International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

To Secure Query Services in the Cloud with RASP Data Perturbation

Puja Bhaganagarkar[1], Dhanshree Kulkarni[2]

[1]PG Student, Dr. D. Y. Patil College of Engineering, Pune, Maharashtra, India

[2]Project Guide, Dr. D. Y. Patil College of Engineering, Pune, Maharashtra, India

Abstract: ***To host day services in public cloud is a best solution to save operating expense. However users have concerns on data security to lost control of infrastructure. RASP used to provide security to the setting of cloud based computing while enabling much faster query processing compared to the encryption based approach. In RASP encryption data confidentiality and query privacy are guaranteed when appealing it for range query and kNN. In order to process the range query to kNN query here we used kNN-R algorithm.***

Keywords: Confidentiality, Query Services in cloud, Range Queries, kNN-R Algorithm, RASP Algorithm, RC6 Algorithm

1. Introduction

Cloud computing is used as a storage based strategy. It is used to store and retrieve files, datasets and applications. Number of people uses the cloud because of its different features like privacy service, large storage space and user stratification, less cost and can access at any time, and also number of user can access data at the same time. With the developing of data on Internet (World Wide Web) [1], Search Engines have twisted into the main viewpoint to get to data on the web. A usual authenticity in Web Search is that a user frequently needs many iterations of query modification to find out the preferred results from an internet search engine. In the cloud query services are highly increased because of one point of interest in Scalability and saving cost. In cloud, the query service process are regularly used because, the user can save their cost and Time. The cloud owner will give the amount just for their used time of server. This is one of the best features that, the working time of query processing in cloud is very high and it is more costly.

The random space perturbation (RASP) approach is used to construct range query and k nearest-neighbor (kNN) query services in the records called as database. The proposed system will deal with all the four aspects of the CPEL criteria and aim to achieve all the four aspects. The basic initiative is to arbitrarily make over the multidimensional data sets with a grouping of order preserving encryption (OPE) , dimensionality growth, random project and random noise injection, so that the service for processing range queries is conserved.

The RASP perturbation is considered in such a way that the query range are strongly altered into polyhedral. We also bring in the structure to construct the query services with the RASP perturbation. We use the algorithm to transform queries and processing range queries, the range query service is used to handle kNN queries. When relating these two different services, we also study the attacks on the query privacy. The data holder export the perturbed data to the records called as database. Only authorized person can put forward range queries or kNN queries to learn statistics or find some records.

In abstract, the planned approach has a number of excellent offerings:

- The Random Space perturbation method conserves multidimensional range in protected transformations, which give permission for indexing and professionally query processing.
- Proposed service is able to reduce the in-house processing workload because of the low down perturbation cost and high accuracy query results. This is a very significant characteristic enabling realistic cloud-based solutions.
- The RASP perturbation is a unique combination of OPE i.e. order preserving encryption, dimensionality expansion, random noise injection, and random projection, which provides very powerful privacy assurance.

2. Related Work

a. RASP

Random Space Perturbation is a method which can securely transformed set of data, so the order is preserved but the distribution and domain are changed [3].So that the hacker cannot successfully pick up the original data and the resulting properties are preserved. RASP is the multidimensional and uses the techniques such as geometric perturbation, random noise injection.

b. KNN Query Processing

The kNN query processing is used to find the nearest neighbor at the k point in the spherical range. Instead of spherical ranges to use square ranges is the basic idea of this algorithm to find fairly accurate result, so that RASP query service can be used. In this query can be given in the nearest neighbor of words like „member =male“ then the result will show all the male members in the dataset which is stored in the cloud. With the help of using this technique it will search the nearest neighbor of letter „male“.

Licensed Under Creative Commons Attribution CC BY

c. User Interface Design

The User Interface Design is a very important part for the user to login the Application. This has been doing only for security purpose. In this there are two sections one is for user and another is for user. In this login form first user has to login by entering user name and his password. Suppose this information is right then user can upload or download the files or can do further actions and it proofs that he is an authorized user but if it is not happened then it will show an error message. So we are preventing from unauthorized user entering into the login page to user page which will provide a good security for our project.

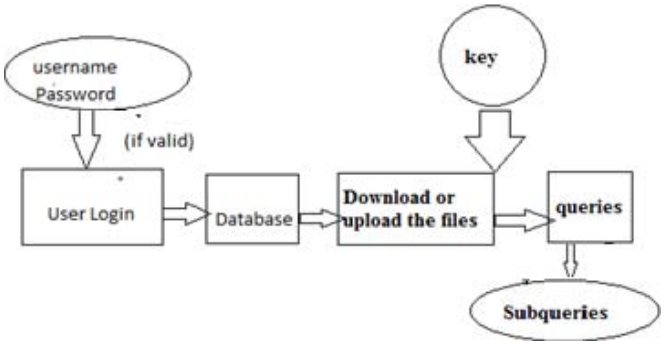

Figure 2.1: Data flow diagram of system architecture

3. Proposed System

A. Problem Definition

To provide security to the data this is stored on cloud while storing or retrieving the data and to find the nearest neighbor from the k point.

B. System Design

The proposed system will give all the four aspects of the CPEL criteria and aim to achieve those criteria. The RASP perturbation is planned in such a way that the queried ranges are confidently transformed into polyhedral in the RASP-perturbed data space, which can be efficiently processed with the support of indexing structures in the perturbed space. To find the nearest neighbor the RASP kNN query service (kNN-R) uses to process kNN queries.

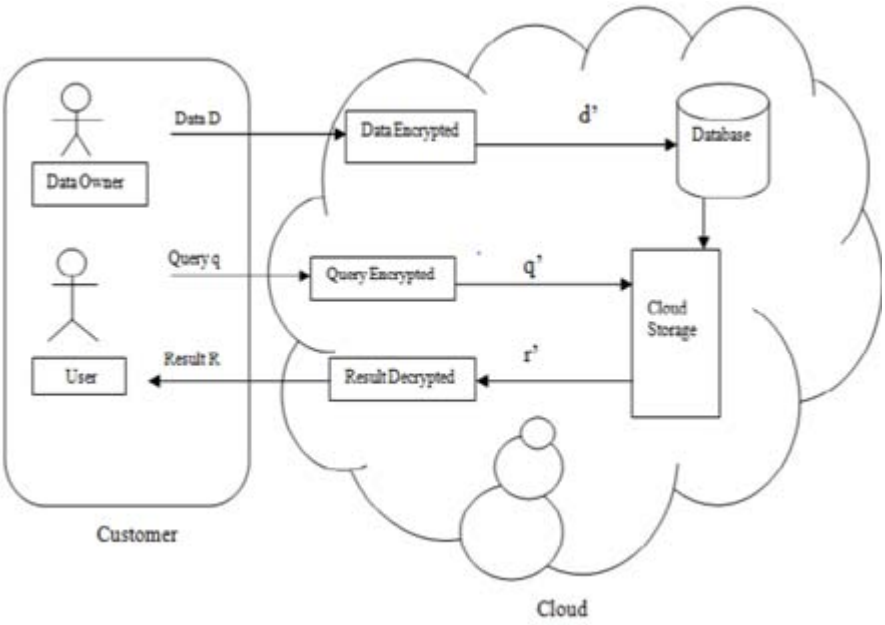

Figure 3.1: System Diagram

C. Algorithm

1) The client generates the initial range and sends its secure form to the server;
2) The server works on the secure range queries and finds the inner range covering at least
3) k points;
4) The client decodes the secure inner range from the server and extends it to the outer range, which is sent back to the server;
5) The server returns the points in the outer range
6) The client decrypts the points and extracts the k nearest points;

4. Results

Figure 4.1: Clint gives the initial range and outer range

Licensed Under Creative Commons Attribution CC BY

Figure 4.2: Find nearest neighbor using KNN algorithm

Figure 4.3: As per initial and outer range the nearest neighbor has been found and user can upload the file with one private key

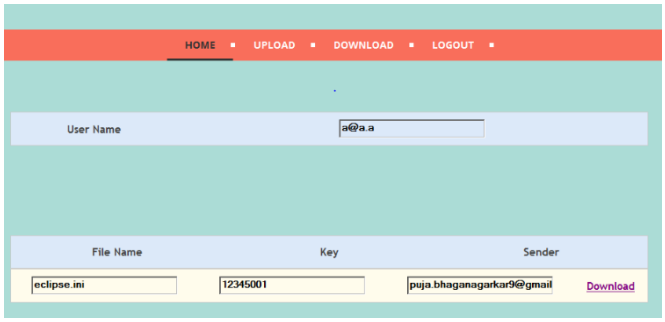

Figure 4.4: Received receives the file with one private key and with the help of that private key he can download the file

5. Conclusion & Future Scope

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 and the processing time of the query is minimized.

We propose to study an outsourced service based on the CPEL criteria: data Confidentiality, query Privacy, Efficient query processing, and Low in-house workload. With the CPEL criteria in mind, we develop the kNN-R approach for secure outsourced kNN query service. The kNN-R approach takes advantage of fast and secure RASP range query processing to implement kNN query processing. It can find high precision kNN results and also minimize the interactions between the cloud server and the in house client. High precision kNN results and minimized interactions result in low in-house workload.

References

[1] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. Order preserving encryption for numeric data. In Proceedings of ACM SIGMOD Conference (2004).
[2] Boneh, D., and Waters, B. Conjunctive, subset, and range queries on encrypted data. In the Theory of Cryptography Conference (TCC (2007), Springer, pp. 535–554.
[3] Chen, K., and Liu, L. VISTA: Validating and refining clusters via visualization. Information Visualization 3,4 (2004), 257–270.
[4] Curtmola, R., Garay, J., Kamara, S., and Ostrovsky, R. Searchable symmetric encryption: improved definitions and efficient constructions. In ACM CCS (2006), pp. 79–88.
[5] Xu, H., Guo, S., and Chen, K. Building confidential and efficient query services in the cloud with rasp data perturbation. IEEE Transactions on Knowledge and Data Engineering 26, 2 (2014)
[6] J. Bau and J. C. Mitchell, "Security modeling and analysis," IEEE Security and Privacy, vol. 9, no. 3, pp. 18–25,2011.
[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data,".
[8] K. Chen, R. Kavuluru, and S. Guo, "Rasp: Efficient multidimensional range query on attack-resilient encrypted databases," in ACM Conference on Data and Application Security and Privacy, 2011, pp. 249–260.
[9] K. Chen and L. Liu, "Geometric data perturbation for outsourced data mining," Knowledge and Information Systems, 2011.
[10] M. L. Liu, G. Ghinita, C. S.Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The International Journal of on Very Large Data Base, vol. 19, no. 3, 2010
[11] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS), 2010.
[12] M. L. Yiu, C. S. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services," in Proceedings of IEEE International Conference on Data Engineering (ICDE), Washington, DC, USA, 2008, pp. 366–375.
[13] S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest neighbor search with strong location privacy," in Proceedings of Very Large Databases Conference (VLDB), 2010.
[14] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," Proceedings of IEEE International Conference on Data Engineering (ICDE), pp. 601–612, 2011.
[15] M. L. Liu, G. Ghinita, C. S.Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The Inter-national Journal of on Very Large Data Base, vol. 19, no. 3, 2010.

Licensed Under Creative Commons Attribution CC BY