Third partyAuditing and verifying the cloud storage

Team(7)

Akshay Tak
Student Number(x16110234)

Mohammed Farooq(x16105583)

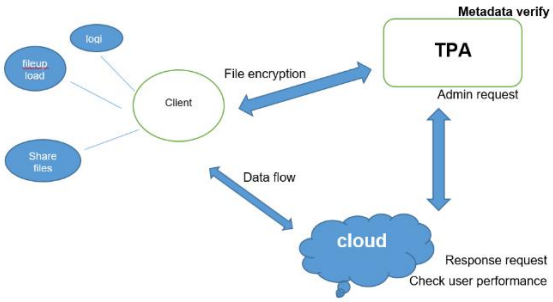
Abstract

This application is a third party auditing service which enhances the security and eliminates the key exposure in cloud application. The TPA helps the client to complete a high security file upload and download with transparency in the key updation. Thus inclusion of a third party auditing will eliminate the burden on the client's side. Thus TPA will generate a highly encrypt class of the key which is private key of the client. The client can authenti- cate the encrypted private key. This key updation will en- able the users to validate and verify the secret keys provid- ed by the TPA. This is a feature which helps in implement- ing safe and clear auditing for the users or the clients.

INTRODUCTION

Today cloud computing is a new platform for the internet users, It is becoming more and more popular and user friendly in the field of telecommunication and multimedia . As the cloud computing is expanding to millions of users with unlim- ited resources and promising furthermore, however cloud computing is providing unlimited storage to users . As one of the most important services of cloud computing is viewed universally by cloud storage and cloud infrastructure with services. all though it provides great benefits to end users. Hence it leads to very important security challenges. Identify- ing and finding proper solution of this problem is very impor- tant as data stored in cloud can become more susceptible or vulnerable. Thus applying necessary security measures with advanced techniques may help the one of the important security problem is to efficiently check the integrity of the stored data in the cloud. The several outcomes are privacy protection of the stored data and many dynamic data operations and sharing. However the cloud needs to satisfy the security loopholes and maintain the necessary security aspects. The failure in this aspect may lead to a huge loss in data and breach of security. Thus our application provides security to the transaction through the third party application. This application TPA encrypts the files and secures the con- tent. The file security has been done through the secret key provided by the application.

ARCHITECUTRE GOALS AND CONSTRAINTS



Modules :

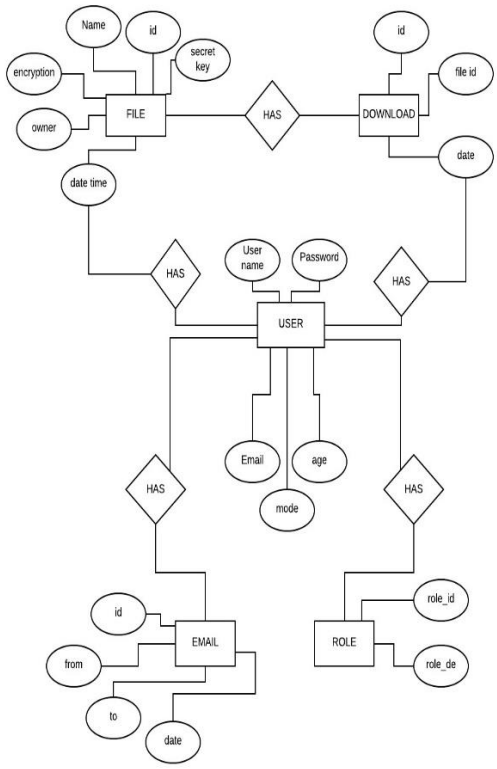
Setup: The working of the algorithm takes place in such a way that when the algorithm takes an input a security criterion/parameter Ck which returns two keys such as a public key and a Master key as Pk and Mk respectively. The Master key Mk generates a secret key for the user and the Pk is used for encryption by the message sender .

Encrypt : For the successful Encryption and generated output cipher text CT , the input parameter such as Pk , Message M and a access Structure T is used by the algorithm.

Key-Gen : This algorithm functions when the Master and secret key Mk feeds value to the master secret key Mk generating a secret key key Sk that enables the user to decrypt a message with the access tree T if only it matches the T.

Decrypt : In this algorithm for an attribute set the cipher text CT and the secret key SK feeds an output which enhances the performance over the disadvantage of the private key. So an user only use this set of attributes to satisfy the access structure in the encrypted data. This in case of KP-ABE enhances the access control which in addition makes the users private key a set of the attributes that satisfies the given structure along with the encrypted data.

ER diagram:



Architecture compliance

Minimum 3 tier arch a system should involve they are

PRESENTATION TIER

The presentation tier is an interface between the system and user . The interface should be a common web application that is accessible by commercial web browsers such as mozilla firefox ,chrome which should be run on ios , windows ,android .The interface must be light in the clients device and should be accessible anywhere anytime .

APPLICATION TIER

In the application tier the programming functions , business logics , module or processes are stored . The program coding should be clean , efficient and well documented .

DATABASE TIER .

In this tier the data is stored related to system and rhe application . There should be full backup and stored regularly .

Design:

The TPA application consist of the following tier .

For web application tier The Spring Frame work is used :

The application consist of four layers:

Main controller: the controller layer is used to add data into the presentation layer And navigate the pages asper requested

2 DOA layer: the data acess object layer is used to perform the database logic operation . by mapping the application calls to persistence layer the dao provides some specific data operations and without exposing the details of the database

3 Entity layer: this layer is the main entry point for accessing the database object the object service is responsible to materialized which process the data conversion which is returned from the entity client

4: Service Layer: the service layer is used to writing the business logic operation which abstracts the business logic and the data success. It can support multiple presentation layers.

Design aspects:

The spring framework is an application framework for java platform. It provides functions such as inversion of control for java application.

Features:

1)Spring web framework consists of a MVC frame work which is used in this application. Its use can eliminate number of patterns and factory classes.

2)Spring framework is both complete and modular, because spring framework has a layered architecture.

The spring framework in this application uses layered architecture. Its properties also includes modular and complete behavior.

Hibernate:

Hibernate is the framework for java that simplifies the development with the interaction with the components of the data base .Hibernate being open source is a mapping tool for relation databases .

An ORM is used to manipulate data and data access. It is a good programming technique that maps the object to the data stored in the database

This mapping tool simplifies the manupulation of data in it for activities such as data creation , addition , deletion and editing . In this programming this technique maps the object .

Features:

In the context of natural programming model the hibernate uses number of functions such as :

1) Polymorphism
2) Inheritance
3) Java collection framework
4) Composition

In case of thid application hibernate provides us with the necessary scalability. It provides a multi layered cache architecture which is used in cloud cluster.

Hibernate give a proper insertion and extraction of objects from the database making the tasks more simplier.

. The use of enterprise java beans provides the very much needed persistence between the API and query language.

Hibernate is important because it provides a persistence as a service instead of the framework which in case integrates various application architecture.

Library description:

Manifest-Version: tpa-util-1.0.0-SNAPSHOT
Created-By: Mohammed farooq
Name: java/util/
Specification-Title: Java Utility Classes
Specification-Version: 1.0.0
Implementation-Title: tpa.util

Jar methods	description
Public Boolean audit file path(String path,String Key words)	This method Sets up the file path and traverse the file content line by line and identifies the keywords and returns the condition either true or false
Public string encrypt(String,String)	This method encrypt the given string by using AES Algorithm And returns Encrypted key
Public generate SeceretKey()	This method generates random seceret key for encrypted string and reaturns a key
Public string decrypt(String String)	This Methods decrypts the encrypted key to original string

Manifest-Version: tpa-util-1.0.0-SNAPSHOT
Created-By: Akshay tak
Name: java/util/
Specification-Title: Java Utility Classes
Specification-Version: 1.0.0
Implementation-Title: email.util

Jar methods	Description
Public static setCardentials(String,String)	This methods sets username password of user
Public void generate And send email Gmail	This method sets mail body to send mail

External JAR used.

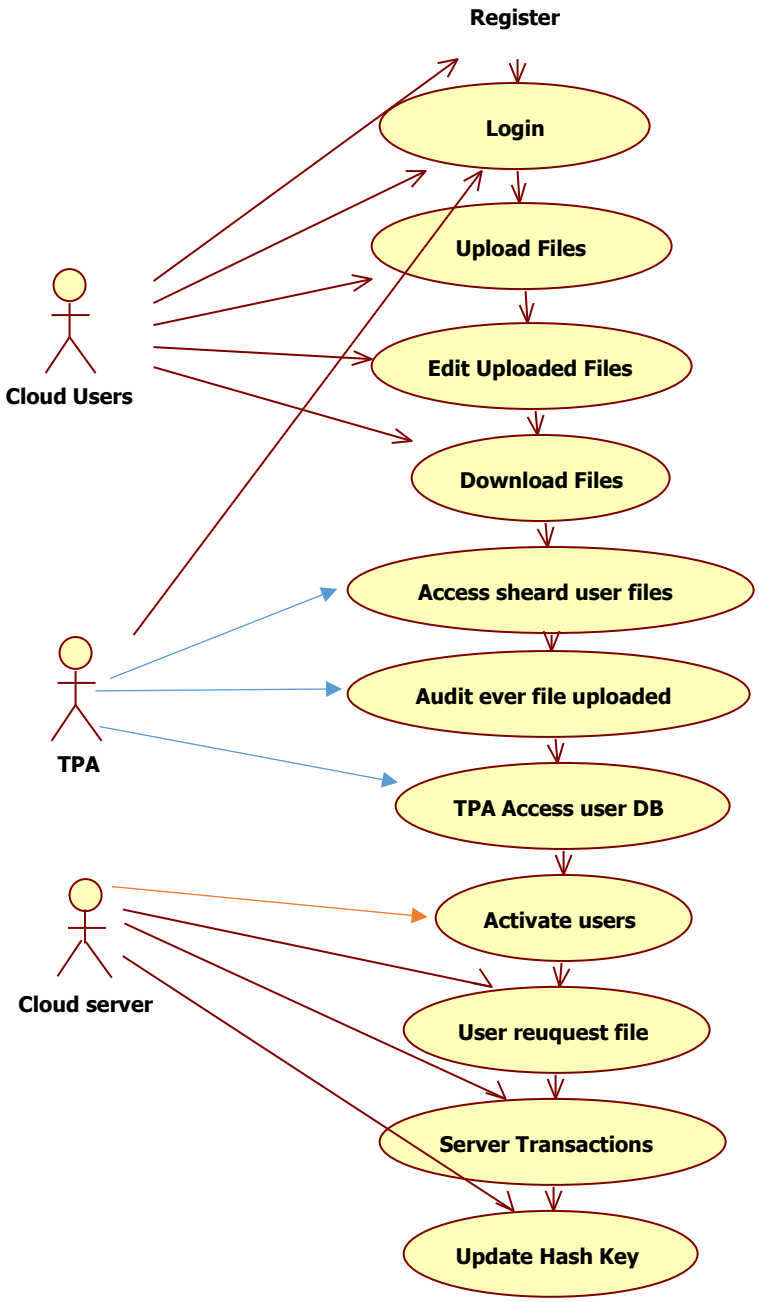
Jar methods
Mysql-connector-5.1.9
hibernate-core-4.2.2.Final.jar
junit-4.12.jar
spring-beans-3.2.3.RELEASE.jar
spring-security-core-3.0.5.RELEASE.jar
Standard.jar
commons-codec-1.10-javadoc.jar
spring-jdbc-3.2.2.RELEASE.jar
spring-web-3.2.9.RELEASE.jar
spring-webmvc-3.2.9.RELEASE.jar
Jxl.jar
Javassist.3.12.1.GA.jar
Gson-2.2.2.jar

IMPLEMENTATION:

IMPLEMENTATION (DEVELOPMENT VIEW)

Web and application tier/ Spring framework
Spring frame work enhances and provides a comprehensive programing and configuration
Model for the java based applications can be deployed on any platform.

UML diagram:



USE CASE VIEW

Important use case scenarios

The various functionalities are proposed based on the role defined.

CLIENT OUTFLOW .

- Register user account
- Login to their account
- Check their uploaded files
- View their uploaded files
- User can view their files
- User can download their files
- User can modify files
- Can view multiple user files.

TPA OUTFLOW

- TPA checks the user uploaded files
- Sends the Request to admin for the TPA

CLOUD FLOW

- Check the user shared files
- Response to request of the TPA
- Check user details
- Can check user performance and
- Generates reports via charts

Important use case scenarios

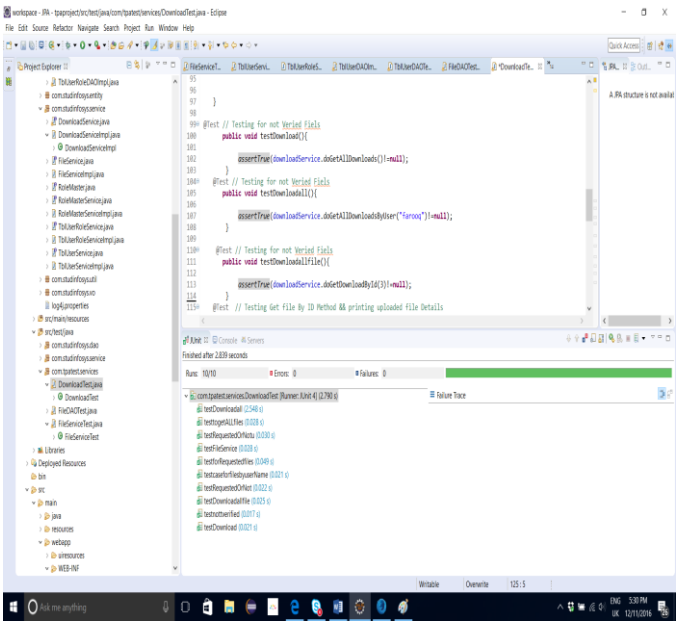
The various functionalities are proposed based on the role defined.

TEST ENVIRONMENT:

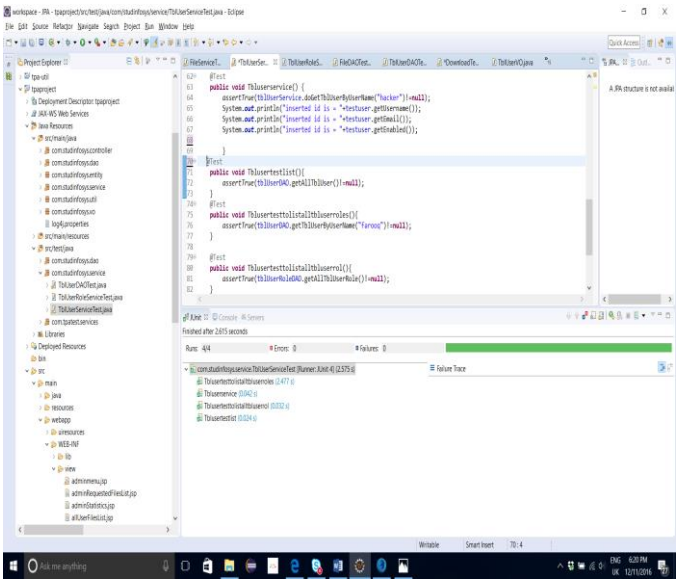
Junit testing:

J unit testing refers to the java development's testing framework. J unit help the developer to develop test driven approach for the development which allows him to eliminate the errors and overall enhance the output and performance of the program. It is a test-driven development. This testing approach is collectively also known as X unit. In java programming the unit is linked with JAR at the time of compilation.

Testing cases by Mohammed farooq.



Testing cases by Akshay Tak



DESIGN PATTERNS:

The application consists of the following design patterns.

1)Dependency injection.
2)composite entity pattern
3)Singleton
4)MVC

The application consists of four different layers .
1)Entity layer
2)Dao layer
3)Service layer
4)Main controller

Design patterns are the best way software development using object oriented programming concepts. It enhances the performance of the software and its output.
The use of design patterns defines the type of reusable objects and classes.
There are number of design patterns that are used to set and develop a program in a sequential a manner and a more emphasized object oriented programming.
The design patterns used in this project are the singleton pattern and the dependency injection. We will have a detailed view of both the design pattern.

Dependency injection

The dependency injection is a design pattern which holds the functionality such as inversion control for further resolving the dependencies. Here dependency can be defined as an object which the injection s the passing of an dependency object.
It is a very useful technique for testing where different objects collaborate to each other for executing a particular task.

Singleton

The single pattern is believed to be the most simplest and favorite design patterns of developers. The singleton pattern is responsible for the instances. In the same time it provides a global point of access to the particular instance. In this case the same instance can be used from number of ways which makes it impossible to invoke directly the constructor each time.

The Singleton design pattern addresses all the concerns in the application which allows the user to :
1)At a time one instance is created of a particular class.
2) Object have the global point of access
3)Allow multiple instances in the future without affecting a singleton class's clients.
4)The number of multiple instances are allowed which cannot make or change the singleton class clients.

MVC architecture pattern:
The MVC framework is used in this particular application to implement the user interface. the source code can be differentiated into three different layers. Model View and Control : The Development in model view control helps to organise all the programming content while developing . The MVC in this application has helped the developers to maintain and develop in three different layers which allows The MVC framework is used in this particular application to implement the user interface. the source code can be differentiated into three different layers. Model View and Control : The Development in model view control helps to organise all the programming content while developing . The MVC in this application has helped the developers to maintain and develop in three different layers which allows

SYSTEM REQUIREMENTS :

- Front end technologies: HTML5 , CSS3 ,javascript
- Back end technologies: java, jdbc, hibernate, jpa, spring
- Application servers: Tomcat
- Operating systems: windows 10/ Linux / mac
- Hardware: 4gb RAM , 40gb memory , intel dual core processor

Deployment:

The web application is hosted on open stack server .
Application server used is tomcat server.
Application URL : http://87.44.4.147:8080/tpaproject/login

Conclusion:

In this paper , we thoroughly examined about the key factors that are responsible for the data security on cloud storage while uploading and downloading a file. In this project we also propose the cloud auditing protocol with the verifiable outsourcing of key updates. Here the whole process is trans-parent to the client . In addition here the TPA project can only be able to see the clients version of secret key whereas the client will be able to use the encrypted key at the time of downloading his content from the TPA. Hence here we offer the general security and this proposed scheme is used for better preformance and simulation.

REFERENCES

1) wikipedia
2) http://ieeexplore.ieee.org/document/7404239/
3)Ace theme template for (UI)
4)AES Algorithm used
5)Email methods used from internet