International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

Security on Cloud Computing

Deepa Suresh Tandale
Deogiri Institute of Engineering and Management Studies
Aurangabad, India

***Abstract*:- Now days, cloud computing is getting popular for data storage and using a network of remote servers. Cloud computing has many benefits like scalability, flexibility, cost savings, reliability, maintenance and mobile accessibility. Since cloud computing technology is growing day by day, it concerns with some particular security issues as well. The issues like unauthorized access, service traffic hijacking, data loss etc. To work with data storage security in cloud, there are many encryption algorithms. In this paper, there are two methods described for data storage security. First method called range and knn query, where range query algorithm is used to encrypt the data and knn query algorithm is used to decrypt the encrypted data. The second used method is MuteDB where SQL operations can perform on encrypted data and access control policies to cloud provider. At last we compare these two methods on the basis of different parameters.**

***Keywords**: Cloud data storage, knn and range query algorithm, MuteDB, security.*

I. INTRODUTION:

Cloud computing is a technology which can be used in a different scenarios like providing computational resources over internet, a distributed system and it allows to share the business information to the another different parties and it also includes not only the data storage, user and cooperate applications but also it provides IT services and mobile interactive applications along with parallel batch processing etc. Cloud computing uses the vendors like Amazon EC2 which is commonly used also the Microsoft Azure and Google App Engine[1]. There are number of cloud computing advantages but it is major concern to provide proper security for cloud storage. There are different approaches for cloud computing security like encryption approach in which plain text is encrypted and stored in secured way. The next approach is framework approach where trusted of multi-tenant type of framework are there, the striping algorithm and data concealment component is the privacy preserving technique which is rarely used. But all along with these approaches the suitable and most of the time using approach is Encryption[6]. There are many popular encryption algorithms for cloud storage basically divided into two parts symmetric algorithms and asymmetric algorithms. The first well known type symmetric algorithms only provide one key for encryption and decryption purpose like Data encryption standard and Advanced encryption standard. The asymmetric algorithms provide private as well as public keys for encryption and decryption purpose like RSA and Digital signature algorithm [2].

Cloud computing security is based on encryption mechanism. Where the user can store the database in the encrypted format, it also provides the private key so that an unauthorized user could not access the file. There is a known encryption algorithm named OPE i.e. order preserving encryption, in which it adds a secrete offset to the message before encryption and preservers dimensional value order after encryption. Here attacker knowledge is important; if attacker knows the original distribution then it can easily break the encryption for particular database. OPE scheme provides the required security for data storage without loosing the efficiency but standard range queries are not supported by OPE[3]. There are other advanced algorithms for security purpose like crpto-index, which is a in-house infrastructure used to improve security and privacy purpose, a column-wise bucketization is used here. Each bucket has its own ID and values in buckets are replaced by bucket ID for indexing purpose [4] and Casper approach, which uses cloaking boxes for improving efficiency of query processing [5].

In this paper, we presented two different scenarios for cloud computing security. Those are knn-range query algorithm and MuteDB Architecture. Section 1 represents knn-range query algorithm, section 2 represents a brief description of MuteDB Architecture and in section 3 the conclusion of these methods is defined.

II. KNN-RANGE QUERY ALGORITHM

We now represent the two different algorithms known as Range query algorithm and Knn query algorithm. The range query algorithm is used to encrypt the stored data and knn query algorithm decrypts the encrypted data.

A. Range Query Algorithm

It simply transforms the range query in the original space to polyhedron query in perturbed space. After this, we simply develop two stage query processing. In transforming Range Queries, firstly OPE is transformed the original hyper cubic area to another hyper cubic area. When this is done query services need to find the records.

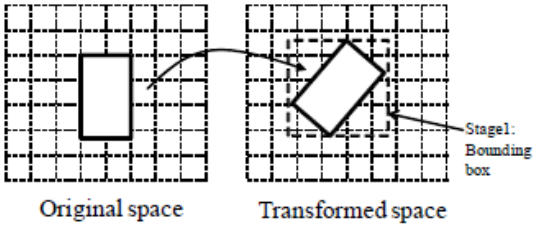

Fig 1: Two-stage processing algorithm

When queries are transformed successfully, then we have to process the queries efficiently. For this Processing Multidimensional Tree is used. The R-Tree algorithms[7], i.e.

the algorithms used for multidimensional information like rectangles or polygon ,which follows the Minimum Bounding Region (MBR), which is the construction block for indexing the multidimensional data as shown in fig 1. Here we show the transformation of rectangles in r-tree.

B. knn Query Processing

The basic operation in knn processing algorithm is to find the nearest given points in the given range that is centred at the query point. Here we first use the square ranges, then find the result for knn and after that we use RASP range query service on that. A square range is nothing but a hyper-cube which contains inner range and outer range. The inner range contains at least k-points whereas the outer range encloses the inner range. The knn algorithm provides the interactions between client side and server side as shown in fig 2.

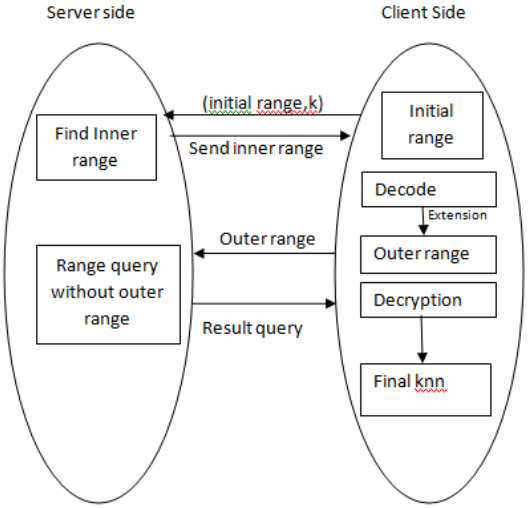

Fig 2: knn-range algorithm

At first client sends initial upper-bound range having more k-point while lower-bound has less k-points to the server. Then it returns to client after server finds the inner range. At second stage, client calculates outer range and sends it back to server, which finds the records of outer range. At last client decrypts the records and finds k as a final result. The important step in KNN algorithm is to find the compact inner range which is done by updating higher and lower bounds and also finding the number of points in square range[8].

This is how the range query algorithm is used to process the knn query algorithm. Based on this knn-range query algorithm only the authorized user query will be processing and it finds the outer range query result as shown in fig 3.

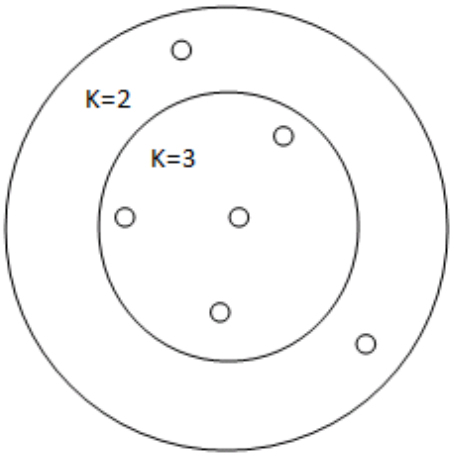

Fig 3: knn-range query processing

III. MUTEDB ARCHITECTURE:

The Multi-User Relational Encrypted Database is a technique that guarantees data confidentiality by executing SQL operations on encrypted database as well as allowing access control policies to cloud provider. It ensures us to provide the data confidentiality even in the worst case scenarios. This can be achieved by translating the access control policies with the access control Matrix. MuteDB also works dynamically so that we did not need to renew and redistribute the credentials. The MuteDB does not need any trusted server; still it provides the same availability and scalability. The architecture for MuteDB is shown in fig 4.

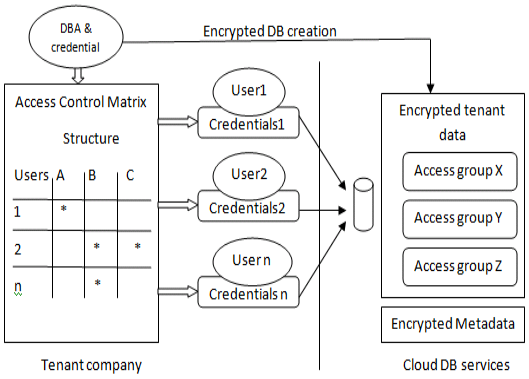

Fig 4. Architecture of MuteDB

As shown in fig 4. There are two partitions as Tenant Company and cloud database services which is connected by creation of encrypted database. All the users of Tenant Company are allowed SQL operations directly from any distributed location. The tenant data is stored in the form of encrypted format in cloud databases. DBA owns the users credentials so that no one can access the unauthorized data. The DBA manages the user account and all kind of access control policies. The access control policies are hard to define in cloud database so we provide the separate credential for separate user.

To describe access control policies we defined the access control matrix which is a table where each row is associated with a database user and each column is associated with a structure. Each cell of matrix defines whether or not it can access the corresponding structure. Suppose there are users 1,2....n and structure as A, B, C, user 1 can access the A structure only and user 2 can access structure B & C only. We provide the access group of encrypted tenant data in cloud database services to specified structures like for structure A, there is access group X and for structure B, access group Y and so on.

Now each user credential consists of small information having a secrete key which is used to encryption process. The key is encrypted through the AES algorithm and the derivation key, so that user can access the data. This is very useful technique for providing cloud security and improving the cloud performances and scalability [9].

IV. CONCLUSION:

This paper gives the cloud computing security methods so that we can increase the performance level in cloud. We can store the data and none any unauthorized party could able to upload it. The range-knn method provides a trusted server and save the data in the encryption format on the cloud server while the MuteDB method allows multiple users to work on server and it provides a secrete key to encrypt and decrypt the data. The MuteDB method has an advantage that it does not need any trusted server so that no reason for failure and trouble issues. In future work, we can compare these methods on the basis of performance evaluation, usage estimation and cost evaluation, so that we can improve the cloud storage security.

REFERENCES

[1]. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Electrical Engineering and Computer Sciences University of California at Berkeley Technical Report No. UCB/EECS-2009-28.

[2]. Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing," International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 3, March 2014.

[3]. Alexandra Boldyreva, Nathan Chenette, Adam O'Neill,"Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions," A preliminary version of this paper appears in Advances in Cryptology - CRYPTO 2011, 31st Annual, International Cryptology Conference, P. Rogaway ed., LNCS, Springer, 2011.

[4]. B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in *Proceedings of Very Large Databases Conference (VLDB)*, 2004.

[5]. M. F. Mokbel, C. yin Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proceedings of Very Large Databases Conference (VLDB)*, 2006, pp. 763–774.

[6]. Aized Amin Soofi, M. Irfan Khan, Fazal-e-Amin, "A Review on Data Security in Cloud Computing," International Journal of Computer Applications (0975 – 8887) Volume 94 – No 5, May 2014.

[7]. Y. Manolopoulos, A. Nanopoulos, A. Papadopoulos, and Y. Theodoridis, *R-trees: Theory and Applications*. Springer-Verlag, 2005.

[8]. Huiqi Xu, Shumin Guo, Keke Chen, "Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation," IEEE Transactions on Knowledge and Data Engineering VOL: 26 NO: 2 YEAR 2014.

[9]. Ernesto Damiani, S.De Capitani diVimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati, "Key Management for MultiUser Encrypted Databases," in Proceedings of the 2005 ACM Workshop on Storage Security and Survivability, Alexandria, Virginia, USA, November 11, 2005.