SECURE DATA SHARING AND REMOTE ACCESSING OF FILES USING CLOUD

Pooja Awasare[1], Priya Bansode[2], Pankaj Dandge[3],

Aishwarya Kudale[4], Seema Shabadi[5]

Computer Engineering RSCOE,

Savitribai Phule Pune University, Pune (India)

ABSTRACT

Cloud is being used by much type of users to fulfill their storage needs and sharing requirements. Cloud is one of the emerging techniques in today's era. As there are many cloud service providers in industry it is extremely easy to avail cloud storage. But while doing so users compromise security and privacy of data willingly or unwillingly as these cloud storage services are not very proficient when it comes to data security. We are proposing a system that can overcome these issues. Our system introduces encryption for security of data. As data is stored in encrypted form it will be hard for cloud storage owners also to decrypt the data. By doing so some other problem arrives like searching becomes impossible. For that we are maintaining a keyword database that will be used when user search for a file. User can see graph that will show categories of documents uploaded on cloud. Storage usage on cloud will be traced. There is another unique feature of our system. If user enters # with correct password, system will prevent user from accessing any files and SMS will be sent to emergency contacts of user.

Keywords: Cloud Storage: Access Control, Authentication, Database Processing, Privacy, Security Unauthorized Access (e.g. Hacking).

I. INTRODUCTION

Cloud as an emerging technique in today's era is being used by many types of users to fulfill their storage needs along with sharing requirements. Now days, it is extremely easy to avail cloud storage, due to abundant availability of cloud service providers. But on the other hand, these cloud storage services are not very proficient when it comes to data security and the users have to compromise security and privacy of data. . We are proposing a system that can overcome these issues. Firstly our system introduces encryption for security of data .It will be hard for cloud storage owners also to decrypt the data, as data is stored in encrypted form. Due to such things, some other problem arrives like searching becomes impossible. For that we are maintaining a keyword database that will be used when user search for a file. User can see graph that will show categories of documents uploaded on cloud. Storage uses on cloud will be traced. There is another unique feature of our system. If user enters # with correct password, system will prevent user from accessing any files and SMS will be sent to emergency contacts of user.

II. RELATED WORK

Protecting user’s data is an essential task in current systems. Researchers are proposing approaches and solutions to maximize the confidentiality of user’s data. Study of different types of algorithm like AES, RSA, Blowfish and distinguishing between them to recognize which algorithm is best suitable for our system. In the first paper,the proposed system is a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security. These parameters provided us a better assessment of AES for increasing security [1].

The second paper,presents the implementation of RSA through an encryption and decryption procedures, which are readily available for commercial use. Experiments were conducted on different text sizes. The results obtained in encryption and decryptions of RSA were given in seconds [2].

In the third paper, proposed scheme is used to provide for enhancing security on the cloud server. For this we use Blow-fish and MD5 as a hybrid security mechanism. Encryption and decryption is done by Blowfish and MD5 is used for data digestion form which enhances the security .From this we learned the blowfish approach for data security [3].

In the fourth paper, the performance characteristics of RSA are observed by implementing the algorithm for computation. In this paper, RSA was implemented through an asymmetric key algorithm, encryption and decryption procedure over different key size [4].

In the fifth paper, they have proposed an efficient and secure cloud computing framework which support security for the cloud users and data control is being provided at the cloud user side. The cloud user can use the privilege of inter cloud communication with the data security of AES and RSA security hybridization which will provide four key security. The encryption is provided by the server. Then the receiver cloud can view the request file by applying the four keys. If any malicious behavior is identified before the cloud user read operation then our document identification bit alert the client and server for the possible attack. So this framework supports secure data inter communication with malicious identification also.In this paper we have designed a secure user cloud framework with the help of AES and RSA algorithms. Our approach provides an authenticated way of entering the cloud user and provides inter clod communication virtualization environment. For data security in inter cloud communication AES and RSA capability are used as the four key security. The key control with the user side protection is the main benefit of our dissertation. Then we have provided the data identification bit control for controlling any malicious behavior detection [5].

III. SYSTEM ARCHITECTURE

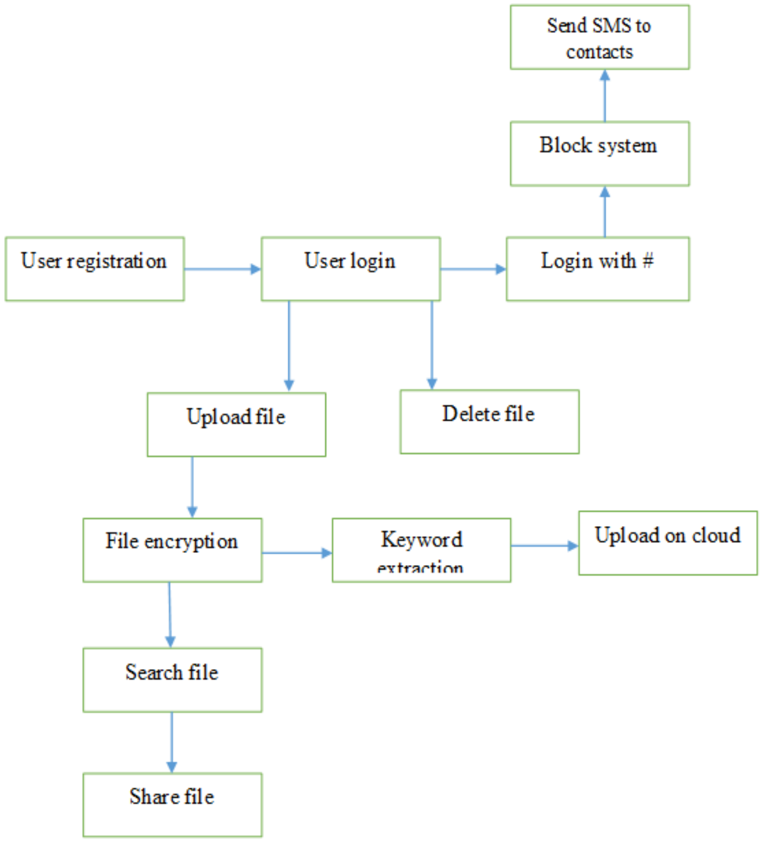


Fig: System Architecture

As shown in system architecture

First step is that user needs to register to our system using email-id, mobile number and password. After the registration process is completed user can login to the system upload a particular file or delete a file. While uploading a file encryption takes place. Keyword extraction is done and is uploaded on cloud. Moreover we can search for a particular file using keyword search functionality and also share the file to other user. We are using one more unique functionality that is if we press # symbol after the correct password our system gets blocked and sms is send to our registered mobile number.

In our project we use AES, DES and Hibernate. Hibernate is an object relational mapping tool for the Java programming language. We have used hibernate for mapping an object oriented domain model to relational database. And also mapping of Java data types to SQL data types is done. Hibernate also provides data query and retrieval facilities. We create an hibernate application in eclipse IDE for mapping database in our project .we also use AES and DES algorithm to encrypt and decrypt data securely.This algorithm may create separate key to encrypt and decrypt data securely.

IV. MODULES

4.1 MODULE 1- Data Owner

Input to module – {user ids, files}

Output from module – {encrypted files, keys}

It contains following steps

a) Account Creation

b) Upload data

c) Encrypt data

d) Exchange keys

(a)Account creation

Data owner will create an account where users can access their data.

(b)Encrypt Data

In this module Data owner will encrypt data with a security key.

(c)Upload Data

In this module encrypted data is uploaded from data owner to the cloud. (Data is outsourced to cloud).

(d)Exchange keys

In this module data owner will share/exchange keys with CSP (Cloud Service Provider) and User.

4.2 MODULE 2- User

Input to module – {user details, user id}

Output from module – {decrypted files}

It contains following steps

a) User Registration

b) Login

c) Uploading documents

d) Downloading documents

e) Sharing documents

f) Decrypt the file

(a)User Registration

In this module new user register the information in order to use the cloud for accessing files Uploaded by DO (Data Owner).

(b)Login

In this module user can login by using his/her username and password.

(c)File Access Request

In this module each user can request for accessing the file and requirements to the cloud service provider.

(e)Download

In this module each user can download encrypted data/ file from cloud service provider.

(f)Decrypt the file

In this module user will request for keys and then after achieving a desired threshold, he/she can decrypt the file successfully.

4.3 MODULE 3- Cloud Service Provider

Input to module – {encrypted files}

Output from module – {authorized file access}

It contains following steps

a) Save Data

b) Update meta Lists

c) Send data

(a)Save data

In this module CSP will receive data/bundle from data owner and decrypt the bundle using DO’s public key. The data received from DO is saved on cloud.

(b)Update Meta Lists

In this module CSP separate out the bundle by decrypting the outer encryption and will update various lists such as file lists etc.

(c)Send data

In this module CSP will accept requests from users and will provide requested data (encrypted data) to corresponding user.

System Block Functionality

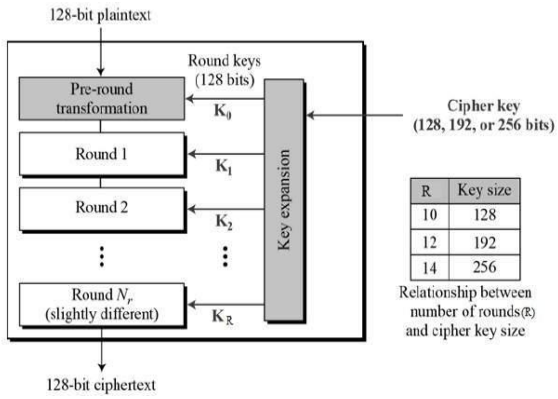
To provide emergency functionality to the users, if anybody force user to login to the system, and if user type # after correct password then system will block and SMS will send to registered contact numbers.

V. EXPERIMENTAL ENVIRONMENT AND METHODOLOGY

5.1 AES

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.In our project we have used AES for encryption and decryption purpose.The advantages of

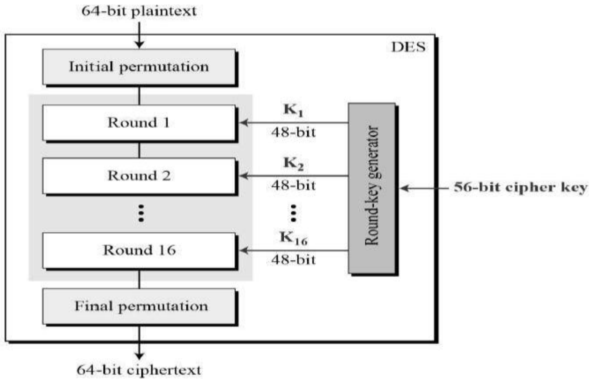
AES are many. AES is not susceptible to any attack but Brute Force attack. However, Brute Force attack is not an easy job even for a super computer. This is because the encryption key size used by AES algorithm is of the order 128, 192 or 256 bits which results in billions of permutations and combinations. High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware; from 8-bit smart cards to high-performance computers. AES is also much faster than the traditional algorithms; therefore in our work AES is adopted recently Compact AES S-box is developed to be more efficient.



5.2DES:

The **Data Encryption Standard** is a symmetric-key algorithm for the encryption of electronic data. Although now considered insecure, it was highly influential in the advancement of modern cryptographies.DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

According to our project, Users first enter a password parameter and keep it. The key generated from the password parameter. Then users select the data file that need to be encrypted. According to DES algorithm and the generated key, thesystem encrypts the data file. When users need the encrypted data, select corresponding cipher text file and simultaneously enter the reserved password parameter, the system will perform the appropriate decryption operation.



5.3Hibernate

it is an object relational mapping tool for the Java programming language. We have used hibernate for mapping an object oriented domain model to relational database. Hibernate solves object relational impedance mismatch problems by replacing direct persistent database access with high level object handling functions. Using this mapping of Java classes to database tables is done using Java Annotations. And also mapping of Java data types to SQL data types is done. Hibernate also provides data query and retrieval facilities. It generates SQL calls and retrieves the developer from manual handling and object conversion of result set.

We createahibernate application in eclipse IDE using following steps

1. We created the java project

Create the java project by **File Menu** - **New** - **project** - **java project.**

2. Added jar files for hibernate

Selected all the jar files and opened it.

3. Created the Persistent class
4. Created the mapping file for Persistent class
5. Created the Configuration file

   The configuration file contains all the information's for the database such as connection_url, driver class, username, password etc. The hbm2ddl.auto property is used to create the table in the database automatically.

6. Created the class that retrieves or stores the persistent object

In this class, we are simply storing the object to the database.

7. Used this for running our project

VI. EXPERIMENTAL RESULT

Main objective of the system is to provide easy searching of document on cloud, because when users upload some document on cloud some time it is difficult to find out itself by user. So system provides keyword database functionality for searchingparticular file. System generates graphical format of uploaded documents which shows type of documents. There is functionality, if anybody force user to login to the system, and if user type # after correct password then system will block and SMS will send to registered contact numbers. User is able to Search file, Upload file, Download file using this system with security and easy search method.

VII. CONCLUSION

In this paper, we proposed that system provides solution for achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud. Hence the data remain information-theoretically secure against the Cloud provider and other malicious users. In this technique searching of files is managed by the system it provides Graphical representation of file types and the secure sharing of data are provided.

VIII. ACKNOWLEDGEMENT

We would like to acknowledge the guidance of Ms. S. A. Shabadi for her insightful support and inspiration throughout the various stages of this paper. We sincerely appreciate the help and advice given by her which went a long way in helping us understanding the key concept of this paper.

REFERENCES

[1] Enhancing Cloud Computing Security using AES Algorithm.

[2] An Efficient data storage security algorithm using RSA Algorithm.

[3] Data Security in Cloud Computing Using Various Encryption Techniques.

[4] SECURE CLOUD ENVIRONMENT USING RSA ALGORITHM.

[5] A hybrid security approach based on AES and RSA for cloud data.