ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

A Privacy Preserving Multi Owner Secure Search in Cloud Computing

[1]K. Meghanareddy [2]B. Ravinder Reddy [3]G. Vishnu Murthy

[1]M.Tech Student, Software Engineering, Anurag Group Of Institutions, Ghatkesar, Medchal District, Telangana.

Mail Id: pandirimeghana78@gmail.com

[2]Assistant Professor, CSE Dept., Anurag Group Of Institutions, Ghatkesar, Medchal District, Telangana.

Mail Id: ravinderreddycse@cvsr.ac.in

[3]Professor and HOD, CSE Dept., Anurag Group Of Institutions, Ghatkesar, Medchal District, Telangana.

Mail id: hodcse@cvsr.ac.in

ABSTRACT:

The promising advantage of cloud computing is outsourcing of large data service, by means of which the data owners save their larger data in the public data centers with the aid of economically saving their capital investment in the direction of data control. Cloud storage offers customers with considerable storage area and makes it user pleasant for fast obtaining of records, which is the inspiration of all sorts of cloud programs. Data outsourcing within the commercial public cloud additionally improve the trouble for unauthorized data accessibility and the cloud storage does no longer make experience if the outsourced data is not efficiently utilized. In context of this paper, we introduce schemes to address privacy protecting ranked multi-keyword search in a multi-owner platform (PRMSM). To allow cloud servers to carry out comfortable search without knowing the real data of each keywords and trapdoors, we systematically construct a unique comfortable searching protocol. To rank the search outcomes and maintain the privateness of relevance ratings between key phrases and files, we endorse a unique additive order and privacy maintaining Characteristic family. To avoid the attackers from eavesdropping private or secret keys and pretending to be legal data users filing searches, we endorse a novel dynamic secret key creation protocol and a novel information user authentication protocol. Moreover, PRMSM helps effective data user revocation.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

I. INTRODUCTION

Cloud offers big organization of remote servers to be in a community in an effort to allow the centralized data repository and get entry to the computer services or resources on every occasion required. Many IT establishments and individuals are outsourcing their databases to cloud server. Different types of users can get entry to and share statistics stored inside the cloud independent of locations. The outsourced records might also include very sensitive facts which include e-mails, organization economic data, government files, private health Care information, facebook pictures and commercial enterprise files. Cloud service providers (CSPs) can get admission to consumer's sensitive information without any authorization. Fashionable method of CSPs is to defend the records confidentiality wherein information is encrypting earlier than outsourcing it to cloud servers and this will affect a huge value of information usability. In comfortable search over encrypted records, data proprietors outsourced their information to cloud server in encrypted shape to maintain their secrecy. While data user wants to search any record, data user will send keyword request to cloud server. Cloud server then generate top similar outcomes to information user. secure searching over encrypted data not only reduce computation expenses and storage value for secure keyword search but also assist multi-keyword ranked search operation, fuzzy key-word search and similarity search operation. Most of these schemes are restrained to single-owner model.

Previous works assist single-owner version, wherein data owner has to live on-line to generate trapdoors for data consumer. Consequently, this paper proposes a multi-owner model to triumph over the constraints of past strategies, where encrypted records are saved by using more than one data proprietors and simultaneously data proprietors live online to generate trapdoors. Multiple data owners share exclusive own secret keys to encrypt their secret information with exceptional secret keys. On this paper, secure searching protocol is suggests wherein cloud server can perform comfortable data without knowing the actual value of keywords and trapdoors. In multi-owner and multiuser cloud computing version, 4 entities are involved such as information owners, information customers, cloud server and administration server proven in fig 1. Data owners have collection of documents. Data owners build strong and secure searchable index of key-word set and key phrases are extracted from files. Information proprietors put up keyword index to admin server.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

Data owners encrypt documents and outsource encrypted documents to cloud server. While administration server gets encrypted key-word index then management server re-encrypt key-word index. Administration server then outsource re-encrypted key-word index to the cloud server. While a user wants to search files from the cloud server, he computes required trapdoor and submits to the admin server. Administration server authenticates information consumer then re-encrypts trapdoors and submit them to cloud server. Cloud server searches encrypted index of information owner and returns top-k applicable encrypted documents to the data user. When data user gets top-k documents from cloud server, then data user down load documents and decrypts those documents.

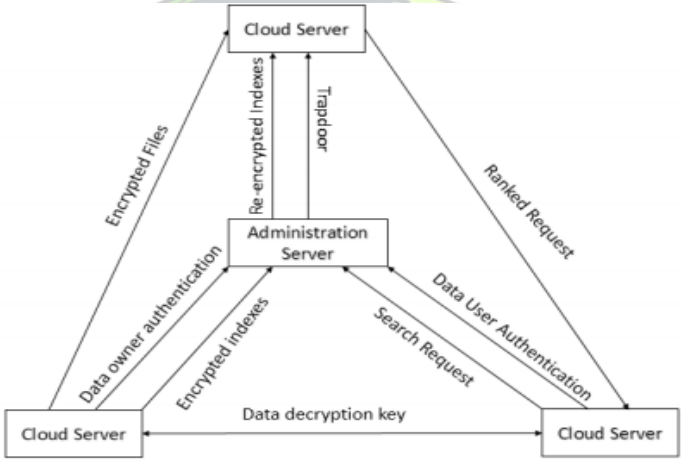

Fig.1. Multi Keyword Ranked Search over Encrypted Data.

II. RELATED WORK

On this section, we evaluate three ways of work: searchable encryption, secure key-word search in cloud computing, and order maintaining encryption.

The earliest strive of searchable encryption was made by means of track et al. In [3], they suggest to encrypt every phrase in a record independently and permit the server to discover whether or not a individual queried keyword is contained in the report without understanding the exact word. This concept is greater of theoretic pastimes because of excessive computational expenses. The first public key scheme for keyword search over encrypted records is offered in [6]. The authors in [7] further increase the search functionalities of searchable encryption by presenting schemes for conjunctive key-word search. [8]

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

discussed about a method, Optimality results are presented for an end-to-end inference approach to correct(i.e., diagnose and repair) probabilistic network faults at minimum expected cost. One motivating application of using this end-to-end inference approach is an externally managed overlay network, where we cannot directly access and monitor nodes that are independently operated by different administrative domains, but instead we must infer failures via end to-end measurements. We show that first checking the node that is most likely faulty or has the least checking cost does not necessarily minimize the expected cost of correcting all faulty nodes. In view of this, we construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. Due to the difficulty of finding the best node from the set of candidate nodes, we propose several efficient heuristics that are suitable for correcting fault nodes in large-scale overlay networks. We show that the candidate node with the highest potential is actually the best node in at least 95% of time, and that checking first the candidate nodes can reduce the cost of correcting faulty nodes as compared to checking first the most likely faulty nodes. The searchable encryption cares basically approximately single keyword search or Boolean keyword search. Extending those strategies for ranked multi-keyword search will incur heavy computation and storage expenses. The system model of those previous works simply take into account one data owner, which suggests that during their solutions, the data owner and data users can effortlessly speak and exchange mystery data. When several data proprietors are concerned inside the system, private information replacing will purpose enormous conversation overhead. Sun et al. [15] and Zheng et al. [16] proposed relaxed attribute-primarily based key-word search schemes within the difficult situation wherein more than one owners are worried. But, making use of CP-ABE inside the cloud platform could introduce problems for information consumer revocation, i.e., the cloud has to replace the large quantity of records stored on it for a data consumer revocation [17]. Additionally, they do now not aid privateness maintaining ranked multi keyword seeks. Our paper differs from preceding studies concerning the emphasis of a couple of information proprietors in the system model. This paper seeks a solution scheme to maximally relax the requirements for data proprietors and customers, so that the scheme may be suitable for a large wide variety of cloud computing users.

III. FRAMEWORK

A. System Model

In the proposed multi-owner and multi-user cloud computing Approach, four entities will involve, as illustrated in the Fig. 2; those entities are owners, cloud server, administration server, and the data users.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

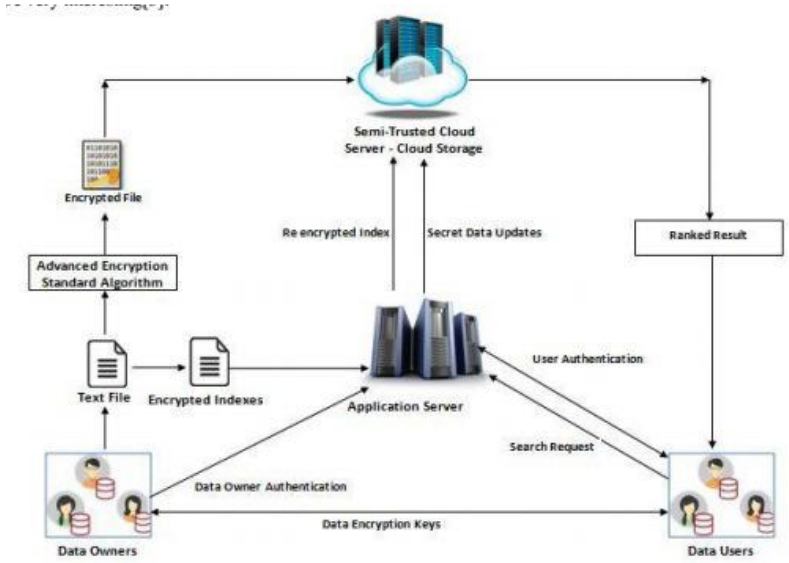

Fig.2. System Architecture

Data owners will have a set of files F. To activate efficient searching operations on these encrypted files, the data owners initially build a secure searchable index I on a keyword collection W extracted from collection F, then they submit index I to the administration server. At last, data owners encrypt their files and engage the corresponding encrypted files Collection C to the cloud server. Upon receiving index I, administration server will re-encrypt I for authenticated data owners and will outsource the re-encrypted indexes to the cloud server. Once a data user needs to search t number of keywords over these encrypted files stored in the cloud server, he first calculates the corresponding trapdoors and submits them to admin server. If a data user is authenticated by the administration server, it will further re-encrypt the trapdoors and then submit them to cloud server. After that, upon receiving the trapdoor T, a cloud server will search encrypted index I of each of the data owner and then returns corresponding set of encrypted documents. To further improve the file retrieval accuracy and reduce communication cost, a user would tell cloud server a parameter k and also cloud server will return the top-k relevant documents to user. Once a data user receives the top-k relevant encrypted files from cloud server, he will decrypt the received files.

B. User Authentication

To avoid attackers from pretending to be legal information users performing searches and launching statistical assaults based on the search end result, information users have to be authenticated before the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

management server re-encrypts trapdoors for information users. As proven in Fig. 3, the authentication data includes 5 elements.

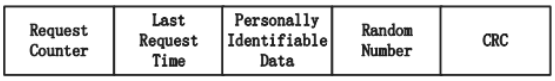

Fig.3. Authentication data format.

The request counter area records the quantity of search requests that the data consumer has submitted. The closing request time area asks the information user to offer the historical data of his preceding request time. The in my view identifiable information (e.g., passport quantity, phone variety) area is used to discover a specific information user, even as the random number and CRC discipline are in addition used to check whether or not the authentication data has been tampered with. The important thing point of a successful authentication is to provide both the dynamically converting secret keys and the historical facts of the corresponding data person.

C. Illegal Search Detection

In our scheme, the authentication procedure is covered through the dynamic strong secret key and the historical statistics. We count on that an attacker has efficaciously eavesdropped the secret key k0;j of Uj. Then he has to assemble the authentication statistics; if the attacker has now not efficaciously eavesdropped the historical facts, e.g., the request counter, the last request time, he can't construct the proper authentication information. Consequently this illegal action will soon be detected by the administration server. Further, if the attacker has effectively eavesdropped all information of Uj, the attacker can efficaciously assemble the authentication records and fake himself to be Uj without being detected by way of the administration server. However, once the criminal data person Uj plays his search, since the secret key at the administration server facet has changed, there may be contradictory secret keys among the administration server and the legal records person. Therefore, the records user and administration server will quickly come across this illegal action.

D. Keyword Encryption

For key-word encryption, the subsequent conditions have to be glad: first, distinct records owners use their own secret keys to encrypt key phrases. Second, for the equal key-word, it'd be encrypted to one of kind cipher-texts on every occasion. Those properties benefit our scheme for two reasons. First, dropping

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

the important thing of one data proprietor could not lead to the disclosure of other owners' statistics. Second, the cloud server can't see any relation amongst encrypted keywords.

E. Trapdoor Generation

To make the data users generate trapdoors securely, comfortably and successfully, our proposed scheme should satisfy essential conditions. First, the information user does now not need to ask a large amount of records proprietors for secret keys to generate trapdoors. Second, for the equal keyword, the trapdoor generated every time ought to be one of a kind. To meet this condition, the trapdoor technology is performed in two steps: First, the records user generates trapdoors based on his seek key-word and a random variety. Second, the administration server re-encrypts the trapdoors for the authenticated data person.

IV. EXPERIMENTAL RESULTS

To rank the search outcomes and preserve the privacy of relevance scores between key phrases and files, we suggest a singular additive order and privacy keeping characteristic family. Moreover, we show that our method is computationally green, even for large records and keyword units.

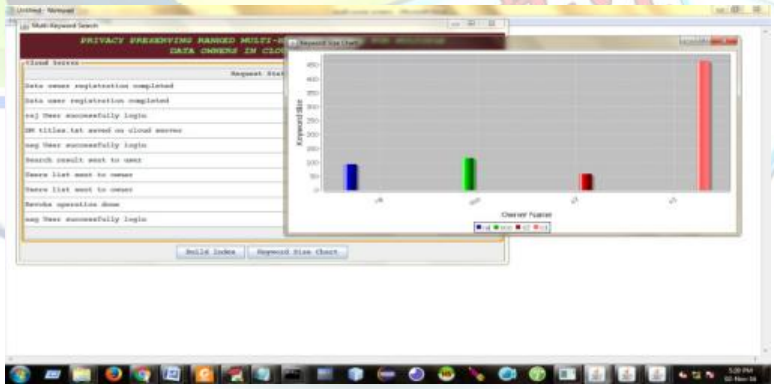

Fig.4. Experimental Values

V. CONCLUSION

On this paper, we discover the problem of comfortable multi-key-word look for more than one data proprietors and more than one data users in the cloud computing platform. different from earlier works, our schemes allow authenticated data customers to obtain comfortable, convenient, and effective searches over more than one data proprietors' records. To efficiently authenticate data customers and locate

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

attackers who steal the secret key and carry out unlawful searches, we endorse a unique dynamic secret key generation protocol and a novel data consumer authentication protocol. To allow the cloud server to perform comfortable search amongst more than one owners' statistics encrypted with extraordinary secret keys, we systematically assemble a novel secure searching protocol. To rank the search consequences and keep the privateness of relevance rankings between multiple keywords and files, we endorse a unique additive order and privacy maintaining characteristic set. Furthermore, we prove that our approach is computationally effective, even for huge data and key-word units.

REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[3] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Int. Symp. Security Privacy, Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003). Secure indexes [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, Oct. 2006, pp. 79–88.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology Eurocrypt 2004, Springer, 2004, pp. 506–522.

[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Appl. Cryptography Netw. Security, Yellow Mountain, China, Jun. 2004, pp. 31–45.

[8] Christo Ananth, Mona, Kamali, Kausalya, Muthulakshmi, P.Arthy, "Efficient Cost Correction of Faulty Overlay nodes", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:26-28

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distrib.Comput. Syst., Genoa, Italy, Jun. 2010, pp. 253–262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM, Shanghai, China, Apr. 2011, pp. 829–837.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[12] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 11, pp. 3025–3035, Nov. 2014.

[13] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multikeyword ranked query on encrypted data in the cloud," in Proc. IEEE 19th Int. Conf. Parallel Distrib. Syst., Singapore, Dec. 2012, pp. 244–251.

[14] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–5.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

[15] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained ownerenforced search authorization in the cloud," in Proc. IEEE INFOCOM, Toronto, Canada, May 2014, pp. 226–234.

[16] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attributebased keyword search over outsourced encrypted data," in Proc. IEEE INFOCOM, Toronto, Canada, May 2014, pp. 522–530.

[17] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271– 2282, Oct. 2013