International Journal of Research in Engineering, Science and Management
Volume-3, Issue-3, March-2020
www.ijresm.com | ISSN (Online): 2581-5792

Privacy Preserving using Distributed, Concurrent and Independent Encrypted Cloud Databases

Trupti Patil[1], Manali Kadam[2], Aditi Kadam[3], Sonali Kadam[4], Rutuja Jadhav[5], Shatakshi Kokate[6]

[1,2,3,4,5]*Student, Department of Computer Science and Engineering, D. Y. Patil College of Engineering and Technology, Kolhapur, India*

[6]*Assistant Professor, Department of Computer Science and Engineering, D. Y. Patil College of Engineering and Technology, Kolhapur, India*

***Abstract*: The main objective of our project is to place critical data in the hands of cloud provider and should come with the guarantee of security and availability for the data at rest, at motion and in use. Secure DBaaS is designed to allow multiple and independent clients to connect directly to the un-trusted cloud DBaaS without any intermediate server. The DD-PLAC architecture is a proxy-less architecture that store metadata in the cloud database but to provide the more availability and to improve the performance by using the distributed cloud database which will allow the databases to truly support the elastic requirements of cloud computing applications. Our system is an upgraded version of the old PLAC architecture which provides the Security, Availability and Confidentiality. The success of implementation and development of this project is expected in eliminating proxies help in achieving elasticity, availability and scalability properties that are basic factors in cloud-based services.**

***Keywords*: Cloud, security, Confidentiality, Secure DBaaS, Database.**

1. Introduction

Now a day's information is increasingly important in any once daily life. All have become information dependent, so living in on command, on demand world, which means individual needs information when and where it is required. Everyone access the internet every day to perform searches, participate in social networking, send and receive emails, share pictures and videos. This will create huge information, but it has no value until it is shared with others. To be shared, this information need to be uploaded to central repository via network. Businesses are also depending on fast and reliable access to information. The increasing dependence of businesses and individual all information has amplified the challenges in storing, protecting and managing data. Organizations usually maintain one or more data centre to store and manage information. The data centre is a facility that contains information storage and other physical information. Technology resources for computing, networking and storing information are used. So the cloud computing is one of that data centre which brings in a fully automated request fulfilment process that enables users to rapidly obtain storage and other IT resources on demand.

One of the services provided by cloud computing is the cloud database, which stores the data online, on demand. A cloud database is a database that generally runs on a cloud computing platform, like Amazon, EC2, GoGrid, SalesForce, Rackspace and Microsoft Azure. There are two deployment

models, users can run databases on the cloud independently, using virtual image machine and the second is they can purchase access to a database service which is maintained by a cloud database provider. Cloud Computing is a tool that offer enormous benefits to its subscribers. As it is tool it comes with its set of problem and in efficiencies. The main and measure concern is about security and privacy in cloud.

The proposed DDPLAC architecture allows you to upload data in cloud storage in the form of encipherment and allow concurrent access to distributed database applications. SQL operations can be fired over the encrypted data. These approaches preserve, data confidentiality in scenarios where the DBMS is not trusted. Operations over encrypted data are carried out through SQL-aware encryption algorithm.

2. Need of work

The public nature of cloud computing has significant implications to data privacy and confidentiality. Cloud data is stored in plain text and few companies have an absolute understanding of the security levels their data stores hold. A recent report by the Cloud Security Alliance lists data lost and leakage as of top security concerns in the cloud. Recent loss regulations compound the risks of ending. Companies can be held responsible for the loss of sensitive data and may face heaviness over data breaches. To lose data security practice also harm on personal level. Loss 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 ownership. Different architectures are designed to overcome primary issues. The recent designed architecture is PLAC. In PLAC architecture it has drawbacks such as single point of failure and bottleneck. This architecture does not guarantee data isolation and confidentiality against the collusion threats. To overcome this drawback, the architecture DDPLAC is introduced. DDPLAC architecture is an extension of PLAC architecture which operates on distributed database storage system and databases have been distributed in terms of instances running on server that have access to a high speed network for a while. It also provides concurrent applications to run simultaneously [1].

3. Objectives

- To overcome the single point of failure and system bottleneck, which in turn increase the availability and scalability.
- To build an application with stronger level of security and privacy of data on cloud storage.
- To provide direct, independent and concurrent access of data on cloud storage.
- To reduce the reliability on third party.

4. Methodology

A. Modules

System consists of four modules:

1) Front end (Application)

Applications are used to input the data from the user and differentiate it according to design instances according to vertical fragmentation. Therefore, user can access his/her personal confidential documents.

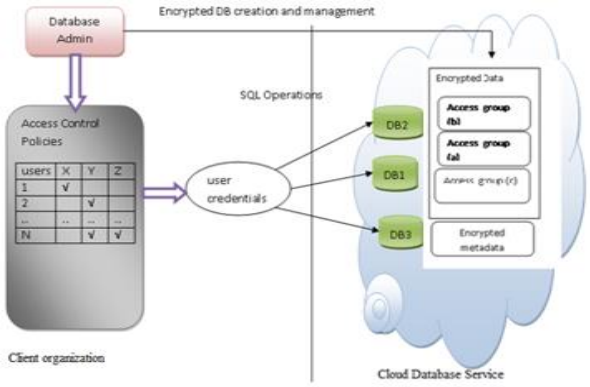

Fig. 1. DD-PLAC architecture

Developing Applications:

The web application is used to take input from user. It includes following details:

1. Personal Details.
2. Professional Details.
3. Banking Details.
4. Insurance Details.

Admin:

Admin is the owner of the application. The admin is supposed to design the database and send the email to the officer.

Officer:

Different officers perform different tasks such as GramSevak will do the birth registration of citizen. All officers have same task to register the data of citizen based on his/her demand. Officer sends the email to the user.

User:

In this module, it receives the mail from officer which includes user id and password. User is facilitated with citizen's login, change password, change details, etc.

Implementation of Security Algorithm:

The AES SHA-512 algorithm is used for maintaining security in application. The encryption key is generated based on the information entered by user.

Step 1: Random string is generated from the details provide by the user.

Step 2: This bit string is appended with any random string and generate a single random string.

Step 3: This single random string form a string of length of 16 bit:

Step 4: Hash function is applied (SHA-512) to this 16-bit string which in turn generates a Secret key of 128 bits.

2) Back end

Distributed Database:

At the back-end, database exists. After the user enters the data through the web application, the data is distributed according to the design of database designed by the admin. This distributed data is stored in encrypted format [2].

Generating Metadata:

A Metadata describes data about data. Metadata generation takes place by certain fields such as unique id, metadata id, encryption key. This fields of metadata are kept safe from the trusted party by keeping it in secured way. Here the primary key is unique id [1].

5. Experimental Setup

A. Technology Used

1) Description of technology

XAMPP:

XAMPP is one of the most widely used open source platform developed by Apache Friends. It is used to build software applications with concise, clean, and readable code base. XAMPP provides Apache, Tomcat, MYSQL, etc.

PHP:

PHP (Hypertext Pre-processor) is a server side scripting language that is embedded in HTML and including popular databases such as MYSQL, Oracle, Sybase etc. It manages dynamic content, databases, session tracking, even build entire E-commerce sites. PHP added support for Java and distributed

object architectures making n-tier development possibility for the first time [3].

HTML and CSS:

HTML (Hypertext Mark-up Language) and CSS (Cascading Style Sheets) are two of the core technologies for building web pages. HTML provides the structure of the page; CSS provides the layout, for a variety of devices. HTML and CSS with PHP is used to build a web app with a PHP.

MYSQL:

MYSQL is widely used open source database technology and data storage. MYSQL provides reliability, scalability and flexibility ease of use. MYSQL offers exceptional security features that benefits absolute data protection [3].

2) Important classes, function & libraries

Web application using AI Therapist is created by PyCharm Community 2019.2 having a GUI which contain following packages.

mysqli_connect():

This function is used to open a new connection to the MySQL Server. It includes parameters such as host, username, password, database name, port, socket.

session_start():

Creates new session and generate a unique session ID for the user. The PHP code in the example below simply starts a new session. If a session fails to start then, it returns false, else return true.

version_compare():

Here, it compares the two PHP–standardised version number strings. It is useful if one would like to write programs working only on some version of PHP. It includes some parameters such as PHP_Version, version sequence and greater than acceptable version range.

function generate_key():

Generate key function has been used to generate a random key from the inputted data by user by using shuffle function. This string is of length 16 bits. This 16 bits of string is known as key.

B. Software Requirements

1. Operating System: Windows 8
2. Software: XAMPP
3. Front-end: PHP
4. Back-end: MYSQL

C. Hardware Requirements

1. Processor: Minimum Pentium-IV
2. Hard disk:500MB
3. Memory: 128MB

6. Result Analysis

Cloud computing has drastically changed the way of storing the data in more secure way. SHA-512 is most important strategic algorithm that stores the data in the form of cipher text instead of plain text.

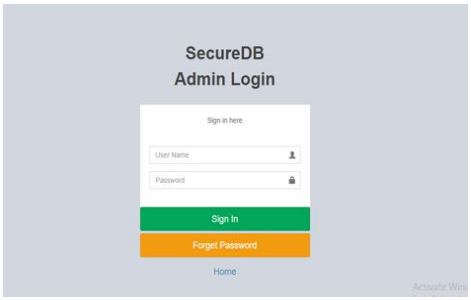

Fig. 2. Admin Login

The figure shows the admin login page where the admin has to login by using his/her login details.

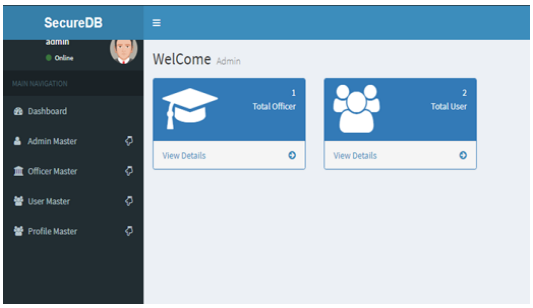

Fig. 3. Admin dashboard

The figure shows the Admin Dashboard which contains total number of officer, user those who have registered.

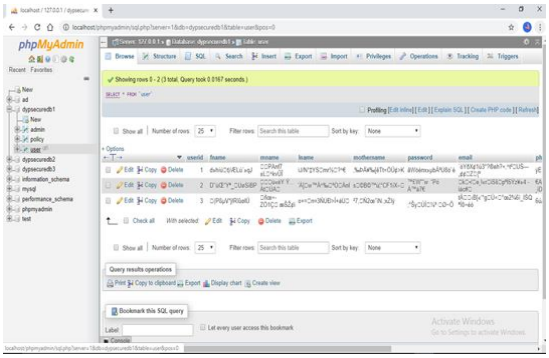

Fig. 4. PhpMyAdmin Database

The figure shows 3 databases and a user table where data is stored by applying vertical partitioning technique.

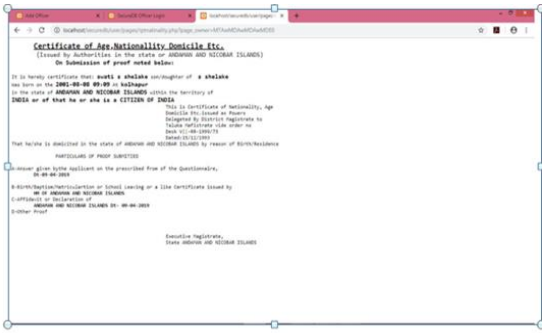

Fig. 5. Certificate generator

This figure shows certificate of nationality for authorized users. This certificate is visible to users those who have authenticated.

7. Conclusion

The web application refers proxy-less architecture. It is designed for analyzing high level of security and privacy. All the data which is provided by user is encrypted through cryptographic algorithms which allows the execution of standard SQL queries on encrypted data. Metadata is used to store the unique id and encryption key in encrypted format so the trusted third party access control to cloud data. Further work includes encryption algorithm for the user id and password sent by email to prevent the trusted party involvement.

References

[1] L. Ferretti, M. Colajanni and M. Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 437-446, Feb. 2014.
[2] https://www.jpinfotech.org/distributed-concurrent-and-independent access-to-encrypted-cloud-databases/
[3] https://www.tutorialspoint.com/php
[4] https://www.asp.net/aspnet/overview/developing-apps-with-windows-azure/building-real-world-cloud-apps-with-windows-azure/data-partioning-strategies