INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 2 DEC 2015

Determining the Encryption and Adaptive Encryption Cost of Data Confidentiality

[1] N.Raghu, [2] A.Bakiya Lakshmi, [3] T.Malathi

[1]M.Tech Student, Department of CSE, Aurora's Scientific Technological And Research Academy, Bandlaguda village, Hyderabad Mandal, Hyderabad District, Telangana, India.

[2]Assistant Professor, Department of CSE, Aurora's Scientific Technological And Research Academy, Bandlaguda village, Hyderabad Mandal, Hyderabad District, Telangana, India.

[3]Sr.Assistant Professor, Department of CSE, Aurora's Scientific Technological And Research Academy, Bandlaguda village, Hyderabad Mandal, Hyderabad District, Telangana, India.

*Abstract— **Cloud computing is a common term for the release of hosted services over the internet. Cloud computing enables organizations to use the resources and compute their utility rather than building and maintaining computing infrastructure. A cloud database is a database that has been optimized or made for a virtualized computing environment. Since these data-centers may be located in any part of the world beyond to accomplish and control of users, there are multifarious security and privacy challenges that required to be understood and addressed. Cloud has been prone to various security issues like storage, calculation and attacks like Denial of service, Distributed Denial of Service, Eavesdropping, insecure authentication or logging etc. We propose a novel cloud database architecture that uses adaptive encryption technique with no intermediate servers. This system provides cloud provider with the best level of confidentiality for any database workload. We can establish the encryption and adaptive encryption cost of data confidentiality from the research point of view.***

1. INTRODUCTION

The "Secure cloud information storage with a strong secret writing scheme" may be a web base application that alter us to store knowledge on cloud information and access securely by alternative users who needs the info. This cloud information storage allows us to share the resources to multiple remote users to any a part of the globe instantly. This application may be a very straightforward and user friendly applications which might be simply perceive and use by the users of it. this method largely focuses on the information confidentiality of user and accesses those data solely with the consent of owner. It provides extreme level of knowledge confidentiality by victimization an encryption theme that is thus sturdy that it'll work undoubtedly well within the dynamic atmosphere. Upon with secret writing this method can permit access to the owner's knowledge solely with the consent of the owner, he/she can give a secure key to the user who need the actual knowledge at the moment solely a user will transfer a file. thus probabilities of loosing knowledge or misuse area unit very less. If just in case any knowledge has been lost then there's make a copy system from that you'll retain your knowledge back. It additionally reduces the price and maintenance charges rather than keeping our own information which might be much more dearly-won. we are able to scale up or scale down the uses of cloud information per our would like. This application is nearly kind of like electric bill payment, were we are needed to pay per what we used. Value of victimisation cloud resources area unit thus clearly such as per the amount of usage in order that the tenant or shopper will estimate what quantity it'll cost to use for a few period of your time. Since the rating is thus clear the client of this method.

Relational database management systems (DBMSs) are an integral and indispensable component in most computing environments these days, and their importance is unlikely to diminish. With the appearance of hosted cloud computing and storage, the chance to offer a DBMS as an outsourced service is gaining momentum, as witnessed by Amazon's RDS and Microsoft's SQL Azure. Such a database-as-a-service (DBaaS) is engaging for 2 reasons. First, attributable to economies of scale, the hardware and energy prices incurred by users are likely to be much lower after they are paying for a share of a service instead of running everything themselves. Second, {the prices|the prices} incurred in an exceedingly well-designed DBaaS are proportional to actual usage ("pay-per-use")—this applies to each software system licensing and body costs. The latter area unit usually a major expense attributable to the specialised experience needed to extract sensible performance from goods DBMSs. By centripetal and automating several management tasks, a DBaaS will well cut back operational prices and perform well. From the point of view of the operator of a DBaaS, by taking advantage of the shortage of correlation between workloads of various applications, the service will be run exploitation so much fewer machines than if every employment was severally provisioned for its peak. This paper describes the challenges and necessities of an outsized scale, multi-node DBaaS, and presents the planning principles and implementation standing of relative Cloud, a DBaaS we are building at MIT. relative Cloud is acceptable for one organization with several individual databases deployed in an exceedingly "private" cloud, or as a service offered via "public" cloud infrastructure to multiple organizations. In each cases, our vision is that users should have access to any or all the options of a SQL relative DBMS, without concern concerning provisioning the hardware resources, configuring software system, achieving desired security, providing access management and information privacy, and standardization performance. of these functions are outsourced to the DBaaS.

2. RELATED WORK

Some analysis work has concentrated on evaluating the price of execution applications within the cloud. These applications are data-intensive and therefore the execution time of their process tasks is extremely short. Therefore, rather than analyzing the foremost appropriate variety of computing instances to execute their tasks, these approaches have an interest in exploring the price of storing their knowledge victimization the various facilities offered by cloud providers. in contrast to these works, the speed-up of an application within the field of knowledge retrieval is evaluated victimization differing types of computing cloud instances. even so, the experiment is unnatural to the utilization of solely ten computing instances within the most complicated experiment and doesn't think about price aspects. In any case, the most disadvantage of those experimentation-based techniques is that the worth to get hold of the execution of the experiments. The definition of models for estimating prices is another and fascinating approach. In general, these solutions need that customers know/estimate the necessities of their applications (such as execution times, input and output knowledge, or storage needs, for instance). Then, these operational parameters square measure mapped onto the fundamental costs provided by cloud providers so as to estimate execution prices. during this paper we have a tendency to have an interest on analysis approaches gazing minimizing the price of execution applications within the cloud. allow us to currently discuss the ways planned by these approaches and their main contributions. Some approaches calculate the most range of computing instances that would be provisioned supported the on the market budget and time and, then, change the amount of resources in step with however well they might be utilized by the appliance. These solutions ignore the nonuniformity of computing resources offered by the IaaS cloud suppliers as a result of all the computing instances provisioned before beginning the appliance execution need to be of a similar instance sort. in contrast to these proposals, think about the nonuniformity of the computing resources from totally different views. On the opposite hand, the authors focuses on price driven provisioning and scheduling activities. In [8] the goal is to reduce the price of execution workflows in IaaS cloud providers. At the start, a value driven schedule is computed for every work flow. This schedule determines the computing resources required to execute the work flow and therefore the mapping of tasks to resources, taking into consideration the data-flow and control-flow dependencies among tasks, in addition because the computing needs of every task. Then, throughout the work flow execution resources are reserved and free with the aim of minimizing the overall execution price in step with the computed schedule. rather than provisioning and programming resources earlier, divides the execution timeline in one or a lot of stages. In every stage, the previous provisioning selections are evaluated, adapting them to the future computing needs. These price driven evaluations attempt to minimize the price of provisioned resources having the ability to manage the uncertainty of consumer's future demand and provider's resource costs.

3. FRAME WORK

The projected design guarantees in associate accommodative manner the simplest level of knowledge confidentiality for any info employment, even once the set of SQL queries dynamically changes. The accommodative encoding theme, that was at first projected for applications not pertaining to the cloud, encrypts every plain column into multiple encrypted columns, and every price is encapsulated into totally different layers of encoding, so the outer layers guarantee higher confidentiality however support fewer computation capabilities with relation to the inner layers.

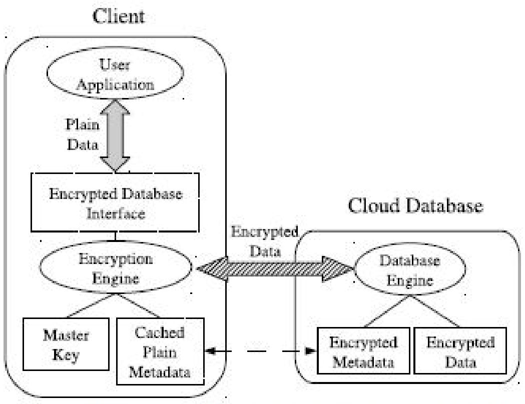


Fig. 1: Encrypted cloud database architecture

We propose the primary analytical price estimation model for evaluating cloud info prices in plain and encrypted instances from a tenant's purpose of read in an exceedingly medium-term amount. It takes conjointly into consideration the variability of cloud costs and also the chance that the info employment could modification throughout the analysis amount. This model is instanced with relation to many cloud supplier offers and connected real costs. evidently, accommodative encoding influences the prices associated with storage size and network usage of a info service. However, it's vital that a tenant will anticipate the ultimate prices in its amount of interest, and might opt for the simplest compromise between knowledge confidentiality and expenses.

A. New Adaptive Encryption Scheme

The proposed adaptive encryption schemes with a proxy free architecture use SQL-aware encryption algorithms that guarantee data confidentiality and allow the database server to execute SQL operations over encrypted data. As each algorithm supports of SQL operators, encryption schemes are referred as Random (Rand), Deterministic (Det), Order Preserving Encryption (Ope), Homomorphic Sum (Sum), Search (Search), Plain. In this model we define different types of encryption schemes by using that the data can be encrypted, here the encryption can be done on two formats of data that is file encryption and database encryption. In file encryption the file is encrypted while in data base encryption we can encrypt the columns of the data base. Here the cloud user first send the key request to the admin and admin send the master secret key to the cloud user, with the help of this key and selected encryption scheme from the model, plain data is encrypted after that it is uploaded on cloud in unreadable format. Whenever the cloud user wants to access the data that is a legitimate user can be able to decrypt the data by the master secret key. The encryption algorithms are organized into structures called onions; each plaintext value is encrypted through all the layers of its onions. Besides data confidentiality, the cost is addressed by an analytical cost model and a usage estimation methodology that allow a tenant to estimate the costs deriving from cloud database services. The cloud database service is characterized by plain, encrypted and adaptively encrypted databases over a medium-term horizon during which it is likely that both the database workload and the cloud prices change. Focus on database services and takes an opposite direction by evaluating the cloud service costs from a tenant's point of view.

B. Cost Estimation Process

We have to identify the factors which demand charge, and then we can shift onto estimating the cost for overall process. First step is to look for deployment cost. It means originally how much resource is allocated to the system for service. If additional resource is required in-between the service period, the charge for the same is included in overall cost.

Pricing Unit: occurrence usage is charged at per hour basis means duration and input/output traffic is usually charged at memory basis i.e. per GB usage and backup or storage is charged per memory requirement basis means per tera-byte. So various IaaS service providers opt different pricing models for charging. Hence due to complexity a general pricing model is decided and total duration of using software is calculated for network traffic.

Pricing for Storage: When a user uses the service, he doesn't know the software specification so a document containing the inter communication among them is necessary because at running time of that software it may require additional memory like 1GB or 1 TB. To meet this requirement additional memory is required over the local storage memory. If a user is using a particular service which demands additional memory at some particular time which is different from normal usage then that pricing band falls in various category. Because previously used standard instance storage, bandwidth allowance and charging rate are different. So there ought be a single pricing band for the whole total usage for the additional storage.

Boundary of Network: Various pricing models are deployed for different resource allocation in different places. Bandwidth calculation based on what traffic comes into services means what traffic is generated and distributed within service. So to calculate the bandwidth usage network boundary concept is created. We can calculate incoming and outgoing traffic with this mechanism.

Data transfer count: How much data is transferred between resources can be monitored by a resource connection point. So we can estimate the network bandwidth usage.

C. Cost Estimation of Cloud Database Services and Cost Model

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.

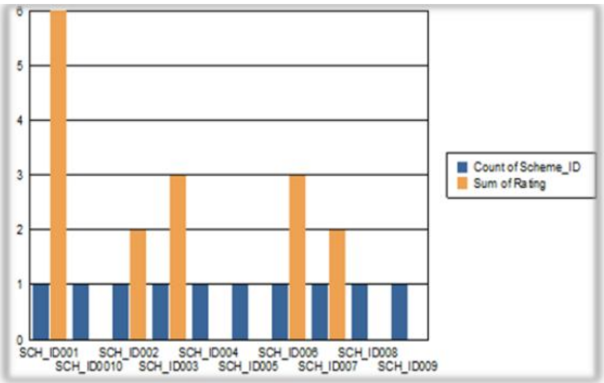
Cost model: The cost of a cloud database service can be estimated as a function of three main parameters: Cost = f (Time, Pricing, and Usage) where:

- **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 policies: the on-demand policy allows a tenant to pay-per-use and to withdraw its subscription anytime; the reservation policy requires the tenant to commit in advance for a reservation period. Hence, we distinguish between billing costs depending on resource usage and reservation costs denoting additional fees for commitment in exchange for lower pay-per-use prices. Billing costs are billed periodically to the tenant every billing period.

4. EXPERIMENTAL RESULTS

Below figure shows to verify whether or not the overheads of adaptive secret writing represent an appropriate compromise from the performance purpose of view for guaranteeing information confidentiality in cloud information services.



To this purpose, we have a tendency to design a set of performance tests that enable us to evaluate the impact of secret writing and adaptive secret writing on reaction time and output for various network latencies and for increasing numbers of coinciding clients. The TPC-C commonplace benchmark is employed because the work model for the information services. The experiments are disbursed in Emulab that provides us with a collection of machines in a very controlled atmosphere.

5. CONCLUSION

We Conclude that data security referred by introducing a secure cloud information design the uses the adaptative encrypt theme with none servers between them.This technique facilitate with the high level of security for any storage server/database work load that's in all probability to change in medium -term amount we tend to inquire the practicableness and performance of the planned style by a large set of undertake supported computer code model futher a lot of we tend to introduce a style and a technique that give the user to estimate the worth of the info in cloud storage.

REFERENCES

[1] 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.

[2] 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.

[3] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security andprivacy: an enterprise perspective on risks and compliance. O’ReillyMedia, Incorporated, 2009.

[4] H.-L. Truong and S. Dustdar, “Composable cost estimation andmonitoring for computational applications in cloud computingenvironments,” Procedia Computer Science, vol. 1, no. 1, pp. 2175 –2184, 2010, iCCS 2010.

[5] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, “Thecost 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.

[6] H. Hacig¨um¨us¸, B. Iyer, and S. Mehrotra, “Providing database as aservice,” in Proc. 18th IEEE Int’l Conf. Data Engineering, Feb. 2002.

[7] Google, "Google Cloud Platform Storage with server-side encryption,"http://googlecloudplatform.blogspot.it/2013/08/ google-distributed storage now-provides.html, Mar. 2014.

[8] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, "Executing sql over encoded information in the database-administration supplier model," in Proc. ACM SIGMOD Int'l Conf. Administration of information, June 2002.

[9] L. Ferretti, M. Colajanni, and M. Marchetti, "Dispersed, simultaneous, furthermore, free access to scrambled cloud databases," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, Feb. 2014.

[10] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: ensuring privacy with scrambled inquiry preparing," in Proc. 23rd ACM Symp. Working Systems Principles, Oct. 2011.