SECURE DATA SHARING IN CLOUD

Pooja Sagathia, Saylee Salgaonkar, Akshata Sawant, Hammad Shaikh

Department Of Information Technology

Xavier Institute Of Engineering, Mumbai, India.

Abstract - Cloud Computing is useful in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as user store sensitive information in cloud. This paper proposes a model to securely store information on cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that maintain data confidentiality ,integrity and availability. Our approach protects client sensitive information by storing data across cloud, using a secret sharing approach that uses Shamir's secret sharing key algorithm.

Index Terms - OwnCloud, Shamir Secret Sharing Algorithm, Ubuntu15.10

1. INTRODUCTION

Cloud computing has brought an innovative change in the IT industry. All the industries depend upon IT industry for managing and storing their business related data. Ensuring the security is considered to be the most critical issue that cloud service providers are facing, as users often share private information with the cloud blindly and they can not be sure that providers are trusted or not. There are many security vulnerabilities for CC as it combines many technologies including networks, databases, operating systems, virtualization, resource scheduling and memory management. Security issue faced by these systems are applied to cloud computing as well, therefore cloud providers should address security issues as a matter of high and urgent priority.Even though CC offers limitless flexibility, reliability, enhanced

This project is very useful to all the people in the society as well as the world. As everyone can store their data into the cloud and use the same in emergencies. This project is very easy to use and the users can also set their privacy as in with whom they want to share the data. The user can store data in form of text. Secret key algorithm provides secure cloud database that will prevent security risks. We apply Shamir's Secret Sharing algorithm in cloud that helps us to reduce risk of data intrusion and service availability for ensuring data.

1.1 Need of the proposed system

In college based system, a large amount of student data are involved, and student start to realize that they would completely lose control over their personal information once it enters the system. There are good reasons for keeping student data private and limiting the access. Proposed system will use key sharing algorithm for confidentiality.

Disadvantages of Existing System:

Privacy issues are not addressed adequately at the technical level and efforts to keep student data secure have often fallen short. The storage privacy in existing system is weaker form of privacy because it does not hide search and access patterns and systems assuring privacy and security to safeguard personal digital information.

Managing health care data is a tedious task for the college system. Storing this data on a cloud would resolve the issues and will reduce the maintenance cost. The existing solutions to ensure data privacy by data encryption is not sufficient just because the data has been encrypted the user's information can't be changed in the virtual machines of cloud providers. Administrator assume that if the data is processed and collected from different client then the data encryption cannot ensure privacy in the cloud.

2. PROPOSED SYSTEM

In this proposed system, we will create a web application of college management system implemented in cloud. This application will contain constraints like Admin & Users, where admin will logon into and upload the files on cloud, and users can login into to download the files they need to download where each user may receive limited no. of keys. Following user's need to combine the keys received to all the user in order to generate the secret key using certain mathematical combinations which will authenticate the user to download the files that will provide a very high level of security to the confidential files.

2.1 OwnCloud:

OwnCloud is a client-server software for creating file hosting services and using them. OwnCloud functionally very similar to the Dropbox, with the primary functional difference being that OwnCloud is free and open-source, and therefore allows everyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

OwnCloud Design:

In order for desktop machines to combine files with their OwnCloud server, desktop clients are available for PCs running Windows, OS X, FreeBSD or Linux. Files and other data (such as calendars, contacts etc.) can also be accessed using a web browser without any additional software. Any updates to files are pushed between all computers connected to a user's account.

The OwnCloud server is written in the PHP and JavaScript languages. For remote access, it employs sabre/dav, an open-source WebDAV server. OwnCloud is designed to work with many database management systems,including SQLite, MariaDB, MySQL, Oracle Database..

OwnCloud Features:

- Bookmarking
- URL shortening Suite
- Photo gallery.
- Video viewer.
- File storage in conventional directory
- Encryption of user files or data.
- Synchronization of clients running Windows (Windows XP, Vista, 7 and 8), OS X (10.6 or later), or Linux

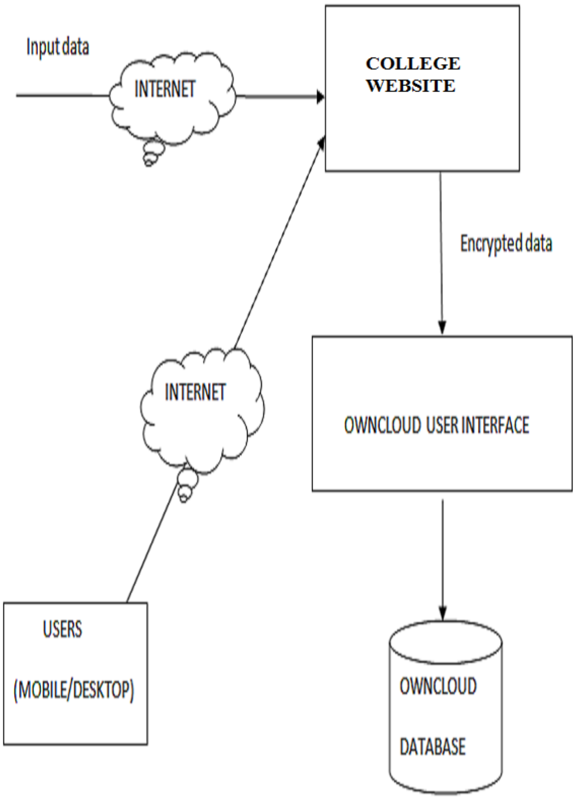

Fig.1 System Architecture

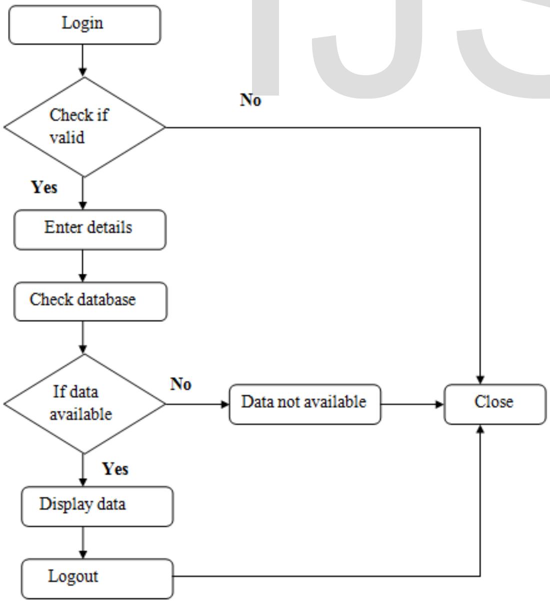

Fig.2 Flow Chart of the Proposed System

3. ALGORITHM

3.1 Shamir Secret Sharing Algorithm

Shamir's secret sharing, there is distribution a secret among a group of n participants, each of whom is allocated a part of secret. The strong point of this method is that the secret can be reconstructed only if a predefined number of shares are clubbed together; individual shares are of no use on their own, so anyone with less than t out of n shares has no extra information about the secret than someone that has 0 shares.

A. Basic Principle

This scheme consists of dealer and n players. The dealer is in charge of dividing a certain data D into n parts say, D1, D2, ..., Dn in such a way that:

- The knowledge of any t or more Di pieces makes the value of D known.
- A complete knowledge of t − 1 shares reveals no information about D (in the sense that all possible values are equally split). t should be less than n to keep the value of shares unconstructible and ensure that the intruder cannot access t pieces of data.
- Such a system is called a (t, n) – threshold. The value of factor t can be decided depending on the level of security we desire.

The use of a secret sharing scheme allows us to achieve confidentiality, guarantees to the stored data without using a key distribution mechanism which imposes sharing of a secret key.

B. Mathematical Implementation

Goal is to divide data D (e.g., the safe combination) into n pieces D1,D2….Dn in such a way that,

• Knowledge of any k or more D pieces makes D easily computable.

- Knowledge of any k -1 or less pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

- This scheme is called (k,n)threshold. If k=n then all participants are required to reconstruct the secret.

- Suppose we want to use (k,n) threshold scheme to share our secret S where k < n.

- Choose at random (k-1) coefficient a1, a2 ,a3…ak-1 , and let S be the a0

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots.. + a_{k-1}{}^{k-1}$$

- Construct n points (i,f(i)) where i=1,2…..n

- Given any subset of k pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S , which is the secret.

- In order to reconstruct the secret any 3 points will be enough

- We will compute Lagrange basis polynomials:

$$l_0 = \frac{x-x_1}{x_0-x_1} . \frac{x-x_2}{x_0-x_2}$$

$$l_1 = \frac{x-x_0}{x_1-x_0} . \frac{x-x_2}{x_1-x_2}$$

$$l_2 = \frac{x-x_0}{x_2-x_0} . \frac{x-x_1}{x_2-x_1}$$

Therefore,

$$\sum_{j=0}^{2} y_j \, l_j \,(x) = a_0 + a_1x + a_2x^2 + \ldots a_{k-1}^{k-1}$$

Recall that the secret is the free coefficient, which means that a0 = secret, and we are done.

ACKNOWLEDGMENT

We are thankful to our Project Guide Prof. Jaya Jeswani, and all staff members of IT department who have provided us various facilities and have guided us whenever required. We would like to express my heart-felt gratitude towards our parents and all those who encouraged us to accomplish and supported us in our work.

REFERENCES

[1] https://en.wikipedia.org/wiki/cloud computing

[2] http://www.owncloud.com/

[3] Vijaya Pinjarkar, Neeraj Raja, Krunal Jha, Ankeet Dalvi, “Single Cloud Security Enhancement using key Sharing Algorithm,” *Recent and Innovation Trends in Computing and Communication*, 2016.

[4] V. Vankireddy, N. Sudheer, R. Lakshmi Tulasi, “Enhancing Security and Privacy in Multi Cloud Computing Environment,” *International Journal of Computer Science and Information Technologies*, 2015.

[5] Rajesh Shah, Makhan Kumbhkar, “Cloud-Based College Management Information System for Autonomous Institute,” *International Journal of Advanced Research in Computer Science and Software Engineering*, 2015.