Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-9, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Concurrent Access to Encrypted Cloud Database

Bhupendra G. Hatzade & Deepa Amne

Abstract*: Now a days "cloud computing" is a renowned technology. Most of the organizations prefer to store the data on cloud, because every user wants to access their data at any time and at anywhere. Cloud is one of the storage device used to access their data at anywhere through networks. But because of this service, users always worry about privacy and confidentiality for their personal data. This paper gives quick introduction of a new technique that provides data confidentiality and concurrent access of encrypted cloud database, and discuss about cloud computing security issues and their solutions.*

1. Introduction

The concept of "cloud" is not new for us. We have been using cloud computing from many years in one or other form. Cloud computing is a way of using the computing resources that are available and accessing over the network. Cloud storage is used to store large amount of data as in the form of pay-per-use. It is most popular storage to store data in geographical environment with infinite computing resources and users can access data at anywhere without worry about data loss. But placing critical data in cloud infrastructure should come with the guarantee of security and availability of data at any motion. This paper show features of cloud deployment models and cloud services. And also give introduction of new technique i.e. Secure DBaaS that provide data confidentiality and geographically distributed users can access encrypted cloud data concurrently.

A. Deployment Models:
There are four types of deployment models in cloud computing [8].

1) Public Cloud
This model can be used by general public. This includes Individuals or large industry group and owned by the Cloud providers. These are also called providers cloud.

2) Private Cloud
This model is limited within an organization. It is also called internal cloud. It is manage by the cloud computing providers.

3) Hybrid cloud
Hybrid cloud is a combination of public cloud and private cloud.

4) Community cloud
This model is shared by group of organizations.
B. Cloud Services:

1) IaaS(Infrastructure as a Service)
This provides a service to the user for the storage and infrastructure resources that needed to deliver the cloud services over the network [10]. To use this service over the network users need to pay charges. In this mechanism cloud computing provide a service over the internet, software, and hardware in data center as a service.

2) SaaS(Software as a Service)
This provides a service to the user by offering different software to different user across the internet. Cloud service provider hosts the software upon their server. A different instance of service which runs in cloud, here multiple users can utilize the service. No charges are taken from user for the service or software license. In some cases charges may taken for maintenance of the service [10].

3) PaaS(Platform as a Service)
This provides development environment as a service to the user. PaaS provides combination of infrastructure and application. Here user can develop their own applications and deliver it through internet and servers. It offers predefined components of combined OS and application server.

Here introduce secure database as a service (SDBaaS) to overcome the issue of concurrent access in proxy based architecture. In some cases users have worry about security and privacy problem from the cloud provider. SDBaaS supports geographically distributed client to connect directly to the encrypted cloud database and to support concurrent and independent operations to the encrypted database. This architecture does not depend on any intermediate proxy server between cloud database and client in order to availability and scalability. SDBaaS also provide data confidentiality by adapting various encryption algorithms technique and gives guarantee for data consistency [1].

2. SDBAAS(secure database as a service)

Page Secure database as a service is the first approach to allow geographically distributed client to directly connect to secure cloud database. This approach has three main goals: to allow multiple clients to perform concurrent operation on encrypted cloud database by using SQL statements and also can modify the structure with the help of this, to provide data confidentiality and integrity at both client and cloud level, to make proxy less design by eliminating proxy server between cloud client and provider[11].

Previous techniques provide confidentiality by distributing data between multiple providers and do secrete sharing, in this way prevent one cloud provider to read its data but raise collision problem. Secure database as a service does not use multiple providers to preserve confidentiality, and use SQL known encryption algorithms. SDBaaS preserve data confidentiality through various encryption algorithms and allow performing SQL operations on encrypted data. In proxy based architecture, if client request for any data that request must passed through trusted broker or trusted proxy. But with this distributed client cannot access encrypted cloud database concurrently. Because that makes more overloads on trusted proxy or system and that's why architecture represents single point failure and bottleneck problem that limits main benefits of a database services deployed in cloud. Proxy based architecture relay on intermediate server that does not support geographically distributed client concurrently access to encrypted cloud database. Secure database overcome system bottleneck problem by eliminating intermediate server between clients and cloud database. SDBaaS does not relay any intermediate server and geographically distributed client can access encrypted cloud database concurrently.

A. Architecture

SDBaaS architecture is design to allow multiple clients to connect directly to the untrusted cloud database without any intermediate. Fig. 1 shows the overall architecture of SDBaaS. It consists of one or more client with SDBaaS and untrusted cloud database. Client allows users to connect to the DBaaS to administer it, to read and write data, and even to create and modify the database tables after creation. SecureDBaaS consists of plaintext data, metadata, encrypted metadata and SDBaaS is different from previous method and provide high confidentiality. Proxy based architecture store only user's data in the cloud database, and store metadata in the client machine[2] or distribute metadata between cloud database and trusted proxy server[3]. Due to this design previous method introduce system bottleneck that reduces availability, elasticity and scalability of cloud database services. In SecureDBaaS both users' data and metadata stored in the cloud database, so multiple clients can access cloud database independently with the guarantee of availability, elasticity and scalability of typical cloud database services [1].

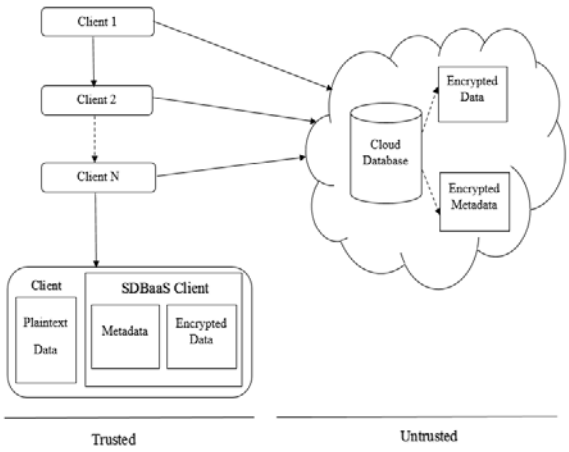

Fig. 1 Cloud database Design

B. Data and Metadata Management

In SDBaaS, both data and metadata store in cloud database. So to preserve confidentiality, data and even structure of data must be encrypted. User data store in secure table and table name also encrypted and that encryption key known to all secure DBaaS clients. Table column name also encrypted. Users can access data concurrently by performing SQL operation on encrypted data. Here one more concept is introduced which is related to data type of traditional database i.e. secure type. Secure type is related to column of a secure table. Secure type is generated by using three fields that is data type, encryption type, and field confidentiality. In SDBaaS model different encryption key are used for each column, so even two columns contain same data that represents in different encryption form. This design provides high level of confidentiality. This model uses three types of field confidentiality, column, multicolumn and database [1].

This is the first approach, that store metadata in untrusted cloud database. Metadata contains information that need to encrypt user's data and to perform SQL statement over encrypted cloud database. This model uses two types of metadata, database metadata and table metadata. Metadata about whole database is a database metadata, that is consists of only one object for each database. Database metadata contain encryption key which is used to generate secure type with field confidentiality database. Table metadata related to single secure table. Each table metadata consists of information that is needed to encrypt and decrypt

data of the particular table. Table metadata contains plaintext name and encrypted name of related secure table and also contain column metadata, which consists of plaintext and encrypted name of related column, encryption key and secure type.

3. Security Threats And Solution

A. Data control

In cloud computing data store in cloud, that's why user can access their data at any time but user, who does not have any authority to access data they can also access the data from cloud database without user permission. Controlling the user's data from the unauthorized use is one of the major issues in cloud computing. Physical control is best method to avoid data control issue. When compare to physical scheme an automatic control mechanism can provide a secure one in the possible of the every time [4]. Visualization is important to control the user's data and maintain control over access to user resources.

B. Distributed Data

During roaming time user need their data, this mechanism is used to share data of the user in networks while their roaming. Data distribute in different locations and multiple clients need concurrent access of an encrypted data. But with the proxy based architecture client cannot access data concurrently because each request is passed from the intermediate server thus causing more overloads on trusted proxy. So to access distributed data concurrently, eliminate the intermediate proxy server between user and cloud provider to preserve privacy and availability. We can distribute data without any intermediate in secure manner.

C. Data Privacy

When placing critical data in cloud environment should come with guarantee of security. User's original data must be accessible only trusted user. Maintain privacy of user's data who stored their data in the cloud environment is one of the main issues. Every user want their personal data in secrete manner [5]. Sometimes cloud provider compromise the data to the malicious attackers, so problem may raises for the data user. With the use of intermediate data may loss. Encryption is one of the best methods to protect the data. Convert plaintext data into unreadable form and generate cipher text. User can encrypt their data so no one can access their data without permission.

D. Concurrent and Independent access

In cloud environment, accessing data concurrently and independently is important. Because multiple clients distributed in different locations and accessing the data which are store in cloud database. Sometimes multiple client try to access same data from cloud database, in this condition occurs system bottleneck problem. SDBaaS model is created for concurrent and independent access of cloud database. This model integrate cloud database with secure provider for data privacy and security. It eliminates a trusted proxy or trusted broker.

E. Identity and access management

In cloud computing data is stored in different locations. To accessing the data over network may occurs an untruthful problem because of attackers in the network. So anyone can access our data without permission. To avoid unauthorized access, provide an access control tool, to control the data over distributed network. Access control tool works on the basis of authenticate the authorized user. To monitor accessing data limits it provides a data access matrix. Identity mechanism is used to identify authorized user by sign on of instant user when an actual user is signed in. Identity mechanism is used to manage the multiple users in a network.

4. Implementation

A. Module1 (Creation and encryption of database and its metadata) Representation using Sequence Diagram

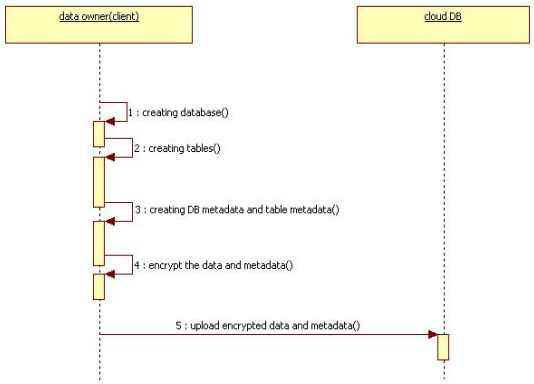

Fig. A. Sequence Diagram of module

B. Implementation Steps and Code for Creation and encryption of database and its metadata

Steps:
1. Create database
2. Create table
3. Create database metadata and table metadata
4. Encrypt the database and metadata

Code:

```
public class DatabaseGeneration extends javax.swing.JFrame
{
private int[] S;
```

```
    private int[] T;
    // JDBC driver name and database URL
static _nal String JDBCDRIV ER = "com:mysql:jdbc:Driver";
static _nal String DBURL = "jdbc : mysql : ==localhost=bank";
public DatabaseGeneration()
{
    initComponents();
    jPBlank.setVisible(true);
    jPRC4.setVisible(false);
    jPCreateDatabase.setVisible(false);
    jPDMetadata.setVisible(false);
    jPTMetadata.setVisible(false);
}
private void jBtDoneActionPerformed(java.awt. event.ActionEvent evt)
    {
    this.dispose()
    }
private void jButton1ActionPerformed(java.awt. event.ActionEvent evt) {
    jPBlank.setVisible(false);
    jPRC4.setVisible(true);
    jPCreateDatabase.setVisible(false);
    jPDMetadata.setVisible(false);
    jPTMetadata.setVisible(false);
    }

Private void jButton5ActionPerformed (java.awt. event.ActionEvent evt) {
    int K = Integer.parseInt(jTxtSK.getText());
    int BL = Integer.parseInt(jTxtBL.getText());
    S = new int[BL];
    T = new int[BL];
    DefaultTableModel edtm = (DefaultTableModel) jTable1.getModel();
    for (int i = 0; i < BL; i++)
    S[i] = i;
    T[i] = (i K) %BL + 1;
    edtm.addRow(new Object[]S[i], T[i]);
}
//Register JDBC driver
Class.forName("com.mysql.jdbc.Driver");
//Open a connection
System.out.println("Connecting to a selected database...");
    conn = DriverManager.getConnection(DBURL; USER; PASS);
System.out.println("Connected database successfully ...");
```

5. Conclusion

In this paper presents cloud deployment models and services, also give introduction about SecureDBaaS. That allows multiple users to connect directly to the untrusted cloud database, and allow concurrent and independent access of cloud database without any proxy server. It also preserves confidentiality of user's data by adapting various encryption techniques. Cloud computing is important for cloud users to access data through network at anytime and anywhere, so they worried about the security of their personal data stored in cloud database. This paper present cloud computing security issues and their solutions.

6. References

[1] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Concurrent, and Independent Access to Encrypted Cloud Databases," IEEE TRANSACTIONSON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY2014.

[2] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp Operating Systems Principles, Oct. 2011.

[3] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June2002.

[4] 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.

[5] S.Mekala, M.Senthil Prabhu M.E, V.Gayathri, "SURVEY ON ACCESSING ENCRYPTEDDATABASE IN CLOUD, International Journal of Advanced Research in Computer and Communication Engineering. Vol. 3, Issue 10, October 2014.

[6] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti, "Security and Confidentiality Solutions for Public CloudDatabases Services," SECURWARE 2013: The Seventh International Conference on Emerging Security Information Systems and Technologies2013.

[7] Jens-Matthias Bohli, Nils Gruschka, MeikoJensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013.

[8] SRINIVASA RAO V., NAGESWARA RAO N. K., E. KUSUMA KUMARI, "CLOUD

COMPUTING: AN OVERVIEW," Journal of Theoretical and Applied Information Technology, © 2005 - 2009 JATIT.

[9] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Supporting

Security and Consistency for Cloud Database," Y. Xiang et al. (Eds.): CSS2012, LNCS7672, pp. 179–193, 2012.

[10] Sherif Sakr, Anna Liu, Daniel M. Batista, and Mohammad Alomari, "A Survey of Large Scale Data Management Approaches in Cloud Environments," IEEE COMMUNICATIONSURVEYS & TUTORIALS, VOL. 13, NO. 3, THIRD QUARTER 2011.

[11] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti, "Performance and cost evaluation of an adaptive encryption architecture for cloud databases," IEEE TRANSACTIONS ON CLOUD COMPUTING VOL: 2 NO: 2 YEAR 2014.