Review on Performance Evaluation for Cloud Database using Adaptive Encryption Architecture

Miss. Autade Dhanshri P. , Prof. Raut S.Y.

***Abstract*— For several Internet based application, the new service is required called as cloud database. In cloud database, all information is encrypted for security purpose. Here, we present architecture for adaptive encryption of public cloud database. At design time, there is trade of between data confidentiality level and flexibility of the cloud database structure. Using software prototype, the feasibility and performance of the proposed solution is demonstrated .It is oriented to evaluation of cloud database service in plain and encrypted instances.**

***Index Terms*— Adaptive Encryption, Metadata structure, encrypted data, encrypted metadata**

I. INDRODUCTION

The Cloud computing paradigm is limited by concern about information confidentiality and over a medium long term. There are several research challenges in database service in terms of security.Some encryption schemes are in applicable to database paradigm. Otherencryption schemes which allow execution of SQL operation over encrypted data, either suffer from performance limit or they require the choice of which encryption scheme must be adaptive for each database column and SQL operation.

In this paper,we propose an architecture for adaptive encryptionof public cloud database that offers a proxy free alternative. Even when the set of SQL queries dynamically changes, the propose architecture guarantees in an adaptive way the best level of data confidentiality for any database workload. The older adaptive encryption scheme not referring to the cloud, encrypts each plain column into multiple encrypted column and each value is encapsulated into different layers of encryption , so that the outer layer guarantee higher confidentiality but support fewer computation capability with respective inners layer. The outer layer is dynamically adopted at run time when new SQL operation is added to the workload. In this architecture , it does not required to define which database operation are allowed on each column , it poses novel issue in terms of feasibility in a cloud context and storage and network cost estimation.

The first we implement proxy free architecture for adaptive encryption of cloud database. The concurrent clients can issue parallel operation without passing through, same centralized component as in alternative architecture. So that there is not limit an availability elasticity and scalability of a plain cloud database.

II. LITERATURE SURVEY

As stated in paper “The Cost of Doing Science on the Cloud: The Montage Example” ,Cloud computing offers a new business model for supporting computations and provides a new option for Scientific applications to have on-demand access to potentially significant amounts of compute and storageresources. Using the Montage application and the Amazon EC2 fee structure as a case study, we showedthat for a data-intensive application with a small computational granularity, the storage costs wereinsignificant as compared to the CPU costs. Thus it appears that cloud computing offers a cost-effective solution for data-intensive

In the paper **“**Access control enforcement on query-aware encrypted cloud databases” it proposes a novel encryption scheme integrated with anaccess control mechanism that guarantees confidentiality ofinformation stored in cloud databases. Unlike state-of-the-artproposals, the proposed scheme allows a customer companyto encrypt all stored and transmitted data, to enforce standarddatabase access control mechanisms where each tenant userhas a different secret key, and to support the execution ofSQL operations on encrypted data stored in a public cloudprovider. This solution guarantees data confidentiality againsta semi-honest cloud provider and limits the risk of informationleakage due to internal users, even against the theft of accesscredentials, and the possibility that an internal user colludeswith a cloud employee. This paper defines the overall ideaand the formal models that demonstrate the correctness andfeasibility of the proposed scheme. The integration of theproposal into cloud-based architectures is left to future work.[5]

The paper titled as "Distributed, concurrent, and independent access to encrypted cloud databases", propose an innovative architecture that guaranteesconfidentiality of data stored in public cloud databases.Unlike state of the art approaches, our solution does notrely on an intermediate proxy that we consider a singlepoint of failure and a bottleneck limiting availability andscalability of typical cloud database services. A large partof the research includes solutions to support concurrentSQL operations (including statements modifying the databasestructure) on encrypted data issued by heterogeneousand possibly geographically dispersed clients. Theproposed architecture does not require modifications tothe cloud database, and it is immediately applicable toexisting cloud Dbase, such as the experimented PostgreSQL Plus Cloud Database, Windows Azure andXeround. There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithms.It is worth to observe that experimental results based on the TPC-C standard benchmark show that the performanceimpact of data encryption on response time becomes negligible because it is masked by network latencies that are typical of cloud scenarios. In particular, concurrent read and write operations that do not modify the structure of the encrypted database cause negligible overhead. Dynamic scenarios characterized by (possibly) concurrent modifications of the database structure are supported, but at the price of high computational costs. These performance results open the space to future improvements that we are investigating.

In thispaper "Practical Techniques for Searches on Encrypted Data", described new techniques for remote searchingon encrypted data using an entrusted server and provided proofs of security for the resulting crypto systems. Ourtechniques have a number of crucial advantages: they are provably secure; they support controlled and hidden searchand query isolation; they are simple and fast (More specifically, for a document of length n, the encryption and each algorithms only need O(n) stream cipher and block cipher operations); and they introduce almost no space and communication overhead. Our scheme is also very flexible, and it can easily be extended to support more advanced search queries. We conclude that this provides a powerful new building block for the construction of secure services in the untrusted infrastructure.

III. SYSTEM DESIGN

In this system, distributed and concurrent client can issue direct SQL operation .The proposed solution guaranteed same level of scalability and availability of cloud service, avoiding architecture based on one or more multiple intermediate server.

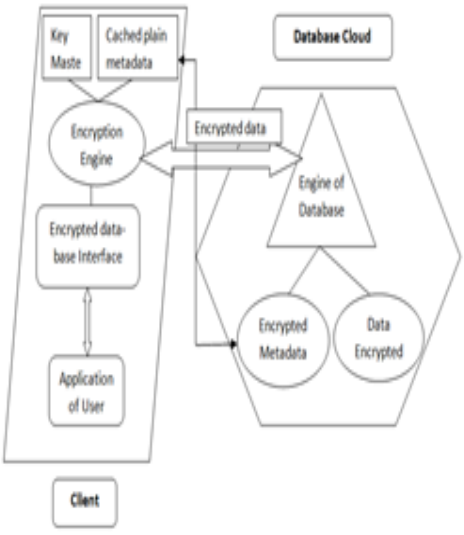

Fig. 1: Encrypted cloud database architecture

Each client execute encryption engine that manage encryption operation. This software module accessed by external user application through the encrypted database interface, five types of information managed by architecture. [3]

1) Plain data is tenant information.

2) Encrypted data stored in cloud database

3) Plain metadata additional information necessary to execute SQL operation on encrypted data.

4) Encrypted metadata is encrypted version of metadata,stored in cloud database.

5) Master key is encryption key of encrypted metadata that is distributed to legitimate client.

In cloud database, all data and metadataare encrypted. Any application running onclient issue

SQL operation to encrypted cloud database through encrypted database interface. Data transferred between user application and encrypted engine are in plain format. Information is always encrypted before sending it to cloud database. When application issue new SQL operation encrypted database interface contacts encryption engine that retrieves the encrypted metadata and decrypted it through master key. The plain metadata are cached locally by client as a volatile information (to increaseperformance).After obtaining metadata, encryption engine able to execute SQL operation encrypted data. Then it decrypted the result .The result are returned to user application through encrypted database interface.

3.1 Adaptive Encryption Scheme

SQL aware encryptionalgorithm guarantees data confidentiality and allow cloud database server to execute SQL operation over encrypted data.

Table no-1 Encryption Scheme

Random (Rand)	**Deterministic (Det)**	**Order preserving encryption**	**Homomorphism sum (Sum)**	**Search(Search)**	**Plain**
It is most secure algorithm	The equality of plain text is preserved	It support comparison SQL operation (=,<,>)	It support sum operation between integer value	It support equality check on full string i.e. LIKE operation	It does not encrypt data
It is not reveal any information about original	It support equality operator	It preserve numerical order of original unencrypted data	It is homomorphism with respect to sum operation so that multiplication of encrypted integer equal to sum of plain text integer		It support all SQL operation on non confidential data

Adaptive encryption scheme preserve maximum level of data confidentiality on column that are never involved in anyoperation. Encryption algorithmorganized into structure called onion. Each onion composed by an order set of encryption algorithm called encryption layer.[4] Outer layer quarantine higher level of data confidentiality and allow less types of operation on encrypted data. Each onion supports a specific set of operation.

Table no-2 onion set of operation

Onion-Eq	Onion-Ord	Onion-Sum	Onion-Search	Onion-Single layer
It support equality operation	It support comparison operation (=,<,>)	It support sum operation	It support string equality operation(LIKE)	It support only one encryption layer
It integrate plain,dte,rand layer	It integrate plain,ope,rand layer	It integrate plain, sum, and layer	It integrate Plain,search,rand layer	

Each plaintext column is converted into one or more encrypted column, each one correspond to onion. Each plaintext value is encrypted though all layers of it's onion.Fig2 Plaintext value associated to onion equation are encrypted thought Det and then Det value is encrypted though rand .Actual layer is most external layer of an onion and correspond to strongest encryptionalgorithm. Cloud database can only see actual layer of onion and has no access to inner layers nor to plaintext data.1st time new SQL operation requested on column then outer layer of appropriate onion is dynamically removed at runtime through the adaptive layer removal mechanism that expose a layer supporting the requested operation.This layer become new actual layer of onion in the encrypted database .The layer removal mechanism is designed to ensure that cloud provider never access the plaintext data. [10]

As shown in example of onion structure, there are two plain text column name as integer data type and varstring .integer column encrypted with onion-eq, onion-ord,onion-Sum.and the string column in encrypted with onion-eq ,onion-Search. The actual layer is rand, not allow computation. When equality check required, rand removed and then det actual layer.

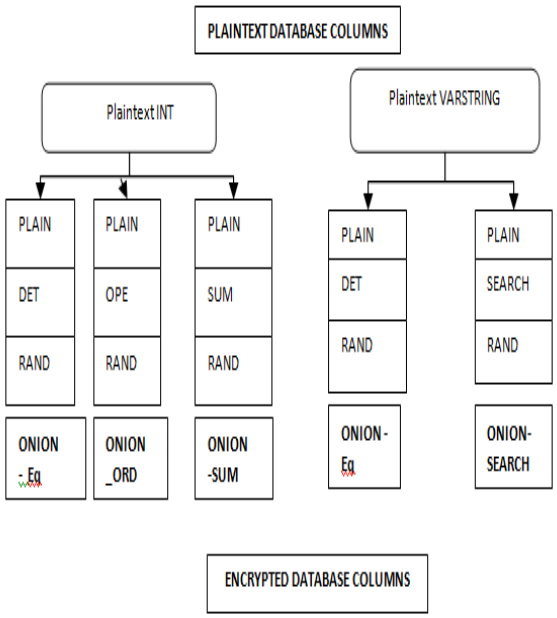

Fig. 2: Example of onion structures

As shown in example of onion structure,there are two plain text column name as integer data type and varstring.integer column encrypted with onion-eq,onion-ord,onion-Sum.and the string column in encrypted with onion-eq,onion-Search. The actual layer is rand, not allow computation. When equality check required, rand removed and then det actual layer

3.2 Metadata structure:-

Metadata contain information to execute SQL operation encrypted database .Information organized in table form.

Table metadata associated with plain name, encrypted name, column met data. The column met data include plain name, data type(int,string, time stamp) and onion met data. onion met data associated with encrypted name (name of onion), field confidentiality (set of keys used to encrypt column data it is of three type, self-represent private set of keys , multi column represent sharing of same set of key among two column, database represent same set of keys on all column of some data type) ,actual layer (external layer name),onion (type of onion eg. Onion-eq). The onion includes layer and encryption key.

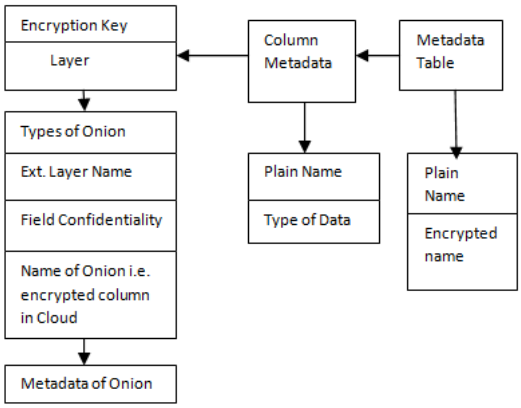

Fig. 3: Metadata structure

IV. IMPLEMENTAION OF ENCRYPTED DATABASE MANGMENT

Database creation,SQL command execution, Adaptive layer removal.

4.1 Database Creation:-

In set up phase database administrator generate master key used to initialize architecture metadata.Distributed toClient. Each table creation requires insertion of new row in metadata table.For each table creation, administration add column by specifying column Name,Data type,Confidentiality. This is important because it include set of onion, actual layer confidentiality parameter. If administrator does not specify conferral parameter of column, then they automatically chosen by client with respective tenant policy.Default policy assume starting layer of each onion is set to it'sstrongest encryption algorithm.Example in fig2 Default integer column encrypted with onion equation

4.2 SQL Condition Execution:

When user application wants to execute operation on cloud database client encryption engine analyze SQL command structure.Algorithm identifies which table column, SQL operation involved.Client issue request for table metadata with master key. [1]Then client determine whether SQL operation are supported by actual layer of onion associated with involved column.If required client issue a request for layer removal in order to support SQL operation at

runtime. By using information stored in metadata client able to encrypt parameter of SQL operation – (table, column name, constant value).client issue encrypted SQL operation (new) to cloud database and execute it over encrypted data.Encrypted result are decrypted using information contained in metadata.[6]

4.3 Adaptive Layer Removal:-

Remove external layer of onion e q .table T with column id of type int and name of type string.following structure issued by client to encrypted cloud database SELECT *FROM T WHEN ID<10.Client encrypt engine analyze SQL statement identify operation id<is to be executed on encrypted database.[2]Then client reads metadata and check whether there is onion order attributes associated to column id(because order onion supporting operation <).If actual layer of onion order associated two id is set to rand then client dynamically involves a stored production a cloud database.Then operation layer is exposed .now client encrypt SELECT query and execute operation (id < 10)on operation layer of onion order.New operation involving comparison an column does not requested to perform operation of remove layer procedure because actual layer of onion order now operation .[7]

Cloud database does not re_encrypted onion back to upper layer (read).each layer has different encryption key. Data remain encrypted and cloud provider cannot access plaintext data.Adaptive layer removal mechanism does never expose plain layer of onion.[9]

V. PERFORMANCE EVALUATIONS

Trade of between performance and data confidentiality in cloud database service .We evaluated impact of encrypted and through put for different network latencies and for increment number of client.For database service the TPC (slandered benchmark is used as workload model) Emulab provide set of machinein (tried environment).each client machine run python client prototype of over architecture on a pc3000k(single 3GHz process,2GB RAM,two 10,000RAM 146 GB SCSI disks).server implemented in postgre SQL 9.1 on a d ..710 machine (quard core xeon 2.4 GHz processor,12GB RAM SATA disk).Each machine run fedora 15 img.Prototypesupports main (SELECT, DELETE,INSERT,UPDATE)and WHERE cluster expression. We consider 3 TPC-C complaint databases having 10 warehouse and scale factor of 5.

Plaintext (PLAIN) based on plaintext data encrypted (ENC)statistically encrypted database where each column encrypted at algorithm time through only one encrypted algorithm.

Adaptively encrypted (ADAPT) database in which each column encrypted with all onion supported by it's data type.In two databases each column is set to highest encrypted layer required to support respective SQL operation of TPC C workload.During each TPC C test lasting for 300second, we monitor number of executed TPC -C transaction and response time of all SQL operation from standard TPC-C workload.We repeat test for each database configuration (PLAIN,ENC,ADAPT)for incremented number of client latency(0 to 120ms).Database uses repeatable read isolation level.

VI. CONCLUSIONS

There is main tenant concern that may present adaption of cloud as fifth Utility called data confidentiality. We address data confidentiality concerns by proposing a novel cloud database architecture that uses adaptive encrypted technology with no intermediate server.This scheme provide tenants with best level of confidentiality for any database workload is likely to change in medium term period

REFERENCE

[1] E. Deelman, G. Singh, M. Livny, B. erriman, and J. Good, "The cost of doing science on the cloud: the montage example," in *Proc. 2008 ACM/IEEE Conf. Supercomputing*, ser. SC '08. Piscataway, NJ, USA: IEEE Press, 2008, pp. 50:1–50:12.

[2] L. Ferretti, M. Colajanni, and M. Marchetti, "Access control enforcement of query-aware encrypted cloud databases," in *Proc. Fifth IEEE Int'l Conf. Cloud Computing Technology and Science*, Dec. 2013.

[3] L. Ferretti, M. Colajanni, and M. Marchetti, "Distributed, concurrent,and independent access to encrypted cloud databases," *IEEE Trans. Parallel and Distributed Systems*, vol. 25, no. 2, Feb. 2014.

[4]D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privacy.*, May 2000.

[5] G. Singh, C. Kesselman, et al., "A Provisioning Model and its Comparison with Best-Effort for Performance-Cost Optimization in Grids," in *HPDC* 2007, pp. 117-126.

[6] H. Zhao and R. Sakellariou, "Advance Reservation Policies for Workflows," in *12th Workshop on Job Scheduling Strategies for Parallel Processing (JSSPP)*,Saint-Malo, France, 2006.

[7] L. Ferretti, F. Pierazzi, M. Colajannni, and M. Marchetti, "Security and confidentiality solutions for public cloud database services," in Proc. of the 7th International Conference on Emerging Security Information, Systems and Technologies, August 2013.

[8] A. Fekete, D. Liarokapis, E. O'Neil, P. O'Neil, and D. Shasha, "Making snapshot isolation serializable," ACM Transactions on Database Systems, vol. 30, no. 2, 2005.

[9] A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. of the Advances in Cryptology – CRYPTO 2011. Springer, August 2011.

[10] Verizon, "IP Latency Statistics," http://www.verizonbusiness.com/about/network/latency, April 2013.