ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 6, JUNE 2015, PP 395-399

Performance and Cost Evaluation of Flexible Architecture with Double Layer Encryption

[1]K. Sravani , [2]D. Praveen Kumar

Abstract: Cloud Computing is an emerging service oriented domain which performs Primitive services as IaaS,PaaS and SaaS along with A Cloud database management system (CDBMS) is a distributed database that delivers computing as a service instead of a product is called as DBaaS (Database as a Service) . Improving confidentiality of information stored in cloud database it is an important contribution to cloud database. Data encryption is the optimum solution for achieving confidentiality. In some native method, encrypt the whole database through some standard encryption algorithm that does not allow the any sql operation directly on the cloud. This formal solution affected by workload and cost would make the cloud database service inconvenient. We propose a novel Flexible architecture for encryption of public cloud database as independent encryption architecture which performs double layer encryption in order to protect Cloud database as well user privacy with data integrity. Adaptive encryption allow any sql operation over encrypted data. The novel cloud database architecture that uses adaptive encryption technique with no intermediate servers. This scheme provides cloud provider with the best level of confidentiality for any database workload. We can determine the encryption and adaptive encryption cost of data confidentiality from the research point of view.

Keywords: Symmetric encryption, SHA-1, Metadata.DBaaS

———————————— ◆ ————————————

1. INTRODUCTION

The cloud computing paradigm is successfully converging as the fifth utility [1], but this positive trend is partially limited by concerns about information confidentiality [2] and unclear costs over a medium-long term [3], [4]. We are interested in the Database as a Service paradigm (DBaaS) [5] that poses several research challenges in terms of security and cost evaluation from a rental service point of view. Most results concerning encryption for cloud-based services [6], [7] are irrelevant to the database paradigm. Other encryption schemes, which allow the execution of SQL operations over encrypted data, either suffer from performance limits (e.g., [8]) or they require the choice of which encryption scheme must be adopted for each database column and SQL operations (e.g., [9]). These latter proposals are fine when the set of queries can be statically determined at design time, while in this paper we are interested to other common scenarios where the workload may change after the database design. In this paper, we propose a novel architecture for adaptive encryption of public cloud databases that offers a proxy-free alternative to the system proposed in [10]. The proposed architecture guarantees in an adaptive way the best level of data confidentiality for any database workload, even when the set of SQL queries dynamically changes. The adaptive encryption scheme, which was initially proposed for applications not referring to the cloud, encrypts each plain column into multiple encrypted columns, and each value is encapsulated into different layers of encryption, so that the outer layers guarantee higher confidentiality but support fewer computation capabilities with respect to the inner layers. The outer layers are dynamically it adapted at runtime when new SQL operations are added to the workload. Although this adaptive encryption architecture is attractive because it does not require defining at design time which database operations are allowed on each column, it poses novel issues in terms of feasibility in a cloud context, and storage and network costs estimation.

In this paper, we investigate each of these issues and we reach original conclusions in terms of prototype implementation, performance evaluation, and cost evaluation. We implement the first proxy-free architecture for adaptive encryption of cloud databases. It does not limit the availability, elasticity and scalability of a plain cloud database, because concurrent clients can issue parallel operations without passing through some centralized component as in alternative architectures [10]. Moreover, we propose the first analytical cost estimation model for evaluating cloud database costs in plain and encrypted instances from a tenant's point of view in a medium-term period. It takes also into account the variability of cloud prices and the possibility that the database workload may change during the evaluation period. This model is instanced with respect to several cloud provider offers and related real prices. As expected, adaptive encryption influences the costs related to storage size and network usage of a database service. However, it is important that a tenant can anticipate the final costs in its period of interest, and can choose the best compromise between data confidentiality and expenses.

2. LITERATURE REVIEW

Hong-Linh Truong and SchahramDustdar: have done experiment by taking few scientific applications and they are only talking about the cost of different components associated with computing environment and most important challenges are to discuss only costs associated with application executions. While cloud service providers give some basic tools for determining computation and data transfer costs, they are trivial. On their work they do not perform the performance prediction but provided a tool for scientists to define the dependency and estimated metrics for their applications based on that the cost is being estimated. Thus, the accuracy of the cost estimation is dependent on scientist knowledge, and this accuracy quality can be improved if our service can also be well integrated with existing performance prediction tools.

- ***K. Sravani*** *is currently pursuing master's degree program in computer science & engineering in Ravindra College of Engineering for Women(JNTUA),India,* ***E-mail:*** Kanakaveetisravani@gmail.com
- ***D. Praveen Kumar***,.Currently he is working as Assistant Professor in Department of Computer Science Engineering in Ravindra College of Engineering for Women, Kurnool. India, **E-mail:** *Praveen.d20@gmail.com*

ZuzanaKristekova at.al [7] suggested to design and develop a simulation model which covers the system dynamic aspect and supports decision makers to analyze costbenefits over cloud computing versus own datacenter [7]. Basically one important thing is for service providers whether it is more economical to move the existing datacenter-hosted services to the cloud or to keep them in the datacenter [7]. This means, that one of the service provider´s primarycriterion for such a decision is costs.In practice, some models exists that support organizations in analyzing and comparing costs, such as "Amazon Simple Monthly Calculator".Amazon Simply Monthly calculatoris a static and do not consider the dynamics of cost development by using cloud computing [8]. To overcome this problem they develop one simulation model, which covers the dynamics of cost development and assists decision makers by analyzing cost benefits associated with cloud computing and own data center. On the other hand the model is based on 'System Dynamic' approach [7] [8]. System dynamics is useful for identifying key decision factors and relationship between them and helps to perform decision making in a more efficient way. System Dynamics is a simulation methodology for modeling dynamic and complex system [7].

3. RELATED WORK:

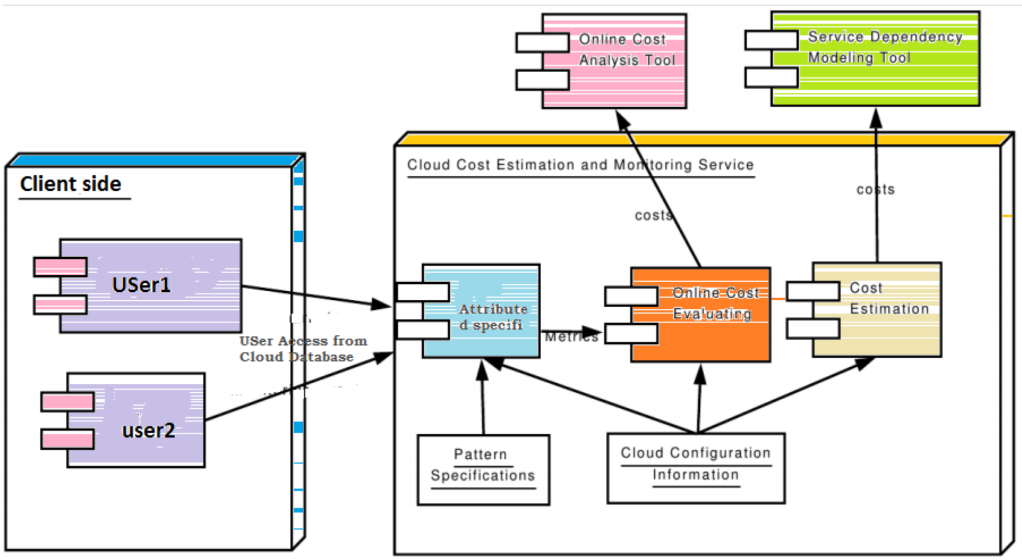

Online Cost Analysis Tool
Service Dependency Modeling Tool
Client side
Cloud Cost Estimation and Monitoring Service
costs
costs
USer1
user2
USer Access from Cloud Database
Attribute d specifi
Metrics
Online Cost Evaluating
Cost Estimation
Pattern Specifications
Cloud Configuration Information

Fig 1.Cloud Cost estimation and Monitoring Service Model

Client Side: Where in the cloud estimation cloud database will be evaluated using cost estimation tools measurements where a client can invoke the cloud data based on some sort of specific attributes , here client need to match with the cloud data specific attributes.In the front end, cloud system acts as the source of information, it collects the information and sends to back end which is nothing but our CCEMSM. CCEMSM connected with online cost analysis tool and service dependency monitoring tool to get the approx cost of the resources used.

Application monitoring sensors:- These sensors collect the data from different PCs or server, relating to each machines performance as well as the performance of applications running on the machines.

Application trace extraction tool:- You can use this tool to verify the flow of logic or to identify bottlenecks within transaction programs. End to End Application Tracing can identify the source of an excessive workload, such as a high load SQL statement, by client identifier, service, module, action, session, an instance. This isolates the problem to a specific user, service, session, or application component.

Online cost analysis tool:- For monitoring and analyzing the cost, data we need to collect is execution time, machine name, data transfer size, data transfer source and destination. This work can be done by different instrumentation techniques, one of them are inserting probes in the beginning and end of the data transfer, application processes, MPI calls and workflows.

Service dependency modeling tool:- This tool keeps the information of dependency among part of applications, computational resources and storages. Mainly 3 types of dependencies are supported: data, control and resource dependency. After getting the data from the application, it keeps checking the dependency tree and generates the events to be sent back to the "cost estimation component".

4. SYSTEM MODEL

PRESENTED SYSTEM:

With Our presented System, there is no adaptive encryption architecture in order to perform data integrity and improve system performance to wards to complete the computation in estimated cost. our presented system has lack of security it means no privacy for user data which are stored at cloud database, who can access the data from Cloud data base by performing SQL operations without decrypting the data they can invoke the cloud database service due to lack of fine grained access control In this connection our presented system fails in providing security, confidentiality, data integrity and improves the system performance

in order to achieve adaptive encryption architecture.

PROPOSED SYSTEM

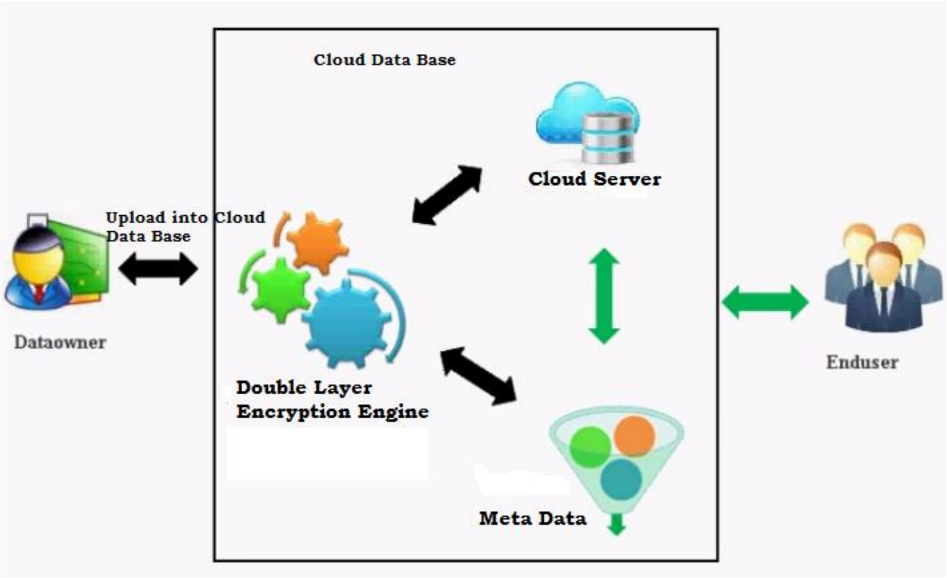
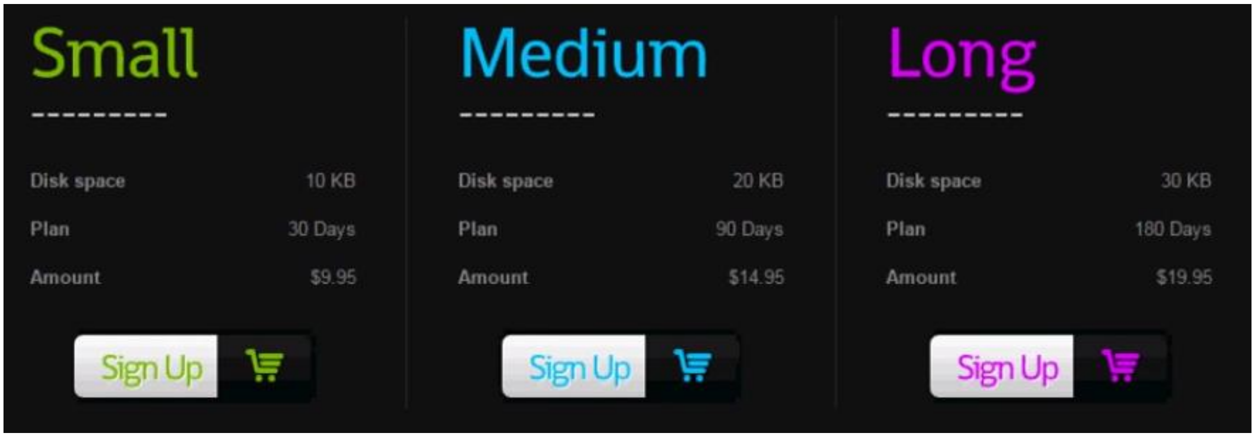


Fig 2. Proposed System Architecture

Where in the Proposed System Data owner can upload data in to Cloud database, as a owner before to upload the data he need to register with policy as Small or Medium or Long And also provide specific attributes as access policy in order to restrict access from un authorized users , soon after getting registration with cloud server , owner can upload double layer encrypted files in to cloud database , as a cloud server can't read that file , data will be available as encrypted formatted as cipher text. So by providing double layer encryption it doesn't allow to read and write to the cloud service providers.When a user want to access cloud database data , he need to be match with access policy with data owner in terms of tenet policy in order to access the data. In this regards we used Blow fish encryption algorithms for layer-1 Encryption and SHA-1 (Secured Hashing Algorithm) is used for 2-layer encryption.



	Small	Medium	Long
Disk space	10 KB	20 KB	30 KB
Plan	30 Days	90 Days	180 Days
Amount	$9.95	$14.95	$19.95

Fig 3. Policy Selection for Adaptive architecture

METADATA include all information that allows a legitimate client knowing the master key to execute SQL operations over an encrypted database. They are organized and stored at a table-level granularity to reduce communication overhead for retrieval, and to improve management of concurrent SQL operations. We define all metadata information associated to a table as table metadata. Let us describe the structure of a table metadata .Table metadata includes the correspondence between the plain table name and the encrypted table name because each encrypted table name is randomly generated. Moreover, for each column of the original plain table it also includes a column metadata parameter containing the name and the data type of the corresponding plain column (e.g., integer, string, timestamp). Each column metadata is associated to one or more onion metadata, as many as the number of onions related to the column.

COST ESTIMATION OF CLOUD DATABASE SERVICES:

A tenant that is interested in estimating the cost of porting its database to a cloud platform. This porting is a strategic decision that must evaluate confidentiality issues and the related costs over a medium-long term. For these reasons, we propose a model that includes the overhead of encryption schemes and variability of database workload and cloud prices. The proposed model is general enough to be applied to the most popular cloud database services, such as Amazon Relational Database Service.

COST MODEL:

The cost of a cloud database service can be estimated as a function of three main parameters:
Cost = f(T ime, Pricing,Usage) where:

- Time: identifies the time interval T for which the tenant requires the service.
- Pricing: refers to the prices of the cloud provider for subscription and resource usage; they typically tend to diminish during T .
- Usage: denotes the total amount of resources used by the tenant; it typically increases during T .In order to detail the pricing attribute, it is important to specify that cloud providers adopt two subscription

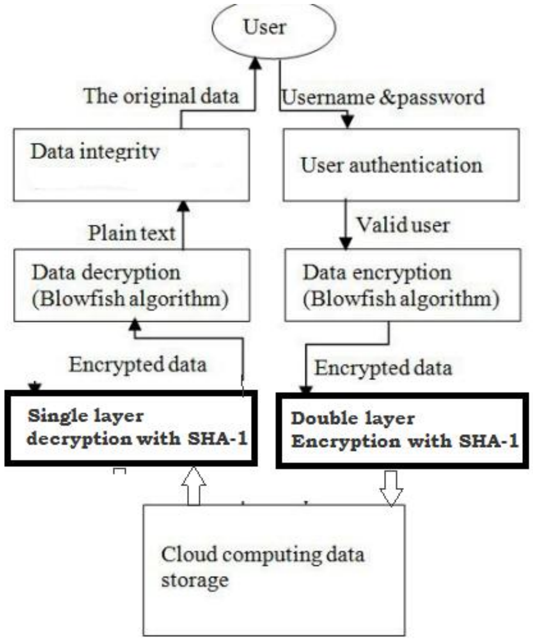

User
The original data
Username &password
Data integrity
User authentication
Plain text
Valid user
Data decryption (Blowfish algorithm)
Data encryption (Blowfish algorithm)
Encrypted data
Encrypted data
Single layer decryption with SHA-1
Double layer Encryption with SHA-1
Cloud computing data storage

Fig 4. Data encryption and Decryption using symmetric algorithms

Authentication method: username and password used for authentication process.

Encryption operation: Blowfish encryption algorithm is used for exchanging information or data for its superiority in terms of the processing time, and no attack is known to be successful against this. Blowfish algorithm used for encryption and decryption operations. The file sent to the cloud computing data store and stored in fully encrypted form and nobody can decrypt it without having the key. And when the encrypted file is uploaded for storing to the cloud data store, the key and the path of the encrypted file along with the user account is kept and maintained in the database table on the cloud data store.

Decryption operation: In the proposed model Blowfish algorithm is used for the decryption operation, whenever the user requests for a file the file moves from the cloud to the user in encrypted form and after receiving an encrypted file from the cloud, the file decrypted with Blowfish algorithm using the same key that used in the encryption operation. Data integrity operation: In the proposed model SHA-1 cryptographic hash algorithm is used for the integrity operation, SHA-1 is that this method is a one way system and unbreakable.

Challenges of data encryption

Despite the benefits and applications of encryption method in safe guarding cloud database, various reasons have hindered the deployment and sending data to the cloud. These factors include, performance impacts, difficulty in performing query over the encrypted data, key management issue, requirements of changes in data application, and data availability. [11].

Solutions to the challenges of data encryption: Solutions to these challenges are provided based on the priority to the cloud data.

Query performance :Execution of query over an encrypted data have been provided with various proposed techniques such as Aggregation queries- partial and fully Homomorphic encryption, Range queries, trusted computing, cipher base and secure server [12], [1] and [4]. A profound flexible and reliable security solution to an encrypted data in the cloud according to [16] is the database should be worked in its encrypted form in the cloud without decrypting in the cloud. This approach would disallow the service provider to know the contents and query processing.

Key management: According to (RSA Security) key management issue in database encryption can be solved using external Hardware Security Module or Wallet. The function of Wallet is to store, manage and protect the

5. CONCLUSION:

In this paper we demonstrate how secure a proposed novel Flexible architecture for encryption of public cloud database as independent encryption architecture which performs double layer encryption in order to protect Cloud database as well user privacy with data integrity. Adaptive encryption allows any sql operation over encrypted data. The novel cloud database architecture that uses adaptive encryption technique with no intermediate servers. This scheme provides cloud provider with the best level of confidentiality for any database workload. We can determine the encryption and adaptive encryption cost of data confidentiality from the research point of view. Further we noticed to implement optimized technique to perform double layer encryption technique to improve the system performance.

6. REFRENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

[2] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: an enterprise perspective on risks and compliance. O'ReillyMedia, Incorporated, 2009.

[3] H.-L. Truong and S. Dustdar, "Composable cost estimation and monitoring for computational applications in cloud computing environments," Procedia Computer Science, vol. 1, no. 1, pp. 2175 – 2184, 2010, iCCS 2010.

[4] E. Deelman, G. Singh, M. Livny, B. Berriman, 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.

[5] H. Hacig¨um¨us¸, B. Iyer, and S. Mehrotra, "Providing database as a service," in Proc. 18th IEEE Int'l Conf. Data Engineering, Feb. 2002.

[6] G. Wang, Q. Liu, and J. Wu, "Hierarchical attributebased encryption for fine-grained access control in cloud storage services," inProc. 17th ACM Conf. Computer and communications security. ACM,2010, pp. 735–737.

[7] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, "Executing sql over encrypted data in the databaseservice-provider model," in Proc.ACM SIGMOD Int'l Conf. Management of data, June 2002.

[8] 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.

[9] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in Proc. 23rd ACM Symp. Operating Systems Principles,Oct. 2011.

[10] C. Gentry, "Fully homomorphic encryption using ideal lattices,"in Proc. 41st ACM Symp. Theory of computing, May 2009.

[11] Boldyreva, N. Chenette, and A. O'Neill, "Orderpreserving encryption revisited: Improved security analysis and alternative solutions," in Proc. Advances in Cryptology – CRYPTO 2011.Springer, Aug. 2011.

[12] P. Paillier, "Public-key cryptosystems based on composite degreeresiduosity classes," in Proc.

ABOUT AUTHORS

K. Sravani graduated B.Tech in Computer Science and Engineering from Ravindra College of Engineering for Women(JNTUA), Kurnool and now pursuing M.Tech(CSE) from Ravindra College of Engineering for Women(JNTUA), Kurnool. Research area of interest includes Cloud Computing, Computer networks and Databases.

Mr. D. Praveen Kumar graduated B.Tech (CSE) from Khader Memorial College of Engineering and Technology (JNTUH), Devarakonda and M.Tech (CSE) from Vidya Vikas Institute of Technology (JNTUH), Chevella. Currently he is working as Assistant Professor in Department of Computer Science Engineering in Ravindra College of Engineering for Women (JNTUA), Kurnool. His areas of interest are cloud computing, Databases and Data Mining.