Constructing Trusted and Capable Demand Services the Cloud with RASP Data Perturbation

M. Nandakishore,
Asst.Professor, MCA,
SVCET, Chitoor,
Andhrapradhesh.
.

V. Haribabu,
Asst.Professor, MCA,
SVCET, Chittoor,
Andhrapradhesh.

***Abstract*-Construct the cloud computing infrastructures using the data services for reducing the cost and increasing the scalability. In that, the data owner don't need move the data unnecessary to another. And the data owner can provide the confidentiality. And in this process reduce the workload on cloud computing. In that we use the random space perturbation for to provide the secure and KNN query can be used for to protect the data in the cloud. Random space perturbation can combines the OSE, random noise injection, dimensionality expansion, random projection. KNN query can use the algorithm also.**

***Index Terms*– KNN query, OSE, Perturbation.**

I. INTRODUCTION

The cloud is represents the hosting data query services for reducing the cost and scalability. The services charges are applied for using services in hours by the owner. The query services are highly dynamic; it can be expensive and inefficient to serve. Whenever lose the data in the cloud, data confidentiality and query privacy service providers can use for make the copy of the data and it will be difficult to detect the cloud infrastructures. The new users are needed to data confidentiality and query privacy. In that, the query services are provide security and privacy assurance. So we can use services of requirements for constructing query services in the cloud are confidentiality, query privacy, efficient query processing and low cost. In that, these requirements are used for increase the complexity. In we can use the two types of approaches are Random space perturbation and K-nearest neighbour query services. In that, the cloud data can be confidential but hackers are hacking the all original data, however the hacker can hack the original data is as following:

1.1 Data Evaluate and Estimation:

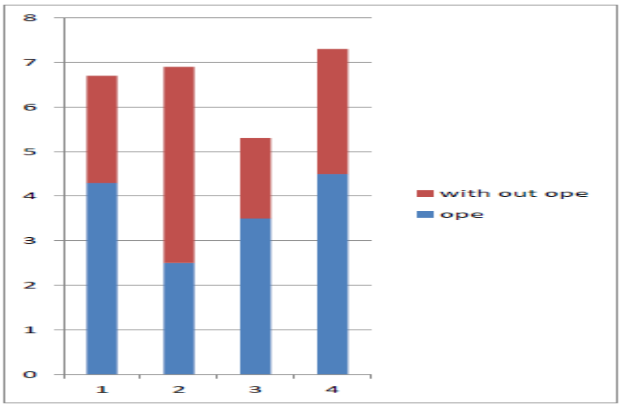
The hacker could not correctly estimate original data but hacker estimates the some data in original data. And hacker estimate on the perturbed data. Hacker not needs exactly original data. In this, hacker use the mean squared error (MSE) is used for effectiveness of attack.

1.2 Prior knowledge based analysis:

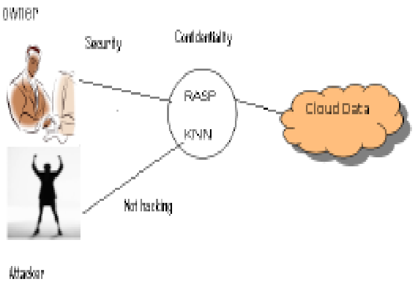
The hacker can be analyzing the security and privacy. The hacker can be analyzing the security using the both exact match and statistical estimation. And the hacker can use the Naive estimation is For a known perturbed dataset P, there exists O(2(d+1)(d+2)n) candidate X datasets in The original space and distribution based estimation is There are O(2dn) candidate projection
Vectors, w, that leads to the same level of non-gaussianity also. This can be represents the how we can secure the data and how to protect the data on cloud. In this we discoursed about these things. They are RASP perturbation expansive, two stage query processing, KNN query processing and advantages.

1.3 Datasets:

The datasets are represents in graphs is a synthetic datasets draws samples. And adult datasets draw from UCI machine learning database. And we can declare the numeric values in mapping.

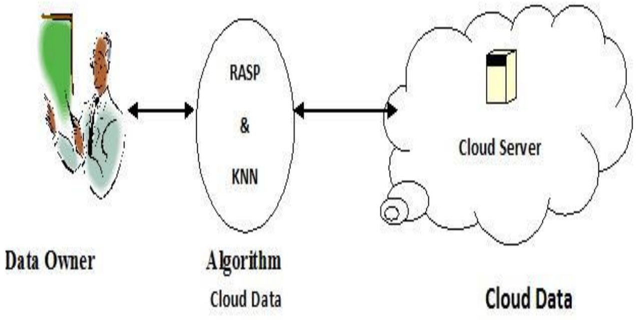


2. ARCHITECTURE:



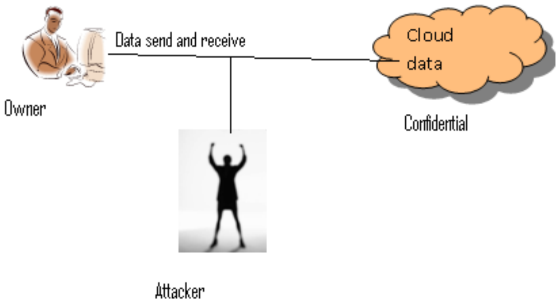
2.1 Module for Protecting Data:

In that, we can represent the query privacy and Confidentiality. If data in RASP. The data can be very implement and efficient .it will be protective from the RASP.



2.2 Module for attacking:

The attacker can be mainly focus on to estimate or to identify or to hacking the data from the original data or perturbed data. However**,** the attacker hacking the data using as following thing. The attacker knows the perturbed data and queries, so these are specifies the cipertext and cryptographic set things. And then the hacker Knows all original data individual and join distributions between the attributes.



2.3 Module for Security:

We can secure our data because the hacker hacking the original data so we can implement another hacker satisfied data and we can represents the effectiveness measure data is used for hacker could not hack and estimate the original data.

2.4 Module for RASP:

The RASP abbreviation is Random Space Perturbation. This RASP is the one of the multiplicative perturbation. It will contain the Order Preserving Encryption, Random noise injection, Dimensions expansion, Random projection. It will represent the multiple data. Order Preserving Encryption can use for to convert all dimensions of the original data to the standard normal distribution in limited domain. Then RASP can have some features. RASP does not preserve the order of dimensional values. And RASP does not preserve the distances between records, which prevents the perturbed data from distance based attacks. And the original range queries can be transformed to the RASP perturbed data space, which is the basis of our query processing strategy.

2.5 Module for data confidentiality:

The attackers need finding the exact original data records and this data can be confidential because hackers are not allowed for hacking.

2.6 Module for KNN query processing:

The KNN Query is can't meet or directly with RASP perturbed data. It can be use the algorithm. The KNN query algorithm returns result with 100% recall. The KNN query algorithm can contains the two types of interactions between the client and server. The client will send the initial upper bound range, calculates the outer ranged based on the inner range and sends it back to the serve.

2.7 Query privacy:

The query privacy can be represents any user will involved in asking questions for cloud data. In cloud having any mistakes and have wrong information displayed automatically problem is occur. So some users are introducing that type of information. Then they are ask questions and rectify the problem using correct solutions.

2.8 Low cost:

The low cost can be used for decrease the cost of the data. Cost can implement by the owner of the data and he decides the particular data can equal to some price. The RASP Data perturbation can be used for reducing the cost.

CONCLUSION:

The RASP can satisfy the data confidentiality, Query privacy, efficient query processing, low *cost. RASP can composition of OPE, Random noise injection, Dimensionality expansion*, Random projection, which provides unique security features.

REFERENCES:

1. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proceedings of ACMSIGMOD Conference, 2004.
2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. K. And Andy Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” Technical Report, University of Berkerley, 2009.
3. J. Bau and J. C. Mitchell, “Security modeling and analysis,”IEEE Security and Privacy, vol. 9, no. 3, pp. 18–25, 2011.
4. S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge University Press, 2004.
5. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacypreserving multi-keyword ranked search over encrypted cloud data,” in INFOCOMM, 2011.
6. 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.
7. K. Chen and L. Liu, “Geometric data perturbation for outsourced data mining,” Knowledge and Information Systems, 2011.
8. K. Chen, L. Liu, and G. Sun, “Towards attack-resilient geometric data perturbation,” in SIAM Data Mining Conference, 2007.
9. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” ACM Computer Survey, vol. 45, no. 6, pp. 965–981, 1998.
10. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2006, pp. 79–88.
11. N. R. Draper and H. Smith, Applied Regression Analysis. Wiley,1998.
12. H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, “Executing sql over encrypted data in the database-service-provider model,” in Proceedings of ACM SIGMOD Conference, 2002.
13. T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning. Springer-Verlag, 2001.
14. B. Hore, S. Mehrotra, and G. Tsudik, “A Privacy- preserving index for range queries” in Proceedings of very large Databases Conference (VLDB), 2004.