International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Secure and Fuzzy Keyword Search over Encrypted Cloud Data

[1]T.Tejaswi, [2] T.Ravindar reddy

[1]M.Tech Student, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, Hyderabad, T.S, India

[2] Professor, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, Hyderabad, T.S, India

ABSTRACT: The major aim of this paper is to solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) at the time of protecting exact method wise privacy in the cloud computing concept. Data holders are encouraged to outsource their difficult data management systems from local sites to the business public cloud for large flexibility and financial savings. However for protecting data privacy, sensitive data have to be encrypted before outsourcing, which performs traditional data utilization based on plaintext keyword search. As a result, allowing an encrypted cloud data search service is of supreme significance. In view of the large number of data users and documents in the cloud, it is essential to permit several keywords in the search demand and return documents in the order of their appropriate to these keywords. Similar mechanism on searchable encryption makes centre on single keyword search or Boolean keyword search, and rarely sort the search results. In the middle of various multi-keyword semantics, deciding the well-organized similarity measure of "coordinate matching," it means that as many matches as possible, to capture the appropriate data documents to the search query. Particularly, we consider "inner product similarity" i.e., the amount of query keywords shows in a document, to quantitatively estimate such match measure that document to the search query. Through the index construction, every document is connected with a binary vector as a sub index where each bit characterize whether matching keyword is contained in the document. The search query is also illustrates as a binary vector where each bit means whether corresponding keyword appears in this search request, so the matched one could be exactly measured by the inner product of the query vector with the data vector. On the other hand, directly outsourcing the data vector or the query vector will break the index privacy or the search privacy. The vector space model

facilitate to offer enough search accuracy, and the DES encryption allow users to occupy in the ranking while the popularity of computing work is done on the server side by process only on cipher text. As a consequence, data leakage can be eradicated and data security is guaranteed.

Keywords: Multi-keyword ranked search over encrypted cloud data, OTP, Product resemblance, Cloud, Data owners.

INTRODUCTION: Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications, and enable users to enjoy ubiquitous, convenient and ondemand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead. Attracted by these appealing features, both individuals and enterprises are motivated to outsource their data to the cloud, instead of purchasing software and hardware to manage the data themselves. Despite of the various advantages of cloud services, outsourcing sensitive information (such as e-mails, personal health records, company finance data, government documents, etc.) to remote servers brings privacy concerns. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt the data before outsourcing. However, this will cause a huge cost in terms of data usability. For example, the existing techniques on keyword-based information retrieval, which are widely used on the plaintext data, cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is obviously impractical. In order to address the above problem, researchers have designed some generalpurpose solutions with fully-homomorphic encryption or oblivious .

EXISTING SYSTEM:

Existing searchable encryption schemes allow a user to securely search over encrypted data through keywords. These techniques support multi keyword search. The similarity measure "coordinate matching" in MRSE has some drawbacks when used to evaluate the document ranking order. First, it takes no account of term frequency such that any keyword appearing in a document will present in the index vector as binary value for that document, irrespective of the number of its appearance. Obviously, it fails to reflect the importance

of a frequently appeared keyword to the document. Second, it takes no account of term scarcity. Usually a keyword appearing in only one document is more important than a keyword appearing in several ones. In addition, long documents with many terms will be favoured by the ranking process because they are likely to contain more terms than short documents. Hence, due to these limitations, the heuristic ranking function, "coordinate matching", is not able to produce more accurate search results. More advanced similarity measure should be adopted from plaintext information retrieval community. On the other hand, the search complexity of MRSE is linear to the number of documents in the dataset, which becomes undesirable and inefficient when a huge amount of documents are present.

PROPOSED SYSTEM:

In the Proposed work, we will discover checking the integrity of the rank order in the search result analysing the cloud server is untrusted. To advise OTP (one Time Password) as our upcoming work. This OTP used to see information in cloud and it can be used once only in a time, when you search a file and be likely to see the file, the OTP will transmit to email and we receive the OTP and apply to see the file.

CONCLUSION:

In this paper, we propose secure search scheme supporting multi-keyword ranked search over encrypted cloud data. We make contributions mainly in two aspects: similarity ranked search for more accurate search result and tree-based searchable index for more efficient searching. In term of accuracy, we adopt the vector space model combined with cosine measure to evaluate the similarity between search request and document and acquire accurate search result instead of undifferentiated result. For the efficiency aspect, we propose a tree-based index structure. We propose a secure scheme to meet privacy requirements in the threat model. Finally, we analyze the performance of our scheme in detail by the experiment on real-world dataset. But, there still exist some problems, such as dynamic update for searchable index. We will do more research in the future.

REFERENCES:

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829- 837, Apr, 2011.

[2] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M.Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50-55, 2009.

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

[4] 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.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in CryptologyEurocrypt 2004.

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

[7] D.A.Grossman and O. Frieder. Information retrieval: Algorithms and heuristics[M]. Springer Publishing, 2004.

[8]W. K. Wong, D. W. Cheung, B. Kao and N. Mamoulis. Secure knn computation on encrypted databases[C]//Proceedings of SIGMOD, 2009: 139–152.

[9]RFC (Request For Comments Database) [DB/OL].

[10] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, 'Public key encryption with keyword search,' in Proc. of EUROCRYPT, 2004.

[11] C. Wang et al., 'Secure Ranked Keyword Search Over Encrypted Cloud Data,' Proc. ICDCS '10, 2010

[12] Wenjun Lu; Varna, A.L.; Min Wu, 'Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization,' Access, IEEE, vol.2, no., pp.125,141, 2014.

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

[14] K. Ren, C. Wang, and Q. Wang, 'Security Challenges for the Public Cloud,' IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[15] Zhangjie Fu et al, 'Multikeyword Ranked Search Supporting Synonym Query over Encrypted Data in Cloud Computing', IEEE Conference, 2013.