International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015

Available at http://internationaljournalofresearch.org

Towards Differential Query Services in Cost-Efficient Clouds

K.L.Narasimha Rao[1]; K.Suresh [2]& A.Anitha [3]

[1]Associate Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

[2]Assistant Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

[3]M.Tech CSE (PG Scholar),Dept of CSE,Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

Abstract

As a characteristic cloud application an organization pledge the cloud services and approves its team to share files in the cloud. Each file is explained by a set of keywords and the staff as authorized users can repossess files of their interests by querying the cloud with certain keywords. In such an environment how to protect user privacy from the cloud which is a third party outside the security boundary of the organization turn into a key problem. The communication cost acquires on the cloud will also be concentrated since files shared by the users need to be returned only once. Most significantly by using a series of secure functions COPS can protect user privacy from the ADL the cloud and other users. The main drawback is that it will cause a heavy querying overhead incurred on the cloud and thus goes against the original intention of cost efficiency. In this paper we present a method termed efficient information retrieval for ranked query (EIRQ) based on an aggregation and distribution layer (ADL) to condense querying overhead deserved on the cloud.

Keywords: Cloud Computing; Cost Efficiency; Differential Query Services; Privacy

I.INTRODUCTION

Cloud computing technology could be a most important technology for info technology. more organizations square measure used cloud computing [1] for source sharing. The organizations must submit access the services of cloud and authorizes organizations employees to separate files within the cloud. every and each file is represented by place keywords. The licensed employees at a company will access the information of their advantages by querying from the cloud with explicit keywords. In Cloud setting, user privacy may be protected on each dealings. User privacy is categorized by two varieties. They're search privacy and access privacy [2]. Search privacy could be a method of looking, however cloud doesn’t understand something regarding what user extremely finding out and Access privacy is looking technique. Here cloud is aware of regarding what user extremely looking on computer program. personal looking was introduced by ostrovsky theme permits to users to recover information from the un-trusted servers n discharge of information. Ostrovsky [1] theme is lofty machine outlay, as a result of the cloud got to method keywords within the every and each get into the cloud. The user will send question a question |a question} to each time to method the query. as a result of this method the cloud is over headed queries from the numerous users from completely different organization. Through this method the communication and computation on the far side the expectation.

Existing System:

Cloud computing as an emerging technology is expected to reshape information technology processes in the near future. Due to the overwhelming merits of cloud computing, e.g., cost-effectiveness, flexibility and scalability, more and more organizations choose to outsource their data for sharing in the cloud. As a typical cloud application, an organization subscribes the cloud services and authorizes its staff to share files in the cloud. Each file is described by a set of keywords, and the staff, as authorized users, can retrieve files of their interests by querying the cloud with certain keywords. In such an environment, how to protect user privacy from the cloud, which is a third party outside the security boundary of the organization, becomes a key problem.

User privacy can be classified into search privacy and access privacy [2]. Search privacy means that the cloud knows nothing about what the user is searching for, and access privacy means that the cloud knows nothing about which files are returned to the user. When the files are stored in the clear forms, a na¨ıve solution to protect user privacy is for the user to request all of the files from the cloud; this way, the cloud cannot know which files the user is really interested in. While this does provide the necessary privacy, the communication cost is high.

Disadvantages:

1. Display the more number of high relevant results.
2. Without any quality display the results
3. Computation cost is high
4. Users are not satisfied with results.

Proposed System:

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

Our key contributions are as follows:

1) We propose three EIRQ schemes based on the ADL to provide a cost-efficient solution for private searching in cloud computing.

2) The EIRQ schemes can protect user privacy while providing a differential query service that allows each user to retrieve matched files on demand.

3) We provide two solutions to adjust related parameters; one is based on the Ostrovsky scheme, and the other is based on Bloom filters.

4) Extensive experiments were performed using a combination of simulations and real cloud deployments to validate our schemes

Module Description:

Differential Query Services:

We introduce a novel concept, differential query services, to COPS, where the users are allowed to personally decide how many matched files will be returned. This is motivated by the fact that under certain cases, there are a lot of files matching a user's query, but the user is interested in only a certain percentage of matched files. To illustrate, let us assume 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 allowing the users to retrieve matched files on demand, the bandwidth consumed in the cloud can be largely reduced.

Efficient Information Retrieval For Ranked Query:

We propose a scheme, termed Efficient Information retrieval for Ranked Query (EIRQ), in which each user can choose the rank of his query to determine the percentage of matched files to be returned. The basic idea of EIRQ is to construct a privacypreserving mask matrix that allows the cloud to filter out a certain percentage of matched files before returning to the ADL. This is not a trivial work, since the cloud needs to correctly filter out files according to the rank of queries without knowing anything about user privacy. Focusing on different design goals, we provide two extensions: the first extension emphasizes simplicity by requiring the least amount of modifications from the Ostrovsky scheme, and the second extension emphasizes privacy by leaking the least amount of information to the cloud.

Aggregation And Distribution Layer :

An ADL is deployed in an organization that authorizes its staff to share data in the cloud. The staff members, as the authorized users, send their queries to the ADL, which will aggregate user queries and send a combined query to the cloud. Then, the cloud processes the combined query on the file collection and returns a buffer that contains all of matched files to the ADL, which will distribute the search results to each user. To aggregate sufficient queries, the organization may require the ADL to wait for a period of time before 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.

Ranked Queries:

To further reduce the communication cost, a differential query service is provided by allowing each user to retrieve matched files on demand. Specifically, a user selects a particular rank for his query to determine the percentage of matched files to be returned. This feature is useful when there are a lot of files that match a user's query, but the user only needs a small subset of them.

II.RELATED WORK

Our aim of this work is to provide differential query services through Aggregation and Distribution Layer while
protecting user privacy from the cloud. Private searching [3] is performed on the keyword based searches on unencrypted data. Private keyword based searching allows a server to filter out streaming data without compromising user privacy. In existing work an efficient decoding [2] mechanism is used which allows the recovery of files that crash in a buffer position. Private searching schemes only support searching for OR of keywords or AND of two sets of keywords. In query searching use Disjunctive normal forms (DNF) of keywords. Thus, when applying these schemes to a heavy cloud environment, querying costs will be increased. The drawback of existing private searching schemes is that both the computation and communication costs high. In existing systems waste of bandwidth [4] when only a small percentage of files are of interest. To avoid this problem, we introduced the concept of differential query services through Aggregation and Distribution Layer concept with low usage of bandwidth and low computational and communication cost.
Co-operate searching protocol (cops) is like a proxy [4] server called as aggregation and distribution layer (ADL) is placed inside an organization. This ADL is act as a mediator between the cloud and an organization. The functioning of ADL is the aggregation and distribution. The ADL only reduces the computation cost.

III.ARCHITECTURE

Co-operate searching protocol (cops) is like a proxy [4] server called as aggregation and distribution layer (ADL) is placed inside an organization. This ADL is act as a mediator

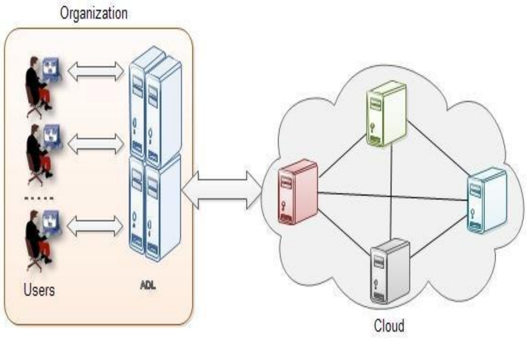

Fig 1 : Architecture

Between the cloud and an organization. The functioning of ADL is the aggregation and distribution. The ADL only reduces the computation cost. Fig. 1 Architecture of EIRQ The working of an ADL [2] is the many users can send many queries to ADL. Then adl can aggregate the different user's queries makes into a single query and then sends to cloud. The cloud will process the query sends response to ADL. Then the adl will distribute the results to particular users. Because of this process to reduce the communication cost and query overhead.

The ADL is deployed inside the security boundary of an organization, and thus it is assumed to be trusted by all of the users. In the supplementary file, we will discuss how the EIRQ schemes work without such an assumption. The communication channels are assumed to be secured under existing security protocols, such as SSL, during information transfer. With these assumptions, as long as the ADL obeys our schemes, a user cannot know anything about other users' interests, and thus the cloud is the only attacker in our security model. As in existing work the cloud is assumed to be honest butcurious. That is, it will obey our schemes, but still wantsto know some additional information about user privacy.

Ref. [2] classified user privacy into search privacy and access privacy. In our work, user queries are classified into multiple ranks, and thus a new kind of user privacy, rank privacy, also needs to be protected against the cloud. Rank privacy entails hiding the rank of each user query from the cloud, i.e., the cloud provides differential query services without knowing which level of service.

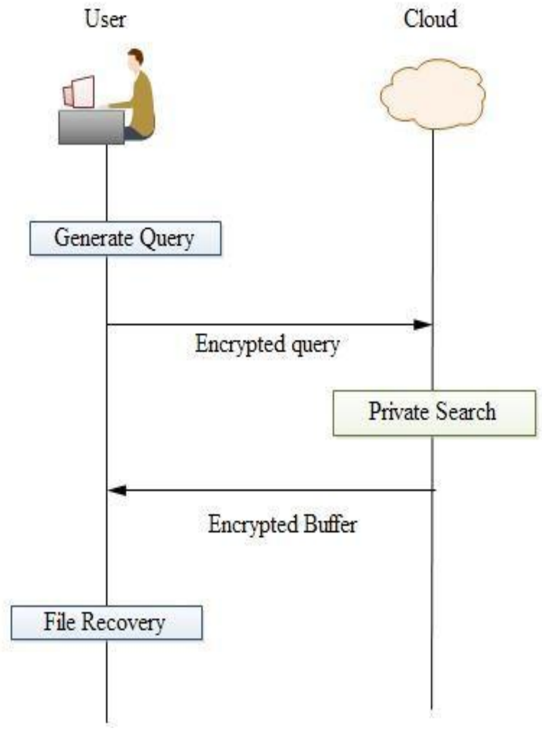

Fig:2 working process of Ostrovsky Scheme

1). Ostrovsky Scheme having the user and cloud. The users are only authorized [3] from the cloud network, and then only accessing is possible otherwise it is not possible.

2).This process is going on both wired network [3] and wireless network also. First send request from the user to cloud for establishment of a connection form the cloud. Then authorized user should have their own login name and passwords.

3).After login to user Generate a query [2]. This query is encrypted into 0's and 1's and then sends to cloud. At the cloud side Private Search has

been done. So those find out the matched files.
4).Cloud sends the matched files to encrypted [1] buffer. Then Files are recovered at the user side. This scheme is very query overhead as well as every time accesses the broadband connection. This process is more costly to accessing files at every query.

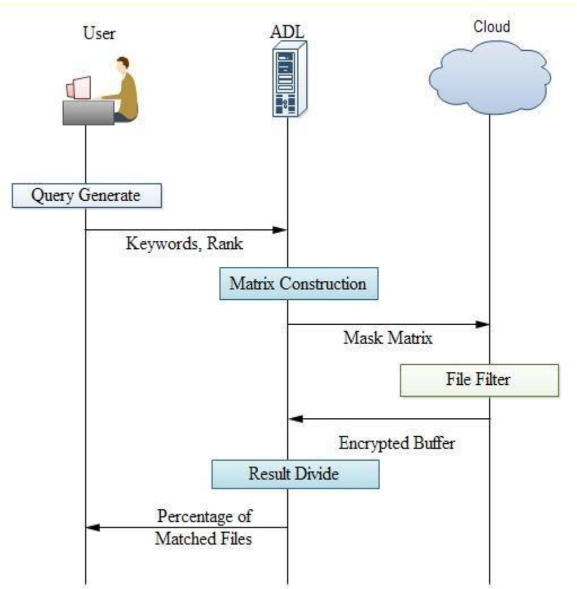

Fig. 3 working process of EIRQ Scheme

1) The EIRQ Scheme having the user and cloud [3]. The users are only authorized from the cloud network, and then only accessing is possible otherwise it is not possible.

2) This process is going on both wired network and wireless network also. First send request from the user to ADL for establishment of a connection form the ADL. Then authorized user should have own login name and passwords.
3) After login to user generate a query. This query is encrypted into 0's and 1's and then sends to ADL. At the ADL side Matrix Construct Algorithm [2] has been done based on that Keywords and Ranks. This process we called as Aggregation.

- **Cost efficiency.** The users can retrieve matched files on demand to further reduce the communication costs incurred on the cloud.
- **User privacy.** The cloud cannot know anything about the user's search privacy, access privacy, and at least the basic level of rank privacy

VI.CONCLUSION

We propose three EIRQ schemes (EIRQ Simple, EIRQ Privacy, and EIRQ Efficient) are worked through ADL. It offers differential query services, which will also protect the user privacy. These schemes are provide, clients are recovered certain percentage of matched records by particular queries of various ranks. Private searching technique is used to cost efficient cloud environments. In our EIRQ scheme assign ranks for each query, then highest rank files are matched and user recovered certain percentage of matched files.

V. Future Work

It facilitates partners to make available services that use the Cloud infrastructure. The Solution EES program is intended to help Partners augment their cloud contribution and widen experience to new customers and global markets. EES offers software, applications and cloud services on top of public Cloud. The program consists of a set of tools such as platform as a service (PaaS) and software as a service (SaaS) vendors provide cloud based services include Application, Database, Development & Testing, Management e.g. Orchestration, Mobile computing,
Monitoring, Multimedia, Platform as a Service, Security, Storage and Technology.

REFERENCES

[1] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, "Efficient Information Retrieval for Ranked Queries in Cost Effective Cloud

Environment", IEEE INFOCOM, 2012.

[2] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, "Towards Differential Query Services in Cost Efficient Clouds" IEEE Transactions on Parallel and Distributed Systems, 2013.

[3] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, "Cooperative Private Search in Clouds", Journal of Parallel and Distributed Computing, 2012.

[4] Wikipedia: http://en.wikipedia.org/wiki/ Efficient Information Retrieval for Ranked Queries.

[5] J. Bethencourt, D. Song, and B. Waters, "New constructions and practical applications for private stream searching," in Proc. ofIEEE S&P, 2006.

[6] Q. Liu, C. Tan, J. Wu, and G. Wang, "Cooperative private search-ing in clouds," Journal of Parallel and Distributed Computing, 2012.

[7] Q. Liu, C. Tan, J. Wu, G. Wang,"Cooperative private searching in clouds", Journal of Parallel and Distributed Computing, 2012.

[8] G. Danezis, C. Diaz,"Improving the decoding efficiency of private search", In IACR Eprint archive number 024, 2006.

[9] "Space-efficient private search with applications to rateless codes", Financial Cryptography and Data Security, 2007.

[10] M. Finiasz, K. Ramchandran,"Private stream search at the
same communication cost as a regular search: Role of ldpc codes", In Proc. of IEEE ISIT, 2012.

[11] X. Yi, E. Bertino,"Private searching for single and conjunctive keywords on streaming data", In Proc. of ACM Workshop on Privacy in the Electronic Society, 2011.