JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 6, ISSUE 05, 2019

A Robust and Secure Multi-keyword Ranked Search over Encrypted Cloud Data

Sasmita Tripathy[1], Priyabrata Nayak[1]
[1]*Assistant Professor,*[1]*Dept. of CSE*

[1]*Gandhi Institute for Technology, Bhubaneshwar, India*

Abstract

Enhancement in the field of cloud computing, most of the owners who were having meta data are transferring to outsource their information to cloud servers for better perfection and mitigated cost for managing the data. To address this, a secured and preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE) is proposed, which utilizes a set of confidential and restricted private requirements for providing security to such cloud data. The basic concept behind the proposed approach is utilization of confidential computation of inner product and then established two essential and enhanced MRSE algorithms to obtain different rigorious requirements in threat models. Once the data get encrypted and will be outsourced by the owner of that data then our proposed methodology set up a privacy desires set for the system that utilizes secure cloud data during separation of the cloud data and stoking the chunk data in various servers. Many multi-keyword etiology methods choose the well-organized similarity measure of "coordinate matching" for searching technique, then according to Top K Query scheme, the sorted results are created.

Index Terms- Cloud, MRSE, OTP, Product similarity, Cloud data, -Multi keyword Retrieval, Cloud data, Data security, Ranked Search, Similarity Matching.

1. Introduction

Communicate the huge number of computers by utilizing the real-time communication network that renders various concepts of computing is known as cloud computing. Non-ambiguous technical or scientific description in cloud computing has not been accepted. Clouds are huge groups of simply utilizable and accessible virtualized resources [1]. The hardware and software security systems such as firewalls, have been utilized by these providers. This sort of solutions was inefficient to protect the cloud data from the unauthorized persons due to the transparency low degree [2]. The outsourced data might get attacked by the unauthorized users due to that the user and provider of cloud are in the different trusted domain [2-3]. Hence, encryption must be done for the data before storing into the cloud [5] and [7]. Encrypting the data can assure that the integrity and confidentiality of data. One must implement an efficient searchable algorithm to preserve the privacy of data, which works on encrypted data [6]. The data can be easily searched and utilized otherwise no purpose of storing information in the cloud. Such ranking system facilitates information users to find the most relevant information rapidly rather than burdensome sorting through every match in the information collection [8]. This will result in anhuge cost in terms of data, ease of use. Which are regularly used on the plaintext information, cannot be applied directly to the encrypted data. [9] constructed. These methods are not practical due to their high computational cost for both the cloud Sever and users. Proposed scheme to achieve flexible search sub-linear search time and deal with the deletion and insertion of documents.

2. Related Work

Ranked search can offer a quicker search of the data that is more relevant to the query. Sending back only the top-k most relevant documents can effectively reduce the traffic of network is designed only for single keyword search [11]. Many researchers form the literature have failed to search efficiently, when there are complex queries, which leads that the most valuable data discloses to the unauthorized persons. Cryptography based symmetric searchable method, which is a simple and easy algorithm named as ranked keyword search over encrypted data in cloud using keyword frequency and order preserving encryption [12]. Only single key is supported by this approach at a time and only top ranked files will be sent to the user instead of entire file data. In [13], author has proposed a methodology that supports conjunctive keyword search to enhance the functionality of searching. Author in [14] presented an index tree construction for entire data in which a hash value was assigned to each leaf node. A hierarchical clustering approach was proposed to improve the semantics of search supporting [15]. In the search phase can obtain a linear computational complexity compared to an

ISSN- 2394-5125 VOL 6, ISSUE 05, 2019

exponential enhance in the document collection size. The proposed approach has an advantage over the conventional method in the Rank Privacy as relevant documents [16].

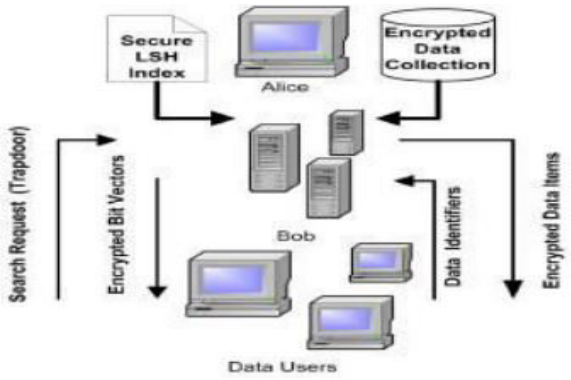

Fig. 1. Basic Secure Search Protocol

3. System Architecture

Hosting of retrieval services and storage of third party information is done by cloud server. These sorts of information consist some sensitive data and protecting this data cannot be entrusted by the cloud server. To address this issue, an encryption of data must be done for the outsourced files. A collection of n files is available for the data owner to outsource the data onto the cloud server in a form of encryption. This encrypted data can be retrieved by the data owner or any other authorized user with a keyword, which will be provided by the cloud server. Our proposed approach resolves and defines the difficult and tuff problem of privacy-preserving multi keyword ranked search over encrypted data in cloud computing (MRSE) [17].

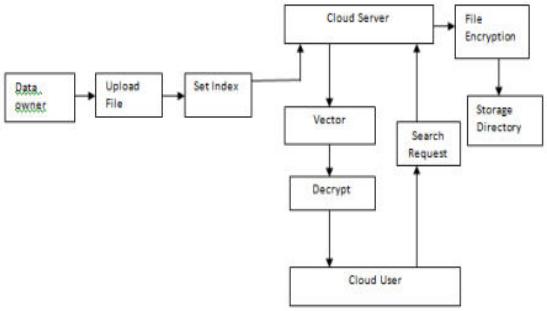

Fig. 2. System Architecture

4. Proposed System

The proposed method is proved to satisfy adaptive semantic security definition. Minhashing- a tiny set named as signature is utilized for representing each document. The signature's vital property is that, it should be feasible to contrast two signatures and find out a distance between the inherent sets without any other information [18]. A new construction of secured search protocol is developed to enable the performance of secured search by cloud server without knowing the original data of keywords and trapdoors. Cloud service providers (CSP) often keep in force the security of data of the user's. These sort of technique does not assist the privacy of user from the CSP itself since it possesses complete organization of the hardware of the system and software stack's minor levels. This OTP (One Time Password) used to observe data in cloud and it can be used only one occasion, when you are looking for a file and be inclined to view the file the OTP will transmit to electronic message and you obtain the OTP and be relevant to see the file

5. Ranked Search

The multi-keyword search schema checks whether queried keywords exist in a document or not. If the user searches for a single keyword is possibly be many correct matches where some of them may not be useful for the user at all the relevancy score of a document is calculated as the number representing the highest-level search

ISSN- 2394-5125 VOL 6, ISSUE 05, 2019

index that the query index matches. All the keywords that exist in a document is included in the first level search index of that document [19]. The higher-level indices the frequent keywords that also occur in its previous level but this time they have to occur the number of times frequency of the corresponding level. The number of levels and the term frequency of each level can be chosen in any convenient way.

Algorithm:

{

For all documents Ri do

{

Compare (level1 index of Ri , query index) j = 1 while match do

{

Increment j

Compare (levelj indices of Ri, query index)

End while

}

Tank of Ri = highest level that match with query index

End for

}

}

6. RSA Algorithm

For doing encryption and decryption, this RSA algorithm is utilized, which is an asymmetric algorithm. Three typical steps involved in this approach. First one is generation of key, second processing of encryption and finally decryption process. For generation of key, public and private keys involved, where the public key is utilized to encrypt the information which is known to everyone and for decrypting the information, private key is utilized, which is a secure one. Generation of these keys is as follows [17]:

1. First, select two discrete prime numbers named as a and b.
2. Now, calculate the product of a and b i.e., ab and denote it as n. This variable n is utilized as the modulus for both the keys i.e., private and public.
3. Then compute Euler's function $\varphi(n) = (a - 1)(b - 1)$.
4. Finally, choose an integer denoted as e in such a way it should satisfy $1 < e < \varphi(n)$ and greatest common divisor of $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co prime. This variable is very short of length and it is a public key exponent.

7. MRSE Framework

In this framework, we haven't shown the operation on the document's information since the owner of data could simply utilize the conventional symmetric key cryptographic algorithms to encrypt the data and can outsource it easily. The proposed MRSE framework consist of four modules by concentrating on the index and query [20] as follows:

1. **Setup (ℓ)**: considering ℓ as a parameter of security, SK is denoted as a symmetric key for the data owner outputs.

2. **BuildIndex (F, SK)**: Let F is a dataset. Now, a searchable index I will be built by the data owner, which will be encrypted with the SK key and then outsourced to the cloud server.

3. **Trapdoor (fW)**: With t keywords of interest in fW as input, this algorithm generates a corresponding trapdoor TfW.

ISSN- 2394-5125 VOL 6, ISSUE 05, 2019

4. **Query(TfW, k, I**): Ranked search on the index I will be performed by the cloud server with the help of trapdoor TfW, once it receives a query request as (TfW, k), and at last returns FfW, the ranked id list of top-k documents sorted by their similarity with fW. The interpreter secrecy guaranty in the relevant work done so far, such as searchable encryption, is that the server should learn nothing but search results [2`1]. We disclosed and set up a set of confidential and restricted private requirements for the framework of MRSE and prevent the cloud server from intruding into the outsourced data successfully.

8. Conclusion

We proposed multiple keyword ranked search over encrypted cloud data and construct many security requirements. from many multi keyword concepts we take the efficient principle of coordinate matching. We can say that secure and efficient and dynamic search scheme is developed, which supports the accurate multicity word ranked search is the dynamic deletion and insertion of documents. Different types of features and classification algorithms can be combined in order to overcome their individual drawbacks and benefit from each other merits, and finally enhance the performance. To rebuild the index and distribute the new secure keys to all the authorized users. To improve the security scheme of dishonest data user will lead to many secure problems. We achieve effective ranking result using k-nearest neighbor technique. This system is currently working on single cloud Provide better security in multi-user systems.

References

[1] K. Ren, C. Wang, Q. Wang et al., “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] Cloud Security Alliance, ‘Security Guidance for Critical Areas of Focus in Cloud Computing,’ http://www.cloudsecurityalliance.org, 2009.

[3] R. Brinkman, ‘Searching in encrypted data,’ in University of Twente, PhD thesis, 2007.

[4] S. Kamara and K. Lauter, ‘Cryptographic cloud storage,’ in RLCPS, January 2010, LNCS. Springer, Heidelberg.

[5] A. Singhal, ‘Modern information retrieval: A brief overview,’ IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2001.

[6] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, ‘Secure knn computation on encrypted databases,’ in Proc. of SIGMOD, 2009.

[7] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, Jan. 2010.

[8] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[9] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88

[11] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009.

[12] I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.

[13] N. Cao,C. Wang, M. Li, K. Ren, and W. Lou,"Privacy-preserving multi-keyword ranked search over encrypted cloud data", INFOCOM, 2011 Proceedings IEEE, (2011).

[14] C. Wang, KuiRen, Shucheng Yu, Urs, K.M.R "Achieving usable and privacy-assured similarity search over outsourced cloud data", INFOCOM, 2012 Proceedings IEEE, (2012)

[15] Chi Chen, Xiaojie Zhu, “An Efficient Privacy-Preserving Ranked Keyword Search Method”, Member, IEEE, IEEE DOI 10.1109/TPDS.2425407, IEEE Transactions on Parallel and Distributed Systems, 2015.

[16] Yi Yang, Hongwei Li, Wenchao Liu, Haomiao Yao, Mi Wen,” Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost”, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Globecom - Communication and Information System Security Symposium, 2014.

ISSN- 2394-5125 VOL 6, ISSUE 05, 2019

[17] Chi Chen, Xiaojie Zhu, "An Efficient Privacy-Preserving Ranked Keyword Search Method", Member, IEEE, IEEE DOI 10.1109/TPDS.2425407, IEEE Transactions on Parallel and Distributed Systems, 2015.

[18] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[19] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," Journal of the ACM (JACM), vol. 43, no. 3, pp.431–473,1996.

[20] 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.

[21] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 50–67.

[22] Hongwei Li, Dongxiao Liu, Kun Jia, and XiaodongLinss "Achieving Authorized and Ranked Multi keyword Search over Encrypted Cloud Data" School of Computer Science and Engineering, University of Electronic Science and Technology of China. IEEE ICC - Communication and Information Systems Security Symposium, 2015.