Concurrent and Independent Access to Encrypted Cloud Databases

Miss Rashmi A. J. Sheikh, Prof. P. N. kalvadekar

1 M.E. (CE) SRESCOE Kopargaon
2 Dean of computer dept. SRESCOE Kopargaon

Abstract: We are moving to future where some or even most of our data will exist in cloud, because cloud provides stored data to be accessed at anywhere through networks. Since data in cloud will be placed anywhere, because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed; it will create other problems also like data confidentiality and bottleneck. This paper presents a new technique that provides data confidentiality and concurrent access of encrypted cloud database with resolving the bottleneck problem.

1. Introduction

The concept of “cloud” is not new for us. We have been used 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. We are moving to future where some or even most of our data will exist in cloud, because cloud provides stored data to be accessed at anywhere through networks. Since data in cloud will be placed anywhere, because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed; it will create other problems also like data confidentiality and bottleneck. This paper presents a new technique that provides data confidentiality and concurrent access of encrypted cloud database with resolving the bottleneck problem.

1.1. Related Work

Kevin Hamlen and the authors discuss security issues for cloud computing and present a layered framework for secure clouds and then focus on two of the layers, i.e., the storage layer and the data layer. The authors Kevin Hamlen, Murat Kantarcıoglu, Latifur Khan and Bhavani Thuraisingham, discuss a scheme for secure third party publications of documents in a cloud and given an aspect of querying encrypted data, as much of the data on the cloud may be encrypted and secure query processing of the data [2]. If we consider the large size of the outsourced data and the owner’s constrained resource capability, the task of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. To fully ensure data security and save data owners’ computation resources, Auditor Bhavna Makhija, Vinit Kumar Gupta, Indrajit Rajput propose to enable publicly auditable cloud storage services, where to verify the outsourced data, the data owners can resort to an external TPA when needed in the paper [3]. M. Armbrust et al, reduces confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional computing, and identifying the top technical and non-technical obstacles and opportunities of cloud computing [4].

Proxy less architecture proposed by L. Ferretti, M. Colajanni, and M. Marchetti does not use an intermediate proxy and metadata are stored in the clients. Since clients connect directly to the cloud database, this architecture achieves availability, scalability and elasticity comparable to those of the original DBaaS. does not use an intermediate proxy and metadata are stored in the clients. All the solutions based on cryptography depend on metadata [5].

By examine all the papers on cloud security we concentrated on proxy less architecture which one is the most secure than other architecture and also can allow the concurrent access to geographically distributed clients with more privacy and security.

2. System Overview

Previous techniques were not suitable when geographically distributed client needs concurrent access to data stored in the same DBMS and data confidentiality were provided by distributing data between multiple providers. In this way prevent one
cloud provider to read its data but raise collision problem.

SecureDBaaS is designed to allow multiple and independent clients to connect directly to the untrusted cloud DBaaS without any intermediate server. 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[6].

2.1. Architecture

The architecture shows the SecureDB concept. The cloud is called as untrusted whereas the clients are trusted one. Because of the nature of cloud as it provides services and interacts with various parties it is untrusted. It assumes 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.

3. System Design And Implementation

Following figure (fig 3) describes the system design having modules and its components as follows:

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.

A. 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. There are various encryption algorithms symmetric and asymmetric, but we will apply symmetric algorithm which proved key distribution only once to all tenants there will be no different private key related to every user.

B. 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.

C. 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 query. 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.

4. Working

Here for encryption of data we are using RC4 algorithm. Why RC4? Because here we are not concentrating only on security bt also we need concurrent access to encrypted database. If we will use strong encryption algorithm then it will take more time to encrypt and decrypt data which will directly affect to accessing time.
4.1. Technologies used

4.1.1. Openshift cloud
For experiment purpose we have used the openshift cloud which provides platform to edit create and store the data.

4.1.2. Ruby and gems
This are necessary while accessing openshift cloud database. To connect with our application with cloud ruby and gems are necessary for database connection.

4.1.3. Netbeans, Sql and JDK
This are the software which we have used to create an application from where by use of sql query we can access the cloud.

5. Snapshots

6. Conclusion
In this paper presents techniques 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.

7. Acknowledgement
This work was supported in part by a grant from the National Science Foundation.

8. References


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