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

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 589-593

Enhanced Independent Access to Encrypted Cloud Databases

[1] **Jollu Jayachandrudu,** [2] **M.Sri lakshmi,** [3]**Dr.S.Prem Kumar**
[1]*(M.Tech), CSE*
[2]*Assistant Professor, Department of Computer Science and Engineering*
[3]*Professor & HOD, Department of computer science and engineering,*
G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract:- Now a days huge amount of data in a cloud will be placed any where in in light of the discriminating way of the applications and it is imperative to keep up secure clouds and the significant security challenge with clouds is that the information's proprietor might not have control of where the information is set on the grounds that if one needs to abuse the advantages of utilizing cloud computing then this necessity forces clear information administration decisions, for example, the first plain information that must be available just by trusted gatherings that do exclude cloud suppliers or middle people and Internet.In instance of any un-trusted connection then the information must be encrypted by which we fulfills these objectives that has distinctive levels of intricacy relying upon the sort of cloud services.In this paper we propose Enhanced Independent Access to Encrypted Cloud Databases such as a Secure DBaaS as the first solution that allows cloud tenants to take full advantage of DBaaS qualities such as availability then reliability and elastic scalability without exposing unencrypted data to the cloud provider and the architecture design was motivated by the goal to allow multiple or independent and geographically distributed clients to execute concurrent operations on the encrypted data including SQL statements that modify the database structure.

Keywords: Cloud, security, confidentiality, SecureDBaaS, database.

———————————— ◆ ————————————

1 INTRODUCTION

In the present era of computers our main aim of writing this paper for implementing the system is to integrate the cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data so we use cloud for uploading owner's data where a data owner is the one who has uploaded his data on cloud and he or she is not ensured about his or her data so we have to store the data on the cloud by encrypting it. Generally this encryption of data takes place at client side and metadata of that data also created that is secureDBaaS concept where the encrypted data is stored at the cloud along with its encrypted metadata and then the authorized clients can access the data by using only metadata.We consider this to be the first solution that supports geographically distributed clients to connect directly to an encrypted cloud database and to execute concurrent and independent operations including those modifying the database structure.Our proposed system includes the advantage of eliminating intermediate proxies that limit the elasticity; availability and scalability properties that are intrinsic in the cloud-based solutions where a secureDBaaS provides several original features that differentiate it from previous work in the field of security for remote database services.

2. LITERATURE SURVEY

A.Advancement of cloud storage

Rapid growth in information and the need to preserve it safety of data will require organizations to integrate how they manage and use their data, from design to end of existence. Now all data can be stored in the internet storage space that is cyberspace. These storages space are delivered and retained by the third party through the Internet [2]. Cloud storage deals with large storage which is available for use, with three major attributes: accessing datathrough Web services APIs on a non-persistent network connection, highly availablehuge quantity of storage space, and pay as per use model. It supports rapid scalability [2]. The evolution of Cloud Storage based on traditional network storage and hosted storage. One of the advantages of cloud storage is the access of your data anytime from anywhere.

Cloud storage providers bring storage varying from small amount of data to entire warehouse of an organization. User has to pay to cloud storage provider for utilization of cloud storage. The payment for usage is according for what resources they are using and how much data they are transmitting to the cloud storage. In the cloud storage environment the user data will be copied into on cloud data center of the cloud. This data remain in data servers that made available on the cloud. This synchronization between data center will be result in high availability of the data server on cloud. Cloud storage is an offering of cloud computing.

B. Security in cloud storage

A security issue over cloud storage is definitely one of the major concerns that many organization are trying to identify. In cloud storage data is placed at third party. A sensitive data in fully controlled by cloud serviceprovider. A cloud provider ensures a security such as allowing only authorized user can access the information in cloud. An organization has a sensitive data and cloud provider is curies. an organization's data might be in danger. Similarly, privacy in the cloud is another major issue.Organizations and users have to trust their cloud service provider. That they are providing confidentiality of data from unauthorized users. Data placed by organizationin cloud is every so often stored in plain text. A recent report by the Cloud Security Alliance lists data leakage and dada lose as security concerns in the cloud storage.Organization can be thought responsible for the loss of critical data and may face heavy fines over data breaches. To lose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin. Sensitive data stored within cloud environments must be safeguarded to protect its owners.

There are many existing technology such Cryptographic file systems and secure storage that will assurance security of the data in cloud. This integrates data which will be stored on untrusted cloud. DBMS engines offers encryption of data using Transparent Data Encryption (TDE) [3]. This TDE make possible to build a trusted DBMS over untrusted cloud storage using this technique. But, in the DBaaS context the DBMS engine is not trusted because it is controlled by the cloud provider; hence the TDE approach is not suitable for the cloud database services. This approach preserves data confidentiality in scenarios where the DBMS is not trusted. However it requires a modified DBMS engine that is not compatible with commercial and open source DBMS software adopted by cloud providers. On the other hand, the we proposed architecture is compatible with standard DBMS engines, and allows customers to make a secure cloud database by leveraging cloud DBaaS readily available. The proposal in [3] uses encryption to control accesses to encrypted data stored in a cloud database. This solution is not applicable to usage contexts in which the structure of the database changes, and does not support concurrent accesses from multiple clients possibly distributed on a geographical scale

3. TYPES OF ARCHITECTURES

3.1. Proxy server based architecture (PSB)

The proxy- server based architectures [5] shown in figure.1 [5] has an intermediate server for encryption and decryption of data. The proxy is a bottleneck and a single-point-of-failure.This limitsthe availability, scalability and elasticity of the cloud database as a service. Another consideration of this architecture is the proxy must be trusted. It cannot be subcontracted to the cloud and it has to be organized and maintained locally. Moreover, proxy-based architectures cannot scale inconsequentially by increasing the number of proxies. Such a naive solution would imply the replication of metadata among all the proxies, but this would require synchronization algorithms and protocols to guarantee consistency among all the proxies.

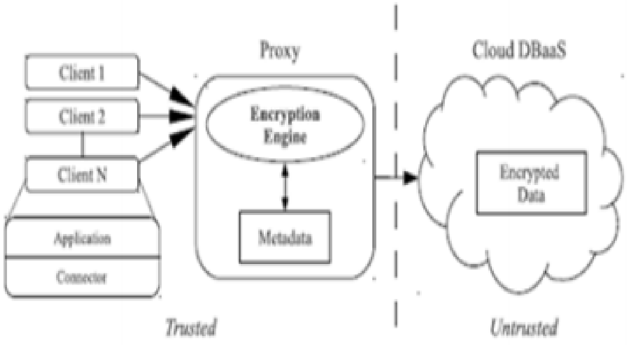

Fig1. **Proxy server based architecture (PSB)**

3.2. Proxy server less architecture with distributed metadata (PSL-DM)

The Proxy server less architecture does not contain any intermediate proxy. By that it try to solve single point failure of PSB architecture. PLS-DM stores metadata in the clients [4]. It distributes metadata among the clients so the clients can connect directly to the cloud database. This architecture provides availability, scalability and elasticity. Each client has its own encryption engine. encrypts the data at client and manages a local copy of metadata. Connect directly to cloud database and store encrypted data. This architecture is differing byPSB by deployingproxy within each client. This architecture for cloud accesses would suffer from the same consistency issues as PSB when multiple clients access same database simultaneously

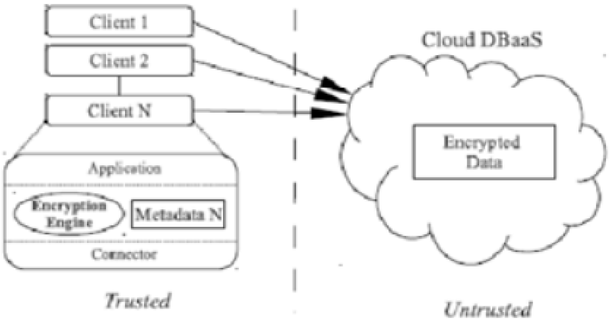

Fig2. PLS-DM Architecture

3.3. Proxy server less architecture with metadata in cloud database (PSL-CD)

The third architecture is proxy server less architectures [6] shown in Fig. 3[6] it tried to eliminate inconsistency problem of PLS-DM architecture. The PLS-DM stored a metadata at client side. When multiple clients access data concurrently, metadata inconsistency occurred. To overcome this problem PLS-CD stores metadata in the cloud database. In this the metadata is stored to the cloud database, the multiple and independent clients access the required metadata and the encryption engine is executed by each client. In this architecture there is no need of synchronization among the clients because metadata stored at cloud. Client machines execute a client software component that allows a client to connect and issue queries directly to the cloud DBaaS. This software component retrieves the necessary metadata from the untrusted database through SQL statements and makes them available to the encryption engine at the client. Multiple clients can access the untrusted cloud database independently, with high availability, scalability and elasticity. The drawback of this architecture is bottleneck and the single point of failure

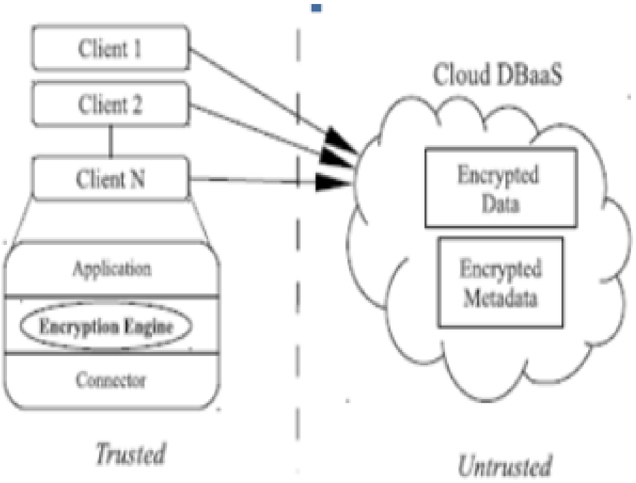

Fig 3.PSL-CD Architecture

4. EXISTING SYSTEM:

This Section mainly focuses on following:

A. Cloud database: We consider that the tenant data is saved in a relational database and we have to preserve the confidentiality of the stored data and even of the database structure because table and column names may yield information about saved data and we distinguish the strategies for encrypting the database structures and the tenant data.

B. Metadata Management: The metadata that is generated by SecureDBaaS contains all the information that is necessary to manage the SQL statements over the encrypted database in a way for transparent to the user as the metadata management strategies represent an original idea because the SecureDBaaS is the first architecture storing all metadata in the un-trusted cloud database together with the encrypted tenant data.

C. Encryption algorithm: The encryption algorithm chooses and used to encrypt and decrypt all the data that is stored in the database table.

In the above figure Fig 4 describes the overall architecture and we assume that a tenant organization acquires a cloud database service from an un-trusted DBaaS provider where the tenant then deploys one or more machines say Client 1 through N and installs a SecureDBaaS client on each of them.This client allows a user to connect to the cloud DBaaS to administer it then to read and write the data and even to create and modify the database tables after creation where the SecureDBaaS is designed to allow multiple and independent clients to connect directly to the un-trusted cloud DBaaS without any intermediate server in the system.

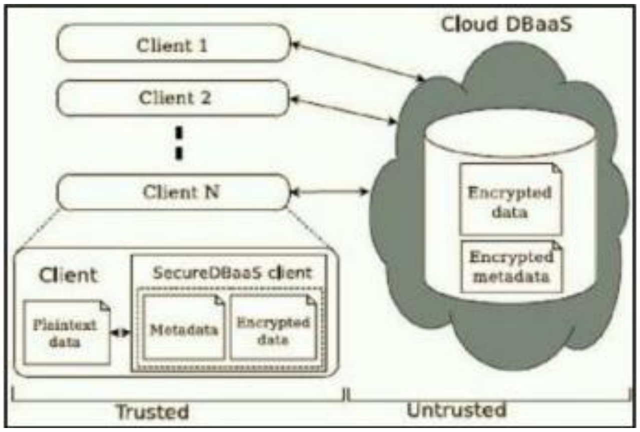

Fig.4. SecureDBaaS Architecture.

In the above figure Fig 4 describes the overall architecture and we assume that a tenant organization acquires a cloud database service from an un-trusted DBaaS provider where the tenant then deploys one or more machines say Client 1 through N and installs a SecureDBaaS client on each of them.This client allows a user to connect to the cloud DBaaS to administer it then to read and write the data and even to create and modify the database tables after creation where the SecureDBaaS is designed to allow multiple and independent clients to connect directly to the un-trusted cloud DBaaS without any intermediate server in the system.

5. PROPOSED SYSTEM:

A.Cloud database: Let us assume that tenant data are saved in a relational database and we have to preserve the confidentiality of the stored data and even of the database structure because table and column names may yield information about saved data as we distinguish the strategies for encrypting the database structures and the tenant data.

B. Metadata Management: Metadata that is generated by the SecureDBaaS contains all the information that is necessary to manage all the available SQL statements over the encrypted database in a way transparent to the user and the metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all the metadata in the un-trusted cloud database together with the encrypted tenant data in the system.

C. Encryption algorithm: In order to choose the encryption algorithms used to encrypt and decrypt all the available data stored in the database table.

6. CONCLUSION:

In this paper we have proposed and discussed concurrent and independent access to encrypted cloud databases and on the same hand we proposed an inventive construction modeling that ensures secrecy of information put away in broad daylight cloud databases and the proposed framework won't oblige changes to the cloud database and it will be quickly appropriate to the current cloud DBaaS and to determine the issue of single point disappointment and a bottleneck restricting accessibility and versatility of cloud database services.

REFERENCES

[1]. Abadi, Daniel J"Data Management in the Cloud: Limitations and Opportunities", IEEE Data Engineering Bulletin, Volume 32, March 2009.

[2] Broberg, RajkumarBuyya, ZahirTari, MetaCDN: Harnessing Storage Clouds or high performance content delivery, Journal of Network and Computer Applications, 1012–1022, 2009.

[3]Damiani, E., De Capitani di Vimercati, S., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Metadata Management in Outsourced Encrypted Databases. In: Jonker, W., Petkovi´c, M. (eds.) SDM 2005. LNCS, vol. 3674, pp. 16–32. Springer, Heidelberg (2005)

[4]H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-ServiceProvider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.

[5] Popa, R.A., Redfield, C.M.S., Zeldovich, N., Balakrishnan, H.: CryptDB: protecting confidentiality with encrypted query processing. In: Proceedings of the Twenty- Third ACM Symposium on Operating Systems Principles, SOSP 2011, pp. 85–100. ACM, New York (2011)

[6] Luca Ferretti, Michele Colajanni, and MircoMarchetti: Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases. IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[8] A. Shamir, ―How to Share a Secret,‖ Comm. of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[9] M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, ―AS5: A Secure Searchable Secret Sharing

Scheme for Privacy Preserving Database Outsourcing,‖ Proc. Fifth Int'l Workshop Autonomous and Spontaneous Security, Sept. 2013.

[10] G. Cattaneo, L. Catuogno, A.D. Sorbo, and P. Persiano, ―The Design and Implementation of a Transparent Cryptographic File System For Unix,‖ Proc. FREENIX Track: 2001 USENIX Ann. Technical Conf., Apr. 2001.