International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey on: Query Services in Cloud Security

Sapana S. Vasave[1], Dr. Kishor R. Kolhe[2]

[1]PG Student of Information Technology, MITCOE, Pune, India

[2]Assosiate Professor of Information Technology, MITCOE, Pune, India

Abstract: ***Now-a-days Cloud computing is become more popular as cloud infrastructure for storing the data. Data owners are stored their data in public cloud for the flexibility and cost-saving. In data privacy protection, before saving sensitive data it is encrypted. User trust, privacy and security are more concerns. Most frequently used queries for online data analytic is the range query. Consumer-centric cloud computing is used for development of smart electronic devices combined with the cloud computing technologies. Different cloud services are provided to the customers with the premise that an effective and efficient cloud search service is provided. Locality-sensitive hashing is provided the approximate queries that to distributed data servers which give problem of the imbalanced load and space inefficiency, in which limits the query accuracy and incurs long query latency between users and cloud servers. This type of query services could be expensive for data owner. More incremented services computing and cloud computing, it is possible to outsource large databases to database service providers and the providers maintain the range-query service. Using outsourced services, the data owner can reduce the cost of storing data in cloud infrastructure. Cloud computing providing reliable, customized, and guaranteed computing dynamic environment for end users.***

Keywords: Cloud computing security, keyword search, Multidimensional Range Query, Random Space Encryption, consumer-centric cloud, Hybrid storage systems, and approximate queries.

1. Introduction

Query services in the cloud computing are increasingly popular because of the unique advantages in scalability and cost-saving. Cloud infrastructures, the service owners can scale up or down the service and only pay for the hours of using the servers. This facility is reducing the workload of query services which is highly dynamic and it may be expensive and inefficient to serve such dynamic workloads with organizations[1].

The basic idea is to randomly transform the multidimensional datasets with a combination of order preserving with encryption, dimensionality in expansion, random noise injection and project, so that it easily used for processing range queries is preserved. The design of RASP perturbation which help the queried ranges are securely transformed into polyhedra in the RASP-perturbed data space, which can be efficiently processed with the support of indexing structures in the perturbed space[2].

The RASP kNN query service is the combination of the RASP range query service to process kNN queries. The RASP contain main components as follows: (1) The definition and properties of RASP perturbation; (2) The construction of the privacy-preserving range query services; (3) the construction of privacy-preserving kNN query services; and an analysis of the attacks on the RASP-protected data and queries. Range query is used query in online data analytics that requires the service provider to respond the queries user. Cloud systems are facing the challenge to handling the many requests of data halting from cloud computing applications such as business transactions, scientific computing, social network webs, mobile applications and information visualization[1][2].

Cloud computing demands not only big capacity for storage, but also the support of low-latency and scalable queries. For this reason to accept query services have received many attentions in the cloud computing communities, such as query optimization for parallel data processing, automatic management of search services, similarity search in file systems, information retrieval for ranked queries, similarity search over cloud data, multi-keyword ranked and fuzzy keyword search over cloud data, approximate membership query and retrieval for content cloud[3][4].

In this paper summarization of two terms as follows: multi-keyword ranked search for exact search results and similar search to support equivalent word queries. Wide experiments on real-world datasets were performed to formalize the approach, showing that solution is very effective and efficient for multi-keyword ranked searching in a cloud environment.

Cloud computing applications challenge the deal of huge volume of data that needs the support of exact and fast approximate queries to increase system scalability and improve quality of service. Locality-sensitive hashing can support the approximate queries that unfortunately suffer from imbalanced load and space inefficiency among distributed data servers, which severely limits the query accuracy and incurs long query latency between users and cloud servers[6][7].

2. Related Work

Range Query Processing with RASP

In this paper Authors state that the RASP encryption is convexness maintaining. A convex set is represented by range query. The processing strategies are based on multidimensional index trees, such as R-Tree, that handles axis aligned minimum bounding boxes. If the transformed queries are depends on multidimensional tree indexing to process, the processing algorithm should be slightly changes to manage arbitrary convex areas, the boundaries of which are not need to be axis-aligned [5].

Licensed Under Creative Commons Attribution CC BY

The method of query transformation, multidimensional indices are used for briefly study for the normal range query processing algorithms, and then gives the solution for processing the transformed queries. An encryption technique called Order Preserving Encryption Scheme in which encrypted data on that comparison operations is directly applied, the operands are not decrypted in that process. So that many queries can be directly processed on encrypted data such as equality, range queries as well as the MAX, MIN, and COUNT. GROUP BY and ORDER BY operations can also be applied similarly as above[1][2]. The values need to be decrypted only when applying SUM or AVG to a group. Order Preserving Encryption Scheme is also give some ability with the following properties:

- The OPES gives exact results of query processing over encrypted data. The best feature of OPES is they are not containing any false positives and not miss any answer tuple and it also differentiates from schemes such as that produce a superset of answer, necessitating filtering of extraneous tuples in a rather expensive and complex post-processing step.
- OPES gracefully handles the update. Without changing in the encryption of other values a column can be modified or a new value can be inserted in a column.
- OPES can be integrated using existing database systems as it has been designed to work with the B-trees such as existing indexing structure. The concept is encrypted database can be made transparent to the applications.

3. Synonym Query with Multi-keyword Ranked Search

Consumer-centric Cloud Services

In this Paper contribution is that the semantics-based multi-keyword ranked search technology which supports synonym queries of encrypted cloud data. The synonyms of the predefined keywords get the input from authorized cloud customers at that time search results can be achieved. Authors presented a cloud computing middleware Media Cloud for Set-top boxes for classifying, searching, and delivering media inside home network and across the cloud. This approach enables the sharing of personalized content and more sophisticated network-based services over a conventional TCP/IP infrastructure[2]. Data privacy and reputation extensions to enable the global scalability and usability for consumer cloud computing. All services are available to consumers with effective and efficient cloud search service.

Searchable Encryption in Cloud

In this concept in encrypted cloud data fuzzy keyword search is used, to construct fuzzy keyword sets wildcard-based technique is combines with edit distance, to solve the problems of minor typos and format inconsistence. In ranked search scheme, each keyword has weight TF-IDF, the cloud server can rank applicable data files with no knowledge of a specific keyword weight. But this scheme supports only single keyword search. A ranked scheme supporting multi-keyword, which uses a vector space model and characteristics of matrix to realize trapdoor unlinkablility and thereby preserves data privacy[8].

A verifiable symmetric search encryption scheme, which can prove the correctness and completeness of results. A multi-keyword ranked search scheme based on vector space model. The vector space model can measure the similarity between document index vector and query vector and hence support more accurate ranked search results[3].

Synonym expansion

Synonyms are words with the same or similar meanings. It is used to improve the accuracy of search results, the keywords extracted from outsourced text documents need to be extended by common synonyms, as cloud customers' searching input might be the synonyms of the predefined keywords, not the exact or fuzzy matching keywords due to the possible synonym substitution and/or her lack of exact knowledge about the data[9].

4. Conclusion

In this paper I have survey on cloud computing security using different query services such as RASP, Synonym Query multikeyword search. In this paper, the effective approach to solve the problem of synonym-based multikeyword ranked search over encrypted cloud data. The main contributions are summarized in two aspects: synonym-based search and similarity ranked search. The vector space model is adopted combined with cosine measure, which is popular in information retrieval field, to evaluate the similarity between search request and document. Finally, the performance of the proposed schemes is analyzed in detail, including search efficiency and search accuracy, by the experiment on real-world dataset.

5. Acknowledgment

I survey this paper in which cloud computing security has different aspects in query services. Query services gives the more security to the database of cloud user in cloud infrastructure.

References

[1] Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2014). "*Privacy-preserving multi-keyword ranked search over encrypted cloud data*."Parallel and Distributed Systems, IEEE Transactions on, 25(1), 222-233.

[2] Wei, L., & Reiter, M. K. (2011). "*Third-party DFA evaluation on encrypted files*". Tech. Rep. TR11-005, Department of Computer Science, University of North Carolina at Chapel Hill.

[3] Xu, H., Guo, S., & Chen, K. *(2012). "Building confidential and efficient query services in the cloud with RASP data perturbation".* arXiv preprint arXiv:1212.0610.

[4] Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010, June). "*Secure ranked keyword search over encrypted cloud data."* In Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on (pp. 253-262). IEEE.

Licensed Under Creative Commons Attribution CC BY

[5] Liu, Q., Tan, C. C., & Wang, G. (2014). *"Towards Differential Query Services in Cost-Efficient Clouds."* Parallel and Distributed Systems, IEEE Transactions on,25(6), 1648-1658.

[6] Hua, Y., Xiao, B., Veeravalli, B., & Feng, D. (2012). *"Locality-sensitive Bloom filter for approximate membership query."* Computers, IEEE Transactions on,61(6), 817-830.

[7] Liu, Q., Tan, C. C., Wu, J., & Wang, G. (2012, March). "Efficient information retrieval for ranked queries in cost-effective cloud environments." In INFOCOM, 2012 Proceedings IEEE (pp. 2581-2585). IEEE.

[8] Cabarcos, P. A., Mendoza, F. A., Guerrero, R. S., Lopez, A. M., & Diaz-Sanchez, D. (2012). Telematic Eng. Dept., Carlos III Univ. of Madrid, Leganes, Spain. Consumer Electronics, IEEE Transactions on, 58(4), 1425-1433.

[9] Fu, Z., Sun, X., Linge, N., & Zhou, L. (2014). *"Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query."* Consumer Electronics, IEEE Transactions on, 60(1), 164-172.

Licensed Under Creative Commons Attribution CC BY