Estimating the Cost and Performance of a Novel Adaptive Encryption Architecture for Cloud Databases

Naresh Bhattacharjee DC[1], V.Mallesi[2]
M Tech Student[1], Associate Professor[2]
Dept. of CSE, Bheema Institute of Technology & Science, Adoni, AP, India[1&2]

ABSTRACT
The cloud databaseadoption requiresthe solution of information confidentiality difficulties and it cansupport numerous web-based applicationsare defenseless to mugging of penetrating information because the opponents can adventure software bugs to expansion contact to isolated information and postures some security responsibilities.Most of the times the malicious bureaucratscan capture and disclosureinformation. We create a software prototype, through that will estimate the cost and feasibility and performance of the adaptive cloud database.Additionally, we recommend the evaluation of cloud database services in plain and encrypted instances using the original cost model. During the intermediate time period this will take the tenant workloads, variability and cloud prices. We proposenoveladaptive encryptionarchitecture to the cloud databases that concerns astimulatingsubordinate to the balance between the required data confidentiality level and the flexibility of the cloud database arrangements at design time.

KEYWORDS:*Confidentiality, Encryption, Adaptivity, Cloud Databases, Performance, Cost Model*

1. INTRODUCTION

The cloud computing decoration is magnificentlycongregating as the fifth utility, but this optimisticinclination is somewhatrestricted by distresses about information confidentiality and undecided costs over a medium-long term. Further encryption systems that consent the execution of SQL operations over encrypted data either have performance boundaries or require the special of which encryption framework must be adopted for each database column and SQL operation. Most results regarding encryption for cloud-based services are inappropriate to the database paradigm. These concluding proposals are acceptable when the set of queries can be statically unwavering at enterprise time, but we are attentive in other common developments where the capacitycould change after the database design. In this paper, we propose a novel architecture for adaptive encryption of public cloud databases that suggestions a proxy-free different to the system defined. We are concerned in the database as a service paradigm (DBaaS) those carriages numerous research contests in rapports of security and cost evaluation from a tenant's point of interpretation. The proposed architecture sureties in an adaptive technique the greatest level of data discretion for some database capacity, uniform when the set of SQL queries vigorouslydeviations.

We primarilyplan the first proxy-free architecture for adaptive encryption of cloud databases that does not frontier the convenience, springiness and scalability of a natural cloud database because multiple clients can issue concurrent operations without passing through some centralized factor as in alternative architectures. Then, we evaluate the performance of encrypted database services by arrogant the standard TPC-C goal as the workload and by seeingunlike network expectancies. These concluding proposals are acceptable when the set of queries can be statically unwavering at enterprise time, but we are attentive in other common developments where the capacity could change after the database design. Thanks to this test bed, we show that most performance outgoings of adaptively encrypted cloud databases are concealed by network latencies that are typical of a geographically distributed cloud consequence.

Lastly, we recommend the first critical cost valuation model for evaluating cloud database costs in plaintext and encrypted arrangements from a tenant's theme of understanding over a medium-term period. This standard also considers the variability of cloud prices and of the database workload through the

ISSN: 2278 – 7798

evaluation period, and consents a tenant to perceive how adaptive encryption affects the costs related to storage and network procedure of a database service.Instinctive solutions encrypt the complete database complete some regular encryption algorithms that do not countenance executing any SQL operation unswervingly on the cloud. By applying the model to numerous cloud provider suggestions and associated prices, the tenant can select the best concession between the data confidentiality level and subsequent costs in his period of awareness.

Cultivating the confidentiality of information stockpiled in cloud databases epitomizes an important impact to the adoption of the cloud as the fifth utility because it addresses most user disquiets. Though data encryption looks the most intuitive solution for confidentiality, its presentation to cloud database facilities is not inconsequential, because the cloud database essential be intelligent to execute SQL operations directly over encrypted data without retrieving any decryption key. As significance, the tenant has two substitutions: move the entire database, decrypt it, execute the query and, if the processadjusts the database, encrypt and upload the new data; decrypt momentarily the cloud database, implement the query, and re-encrypt it.Our proposal is categorized by two main assistances to the state of the art: architecture and cost model.

2. RELATED WORK

Cultivating the privacy of information stockpiled in the cloud databases signifies an essentialinvolvement to the approval of the cloud as the fifth conveniencesince it statementsutmost user disquiets our suggestion is categorized by two main influences.to the formal of the art design and cost model While the data encryption appears most instinctual solution for confidentiality it presentation to cloud database amenities is not insignificantfor cloud database basic be clever to execute SQL operations. Unswervingly over the encrypted data withoutexpurgation any decryption key. Naive solutions encrypt the whole database concludedabout standard encryption algorithms. That do not countenance any SQL operations unswervingly on the cloud as a ensuing the tenant has two substitutes download the perfect database and decrypt it execute the query if the operation adjusts the database encrypt smd upload the new data decrypt momentarily the cloud database execute the query and re-encrypt it. The earlier solution is exaggerated by colossal communication and computational over heads, and resultant cost that kinds cloud databases amenities quiet in-convenient that later solution that not promise data confidentiality because the cloud benefactorattains decryption keys. The right marginal is to execute SQL operations directly on cloud database, without openhanded decryption keys to the provider, an initial solution is provided are existing in data aggregation techniques that associates plain text meta data to sets of the encrypted data however plain text metadata may leak sensitive information and data accumulationdisseminates un-necessary network over heads. The system of wholly holomorphic encryption would guarantee the execution of any operation over encrypted information. But remainingexecutions are unnatural by the massive computational costs; to the extent the execution of SQL operations concluded cloud database would convert im-practical. Further encryption algorithms categorized by adequate computational intricacyfunding the separation of SQL operators.

3. PROPOSED SYSTEM

The proposed architecture guarantees in an adaptive technique the greatestsmooth of data confidentiality for any database capacity, straight when the set of SQL queries dynamically deviations. The adaptive encryption arrangement, which was primarily proposed for presentations not rising to the cloud, encrypts individually plain column to compound encrypted columns, and each value is compressed in changed layers of encryption, so that the outer stratumssecuritycomplex confidentiality neverthelessmaintenancescarcerreckoningproficiencies with respect to the inside layers.

The outer layers are energetically adapted at runtime afterdifferent SQL operations are further to the workload. While this adaptive encryption architecture is strikingfor it does not require describing at design time which database operations are endorsed on each column, it carriages novel concerns in terms of applicability to a cloud framework, and difficulties about loading and network costs. We scrutinizeseparately of these problems and we reach three inventive conclusions in terms of prototype enactment, performance appraisal, and cost evaluation.

ISSN: 2278 – 7798

We primarilyscheme the first proxy-free architecture for adaptive encryption of cloud databases that does not perimeter the disposal, elasticity and scalability of aunadorned cloud database as multiple clients can questionconcomitant operations without momentaryconcludedroughlyintegrated component as in different architectures. Before, we estimate the performance of encrypted database conveniences by arrogant the average TPC-C target as the workload and by bearing in mindunalike network expectancies. Thanks to this test couch, we confirmation that utmost performance outgoings of adaptively encrypted cloud databases are curtained by network hiddenness that are exemplary of a geographically scattered cloud scenario.

Finally, we propose the first systematic cost estimation model for weighing cloud database costs in plaintext and encrypted formations from a tenant's theme of observation over a medium-term period. This model also contemplates the unevenness of cloud amounts and of the database workload through the evaluation period, and allows a tenant to witnessin what technique adaptive encryption stimuluses the costs interrelated to packing and network convention of a database service. By applying the archetypal to some cloud adherentcompromises and interrelated prices, the tenant can choose the superlativemollificationamongst the data preference level and subsequent costs in his archaic of awareness.

The database administrator engenders a *master key* and expenditures it to prepare the architecture metadata. The master key is then dotted to legitimate clients. Each table manufactureinvolves the insertion of a different row in the metadata table. For each table establishing, the administrator adds a column by postulating the column *name*, *data type* and *confidentiality parameters*.

These former are the utmost important for this paper as they embrace the *traditional of onions* to be concomitant with the column, the *starting layer* (symbolizing the actual layer at creation time) and the *field confidentiality* of independently onion. If the administrator organizes not require the decision parameters of a stake, then they are inevitably chosen by the client with respect to a tenant's program. Normally, the nonattendancestrategy assumes that the starting layer of each onion is set to its strongest encryption algorithm.

Advantages:

1. Increases the confidentiality in cloud databases.
2. Here we estimate the cloud cost.

4. SYSTEM ARCHITECTURE

Client

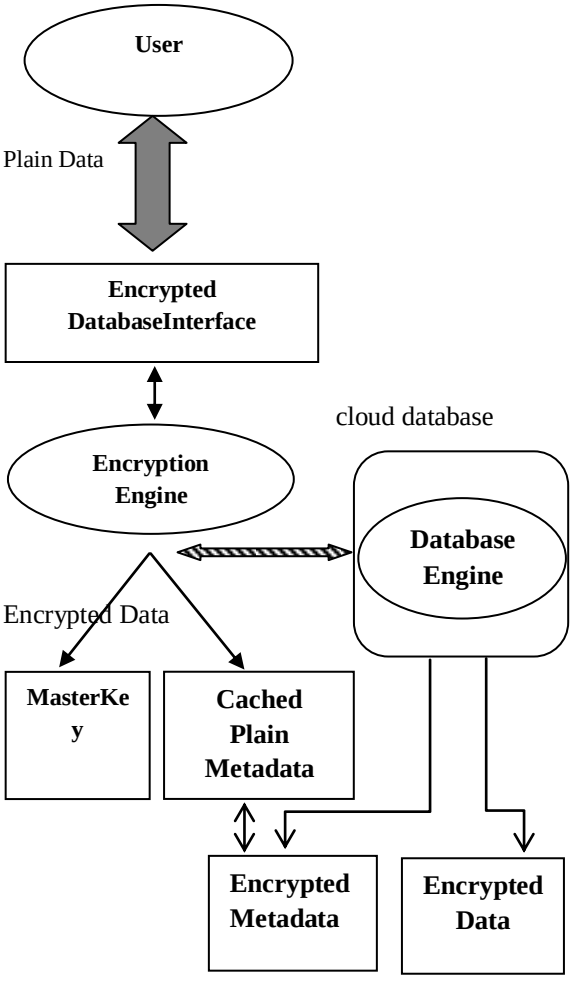

Figure 1: Encrypted Cloud Database Architecture

5. SYSTEM MODULES

i) System Model

The suggested system maintenances adaptive encryption for public cloud database services, wherever distributed and concomitant clients dismissconcernundeviating SQL operations. By

ISSN: 2278 – 7798

escaping an architecture centered on transitional servers among the clients and the cloud database, the suggestedclarificationwarranties the unchangedsmooth of scalability and accessibility of the cloud service. A configuration of the proposed designeverywhereseparately client executes an encryption engine that succeeds encryption operations. This software component is edited by external user presentationsfrom side to side the encrypted database edge. The proposed architecture accomplishes five types of information:

1. Plain data signify the tenant information
2. Encrypted data are the encrypted version of the plain data, and are stockpiled in the cloud database;
3. Plain metadata epitomize the superfluous information that is indispensable to execute SQL operations on encrypted data
4. Encrypted metadata are the encrypted version of the plain metadata, and are stockpiled in the cloud database;
5. Master key is the encryption key of the encrypted metadata, and is well-known by appropriate clients.

ii) Adaptive Encryption Scheme

We envisage SQL-aware encryption algorithms that collateral data cover-up and allow the cloud database contraption to execute SQL operations dismissed encrypted data. As separately algorithm patronages a precisesector of SQL operators, we represent to the succeeding encryption outlines.

1. Random (Rand): it is the extreme secure encryption for it does not expose any information nearby the original plain value (IND-CPA) [20], [21]. It does not sponsorship any SQL operator, and it is recycleddifferent for data renovation.
2. Deterministic (Det): it deterministically encrypts data, so that impartiality of plaintext data is unspoiled. It backings the egalitarianism operator.
3. Directive Preserving Encryption (Ope) [12]: it refuges in the encrypted principles the statisticaldemand of the creative unencrypted data. It supports the evaluation SQL operators (i.e., =; <;<_; >;>_).
4. Homomorphic Sum (Sum) [13]: it is Homomorphic with veneration to the sum operation, so that the multiplication of encrypted integers is equal to the sum of plaintext integers. It provisions the sum operator between integer values.
5. Search: it provisionsequivalencepatterned on bursting strings (i.e., the LIKE operator).
6. Plain: it ensures not encrypt data, but it is convenient to maintenance all SQL operators on non-confidential data.

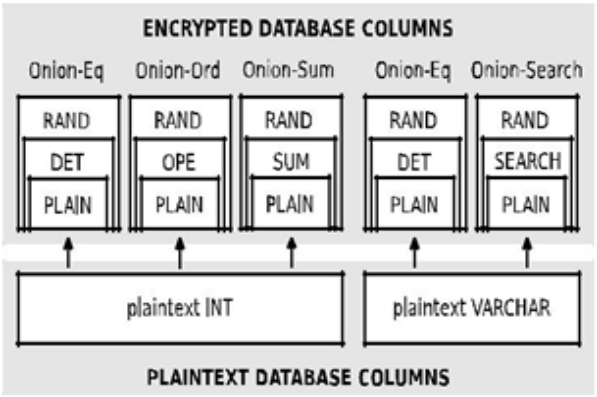

Fig 2: Example of onion structure

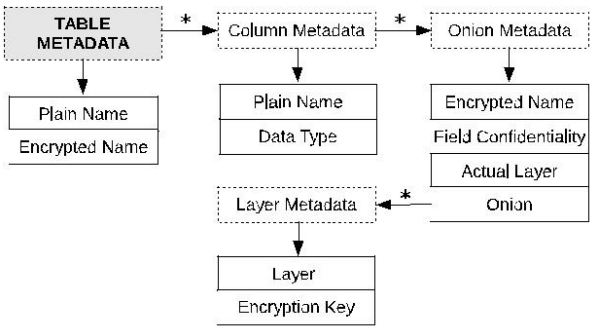

Fig 3: Meta Data structure

iii) Cost estimation of cloud database services

We consider a tenant that is interested in estimating the cost of porting his database to a cloud platform. This porting is a strategic decision that must evaluate confidentiality issues and related costs over a medium-long term. For these reasons, we propose a model that includes the overhead of encryption schemes

ISSN: 2278 – 7798

and the variability of database workload and cloud prices. The proposed model is general enough to be realistic to the supremeprevalent cloud database amenities, such as Amazon Relational Database Service, Enterprise DB, Windows Azure SQL Database, and Rack space Cloud Database.

iv) Performance Evolution

These piecegoals to corroborate whether the outgoings of adaptive encryption denote an adequateconcessionamongstconcert and statistics confidentiality for the tenants of cloud database amenities. To this fortitude, we design a cluster of performance assessments that tolerate us to approximation the dimple of encryption and adaptive encryption on comebackstretches and capacity for unlike network expectancies and for increasing numbers of synchronized clients.

6. CONCLUSION

Here are two main tenant anxieties that mightcheck the adoption of the cloud as the fifth efficacy: data confidentiality and costs. This paper reports both issues in the case of cloud database services. These applications have not yet establishedsatisfactoryresponsiveness by the theoreticalfiction, but they are of ultimatereputation if we contemplate that practically all important amenities are based on one or multiple databases. We address the facts confidentiality anxieties by proposing a novel cloud database architecture that uses adaptive encryption methods with no intermediate servers. This systemaffords tenants with the best level of secrecy for any database load that is expected to modification in a medium-term period. We consider the feasibility and performance of the proposed architecture over a large set of experimentations based on a software prototype matter to the TPC-C standard benchmark. Our results demonstrate that the webinvisibilities that are classic of cloud database atmospherespelt most overheads related to static and adaptive encryption.

REFERENCES

[1] 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.

[2] H. Hacig€um€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.

[3] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. 17th ACM Conf. Comput. Common. Security, 2010, pp. 735–737.

[5] Google. (2014, Mar.). Google Cloud Platform Storage with server side encryption [Online]. Available:http://googlecloudplatform.blogspot.it/2013/08/google-cloud-storage-now provides.html.

[6] L. Ferretti, M. Colajanni, and M. Marchetti, "Distributed, concurrent, and independent access to encrypted cloud databases," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 437–446, Feb. 2014. TABLE 6 Costs of the Cloud Database Service during the Three Years Period in STATIC and DYNAMIC Scenarios 154 IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 2, APRIL-JUNE 2014

[7] 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, pp. 85–100.

[8] 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 Comput. Syst., vol. 25, no. 6, pp. 599–616, 2009.

[9] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. Sebastopol, CA, USA: O'Reilly Media, Inc., 2009.

[10] 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.

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

.

ISSN: 2278 – 7798

AUTHOR

Naresh Bhattacharjee DCB.Tech degree in Computer Science & Engineering in the year 2013 from JNTU Anantapur. Currently his pursuing M.Tech in Computer Science & Engineering from JNTU Anantapur. His Research and area of interest is Cloud Computing.

V.Mallesireceived M Tech degree. He guided many academic projects .He is having 8 years of teaching experience. His research interests are in the field Cloud computing and data base.

ISSN: 2278 – 7798