows technologies. With the help of all expert advices my paper will be more informative. Our thanks to the experts who have contributed towards development of this paper.

References

[1] DomenicoTalia,"Cloud Computing and software agents: Towards Cloud Intelligent Services",ICAR-CNR & University of Calabria Rende, Italy talia@deis.unical.it

[2] The NIST Definition of Cloud Computing, Peter Melland Timothy Grance,NIST Special Publication 800-145.

[3] C. Wang, N. Cao, K. Ren, and W. Lou, ''Enabling secure and efficient ranked keyword search over outsourced cloud data,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, Aug. 2012.

[4] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, and M. Steiner, ''Highly-scalable searchable symmetric encryption with support for Boolean queries,'' in Proc. CRYPTO, 2013, pp. 353–373.

[5] W. Sun, et al., ''Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,'' in Proc. 8th ACM SIGSAC Symp. Inf., Comput.Commun.Secur., 2013, pp. 71–82.

[6] E. Stefanov, C. Papamanthou, and E. Shi, "Practical dynamic searchable encryption with small leakage," 2014.

[7] B. Zhang and F. Zhang, ''An efficient public key encryption with conjunctive-subset keywords search,'' J. Netw. Comput. Appl., vol. 34, no. 1, pp. 262–267, Jan. 2011.

[8] H. Pang, J. Shen, and R. Krishnan, ''Privacy-preserving similarity-based text retrieval,'' ACM Trans. Internet Technol., vol. 10, no. 1, p. 4, 2010.

[9] M. Naveed, M. Prabhakaran, and C. A. Gunter, ''Dynamic searchable encryption via blind storage,'' in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 639–654.

[10] Hongwei Li1, Dongxiao Liu1, Yuanshun Dai1, Tom H. LUAN2 "Enabling Efficient Multi-keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage," In IEEE Transactions On Emerging Topics In Computing, vol:3, issue:1, 6 March, 2015.

[11] Mehmet Kuzu, Mohammad Saiful Islam "Efficient similarity search over encrypted data," In IEEE International conference, 2012.

[12] Research.ijcaonline.org/egov/number1/egov1004.pdf

[13] Wikipedia.http://en.wikipedia.org/wiki/multiagent

[14] D. Cash et al., ''Dynamic searchable encryption in very-large databases: Data structures and implementation,'' in Proc. NDSS, Feb. 2014.

[15] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Con- structions," Proc. ACM Conf. Computer and Comm. Security (CCS '06), 2006.

[16] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, ''Secure dynamic search- able symmetric encryption

with constant document update cost,'' in Proc. GLOBECOM, Anaheim, CA, USA, 2014.

[17] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ''Public key encryption with keyword search,'' in Proc. EUROCRYPT, 2004, pp. 506–522.

[18] 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 '10, 2010.

[19] http://www.cloudcouncil.org/Security_for_Cloud _Computing-Final_080912.pdf