ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel framework for encryption of Public clouds Databses with flexibility to choose and tradeoff various options

J.Amreen Begum
MTech Student,
Department of CSE,
Sree Visvesvaraya Institute Of Technology & Science,
Mahabub Nagar, Telangana,India.

N.Venkatesh Naik,
Research scholar,
Department of CSE,
Jawaharlal Nehru Technological University- Anantapur, (JNTUA)
A.P.,India.

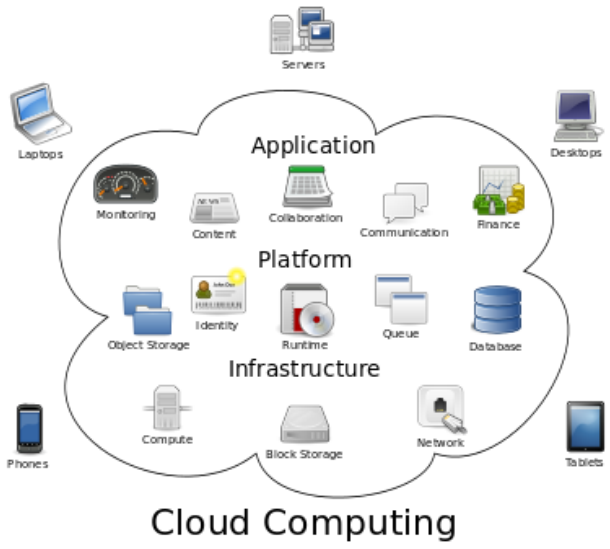
Dr K.Madhavi
Assistant Professor
Department of CSE,
Jawaharlal Nehru Technological University- Anantapur, (JNTUA)
A.P.,India.

Abstract: ***Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. A cloud database is a database that typically runs on a cloud computing platform. Some cloud platforms offer options for using a database as a service, without physically launching a virtual machine instance for the database. In this configuration, application owners do not have to install and maintain the database on their own. Instead, the database service provider takes responsibility for installing and maintaining the database, and application owners pay according to their usage. Data encryption is the optimum solution for achieving confidentiality. In some native method, encrypt the whole database through some standard encryption algorithm that do 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 architecture for adaptive encryption of public cloud database. 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.***

Keywords: ***Cloud database, confidentiality, Architecture, encryption, adaptively, cost model.***

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Adaptive Encryption Scheme

The proposed adaptive encryption schemes with a proxy free architecture. 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. 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.

Existing System:

The cloud computing paradigm is successfully converging as the fifth utility , but this positive trend is partially limited by concerns about information confidentiality and unclear costs over a medium-long term .We are interested in the Database as a Service paradigm (DBaaS) that poses several research challenges in terms of security and cost evaluation from a tenant's point of view. Most results concerning encryption for cloud-based services are in applicable to the database paradigm. Other encryption schemes, which allow the execution of SQL operations over encrypted data, either suffer from performance limits or they require the choice of which encryption scheme must be adopted for each database column and SQL operations .

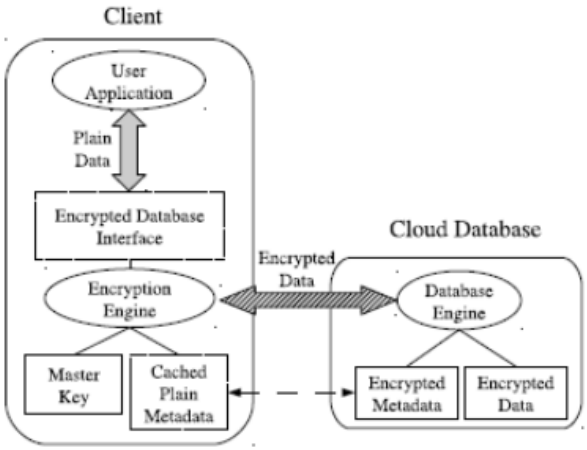
Proposed System:

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. we propose the first analytical cost estimation model for evaluating cloud database costs in plain and encrypted instances from a tenant's point

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

Architecture :



Implementation Modules:

1. **Adaptive encryption**
2. **Metadata structure**
3. **Encrypted database management**
4. **Cost Estimation of cloud database services**
5. **Cost model**
6. **Cloud pricing models**
7. **Usage Estimation**

Adaptive encryption:

The proposed adaptive encryption schemes with a proxy free architecture. 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. 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.
The proposed architecture manages five types of information.

• plain data is the tenant information;
• encrypted data is stored in the cloud database;
• plain metadata represent the additional information that is necessary to execute SQL operations on encrypted data;
• encrypted metadata is the encrypted version of the metadata that are stored in the cloud database;
• master key is the encryption key of the encrypted metadata that is distributed to legitimate clients.

Metadata structure:

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

associated to one or more *onion metadata*, as many as the number of onions related to the column.

Encrypted database management:

The database administrator generates a *master key*, and uses it to initialize the architecture metadata. The master key is then distributed to legitimate clients. Each table creation requires the insertion of a new row in the metadata table. For each table creation, the administrator adds a column by specifying the column *name*, *data type* and *confidentiality parameters*. These last are the most important for this paper because they include the *set of onions* to be associated with the column, the *starting layer* (denoting the actual layer at creation time) and the *field confidentiality* of each onion. If the administrator does not specify the confidentiality parameters of a column, then they are automatically chosen by the client with respect to a tenant's policy. Typically, the default policy assumes that the starting layer of each onion is set to its strongest encryption algorithm.

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

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.*

Cloud pricing models:

Popular cloud database providers adopt two different billing functions, that we call *linear* L and *tiered* T . Let us consider a generic resource x, we define as xb its usage at the *b-th* billing period and px b its price. If the billing function is tiered, the cloud provider uses different prices for different ranges of resource usage. Let us define Z as the number of tiers, and [ˆx1, . . . , ˆxZ−1] as the set of thresholds that define all the tiers. The uptime and the storage billing functions of *Amazon RDS* are linear, while the network usage is a tiered billing function. On the other hand, the uptime billing functions of *Azure SQL* is linear, while the storage and network billing functions are tiered.

Usage Estimation:

The uptime is easily measurable, it is more difficult to estimate accurately the usage of storage and network , since they depend on the database structure, the workload and the use of encryption. We have implemented a methodology for the estimation of storage and network usage due to encryption.

Conclusion:

We implemented an architecture that supports adaptive data confidentiality in cloud database environments without requiring any intermediate trusted proxy. Adaptive encryption mechanisms have two main benefits: they guarantee at runtime the maximum level of data confidentiality for any SQL workload, and they

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

simplify database configuration at design time. However, they are affected by high computational costs with respect to non adaptive encryption schemes. This paper demonstrated that applying adaptive encryption methods to cloud database services is a suitable solution, because network latency masks the overhead caused by adaptive encryption for most SQL operations.

References:

[1] Ferretti, L, Enzo Ferrari, Pierazzi, F, Colajanni, M. , Marchetti, M, Performance and Cost Evaluation of an Adaptive Encryption Architecture for Cloud Databases, The IEEE Transactions on Cloud Computing (Volume:2 , Issue: 2)

[2] N.Jyothirmai & B.Manjusha, Cloud Computing, http://www.yuvaengineers.com/cloud-computing-n-jyothirmai-b-manjusha/

[3] H. Hacigum ¨ us¸, B. Iyer, and S. Mehrotra, "Providing database as a ¨ service," in Proc. of the 18th IEEE International Conference on Data Engineering, February 2002, pp. 29–38.

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

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

[6] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, "The cost of doing science on the cloud: The montage example," in Proc. ACM/IEEE Conf. Supercomputing, 2008, pp. 1–12.

[7] H. Hacigum € u €s, B. Iyer, and S. Mehrotra, "Providing database ¸ as a service," in Proc. 18th IEEE Int. Conf. Data Eng., Feb. 2002, pp. 29–38.

[8] H. Hacigum € u €s, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over ¸ encrypted data in the database-serviceprovider model," in Proc. ACM SIGMOD Int'l Conf. Manage. Data, Jun. 2002, pp. 216–227.

[9] L. Ferretti, M. Colajanni, and M. Marchetti, "Supporting security and consistency for cloud database," in Proc. of the 4th International Symposium on Cyberspace Safety and Security. Springer, December 2012, pp. 179–193.

[10] O. Goldreich, Foundations of Cryptography: Volume 2, Basic Applications. Cambridge university press, 2004.

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

Authors:

J.Amreen Begum

N.Venkatesh Naik