Concurrent and Free Accessing in Encrypted Cloud Databases

G. Sudheer Kumar[1], **P. Pavan Kumar**[2]

[1]M. Tech, CS, Rise Krishna Sai Prakasam Group of Institutions

[2]Assistant Professor, CS, Rise Krishna Sai Prakasam Group of Institutions

Abstract: ***The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing. Cloud computing is one of the most increasing one with the increase number of cloud users. In today's environment every user wants to access their data at any time and at anywhere. In an organization they store their data only on their computers, if they want their data during roaming situation means it is not possible one to carry the data at every time, this is a difficult factors for an organization. Cloud computing can address this problem by providing data storage mechanism to access the data at anywhere. This is one of the storage device used to access their data at any where through networks which is called cloud provider. For this service user worry about the security and privacy issue under this cloud computing for their personal data. For this issue this survey shows various techniques for the security and privacy mechanism for the user data.***

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

1. Introduction

Today user may spend lot of time with a computer to collect lot of data over network and store it where it as portable for the user. During the roaming time user may need the data from their PC (Personal Computer) it is very difficult to take it as a portable one with large datasets. So they may problem occurred while their roaming time. For this reason storing an enough data in network can solve this problem. Cloud storage is used to avoid this problem. Cloud storage refers to storing a large amount of data which in the form of pay-per-use scheme which is referred to cloud computing. It is used to off-site storage scheme maintained by a third party i.e. cloud provider [1]. It is most popular one to store the data in geographical environment with infinite computing resources and access the data where the user need without worry about the data loss. Hence it provides greater availability, scalability, and reliability to the users. This survey shows the features are provided by the cloud provider as a service of Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Database as a Service (DBaaS).

Cloud services:

1) Software as a Service (SaaS: This provides a service to the user by offering different software to the different user over internet. A distinct instance of service which runs in the cloud, here one or more user can utilize the service. Here no charges are detected from the user for the service or software license. In some cases charges may detected for the maintenance of the service [2].
2) Platform as a Service (PaaS): This provides a service to the user for the layer of software platform. It provides a storage mechanism for the various applications and consumptions. User can have an independency to build their personal applications that provides infrastructure for the user. It offers predefined components of combined OS and the application server, e.g. LAMP platforms [2].
3) Infrastructure as a Service (IaaS): This provides a service to the user for the basic storage and processor infrastructure as a service over the network. It provide a service to the computer infrastructure for the servers, network administrators, data centre, etc… to handled the workload of these service through IaaS. For this service user need to pay charges, when they use this service over network. In this mechanism cloud computing provide a service over the internet, hardware and software in datacenters as a services. The datacenter of hardware and software is called as Cloud.
4) Database as a Service (DBaaS): This provides a service to the user for their data. It does not require modifications to the database hence it is controlled by the cloud provider. Cloud provider manage and direct the database and aim to avail the instant services to the data users. Here organizations pay for the database service for getting the service from the service provider. For the organization with fewer amounts of resources limited hardware and time-bound projects, DBaas solve this problem; it is in the bases of pay-per-usage manner.

2. Literature Review

With a massive growth in user data in cloud, user requires changing data storage while their roaming, privacy and security for their personal data, better transferring data, better broadband facilities, etc... And cloud computing led to the emergence of cloud databases. For this issue this survey shows some existing techniques for solving their user problem in this review section. Ryan K L Ko et.al [4] studied the problems and challenges of the trusted cloud, where the unauthorized user can access the entire data without disturbing the actual user. An unauthorized person may do the two things which is accessing the data and putting duplicate data because cloud storage provides a geographical database. It is not a trusted one to store the data of the users. For this problem Ryan K L Ko et al proposed a TrustCloud framework, to achieve a trusted cloud to the user, to provide a service by making use of detective controls in cloud environment. Detecting process has the accountability access with the cloud. Here user is a responsible person for their data, hence user must tell the accountability with the technical and policy based services. By providing the accountability through user it may solve the problem from the untrusted one. Hence this approach provides privacy, security, accountability and auditability. Muhammad Rizwan Asghar et.al [5] discusses the problems of enforcing security policies in cloud environment. With the high growth of data in cloud they where problem arises due to untrused person access of the data. To ensure the security is immature, they didn't ensure for the safe data in cloud environments. Security problem is a great issue; here we enforce the security for the owner's data. Providing high security they may high expensive for the users. For the above mentioned problem Muhammad Rizwan Asghar et.al proposed an ESPOON policy which is Encrypted Security Policies for OutsOurced eNvironments. This policy is used to address the above problem and give better confidentiality to the users. It provides a better security by separating the security policy and the enforcement mechanism. Here M R Asghar uses an encrypted scheme to protect the user's data. This is used to protect confidentiality policies based on user's policy. This method has two main scheme, which is policy deployment and policy evaluation scheme. Policy deployment is used to exploit the user's guidelines and the policy evaluation is used to estimate the user guidelines. By using this method user can safe their data.

L Ferretti et al [6] studied the problem of data leakage of the legitimate user in cloud environment by the cloud provider; they didn't give better security to the user for their personal data or internal data. Main problem arise because of no encrypted data were found, and also it provide the security for the frond-end database only and not controlled the backend database, so the malicious attackers may gain the data access to the outsourced data. L Ferretti et al studied the problem and proposed a multiple key based scheme to allow th e database administrator to obtain a cryptographic key for high access control policies. By providing this key scheme it based on multi user mechanism so every time a key will be generated to the actual user for the data access. By using the key, user may decipher it and use the data over cloud. It provides the service for public cloud DaaS. It enforces the access control mechanism. By this enforcement user can guaranteeing in their data. It minimizes the data leakage problem.

A.J. Feldman et al [7] find the issues of leaking data in server side and study the risk of privacy problem. Due to centralization of information attackers may easily hack the data through cloud computing. Access control under this cloud provider is not a strong one; user data may loss at any time because all a user is not always in the online to check the status of the data. So it is easy to hack the data in anytime by the attackers and also they may modify their data at any time so it is risky one.

3. System Overview

The system mainly focuses on following-

- Cloud database
- Metadata Management
- Encryption algorithm

Cloud database: We assume that tenant data are saved in a relational database. 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. We distinguish the strategies for encrypting the database structures and the tenant data.

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

Encryption algorithm: Choosing the encryption algorithms used to encrypt and decrypt all the data stored in the database table.

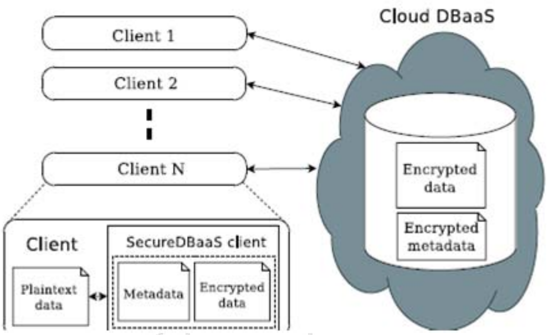

Fig. 1 describes the overall architecture. We assume that a tenant organization acquires a cloud database service from an untrusted DBaaS provider. The tenant then deploys one or more machines (Client 1 through N) and installs a SecureDBaaS client on each of them. This client allows a user to connect to the cloud DBaaS to administer it, to read and write data, and even to create and modify the database tables after creation. SecureDBaaS is designed to allow multiple and independent clients to connect directly to the untrusted cloud DBaaS without any intermediate server

4. System Design

4.1 Cloud Database

We assume that tenant data are saved in a relational database. 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. We distinguish the strategies for encrypting the database structures and the tenant data.

4.2 Metadata Management

Metadata generated by SecureDBaaS contain all the information that is necessary to manage SQL statements over the encrypted database in a way transparent to the user. Metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data.

4.3 Encryption Algorithm

Choosing the encryption algorithms used to encrypt and decrypt all the data stored in the database table.

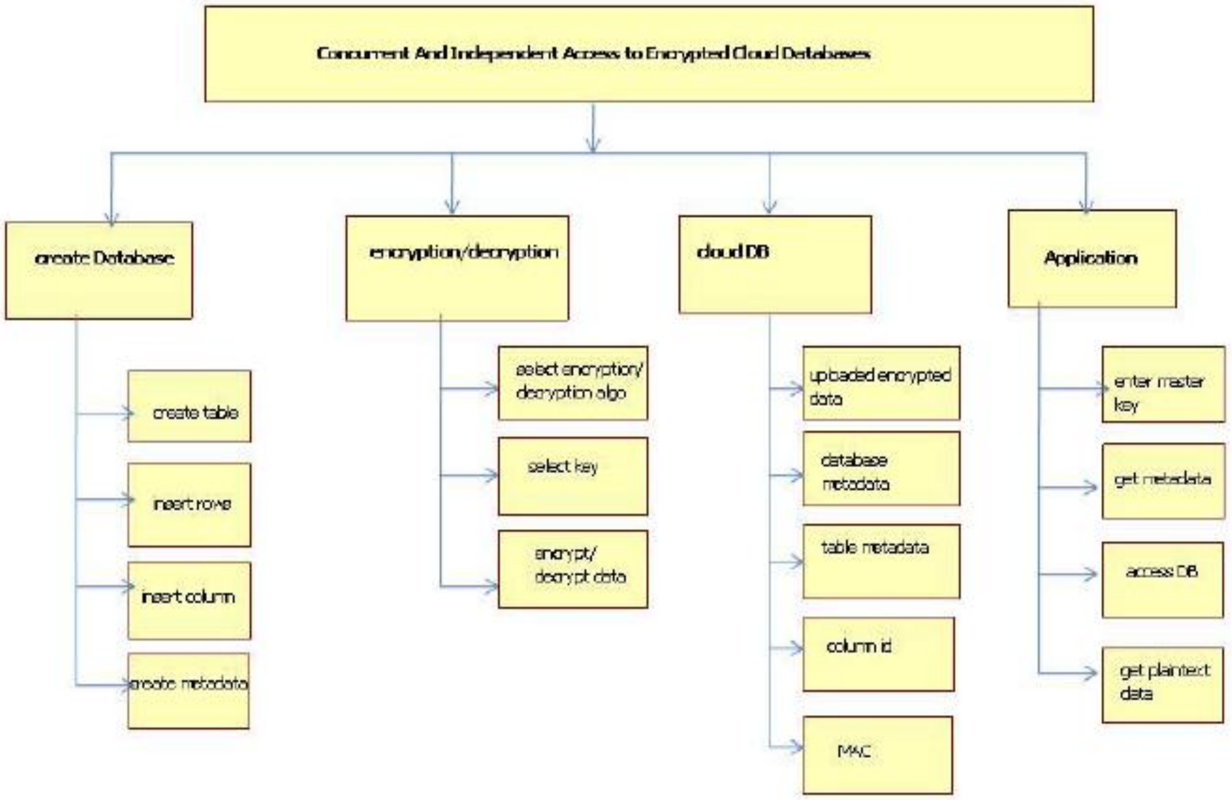

Figure 2: describes the system design having modules and its components.

1) **Creation of database-**
In this module client creates its database and store data in the form or columns and rows. After creation of Database the client also creates its metadata which will help for later communication instead of whole database.

2) **Selection of encryption and decryption algorithm**
In this module we select the encryption algorithm to encrypt and decrypt the created database and its metadata. It will provide security to whole data of client which is to be uploaded on the cloud.

3) **Cloud Database**
Cloud Database is the service provider, which provides services to the tenants. All the encrypted data from data owner is uploaded on cloud which provides concurrent access to cloud DB to the geographically deployed clients. Cloud DB contains encrypted database and its encrypted metadata.

4) **Application**
This module contains the application of system to the cloud. How we will Apply these all on cloud this module explains it. We use master key to access cloud data after data is uploaded on data. First we will get encrypted data if our key is correct then by using random decryption keys we will get the final output in the form of plaintext data. Input is taken from user in the form of sql querry. Firstly client will create Database then, will enter rows into the database. After that the metadata of database is created. Then selected encryption algorithm is applied to the database and its metadata. final output gives the encrypted data with all its information and key used.

5. Implementation

5.1 Data Management

Cloud database acts as service provider for tenants. The cloud is created first for the system. All information or data store in the relational database. So for creating tables and column we have to access it with SQL query only.

5.2 Metadata Management

Metadata generated by SecureDBaaS contain all the information that is necessary to manage SQL statements over the encrypted database in a way transparent to the user. Metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data.

SecureDBaaS uses two types of metadata.

- Database metadata are related to the whole database. There is only one instance of this metadata type for each database.
- Table metadata are associated with one secure table. Each table metadata contains all information that is

necessary to encrypt and decrypt data of the associated secure table.

This design choice makes it possible to identify which metadata type is required to execute any SQL statement so that a SecureDBaaS client needs to fetch only the metadata related to the secure table/s that is/are involved in the SQL statement.

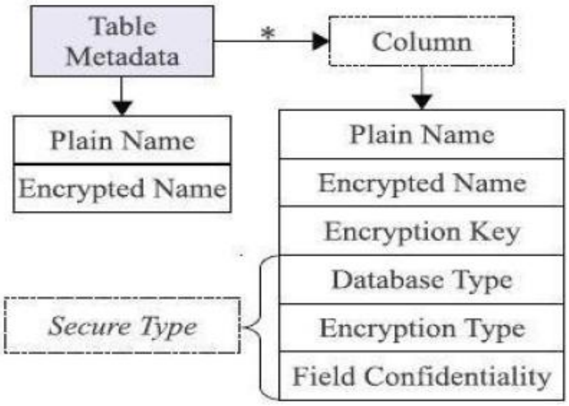

Fig.3. Structure of table metadata.

This design choice minimizes the amount of metadata that each SecureDBaaS client has to fetch from the untrusted cloud database, thus reducing bandwidth consumption and processing time. Moreover, it allows multiple clients to access independently metadata related to different secure tables. Database metadata contain the encryption keys that are used for the secure types. A different encryption key is associated with all the possible combinations of data type and encryption type. Hence, the database metadata represent a key ring and do not contain any information about tenant data. The structure of a table metadata is represented in Fig. 3. Table metadata contain the name of the related secure table and the unencrypted name of the related plaintext table. Moreover, table metadata include column metadata for each column of the related secure table.

Each column metadata contain the following information.

- Plain name: the name of the corresponding column of the plaintext table.
- Coded name: the name of the column of the secure table. This is the only information that links a column to the corresponding plaintext column because column names of secure tables are randomly generated.
- Secure type: the secure type of the column. This allows a SecureDBaaS client to be informed about the data type and the encryption policies associated with a column.
- Encryption key: the key used to encrypt and decrypt all the data stored in the column.

SecureDBaaS stores metadata in the metadata storage table that is located in the untrusted cloud as the database. This is an original choice that augmnts flexibility, but opens two novel issues in terms of efficient data retrieval and data confidentiality. To allow SecureDBaaS clients to manipulate metadata through SQL statements, we save database and table metadata in a tabular form. Even metadata confidentiality is guaranteed through encryption. The structure of the metadata storage table is shown in Fig. 4 This table uses one row for the database metadata, and one row for each table metadata. Database and table metadata are encrypted through the same encryption key before being saved. This encryption key is called a master key. Only trusted clients that already know the master key can decrypt the metadata and acquire information that is necessary to encrypt and decrypt tenant data. Each metadata can be retrieved by clients through an associated ID, which is the primary key of the metadata storage table. This ID is computed by applying a Message Authentication Code (MAC) function to the name of the object (database or table) described by the corresponding row. The use of a deterministic MAC function allows clients to retrieve the metadata of a given table by knowing its plaintext name. This mechanism has the further benefit of allowing clients to access each metadata independently, which is an important feature in concurrent environments. In addition, SecureDBaaS clients can use caching policies to reduce the bandwidth overhead.

6. Conclusion

In this paper, we have discussed concurrent and independent access to encrypted cloud databases,proposes an innovative architecture that guarantees confidentiality of data stored in public cloud databases. The proposed system will not require modifications to the cloud database, and it will be immediately applicable to existing cloudDBaaS. Resolve problem of single point failure and a bottleneck limiting availability and scalability of cloud database services.

References

[1] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Distributed, concurrent, and independent access to encrypted cloud databases." (2014): 1-1.

[2] Ashalatha, r., and m. Vaidehi. "The significance of data security in cloud: a survey on challenges and solutions on data security”.

[3] Arora, Indu, and Anu Gupta. "Cloud Databases: A Paradigm Shift in Databases." *International J. of Computer Science Issues* 9.4 (2012): 77-83.

[4] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang , Bu Sung Lee, “TrustCloud: A Framework for Accountability and Trust in Cloud Computing” 2011 IEEE World Congress on Services.

[5] Muhammad Rizwan Asghar, Mihaela Ion, Bruno Crispo, “ESPOON Enforcing Encrypted Security Policies in Outsourced Environment”, 2011 Sixth International Conference on Availability, Reliability and Security.

[6] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, “Access control enforcement on query-aware encrypted cloud databases” IEEE 2013.

[7] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, “SPORC: Group Collaboration Using Untrusted Cloud Resources,”Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[8] Ferretti, Luca, et al. "Security and confidentiality solutions for public cloud database services." *SECURWARE 2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies*. 2013.

[9] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Access control enforcement on query-aware encrypted cloud databases." *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*. Vol. 2. IEEE, 2013.

[10] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Supporting security and consistency for clouddatabase." *Cyberspace Safety and Security*. Springer Berlin Heidelberg, 2012. 179-193.

[11] Dr. M. Newlin Rajkumar, Brighty Batley C, Dr.V.Venkatesakumar, Ancy George, Scholar, P. G., and P. G. Scholar. "Survey on the Concurrency Control Protocols for Encrypted Cloud Databases."

[12] S.M. Hema Latha , S.Ganesh, “A Brief Survey on Encryption Schemes in Cloud Environments”-2013.

[13] Pathak, Ajeet Ram, and B. Padmavathi. "Survey of Confidentiality and Integrity in Outsourced Databases."

[14] Khan, Abdul Wahid, et al. "A Literature Survey on Data Privacy/Protection Issues and Challenges in Cloud Computing." *IOSR Journal of Computer Engineering (IOSRJCE) ISSN* (2012): 2278-0661.