International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 12, December 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

AN EFFICEINT IMPLEMENTATION OF PUBLIC CLOUD DATABASES THROUGH ADAPTIVE ENCRYPTION SCHEME

Sowmya Gadam[1], D.Satya Prasad[2]

[1]M.Tech Student, [2]Asst.Professor Dept of CSE,

V.S.Lakshmi Engg College For Womens, Matlapalem, Kakinada, (India)

ABSTRACT

The cloud database as a service is novel paradigms that can be support several Internet-based Applications, its adoption requires the solution of the information confidentiality problems. We proposed a novel architecture for adaptive encryption of public cloud databases that offers an interesting alternative to the tradeoff between the required data confidentiality level and the flexibility of the cloud database structures at time. We demonstrate the feasibility and performance of the proposed solution through a software prototype. We propose an original cost model that is oriented to the evaluation of cloud database services in plain text and encrypted instances and that takes into account the variability of cloud prices and tenant workloads during a medium-term period. This paper proposes a novel model for adaptive encryption of public cloud databases that offers a proxy-free alternative to the system. The project demonstrates the feasibility and performance of the proposed solution through a software prototype. The proposed model manages five types of information: plain data represent the tenant information; encrypted data are the encrypted version of the plain data, and are stored in the cloud database; plain metadata represent the additional information that is necessary to execute SQL operations on encrypted data; encrypted metadata are the encrypted version of the plain metadata, and are stored in the cloud database; master key is the encryption key of the encrypted metadata, and is known by legitimate clients.

Keywords- adaptively, cloud database, cost model, confidentiality, and encryption.

I. 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 tenant's point of view. Most results concerning encryption for cloud-based services [6], [7] are inapplicable to the database paradigm. Other encryption schemes that allow the execution of SQL operations over encrypted data either have performance limits [8] or require the choice of which encryption scheme must be adopted for each database column and SQL operation [9]. These latter proposals are fine when the set of queries can be statically determined at design time, while we are interested in 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 described 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 proposed system supports adaptive encryption methods for public cloud database service, where distributed and concurrent clients can issue direct SQL operations. By avoiding an architecture based on one [10] or multiple intermediate servers between the clients and the cloud database, the proposed solution guarantees the same level of scalability and availability of the cloud service. The use of fully homomorphism encryption [11] would guarantee the execution of any operation over encrypted data, but existing implementations are affected by huge computational costs to the extent that the execution of SQL operations over a cloud database would become impractical. Other encryption algorithms characterized by acceptable computational complexity support

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

a subset of SQL opera- tors [12], [13], [14]. For example, an encryption algorithm may support the order comparison command [12], but not a search operator [14]. The drawback related to these feasible encryption algorithms is that in a medium-long term horizon, the database administrator cannot know at design time which database operations will be required over each database column. This issue is in part addressed in [10] by proposing an adaptive encryption architecture that is founded on an intermediate and trusted proxy.
The use of fully homomorphism encryption would guarantee the execution of any operation over encrypted data, but existing implementations are affected by huge computational costs to the extent that the execution of SQL operations over a cloud database would become impractical. Other encryption algorithms characterized by acceptable computational complexity support a subset of SQL operators. For example, an encryption algorithm may support the order comparison command, but not a search operator. The drawback related to these feasible encryption algorithms is that in a medium-long term horizon, the database administrator cannot know at design time which database operations will be required over each database column. This issue is in part addressed by proposing an adaptive encryption architecture that is founded on an intermediate and trusted proxy. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, where in end-users consume power without needing to understand the component devices or infrastructure required to provide the service. Cloud computing is different from hosting services and assets at ISP data center. It is all about computing systems are logically at one place or virtual resources forming a Cloud and user community accessing with intranet or Internet. So, it means Cloud could reside in-premises or off premises at service provider location. There are types of Cloud computing like 1. Public clouds 2. Private Clouds 3. Inter-clouds or Hybrid Clouds, say CIO and IT Leaders and expert in cloud computing. Cloud computing has been changing how most people use the web and how they store their files. It's the structure that runs sites like Face book, Amazon and Twitter and the core that allows us to take advantage of services like Google Docs and Gmail. But how does it work. Before we dig further into how does cloud computing work, first let's understand what the term "cloud" refers to. The concept of the cloud has been around for a long time in many different incarnations in the business world. It mostly means a grid of computers serving as service oriented architecture to deliver software and data. Most websites and server-based applications run on particular computers or servers. What differentiates the cloud from the way those are set up is that the cloud utilizes the resources from the computers as a collective virtual computer, where the applications can run independently from particular computer or server configurations. They are basically floating around in a "cloud of resources", making the hardware less important to how the applications work. With broadband internet, the need to have the software run on your computer or on a company's site is becoming less and less essential a lot of the software that people use nowadays is completely web-based. The cloud takes advantage of that to bring it to the next level.

II. RELATED WORK

Improving the confidentiality of information stored in cloud databases represents an important contribution to the adoption of the cloud as the fifth utility because it addresses most user concerns. Our proposal is characterized by two main contributions to the state of the art: architecture and cost model. Although data encryption seems the most intuitive solution for confidentiality, its application to cloud database services is not trivial, because the cloud database must be able to execute SQL operations directly over encrypted data without accessing any decryption key. Native solutions encrypt the whole database through some standard encryption algorithms that do not allow to execute any SQL operation directly on the cloud. As a consequence, the tenant has two alternatives: download the entire database, decrypt it, execute the query and, if the operation modifies the data- base, encrypt and upload the new data; decrypt temporarily the cloud database, execute the query, and re-encrypt it. The former solution is affected by huge communication and computation overheads, and consequent costs that would make cloud database services quite inconvenient; the latter solution does not

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

guarantee data confidentiality because the cloud provider obtains decryption keys. The right alternative is to execute SQL operations directly on the cloud database, without giving decryption keys to the provider. An initial solution presented in [5] is based on data aggregation techniques [8],that associate plaintext metadata to sets of encrypted data. However, plaintext metadata may leak sensitive information and data aggregation introduces unnecessary network overheads.

III. 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 to multiple encrypted columns, and each value is encapsulated in 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 adapted at runtime when new SQL operations are added to the workload. Although this adaptive encryption architecture is attractive because it does not require to define at design time which database operations are allowed on each column, it poses novel issues in terms of applicability to a cloud context, and doubts about storage and network costs. We investigate each of these issues and we reach three original conclusions in terms of prototype implementation, performance evaluation, and cost evaluation. We initially design the first proxy free architecture for adaptive encryption of cloud databases that does not limit the availability, elasticity and scalability of a plain cloud database because multiple clients can issue concurrent operations without passing through some centralized component as in alternative architectures. Then, we evaluate the performance of encrypted database services by assuming the standard TPC-C benchmark as the workload and by considering different network latencies. Thanks to this test bed, we show that most performance overheads of adaptively encrypted cloud databases are masked by network latencies that are typical of a geographically distributed cloud scenario. we propose the first analytical cost estimation model for evaluating cloud database costs in plaintext and encrypted configurations from a tenant's point of view over a medium-term period. This model also considers the variability of cloud prices and of the database workload during the evaluation period, and allows a tenant to observe how adaptive encryption influences the costs related to storage and network usage of a database service. By applying the model to several cloud provider offers and related prices, the tenant can choose the best compromise between the data confidentiality level and consequent costs in his period of interest. There are two main tenant concerns that may prevent the adoption of the cloud as the fifth utility: data confidentiality and costs. In this we address both issues in the case of cloud database services. These applications have not yet received adequate attention by the academic literature, but they are of utmost importance if we consider that almost all important services are based on one or multiple databases. We address the data confidentiality concerns by proposing a novel cloud database architecture that uses adaptive encryption techniques with no intermediate servers. This scheme provides tenants with the best level of confidentiality for any database workload that is likely to change in a medium-term period. We investigate the feasibility and performance of the proposed architecture through a large set of experiments based on a software prototype subject to the TPCC standard benchmark. Our results will demonstrate that the network latencies that are typical of cloud database environments hide most overheads related to static and adaptive encryption. Moreover, we propose a model and a methodology that allow a tenant to estimate the costs of plain and encrypted cloud database services even in the case of workload and cloud price variations in a mid-term horizon. By instantiating the model with actual cloud provider prices, we can determine the encryption and adaptive encryption cost of data confidentiality. From the research point of view, it would be also interesting to evaluate the proposed or alternative architectures under different threat model hypotheses. The proposed architecture guarantees data confidentiality in a security model in which: the network is untrusted; tenant users are trusted, that is, they do not reveal information about plain data, plain metadata, and the master key; the cloud provider administrators are defined semi honest, that is, they do not modify tenant's data and results of SQL operations, but they could be interested in accessing tenant's information stored in the cloud database.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

IV. IMPLEMENTAION OF ENCRYPTED DATABASE MANGMENT

4.1 Database Creation

In set up phase database administrator generate master key used to initialize architecture metadata. Distributed to Client. 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 assumes starting layer of each onion is set to its strongest 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 results are decrypted using information contained in metadata.

4.3 Adaptive Layer Removal

Remove external layer of onion e q .table T with column id of type into and name of type string. following structure issued by client to encrypted cloud database SELECT *FROM T WHEN 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. Cloud database does not 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.

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) Emu lab provide set of machine in (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 postage 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 its 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. CONCLUSION

We address the data privacy concerns by proposing a novel cloud database model that uses adaptive encryption techniques with no intermediate servers. This scheme provides tenants with the best level of privacy for any database workload that is to change in a medium-term period. We investigate the feasibility and performance of the proposed architecture through a large set of experiments based on a software prototype subject. Our results analysis proved that the cloud networks semantic that are typical of cloud database environments hide most

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

overheads related to static and adaptive encryption. We address the data confidentiality concerns by proposing a novel cloud database architecture that uses adaptive encryption techniques with no intermediate servers. This scheme provides tenants with the best level of confidentiality for any database workload that is likely to change in a medium-term period. We investigate the feasibility and performance of the proposed architecture through a large set of experiments based on a software prototype subject to the TPC-C standard benchmark. Our results demonstrate that the network latencies that are typical of cloud database environments hide most overheads related to static and adaptive encryption. Moreover, we propose a model and a methodology that allow a tenant to estimate the costs of plain and encrypted cloud database services even in the case of workload and cloud price variations in a medium term horizon. By applying the model to actual cloud provider prices, we can deter- mine the encryption and adaptive encryption costs for data confidentiality. Future research could evaluate the proposed or alternative architectures for multi-user key distribution schemes and under different threat model hypotheses.

REFERENCES

[1] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti, "Performance and cost evaluation of an adaptiveencryption architecture for cloud databases", IEEE 2013.

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

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

[8] Google, "Google Cloud Platform Storage with serversideencryption," http://googlecloudplatform.blogspot.it/2013/08/google-cloudstorage-now-provides.html, Mar. 2014.

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

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

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

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

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

AUTHORS PROFILE:

	SOWMYA GADAM is a student of V.S.LAKSHMI ENGINEERING COLLEGE FOR WOMENS. Presently he is pursuing M.Tech [Computer Science and Engineering] from this college and he also completed his B.Tech .
	Mr.D.Satya Prasad, working as a Asst. Professor in the Dept.of Computer Science and Engineering from V.S.Lakshmi Engineering College, Matlapalem, Kakinada.