International Journal of Research

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

Ranked Query Assistance in Untrusted Cloud Helper without Reveal Sensitive Data

[1]S.V.Jyosthna & [2] C.Usha Rani
[1]M.Tech (CSE), Annamacharaya Institute of Technology and sciences -Tirupathi
[2]Assistant Professor, Annamacharaya Institute of Technology and sciences -Tirupathi
[1] venkatajyosthnab6@gmail.com , [2] ch.usha86@gmail.com

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-preserving. In data privacy bulwark, afore preserving sensitive data it is encrypted. Utilizer trust, privacy and security are more concerns. Most frequently used queries for online data analytic is the range query. Consumer-centric cloud computing is utilized for development of keenly intellective electronic contrivances amalgamated with the cloud computing technologies. Different cloud accommodations are provided to the customers with the premise that an efficacious and efficient cloud search accommodation is provided. Locality-sensitive hashing is provided the approximate queries that to distributed data servers which give quandary of the imbalanced load and space inefficiency, in which limits the query precision and incurs long query latency between users and cloud servers. This type of query accommodations could be expensive for data owner. More incremented accommodations computing and cloud computing, it is possible to outsource immensely colossal databases to database accommodation providers and the providers maintain the range-query accommodation. Utilizing outsourced accommodations, the data owner can reduce the cost of storing data in cloud infrastructure. Cloud computing providing reliable, customized, and ensured 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

INTRODUCTION

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

The objective for the cost efficient clouds is to cost of CPU consumption, cost of network bandwidth utilization, increment privacy of users. In this scenario, the bulwark of utilizer will be major issue. Utilizer privacy [2] can be categorized into search privacy and access privacy. Search privacy deals with the user's search and access privacy deals with the fields that are to be returned. Ostrovosky scheme [4] is archaic as it has to process all the keywords in each and every file. This process leads to heftily ponderous query overhead from different users. A novel solution would be to make a rank matrix that enhances the utilizer privacy than the anterior methods. EIRQ scheme address the issues of privacy, aggregation, computational cost and bandwidth wastage.

The cloud kens nothing about what the utilizer is probing for is called Search privacy, and the cloud kens nothing about which files are returned to the utilizer is called access privacy.

I. RELATED WORK

Private searching was proposed by Ostrovsky allows user to retrieve files of interest from an untrusted server without leaking any information. Otherwise, the cloud will learn that certain files, without processing, are of no interest to the user. Commercial clouds follow a pay-as-you-go model [8], where the customer is billed for different operations such as bandwidth, CPU time, and so on. To make private searching applicable in a cloud environment, our previous work designed a cooperate private searching protocol (COPS) [6], where a proxy server, called the aggregation and distribution layer (ADL), is introduced between the users and the cloud.

a) Existing System:

Subsisting system private keyword-predicated file retrieval scheme that was pristinely proposed by Ostrovsky. Their scheme sanctions a utilizer to retrieve files of interest from an untrusted server without leaking any information. The main drawback is that it will cause a cumbersomely hefty querying overhead incurred on the cloud, and thus contravenes the pristine intention of cost efficiency.

Private probing was proposed by Ostrovsky et al. which sanctions a utilizer to retrieve files of interest from an untrusted server without leaking any information. However, the Ostrovsky scheme has a high computational cost, since it requires the cloud to process the query on every file in an amassment. Otherwise, the cloud will learn that certain files, without processing, are of no interest to the utilizer. It will expeditiously become a performance bottleneck when the cloud needs to process thousands of queries over an accumulation of hundreds of thousands of files.

b) Proposed System:

We propose a scheme; termed Efficient Information retrieval for Ranked Query (EIRQ), in which each utilizer can optate the rank of his query to determine the percentage of matched files to be returned. The rudimentary conception of EIRQ is to construct a privacy preserving mask matrix that sanctions the cloud to filter out a certain percentage of matched files afore returning to the ADL. This is not a nugatory work, since the cloud needs to correctly filter out files according to the rank of queries without kenning anything about utilizer privacy. Fixating on different design goals, we provide two extensions: the first extension accentuates simplicity by requiring the least amount of modifications from the Ostrovsky scheme, and the second extension accentuates privacy by leaking the least amount of information to the cloud.

c) System Model:

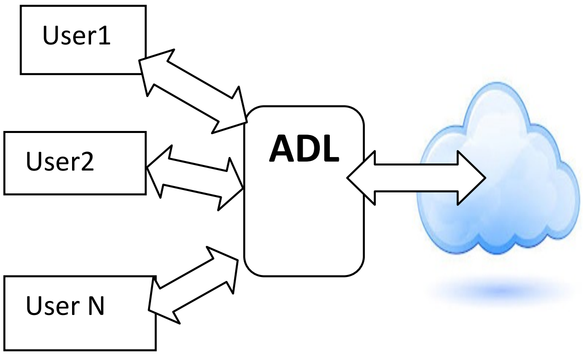


Fig 1: System Architecture Model.

II. IMPLEMENTATION

1) Prong Objection Services:

We introduce a novel concept, differential query accommodations, to COPS, where the users are sanctioned to personally decide how many matched files will be returned. This is motivated by the fact that under certain cases, there are a plethora of files matching a user's query, but the utilizer is intrigued with only a certain percentage of matched files. To illustrate, let us postulate that Alice wants to retrieve 2% of the files that contain keywords

"A, B", and Bob wants to retrieve 20% of the files that contain keywords "A, C". The cloud holds 1,000 files, where {F1, . . . , F500} and {F501, . . . , F1000} are described by keywords "A, B" and "A, C", respectively. In the Ostrovsky scheme, the cloud will have to return 2, 000 files. In the COPS scheme, the cloud will have to return 1, 000 files. In our scheme, the cloud only needs to return 200 files. Therefore, by sanctioning the users to retrieve matched files on demand, the bandwidth consumed in the cloud can be largely reduced.

2) Active Report Regeneration for Ranked Query:

We propose a scheme, termed Efficient Information retrieval for Ranked Query (EIRQ), in which each utilizer can cull the rank of his query to determine the percentage of matched files to be returned. The rudimentary conception of EIRQ is to construct a privacy preserving mask matrix that sanctions the cloud to filter out a certain percentage of matched files afore returning to the ADL. This is not a picayune work, since the cloud needs to correctly filter out files according to the rank of queries without kenning anything about utilizer privacy. Fixating on different design goals, we provide two extensions: the first extension accentuates simplicity by requiring the least amount of modifications from the Ostrovsky scheme, and the second extension accentuates privacy by leaking the least amount of information to the cloud.

3) Gathering and Sharing Layer:

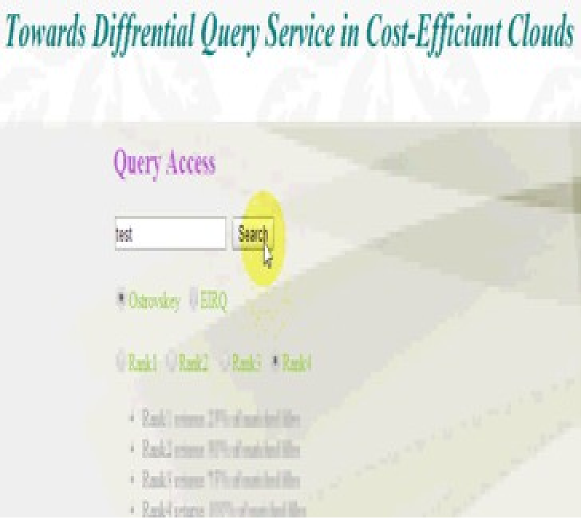
An ADL is deployed in an organization that sanctions its staff to apportion data in the cloud. The staff members, as the sanctioned users, send their queries to the ADL, which will aggregate utilizer queries and send a coalesced query to the cloud. Then, the cloud processes the coalesced query on the file accumulation and returns a buffer that contains all of matched files to the ADL, which will distribute the search results to each utilizer. To aggregate sufficient queries, the organization may require the ADL to wait for a period of time afore running our schemes, which may incur a certain querying delay. In the supplementary file, we will discuss the computation and communication costs as well as the querying delay incurred on the ADL.

4) Rated Inquiry:

To further reduce the communication cost, a differential query accommodation is provided by sanctioning each utilizer to retrieve matched files on demand. Categorically, a utilizer culls a particular rank for his query to determine the percentage of matched files to be returned. This feature is subsidiary when there are an abundance of files that match a user's query, but the utilizer only needs a minuscule subset of them.

III. EXPERIMENTAL RESULTS

Fig 2: A File Uploading.



Towards Diffrential Query Service in Cost-Efficiant Clouds

Query Access

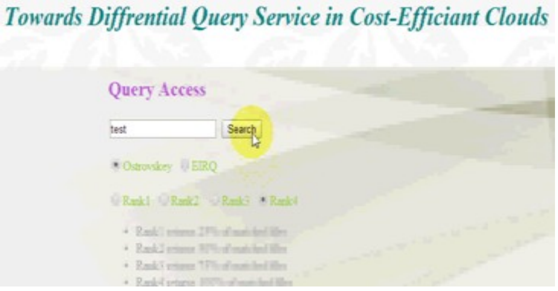
test Search

● Ostrovskey ○ EIRQ

○ Rank1 ○ Rank2 ○ Rank3 ● Rank4

- Rank1 returns 25% of matched files
- Rank2 returns 50% of matched files
- Rank3 returns 75% of matched files
- Rank4 returns 100% of matched files

Fig3: Query Accessing based on cost



Towards Diffrential Query Service in Cost-Efficiant Clouds

Query Access

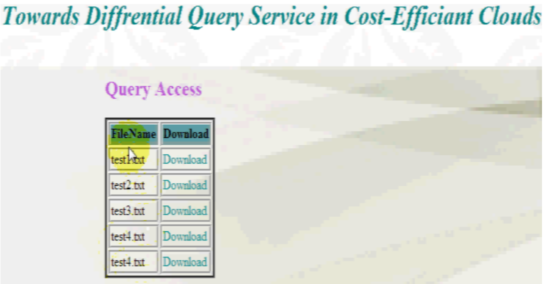
test Search

● Ostrovskey ○ EIRQ

○ Rank1 ○ Rank2 ○ Rank3 ● Rank4

- Rank1 returns 25% of matched files
- Rank2 returns 50% of matched files
- Rank3 returns 75% of matched files
- Rank4 returns 100% of matched files

Fig4: Query Result page.



Towards Diffrential Query Service in Cost-Efficiant Clouds

Query Access

FileName	Download
test1.txt	Download
test2.txt	Download
test3.txt	Download
test4.txt	Download
test4.txt	Download

IV. CONCLUSION

In this paper I have survey on cloud computing security utilizing different query accommodations such as RASP, Synonym Query multi keyword search. In this paper, the efficacious approach to solve the quandary of synonym-predicated multi keyword ranked search over encrypted cloud data. The main contributions are summarized in two aspects: synonym-predicated search and kindred attribute ranked search. The vector space model is adopted cumulated with cosine measure, which is popular in information retrieval field, to evaluate the homogeneous attribute between search request and document. Determinately, the performance of the proposed schemes is analyzed in detail, including search efficiency and search precision, by the experiment on authentic-world dataset.

V. 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.

[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.