International Journal of Advanced Research in Engineering and Applied Sciences

ISSN: 2278-6252
Impact Factor: 4.817

CONFIDENTIAL AND EFFICIENT QUERY SERVICES IN THE CLOUD WITH RASP

P. Sivakamasundari*

C. Masilamani**

Dr. A.Bhuvaneshwari***

Abstract: *Now a day cloud computing is quite popular. By using cloud users can save their cost for query services. But some of the data owners are hesitate to put their data's in cloud because, sometimes the data may be hack like as inside attackers when they use in cloud unless the confidentiality of data and secure query processing will be provided by the cloud provider. In cloud if the user can get secured query service then the efficiency of query processing will be increased as speed of retrieve and the workload of the query processing will also be saved. To provide the confidentiality and efficient query service used RASP method. RASP denotes RAndom Space Perturbation. It also combines order preserving encryption, random projection and random noise injection. To process the range query to kNN query here used kNN-R algorithm and also analyze the RASP method will secure the multidimensional range and it will increase the working process of query.*

***Assistant Professor CSE Dept, Adhiparasakthi engineering college, Melmaruvathur, Tamilnadu

****PG scholar CSE Dept, Adhiparasakthi engineering college, Melmaruvathur, Tamilnadu

*****Professor CSE Dept, Adhiparasakthi engineering college, Melmaruvathur, Tamilnadu

1 INTRODUCTION

Cloud computing is the internet based storage method [2]. It is mainly used for storing the files and applications in it infrastructures. Peoples uses the cloud because of its attractive features like secure service, infinite of storage, it will satisfy the user experience, low cost and multiple user can access the files and applications. In cloud, the query service process are frequently used because, the user can save their cost. The owners in the cloud will pay the amount only for their using time of server. This is an important feature because, the working time of query service in cloud is very high and it is more expensive.

New process are need for the cloud to protect the data and query privacy, so by that new process the query service can be protected. But if the new approaches for providing security will provide sloe query process is not an advantage.

Analyze the CPEL criteria for submit a query in cloud. This CPEL criteria denotes Confidentiality of data, query Privacy, Efficient query processing and Low working cost. This method also used to increase the complexity of query service.

This paper proposes the RAndom space Perturbation (RASP) method to construct the query and here we separate the query as range query and kNN query. The proposed RASP method will use the four concepts of the CPEL criteria and here the multidimensional data can be transformed with the combination of order preserving encryption [1], random projection and random noise injection.

- The RASP method [6] and its combination provide confidentiality of data and this approach is mainly used to protect the multidimensional range of queries in secure manner, with indexing and efficient query processing.
- The range query is used in database for retrieving the stored data's. it will retrieve the records from the database where it can denotes some value between upper and lower boundary.
- The kNN query denotes k-Nearest Neighbor query. K denotes positive integer and this query are used to find the value of nearest neighbor to k [12].

2 QUERY SERVICE

Query is mainly used to search. Queries are constructed by using structured query language. It is mainly used to retrieving the needed information from the database. Query services are the method for services that are exposed through an implementation of service provider.

Here by using RASP, range query and kNN query in cloud provide secure, fast storing and retrieving process of encryption and decryption of a data from database.

2.1 SYSTEM ARCHITECTURE

Cloud computing infrastructures used to store large datasets and query services. The architecture shows two main parts in it. The data's can be stored in the cloud by data owners d=n (d, k) here d represents data, n represents normal form of data, k represents key value given by the data owner. This format will be saved in the cloud as encrypted form d=e (d, k) here e represents encryption.

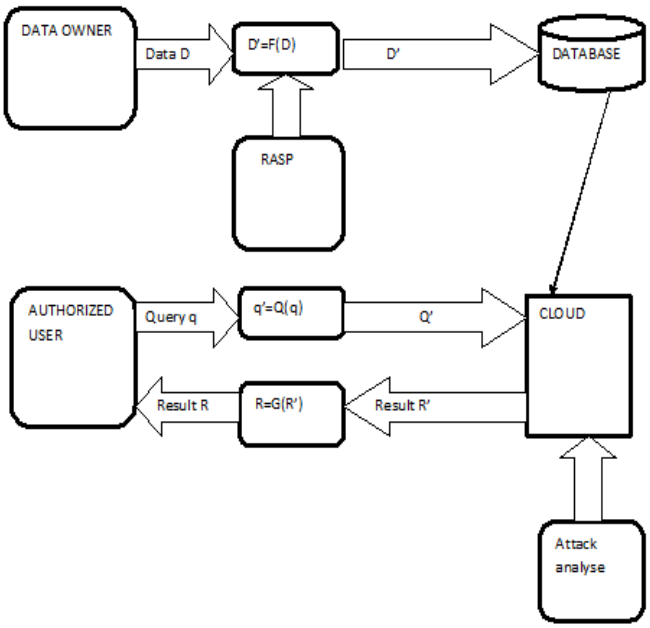


Fig. 1 System Architecture using RASP method

The above diagram shows two separate parties. They are customer who is the trusted party store their data in cloud and second are cloud provider who is storing the data in encrypted format. In the customer party it includes data and service owners, proxy server of in-house process and users. Here the owner can store their data in cloud while those data will encrypted in cloud and stored in the cloud database and also the data owner will provide key value by using that key value only cloud will encrypt the data by using random space perturbation method. The user will send query to retrieve the data from cloud, user can send range query and kNN query to get the data. In the cloud, the cloud provider has to host the user query services and have to protect the data stored in the cloud database.

The basic procedure in the diagram is: (1) the owner sends the data to store in cloud that

data will be encrypted by using random space perturbation method and stored in cloud database. (2) the user will send the range query or kNN query to retrieve the data that query will be encrypted and send to cloud storage. (3) the cloud storage will send the data for that query after processing the query inside cloud storage and it will be decrypted and finally the data will send to the user.

2.2 SECURITY ANALYSIS

The security analysis in the architecture shows the following

- Users have been authorized by using the key value provided by the owner. So an authorized user is not being a malicious and only those users can send the queries for retrieving the data.
- The communication process between the user, owner and cloud and client system are well secured, the data and queries cannot be leaked from the cloud.
- RASP method is used to protect the query privacy and confidentiality of the data.

Attacker Process: The main process of attacker is to hack the data from the database and they will try to find the perturbed data and they will try to find the queries.

3 MODULES

Three modules are used. They are RASP, range query and kNN query.

3.1 RASP

RASP denotes Random Space Perturbation. It also combines OPE, random projection and random noise injection. Here OPE denotes Order Preserving Encryption is used for data that allows any comparison. And that comparison will be applied for the encrypted data; this will be done without decryption. Random projection is mainly used to process the high dimensional data into low dimensional data representations. It contains features like good scaling potential and good performances. Random noise injection is mainly used to adding noise to the input to get proper output when we compare it to the estimated power.

The RASP method and its combination provide confidentiality of data and this approach is mainly used to protect the multidimensional range of queries in secure manner and also with indexing and efficient query processing will be done. RASP has some important features. In RASP the use of matrix multiplication does not protect the dimensional values so no need to suffer from the distribution based attack.

RASP prevents the data that are perturbed from distance based attacks; it does not protect

the distances that are occurred between the records. And also it won't protect more difficult structures it may be a matrix and other components. The range queries can be send to the RASP perturbed data and this range query describes open bounds in the multidimensional space.

In random space perturbation, the word perturbation is used to do collapsing this process will happen according to the key value that is given by the owner. In this module the data owner have to register as owner and have to give owner name and key value. And then the user have register and get the key value and data owner name from the owner to do access in the cloud. Here user can submit their query as range query or kNN query and get their answer. This paper analyze and show the result with encrypted and also in decrypted format of the data for the query construct by the user.

3.2 RANGE QUERY

Range query is the query used to retrieve the data from the database [10]. It will retrieve the data value that is between the upper bound and lower bound. The range query is not usual because user won't know in advance about the result for the query, how much entries will come as result for the query. For example:

```
SELECT id
FROM table name
WHERE id (
SELECT top 15*
FROM United States
WHERE age >55
);
```

The above example shows the sample query for range query. Here the example query is to retrieve the entries from United States it will retrieve the persons who are above 55 years in the top 15 list from the record of United States.

The range search is mainly used to return the values that are present between the two specified values given in the query. For example database name is CLASS workers2014 then

```
Go
SELECT product id
FROM CLASSworkers2014.production
WHERE price BETWEEN 30 and 60
```

The above example will show an another example of range query search it will provide the

entries of what are product id that are present in production database with price above 30 and within 60. So by using range query user can easily retrieve the data's from records and this query process will be done in secure manner and the speed of the query process will also increased.

3.3 kNN QUERY

kNN query represents k-Nearest Neighbor query. This query is mainly used to retrieve the nearest neighbor values of k. here k used to denote positive integer value[12]. kNN algorithm is mainly used for classification and regression. In this it uses kNN-R algorithm to process the range query to kNN query. This algorithm consists of two methods. That is used to make interaction between the client and the server. The client will send the query to the server with initial upper bound and lower bound. This upper bound range has to be more than the k points and the lower bound range have to be less than the k points.

The above process is used to give the inner range of the database by the server. With that inner range the client will calculate the outer range and send this outer range to the server. Then the server will search and find the records in the outer range from the database and send it to client and then the client will decrypt the record and find the top k files to provide the final result. This algorithm is used to find the compact inner square range for providing high precision and it has two difficult processes in it. They are to find the number of points that are present in the square range and updating of the boundary (i.e) upper bound and lower bound is difficult because range queries are well secured by using random space perturbation. The security of kNN query and range query is equal.

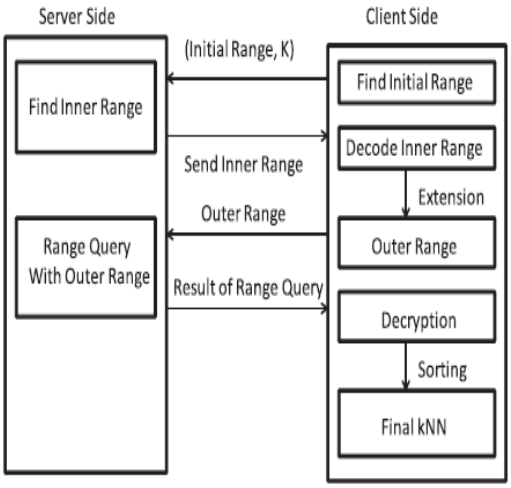


Fig. 2 kNN query process

The above diagram shows the process of k-nearest neighbor query.

3.4 ANALYZED LEAKED QUERY

Analyze leaked query and access pattern of data in cloud. Injection usually occurs when you ask a user for input, like their name and instead of a name they give you a MySQL statement that you will unknowingly run on your database. Never trust user provided data, process this data only after validation; as a rule, this is done by pattern matching. So avoid this sql injection by using security of cloud database. Security of cloud database is provide by encrypt the data and encrypt the query.

4 RELATED WORKS

In this area discussion is based upon OPE, PIR, new Casper and privacy preserving. Clear idea can be gained from reading through in the below topics.

4.1 PROTECTING OUTSOURCED DATA

OPE: OPE represents Order Preserving Encryption is used for data that allows any comparison [1]. And that comparison will be applied for the encrypted data; this will be done without decryption. It allows database indexes to be built over an encryption table. The drawback of this process is the encryption key is too large and implementation makes the time and space overhead.

CRYPTO INDEX: Crypto index method is vulnerable to attacks but the working system of the crypto index has many difficult processes to provide the secured encryption and security and also the New Casper approach is used to protect data and query [7]. Casper achieves high quality location-based services while providing anonymity for both data and queries but the efficiency of the query process will be affect.

4.2 PRESERVING QUERY PRIVACY

PIR: PIR represents Private Information Retrieval protocols allow the user to retrieve data from a public database with communication strictly smaller than n. PIR query is the description of the hash function. The database contents serves as the input to the hash function and the evaluation of the PIR query on the database is the output of the hash function [11]**.**

PRIVACY PRESERVING: This privacy preserving multi keyword search is based on the plain text search. In this the searching process will done by ranking process. The drawback of this concept is because of ranking process in-house processing time will be maximized [5].

And also we had study about RASP method, query privacy, enabling search services on out sourced data and many concepts.

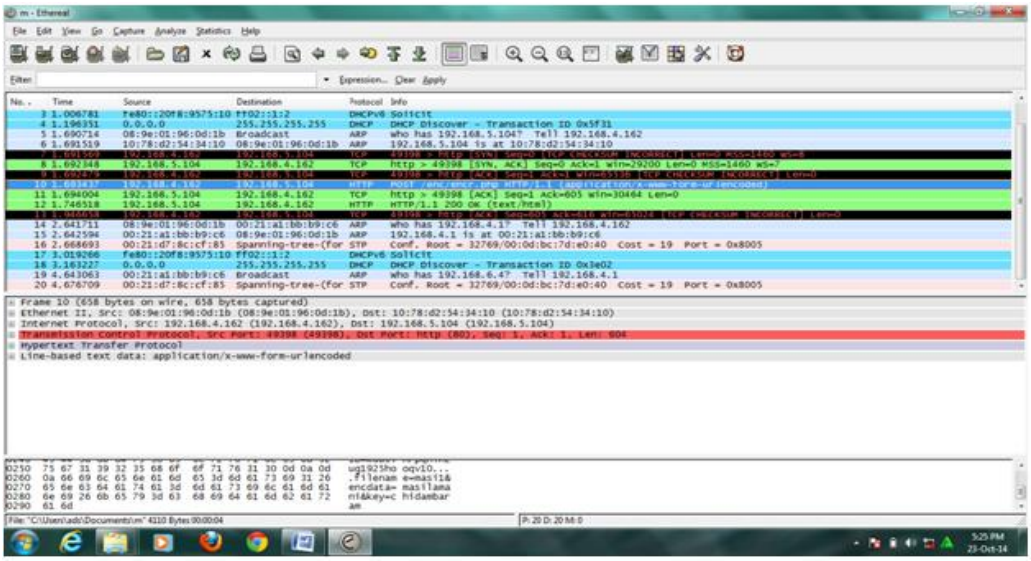
5 COMPARISION BETWEEN EXISTING AND PROPOSED ALGORITHM

PARAMETERS	EXISTING	PROPOSED
Algorithm	Order Preserving Encryption	RAndom Space perturbation
Query processing	Affect the efficiency	Provide confidential and efficiency
Security	Easily hack through sql injection	Avoid hacking through sql injection.
Cost	Increases for filter query result	Saves more in query privacy

6 EXPERIMENTAL RESULTS

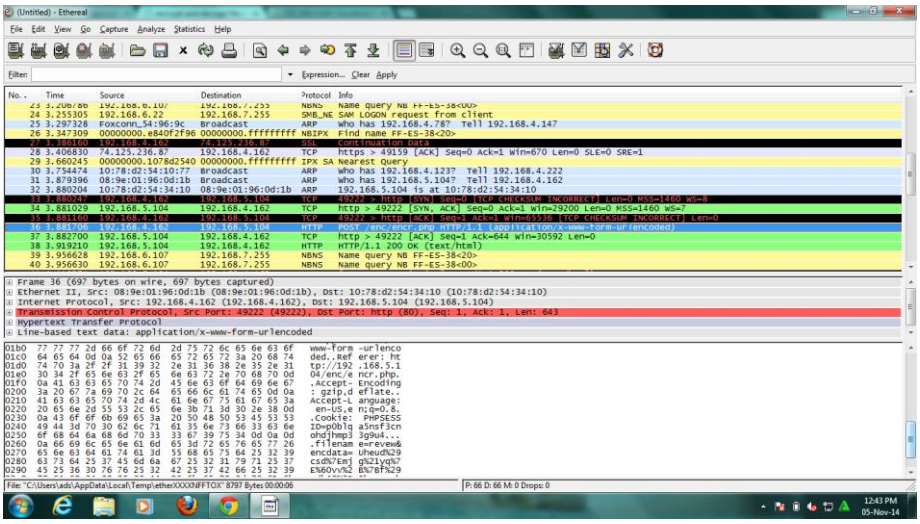
BEFORE QUERY ENCRYPTION

Ethereal tool used to trace out communication between client and server. This tool capture original data send by client. This result is before query encryption.



AFTER QUERY ENCRYPTION

This result is after query encryption by using perturbation method.



7 CONCLUSIONS

This paper proposed RASP method with range query and kNN query. This method mainly used to perturb the data given by the owner and saved in cloud storage it also combines random injection, order preserving encryption and random noise projection and also it has contains CPEL criteria in it. By using the range query and kNN query user can retrieve their data's in secured manner, avoid sql injection and the processing time of the query is minimized. And also formally analyze the leaked query through ethereal tool. we continue our studies to improve the effect of query, and improve the performance of query processing for range query by different cryptography algorithm.

REFERENCES

1. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order PreservingEncryption for Numeric Data," Proc. ACM SIGMOD Int'l Conf.Management of Data (SIGMOD), 2004.
2. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private Information Retrieval," ACM Computer Survey, vol. 45, no. 6, pp. 965-981, 2004.
3. S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge Univ. Press, 2004.
4. M.F. Mokbel, C. yin Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. 32nd Int'l Conf. Very Large Databases Conf. (VLDB),pp. 763-774, 2006.
5. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.K. AndyKonwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing,"technical report, Univ. of Berkerley, 2009.

6. S. Papadopoulos, S. Bakiras, and D. Papadias, “Nearest Neighbor Search with Strong Location Privacy,” Proc. Very Large Databases Conf. (VLDB), 2010.
7. J. Bau and J.C. Mitchell, “Security Modeling and Analysis,” IEEE Security and Privacy, vol. 9, no. 3, pp. 18-25, May/June 2011.
8. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data,” Proc. IEEE INFOCOMM, 2011.
9. K. Chen, R. Kavuluru, and S. Guo, “RASP: Efficient Multidimensional Range Query on Attack-Resilient Encrypted Databases,” Proc. ACM Conf. Data and Application Security and Privacy, pp. 249-260, 2011.
10. H. Xu, S. Guo, and K. Chen, “Building Confidential and Efficient Query Services in the Cloud with Rasp Data Perturbation,”Wright State Technical Report, http://arxiv.org/abs/1212.0610,2014.
11. Ajey Singh, Dr. Maneesh Shrivastava “Overview of Attacks on Cloud Computing “Volume 1, Issue 4, April 2012
12. E.Saral Elizabeth, Ms.K. Padmaveni “Confidential and Efficient Query Services in the Cloud” Volume 2, Issue 1, Feb-Mar, 2014