

A project report on

**Practical constructions protection mechanism for control of web-based
cloud computing services**

Submitted in partial fulfilment of the requirement
For the award of the degree

MASTER OF COMPUTER APPLICATION

Of



Visvesvaraya Technological University
Belgaum, Karnataka

By

ATHIRA S

1CR18MCA55



CMR INSTITUTE OF TECHNOLOGY

132, IT Park Road, Kundalahalli, Bangalore-560037

2019-2020

A project report on

**Practical constructions protection mechanism for control of web-based
cloud computing services**

Submitted in partial fulfilment of the requirement

for the award of the degree

MASTER OF COMPUTER APPLICATIONS

of

Visvesvaraya Technological University
Belgaum, Karnataka

By

**ATHIRA S
1CR18MCA55**

Under the guidance of

Internal Guide

Dr. V. Ilango

Professor, MCA Department,
CMR Institute of Technology,
Bangalore.

External Guide

Mr. Pavan Kumar

DIGIADD Technologies
Bangalore.



CMR INSTITUTE OF TECHNOLOGY

132, IT Park Road, Kundalahalli, Bangalore-560037

2019-2020

CMR INSTITUTE OF TECHNOLOGY
Department of Master of Computer Applications
Bangalore - 560 037



CERTIFICATE

This is to certify that the project work entitled

**Practical constructions protection mechanism
for control of web-based cloud computing
services**

*Submitted in partial fulfilment of the requirement
for the award of the degree of
Master of Computer Applications of the Visvesvaraya
Technological University, Belgaum, Karnataka
bonafide work carried out by*

ATHIRA S
1CR18MCA55

during the academic year 2019-2020.

Dr. V. Ilango
Professor, MCA

Professor Gomathi.T.
HOD, MCA

Dr. Sanjay Jain
PRINCIPAL, CMRIT

External Viva

Name of the Examiners

1.

2

Signature with date

DIGIADD

Technologies

CERTIFICATE OF COMPLETION

This is to verify that Ms. ATHIRA S (1CR18MCA55) a bonafide student of CMR INSTITUTE OF TECHNOLOGY, Bangalore has successfully completed her internship on project domain "Cloud Computing" and titled "Practical constructions Protection Mechanism for Control for web-based cloud computing services" under the guidance and supervision of Mr. Pavan Kumar Technical Head, Digiadd Technologies Bangalore, from 15th Jan 2020 to 13th June 2020 in partial fulfillment for the award of Master of Computer Applications (MCA) from Visveswaraya technological University, Belgaum.

"We wish her all the best in her future endeavors"

Mr. Sridhar p

DIGIADD TECHNOLOGIES
Yes Complex # 19/3&4, 2nd Floor
Dinnur Main Road, R.T. Nagar Post
(H. Manager) 560 032

DECLARATION

I, **ATHIRA S**, student of 6th Sem MCA, **CMR Institute of Technology**, bearing the USN 1CR18MCA55, hereby declare that the project entitled “**Practical constructions protection mechanism for control of web-based cloud computing services**” has been carried out by me under the supervision of External Guide **Mr. Pavan Kumar**, Project Manager, and Internal Guide **Dr. V. Ilango**, Professor, Dept. of Master of Computer Applications and submitted in the partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications by the **Visvesvaraya Technological University** during the academic year 2020. The reports have not been submitted to any other University or Institute for the award of any degree or certificate.

Place: Bangalore

Date:

ATHIRA S

(1CR18MCA55)

ACKNOWLEDGEMENT

I would like to thank all those who are involved in this endeavor for their kind cooperation for its successful completion. At the outset, I wish to express my sincere gratitude to all those people who have helped me to complete this project in an efficient manner.

I offer my special thanks to my external project guide Mr. Pavan Kumar, Project Manager, DIGIADD Technologies, Bangalore, and to my Internal Project guide Dr. V. Ilango, Department of MCA, CMRIT, Bangalore without whose help and support throughout this project would have not been this success.

I am also thankful to Dr. SANJAY JAIN, Principal, CMRIT, Bangalore for his kind support in all respect during my study. I would like to thank Mr. Pavan Kumar, Project Manager, DIGIADD Technologies, Bangalore who gave opportunity to do this project at an extreme organization. Most of all and more than ever, I would like to thank my family members for their warmness, support, encouragement, kindness and patience. I am really thankful to all my friends who always advised and motivated me throughout the course.

ATHIRA S

(1CR18MCA55)

S.NO.	Contents	Page No.
1.	Introduction	
	1.1 Project Description	1
	1.2 Company Profile	2
2.	Literature Survey	
	2.1 Existing System and Proposed System	3
	2.2 Feasibility Study	4
	2.3 Tools and Technologies Used	7
	2.4 Hardware and Software Requirements	12
3.	Software Requirement Specification	
	3.1 User Class and Characteristics	13
	3.2 Functional Requirements	18
	3.3 Non- Functional Requirements	19
4.	System Design	
	4.1 System Perspective	20
	4.2 Context Diagram	21
	4.2.1 Data flow diagram of authority	23
	4.2.2 Data flow diagram of trustee	24
	4.2.3 Data flow diagram of user	25
5.	Detailed Design	
	5.1 Use Case Diagrams	26
	5.1.1 Use case diagram for authority	26
	5.1.2 Use case diagram for trustee	27
	5.1.3 Use case diagram for user	28
	5.2 Sequence Diagram	29
	5.3 Activity Diagrams	30
	5.4 Class Diagram	

	5.4.1 Class diagram for authority	31
	5.4.2 Class diagram for trustee	32
	5.4.3 Class diagram for user	33
6.	Implementation	
	6.1 Screenshots	34
7.	Software testing	39
	7.1 Testing Approaches	40
	7.2 Test Cases	46
8.	Conclusion	49
9.	Future Enhancement	50
10.	Bibliography	51

CHAPTER 1

INTRODUCTION

1.1 PROJECT DESCRIPTION

Information sharing is getting generous consideration in distributed storage for data correspondence innovation, distributed storage is giving proficient and successful stockpiling administrations. Overseen, worked and kept up on a capacity server that are based on virtualization strategies. Information that must be classified those are delicate must be ensured by methods which as a rule apply cryptographic calculation. Information sharers are confronting issue while the information is moved during the information sharing. The cryptographic key test how it very well may be forestalled are. An instrument is utilized for security of distributed storage from lose of the information. The functional development assurance system for ensuring the administration utilized. 1) Two factor assurance is utilized in cryptographic key. One of the components must work, at that point cryptographic key calculation can be held. 2) Re-encryption strategy for giving intermediary and procedures used to key division can be utilized to disavow the cryptographic key for coordinating effectively. 3) The information can be grained in fine approach to ensure and adjust the method of encryption of information.

Driven by highlights and favourable circumstances of the distributed computing administrations, the distributed computing-based application in industry and exploration network they are increasing more impulse on improvement and organization. Distributed computing is a utility processing, since it shares gigantic information the information sharing interest is high. The enormous information that are shared on the double is cost-expending task, the assets can be brought together or a disseminated PC framework. The mutual information cost could be diminished with assistance of distributed storage, secure information the board activities.

In cloud information sharer can transfer the information and afterward get to one side. Subsequent to transferring the document information sharer can get the information. Not just sharing of information is done tossed distributed storage It as likewise presented the odds of sharing the information without approval. Cryptographic plans are constantly utilized secrecy of the mutual information.

1.2 COMPANY PROFILE

DIGIADD Technologies is one of the leading organizations in India, engaging in the field of application development based on web, software and embedded in Bangalore. The organization contains the best in class infrastructure, consulting and out sourcing, training facilities, and experienced research and development team for corporate sectors.

The organization look past the conceivable by Customer Focus, Speedy conveyance, Quality execution moderate estimating and in addition we give extraordinary concentration towards our client relationship. We have customers extending from little new businesses requiring essential web nearness to enormous associations requiring complex programming and web applications. We are resolved to give best quality arrangement all the time by investigating the necessities.

The mission is to furnish our customers with practical, world-class web administrations without settling on quality. In light of your individual necessities be they of a little organization, an individual undertaking or a bigger business gathering – we offer the office of having special, in fact productive, and powerful plans to augment the effect of your site.

The group of experienced Software Developers, Embedded Engineers and Best in class mentors. We have grown more than 6000+ Innovative venture ideas, 300+ sites, programming applications and portable applications as a group.

CLIENTS AND PARTNERS

- † Fillet
- † JVS
- † MEKSOL India
- † Sunrise
- † Avviant
- † Infosensys
- † GOLSEN TRAVELS
- † Pro-Shrine
- † WIG Designs
- † Scepter

CHAPTER 2

Literature Survey

2.1 EXISTING AND PROPOSED SYSTEM

Existing System

In a mutual cloud condition like emergency clinics, the brought together framework may be utilized by various specialist state An and B taking a shot at rotational movements. Put away delicate information are inclined to hazard which are close to home. In these cases, client mystery keys cloud is effortlessly taken or utilized by an unapproved party. At the point when the PC is bolted by a secret key, it very well may be taken by undetected malwares. The security issue can be abrogated by two-factor validation (2FA). In electronic e-banking administrations 2FA is normal. Notwithstanding a username/secret word, the client is additionally required to have a gadget to show a one-time secret word. Cell phone is utilized to give onetime secret word while the cell phone gets SMS to the enlisted number for login process.

Utilizing the secret word frameworks are bolted, the common information can be speculated or taken by undetected malwares. Making sure about the information which are share by information sharers should be possible by two-factor verification (2FA) which is generally utilized in online e-banking administrations to make sure about the information. Notwithstanding a username/secret key, the client is likewise required to have a gadget to show a one-time secret key. A portion of the administrations demand client to contain the enrolled cell phone while login with the goal that one-time secret phrase is sent to the cell phone through SMS and the client can login and utilize the administration.

Disadvantages of the Existing System

- First, the conventional record/secret key-based validation isn't security safeguarding, protection in distributed computing frameworks is a fundamental component that must be thought of.
- Second, Hackers can without much of a stretch introduce spyware to learn login secret phrase since single PC is shared by various individuals.
- In existing, the PC might be bolted by a secret phrase, it can in any case be conceivably speculated or taken by undetected malwares.

Proposed System

In this paper, the system utilized for online distributed computing administration is the fine-grained two-factor get to, utilizing a lightweight security gadget. It is actualized as a component wherein the trait-based access control utilizing the need of both a client mystery key and a lightweight security gadget.

The gadget has the accompanying properties:

1. It can process some lightweight calculations, for example hashing and exponentiation; and
2. It is altered safe, i.e., the data which is put away inside is accepted that nobody can break it and hack the information.

Focal points of the proposed framework

- Our convention gives a 2FA security
- Our convention bolsters fine-grained characteristic based access which ensures the security of the client and as per various situations adaptability of the framework to set diverse access strategies.

2.2 Feasibility study

Feasibility is utilized to distinguish whether a task merits doing. The procedure followed to decide is called as practicality study. The study project factors into account which includes legal, economic and technical consideration of the project completion successfully. The undertaking directors use possibility study to decide the advantages and disadvantages of venture before putting part of time and cash into it. The Viability training is categorized by way of a gauge that the recognized client prerequisites can be met by utilizing current programming and equipment necessities. The fundamental reason for the possibility study is to conclude whether to continue with a progressively nitty gritty investigation.

- Technical Feasibility
- Economic Feasibility
- Operational Feasibility

- Specialized Feasibility
- Behavioural Feasibility
- Permissible Probability

1. Operational Feasibility

Operational considerations are important and it will be achieved in such a way that first we have to properly associate the work so that the users can know that how the system can be utilized for optimal activities. The references of operations are also established in such a way that detailed understandability has to be provided so for these detailed understandability the considerations are acknowledged in terms of documentation.

2. Economic Feasibility

Economic references are important and we have to properly explore the intended financial consideration. All types of financial situations and considerations will be discussed and will be designed with proper visibility. The financial department will have the rights to accomplish a detailed report and will be provided even for the acceptance by the board of directors. The financial understanding is needed because we required that proper cash flow has to be organized because multiple types of users and multiple types of resources and even the environment management is needed.

3. Technical Feasibility

Technical references are quite important to be established because we have to understand that how the technology will be related when we have to undertake different types of features. Technical references are important and we have to find the solutions which is associated with different types of operational features that have included so proper draft for the processes will be acknowledged. The technological references will be first planned and accordingly the resources will be provided to the users so that they can accomplish the task related of development and implementation. Technical requirements in terms of the virtual page setups and other references of multi account working will be also established because the system provides multi approaches for different account holders.

4. Specialized Feasibility

Specialized feasibility focuses on the present framework, it incorporates current PC outline determinations, for example, equipment, programming and so forth it likewise includes budgetary contemplations to suit the specialized upgrades. It focuses on the present framework and to what degree it can bolster the proposed

framework, it incorporates current PC outline determinations, for example, equipment, programming and so forth it likewise includes budgetary contemplations to suit the specialized upgrades. In the event that the spending plan is not kidding imperative, at that point the task is judged not plausible.

In spite of the fact that the framework is created in the summed-up structure, which covers all the strategies and activities completed in a web-based arrangement. The form utilized in the framework is PHP and MySQL. MySQL can oversee enormous measure of information and secure. Utilizing PHP encourages to structure the vibe of the application.

5. Behavioural Feasibility

The customer utilizing various sorts of peripherals gadgets. The system is for giving easy to understand to all the devices.

6. Permissible Probability

It chooses if the proposed structure conflicts with legitimate requirements e.g., The Information Security Act. It will be done by some legitimate aides.

System

A framework is an efficient gathering of associated parts connected together as indicated by an arrangement to accomplish a particular target. Its primary attributes are association, communication, relationship, reconciliation and a focal target.

System Analysis

Framework investigation and configuration are the use of the framework way to deal with critical thinking for the most part utilizing PCs. To recreate a framework the expert must consider its components yield and information sources, processors, controls, input and condition.

2.3 TOOLS AND TECHNOLOGIES USED

JAVA

We are using Java Technology because it is having multiple significant advantages over the other languages and it is also different types of environment. The major references of the Java language is It is object oriented.

Platform independent so it can be easily transferred.

Even the compilation the writing and debugging of the language is easier to understand.

Rich API for the application development is provided and various types of communication among various activities like networking utility and database references can be properly generalized.

It also supports multithreading so that several task can be organized in parallel.

Distributed computing is also properly in hand with the help of Java and even the networking references can be properly associated with secured integrations.



Cascading Style Sheet

This language is assuming a significant job I making the site look increasingly brilliant, appealing where it incorporates the different kinds of shading codes, test dimensions, text dimensions, textual style and so forth the pages created utilizing the outside sheets helps in stacking the pages quicker. The pages created are being responsive and perfect with different programs accessible. This language is for the most part utilized for styling reason where after the page has been structured it is utilized to give the beautiful completion to the pages which makes the page look more brilliant and increasingly appealing.

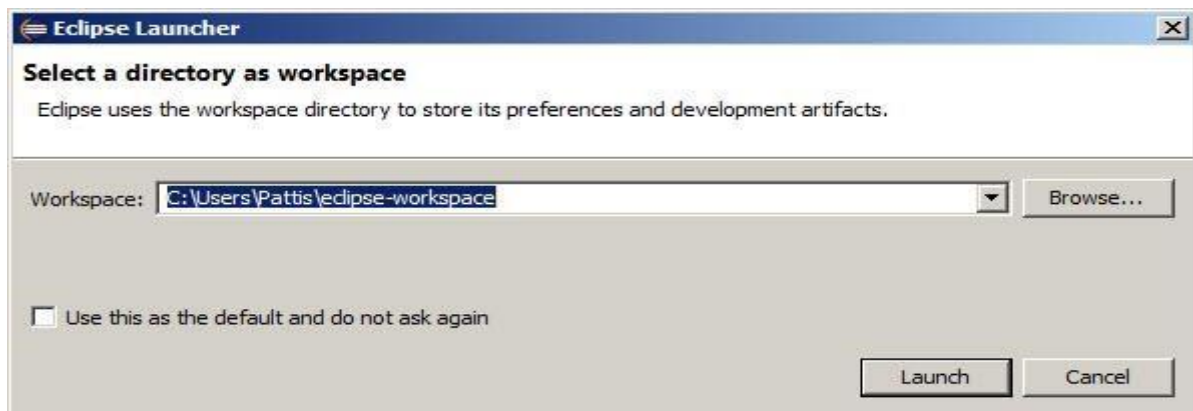
Attributes

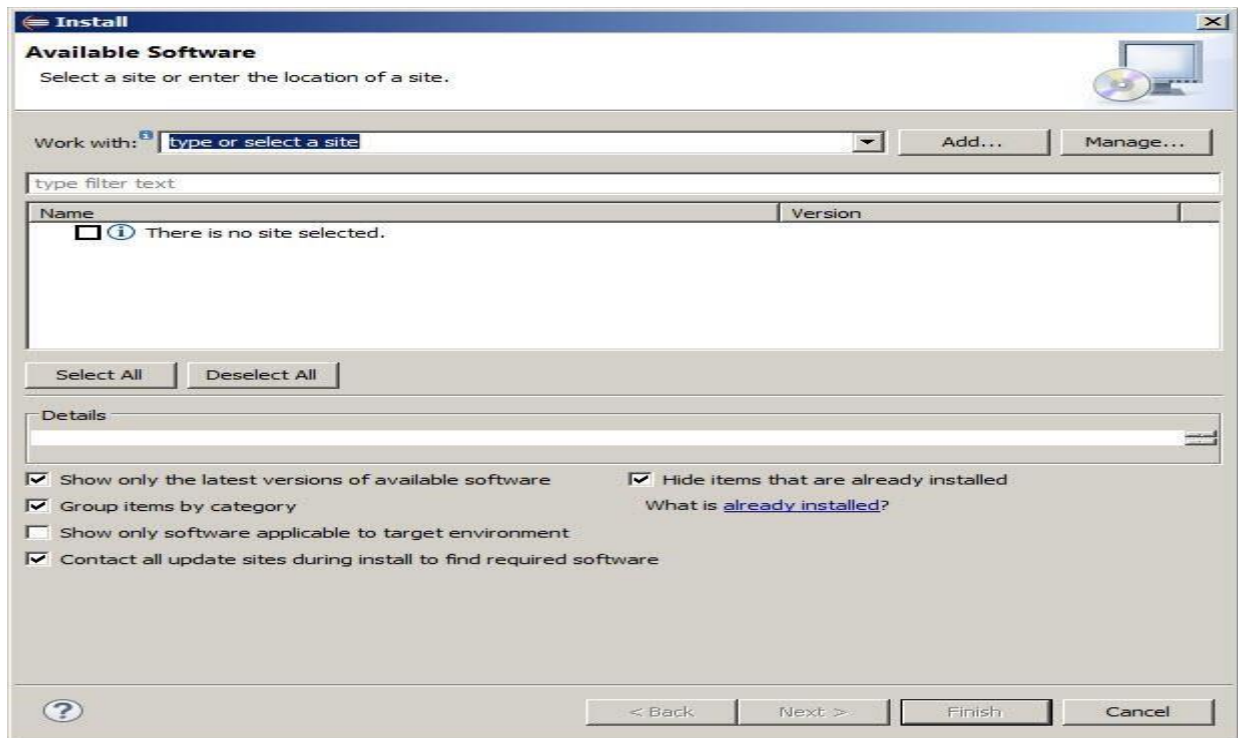
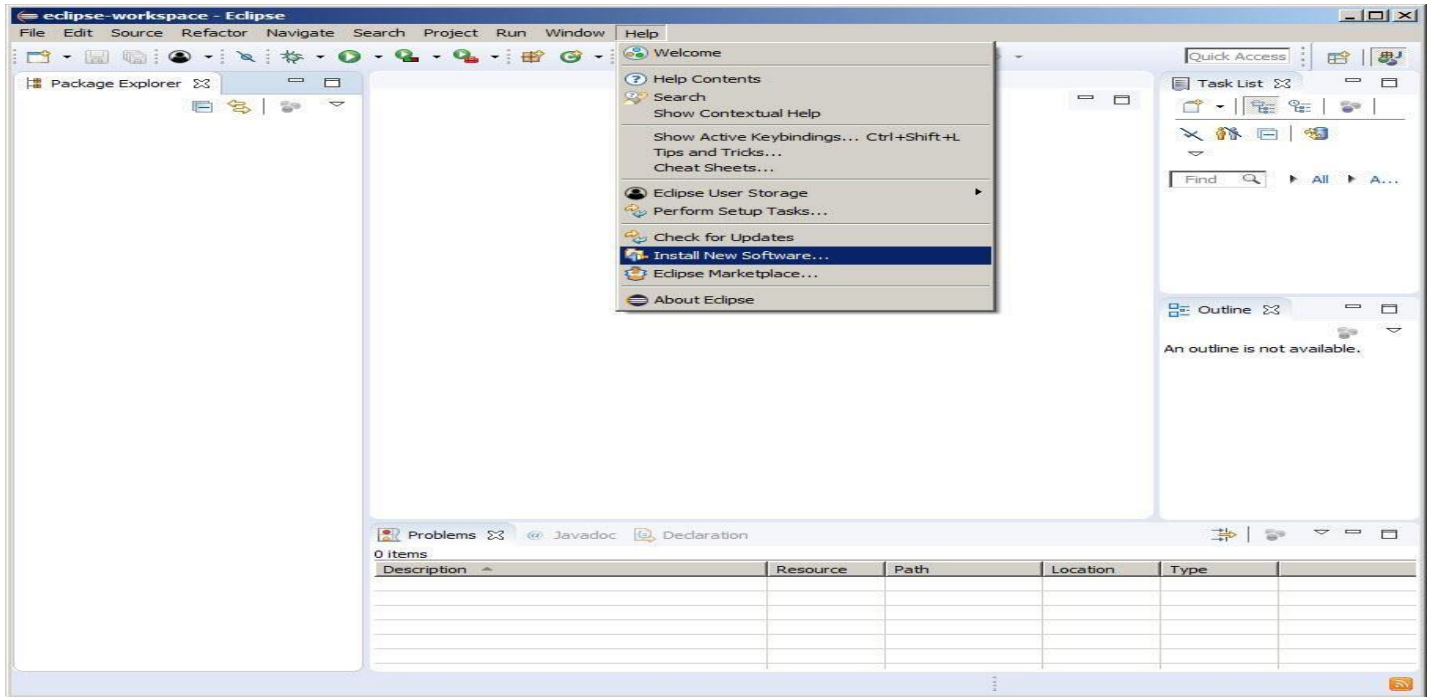
Attributes are a modifier which is used to modify the default functionality of an element type or to enable function for certain element types correctly without them. Start tag is used for attribute.

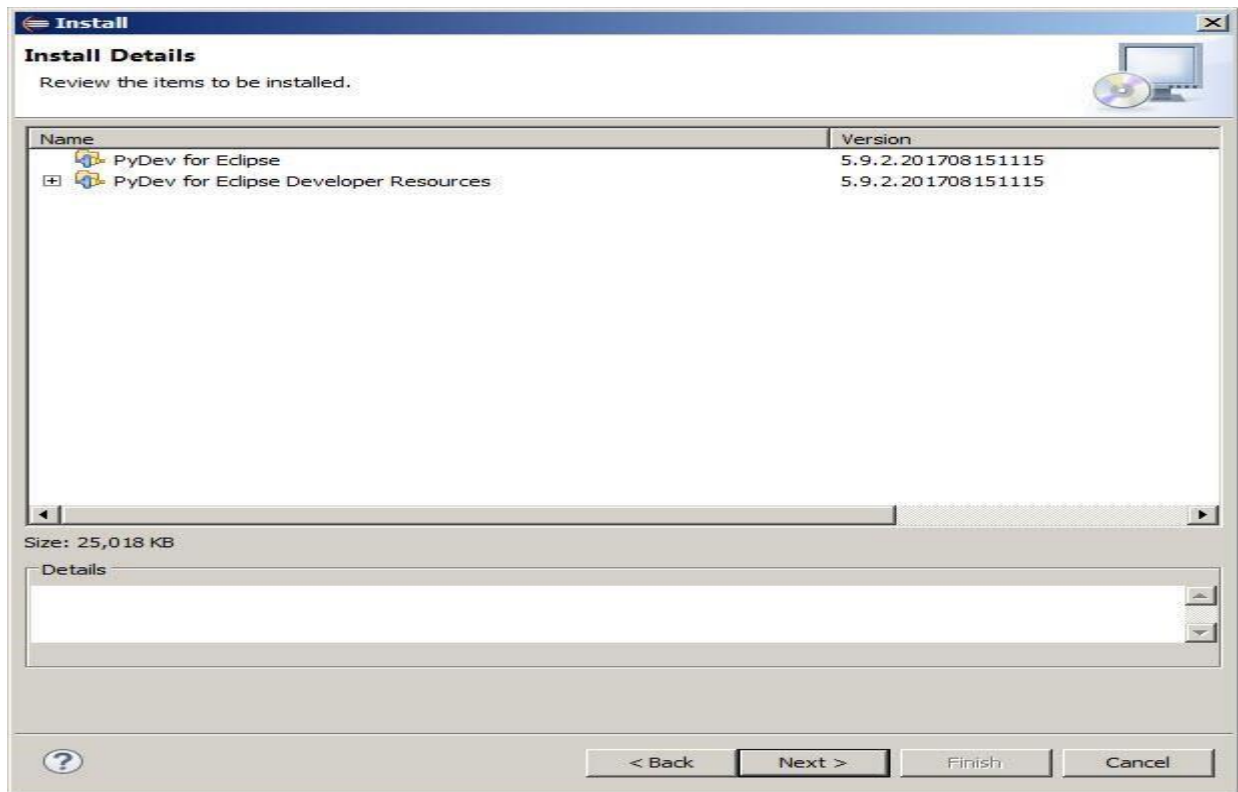
Advantages

1. Elements can have attributes.
2. Attribute provides brief describe.
3. HTML is platform independent.

Eclipse Installation process:







MySQL

Is the creation's maximum notable exposed foundation folder programming, by means of in excess of 100 squillion replicas of its thing being taken, with its chief speed, relentless quality, and accommodation, sources experience programming stack. An ever-growing number of affiliations are utilizing WAMP as an option rather than costly restrictive heaps.

MySQL Server Layer:

This layer deals with all the consistent functionalities of the MySQL social database the broad framework. The cerebrum of the MySQL server is dwells in this tier. The intelligent level is isolated into different sub segments, which are given underneath:

MySQL administrations and utilities:

- SQL interface.
- Streamlining agent.

- Stores and cushions. MySQL similarly gives wide scope of supervisions and conveniences. This is one of the primary explanations behind the prominence of the MySQL. This layer offers the types of assistance and visions for organization and support to the framework, some of them are referenced beneath:

- Reinforcement and recuperation.

- Security.

- Replication.

- Group.

- Dividing.

- Worksurface.

Retrieval for large amount of records can be efficiently and quickly managed

Most references of the database system can be managed without writing the substantial amount of courts

All types of standards are being adopted

Multiple data view can be structure

Supports client server architecture

More interactive in terms of getting the references

Open source and portable that provide the flexibility of usage

The new landing page shows up when the internet browser begins the program demand for the client or the power to sign in or login to the site by giving id name and the secret phrase which was made at the hour of sign in.

The authority and the trustee need to login to do the operation when a user request for the query. The authority is the person who add trustee who acts as the middle man between the user and the authority domain.

2.4 HARD-WARE AND SOFT-WARE REQUIREMENTS

2.4.1 Hardware Requirements:

Here we have examined about the equipment prerequisites required for this task to be grown, for example, the processor and measure of memory required to assemble the application and the speed.

Hardware type	Specification
System	Pentium IV 2.4 GHz
Hard Disk	500 GB
Ram	4 GB

Table 2.4.1 Computer Hardware required

2.4.2 Software Requirements:

The beneath given table determines the PC programming utilized in the improvement of this apparatus. Here we have thought about the OS required and the devices utilized and furthermore front-end what's more, backend alongside the database expended.

Working Framework	Windows XP / 7
Coding Language	Java (Jdk 1.7)
Web Technology	Servlet, JSP
Web Server	Tomcat 7.0
IDE	Eclipse Galileo
Database	My-SQL5.0
UGI for DB	SQL-yog
JDBC Connection	Type 4- native drive

Table 2.4.2 Required software components

CHAPTER-3

SOFTWARE-REQUIREMENT-SPECIFICATION

3.1 Modules

1. Domain Authority

Is a super client who makes the Data Trustee client and keeps up the cloud server's setups.

When the signed capacities.

- Storage
- Data Trustee
- Key-Generation
- Department
- Designation
- Change Password

2. Trustee

Trustee is an individual who will store the records in cloud which thusly got to by the approved Data Consumers. Trustees resemble Liberian who will transfer all the records in the framework. At the point when a document is transferred utilizing Trustee encryption key it will be encoded by the framework. Quality based Decryption Key methods it contains the Trustee Decryption Key and Data shopper Attribution set (Department, Designation).

3. User

Information Consumers are information get to clients, for instance on the off chance that trustee is a school Liberian, at that point information buyers resemble understudies, addresses and administrator staff in a school.

Information Consumers will get their entrance key (Attribute based Decryption key) from separate Trustee through email and lightweight security gadget with the assistance of the entrance key they can download the records which they approach, a recollect get to control is set by information proprietor.

3.1.1 Algorithm:

- DNA Cryptosystem
- Two-Factor Access Control
- Pseudonym Generation Algorithm

DNA Cryptosystem

Calculation for Encryption:

Stage one: Convert double information to DNA groupings.

A=00,

T=01,

C=10, and

G=11.

Stage two: Complementary pair rule.

Integral pair rule is a one of a kind proportionate pair which is appointed to each nucleotide base pair.

Model:

Integral standard: ((AC) (CG) (GT) (TA))

DNA strand: AATGCT

Applying integral standard on DNA strand: CCATGA.

Stage three: Representing DNA groupings as numeric information.

We remove the list of each couple nucleotides in DNA reference succession, numerically.

Model:

Expect the reference grouping to be CT1GA2TC3CC4GC5AT6TT7.

At that point the numerical portrayal will be 040602.

In this implementation, the admin assigns a unique DNA sequence and a unique key to every user which is used to create reference of DNA sequence for the user using rand() function and hash set constructs.

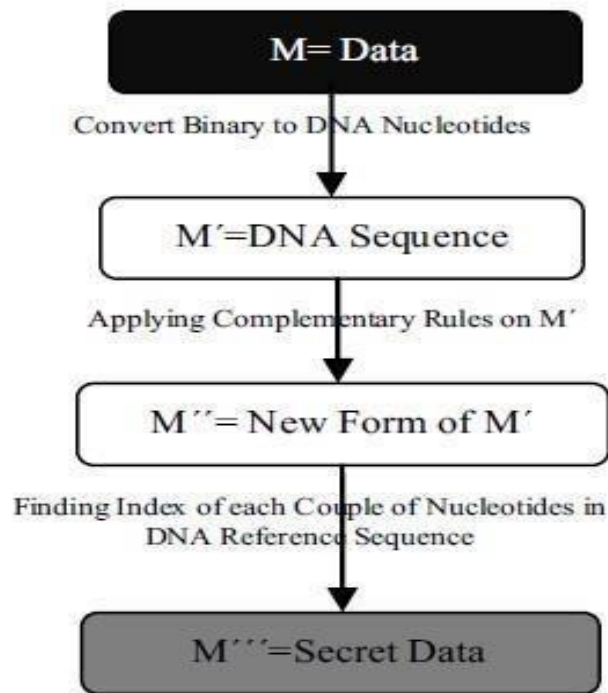


Figure 3.1.1: Encryption Process

The data M is where the client uploads the data through network to cloud computing environment. The uploaded data is then processed and sent through DNA sequence and it creates a new M form. Finally, the data gets a secret key to access. When the client enters the data, it will be in integer format so the computer converts it into binary form.

Changing over twofold information into amino acids utilizing DNA grouping, the base matching guidelines must be utilized. In genuine condition, consistent guidelines are incorporating nucleotides.

Model:

Expect unique information $M=01000001(A)$ ought to be transferred to the cloud

- DNA Reference Sequence:

[TG, TA, AT, GC, CT, GA, CA, AC, AA, GT, CG, AG, CC, TT, TC, GG]

[TG₀₀, TA₀₁, AT₀₂, GC₀₃, CT₀₄, GA₀₅, CA₀₆, AC₀₇, AA₀₈, GT₀₉, CG₁₀, AG₁₁, CC₁₂, TT₁₃, TC₁₄, GG₁₅] •

$M=01000001$ (Original data).

□ Sub-phase 1 (Base blending rule)

(A= 00, T= 01, C= 10, G= 11): $M'= TAAT$

- Sub-phase2 (Applying complimentary principle)

((Air conditioning) (CG) (GT) (TA)): $M'' = ACCA$

- Sub-phase3 (Indexes): $M''' = 0706$ (Encrypted information)

3.2 Phase2:

Extracting Original data

Client2 consist of some numbers which contains the secret data. So, to configure the original data to encrypted data it uses DNA reference sequence so that original data can be extracted by its sub phases.

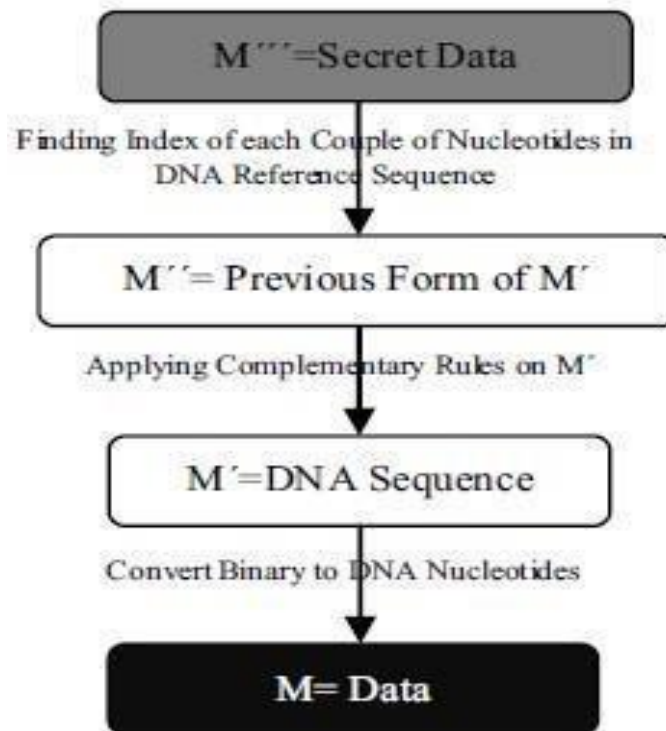


Figure 3.2: Decryption Process

Algorithm for Decryption:

Step One: Converting numeric data into DNA sequences.

We separate the couple nucleotides in DNA reference succession as indicated by the file read from the record.

Step two: Complementary pair.

nucleotides base pair is assigned with complementary pair rule.

Step three: Converting DNA sequences to binary data.

Example:

DNA Reference Sequence:

[TG₀₀,TA₀₁,AT₀₂,GC₀₃,CT₀₄,GA₀₅,CA₀₆,AC₀₇,AA₀₈,GT₀₉,CG₁₀,AG₁₁,CC₁₂,TT₁₃,TC₁₄,GG₁₅]

[TG, TA, AT, GC, CT, GA, CA, AC, AA, GT, CG, AG, CC, TT, TC, GG]

- M''=0706 (Input)
- By alluding the DNA grouping:

Sub-phase1 (Indexes): M''= ACCA.

- Complementary rule:

Sub-phase2 ((AC) (CG) (GT) (TA)):M'= TAAT

- By utilizing Base Pair Rule:

Sub-phase3 (A= 00, T= 01, C= 10, G= 11):

M=01000001 (A)(Output)

3.2 FUNCTIONAL REQUIREMENT

The major functional requirements are:

Domain authority:

Area authority can login utilizing client id and secret phrase. When he gets signed in, he can include information trusty.

Domain trusty:

Domain trusty can be logged in by his/her user name and password. Domain trusty can add users, by providing the user details. The trusty can upload the file and give access to particular user or department.

Data user:

Login using name and password which is provided during the sing in and can download the file.

3.3 Non-Functional requirement

System maintenance will be done by the administrator where each consideration of the preference will be added and even any type of required usability resources can be incorporated where if new requirement arise this related request has to be sent to the provider. The system is scalable and for providing the scalability the system is divided into multiple cloud working space system so different types of categories can be recognized and accordingly multiple types of operation for example the venture management can be associated.

Encrypted security and multiple choices of the related policy implementation is also provided. Central data is associated with cloud synchronization repository so that any type of data that is generated can be synchronized and can be saved. More improved and enhanced accessibility considerations will be provided to the administrator for the accessibility security casting.

Legal associations will be provided so that it is convenient and appropriate provided with the login will be provided in a proper draft. Legal consideration for important as the uses will be in different numbers and multiple accounts are provided for acknowledging the work. Portability: Yes, this system is portable and we can switch server very easily.

Non-functional necessities are those qualities or highlights which is not corresponding to the tweak approach gave by the framework. They are subject to apportion of the frame work properties, anyway it characterizes condition on the construction, for example, the capacity of the Io gadgets and how the information is spoken to utilizing the background as an interface.

Portability

This part states the application module portability in the different configuration systems or the ability of software to be transferred from one machine to another machine

Security

The modules of banking and gateway interaction between application have code with the security session base operations. This give safe and hassle-free operation for all the users and developer side. Security is the main thing to any Software that has to be made to safeguard the data from the hackers here the data security is very important.

Application will permit just legitimate consumers to get to the framework. Access to any appliance asset will rely on the investor assignment. And this mainly depends on the individual username and secret key.

Viability

The details of the products will be effectively available for the buyer.

Accessibility

System will be approachable anytime except for the time required for the backup information.

Transportability

As the database is in MySQL server, porting the info to another server would require some improvement exertion.

Convenience

The connections have accommodated each structure. The client is encouraged to view and make sections in the structure. Approvals are given in each field to stay away from conflicting or invalid section of databases. A few structures comprise hyperlinks, which gives further subtleties.

CHAPTER 4

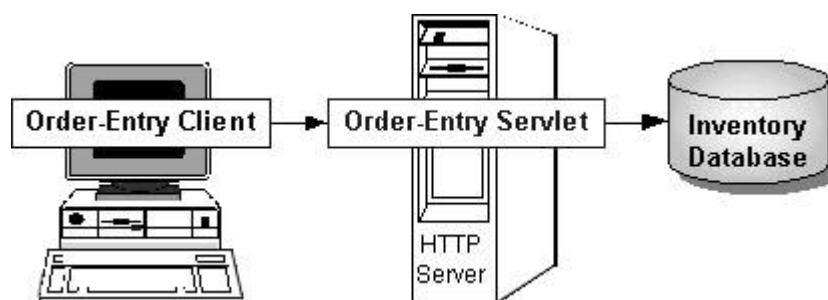
System Design

4.1 SYSTEM PERSPECTIVE

The invention improvement procedure can be categorized as an assortment of stages depicting the different techniques in the advancement procedure. Framework viewpoint includes the exhibition and functionalities of the structure which would portray the background. This can be characterized as a modified measure for distinguishing the arrangement from the commencement of the issue. The plan can be pigeon-holed as delegate among the phases of execution. The yield at this phase is a structure of the archive. In the perspective on a construction one ought not to think about the skeleton as a disengaged substance. The basic point of view symbolizes the functionalities and connections between the earth and the scaffold. It distinguishes how every module in the frame conveys intelligently to deliver a total answer for the difficult which was differentiated. The fundamental objective of SDLC is to make a characteristic and modernizing the prerequisite of a context into the code. At This Time, we essentially illustrate how various modules of a background convey and what the conditions between every outline of the segment are.

DATA FLOW DIAGRAM

A setting outline is commonly remembered for a necessities archive which are utilized from the get-go in an undertaking to get concession to the extension under scrutiny. It must be perused by all undertaking partners and subsequently ought to be written in plain language, with the goal that associates can get things. The goal of the framework setting framework is to concentrate consideration on outer variables and occasion that should be considered in building up a total arrangement of requirements.



J2EE

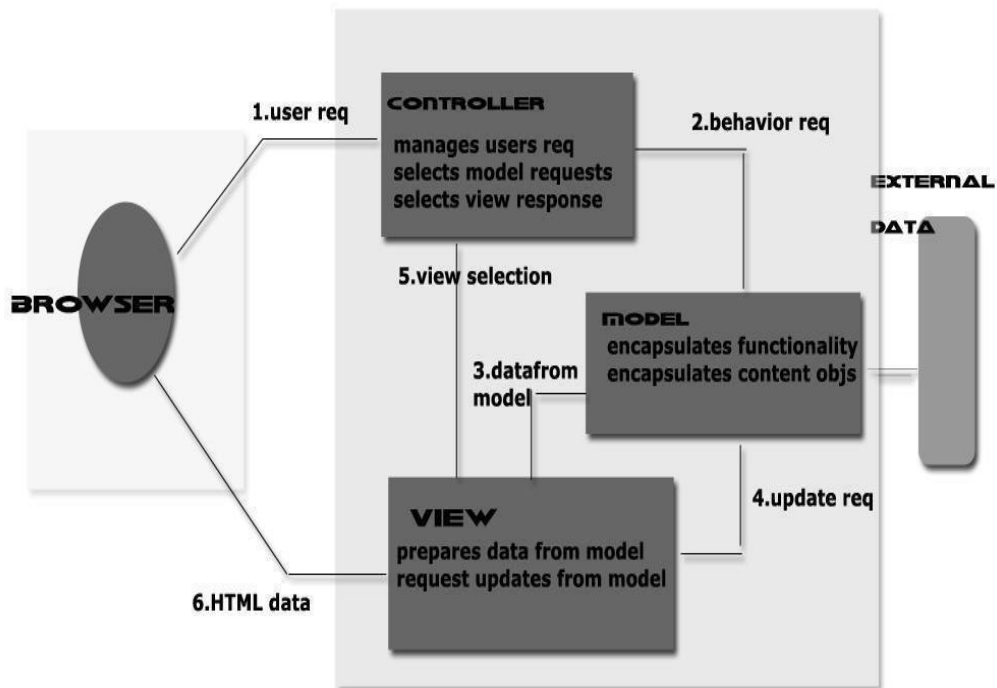


Figure 4.4.2 (a) J2EE uses MVC Architecture

In J2EE the client can access or view the browser the request sent through the browser is accessed and the result is sent back to the client, 1. When an user request some query to the browser the control manages, selects and view the request and check for the data which the cookies and perform encapsulation functionality. If the data is not in model then request is sent to the external data and then collected data is updated to the model. The data is loaded to the view process where the request query is resent to the browser as an HTML data.

The process which takes place within the browser cannot be viewed to end user, system takes an integer type values inside the operating system and provides machine level code to the external browser in which machines can understand only machine code which is binary code which consists of 0's and 1's.

System Architecture

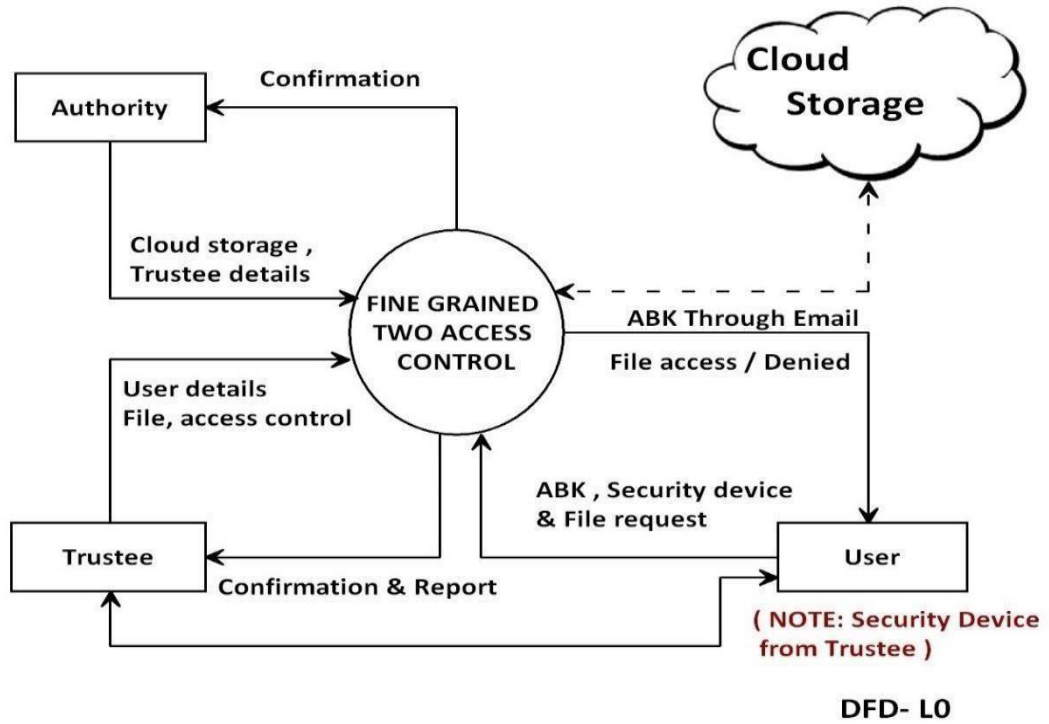


Figure 4.4.2 (b) System Architecture

In the system architecture the authority and the trustee are the two main modules within the cloud, If user request the security device check for file and invokes the fine grain control which is stored in cloud storage. The authority checks and confirm then the details is sent to the trustee to perform the operation. Finally, the trustee checks for the user details and confirms the access control the report is sent from fine grain, the access will be accepted by the cloud.

4.2 Dataflow-Diagram

DFD - Authority Session

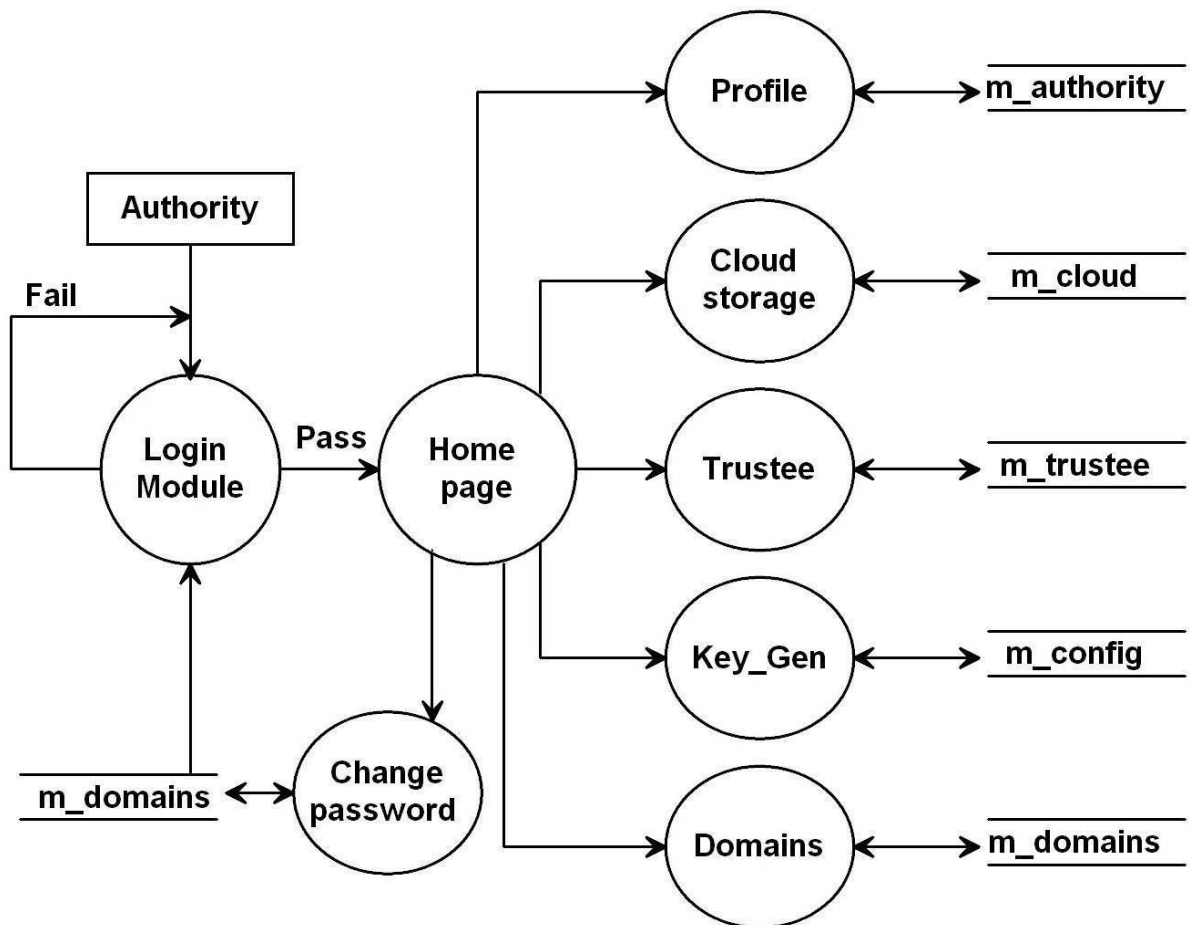


Figure 4.2.1 Authority Data Flow Diagram

In the authority session the domain authority needs to login to the module using the user id if the authority fails to login the session will be terminated, if it is successfully logged in then opens the home page within the home page the domain authority can view profile, check cloud storage, he can edit and view trustee, generate key and check for the domains.

DFD - Trustee Session

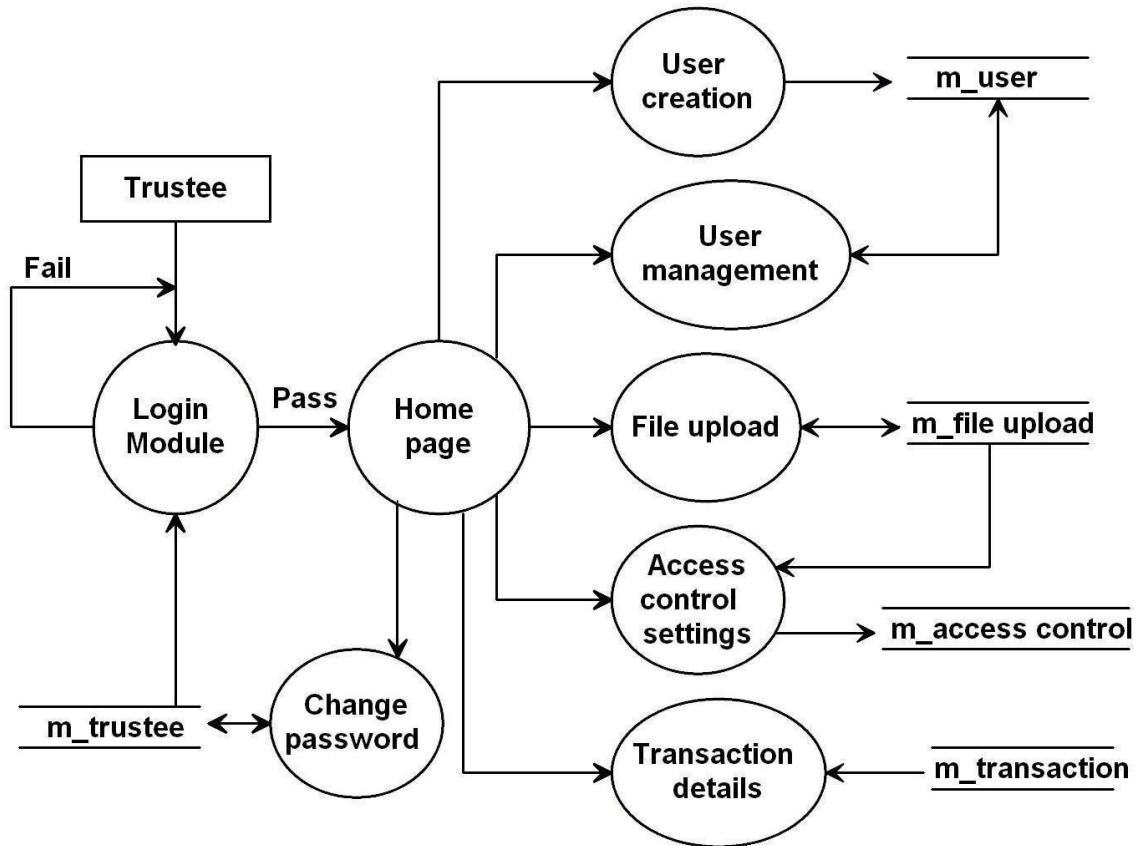


Figure 4.2.2 Trustee Data Flow Diagram

In the domain trustee session the trustee can login to the module using the user id if the trustee fails to login the session will be terminated, if it is successfully logged in then it enters to the home page within the home page the trustee can create user, manage user, files can be uploaded which needs to be sent to the user. The trustee can access control settings finally he / she can view transaction details and can log out of the process.

DFD - User Session

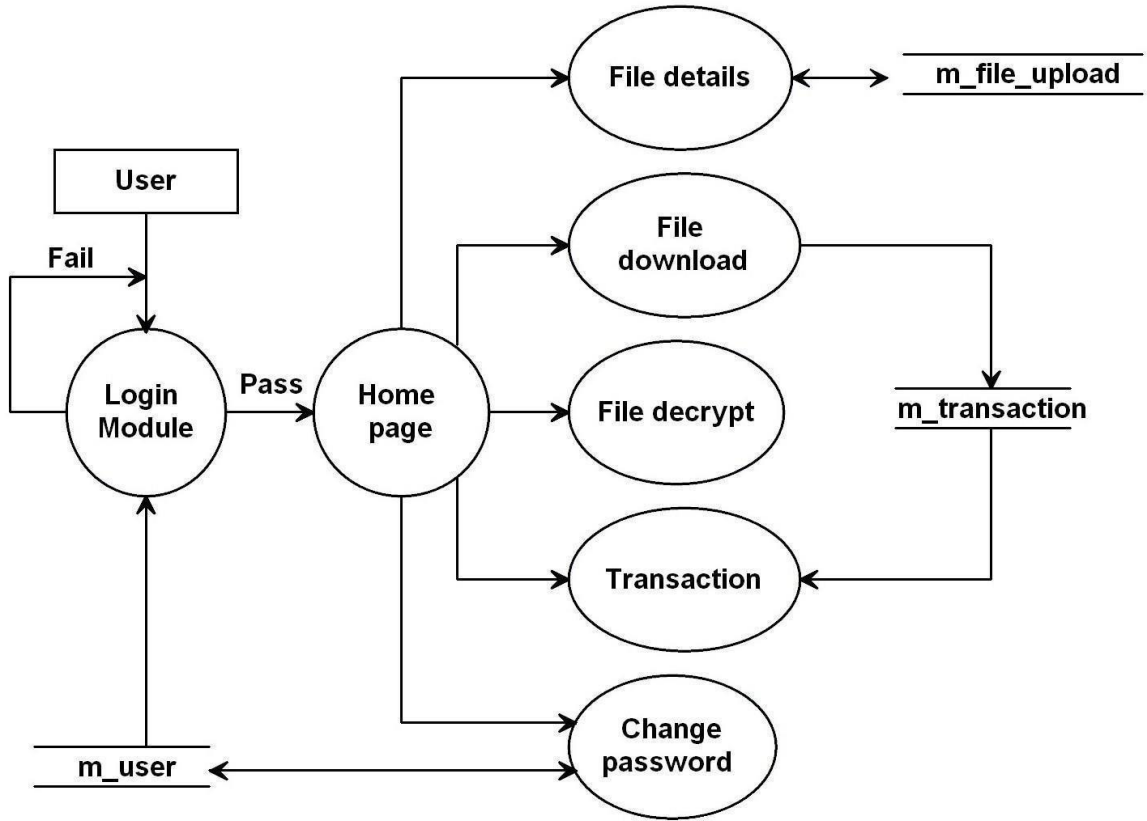
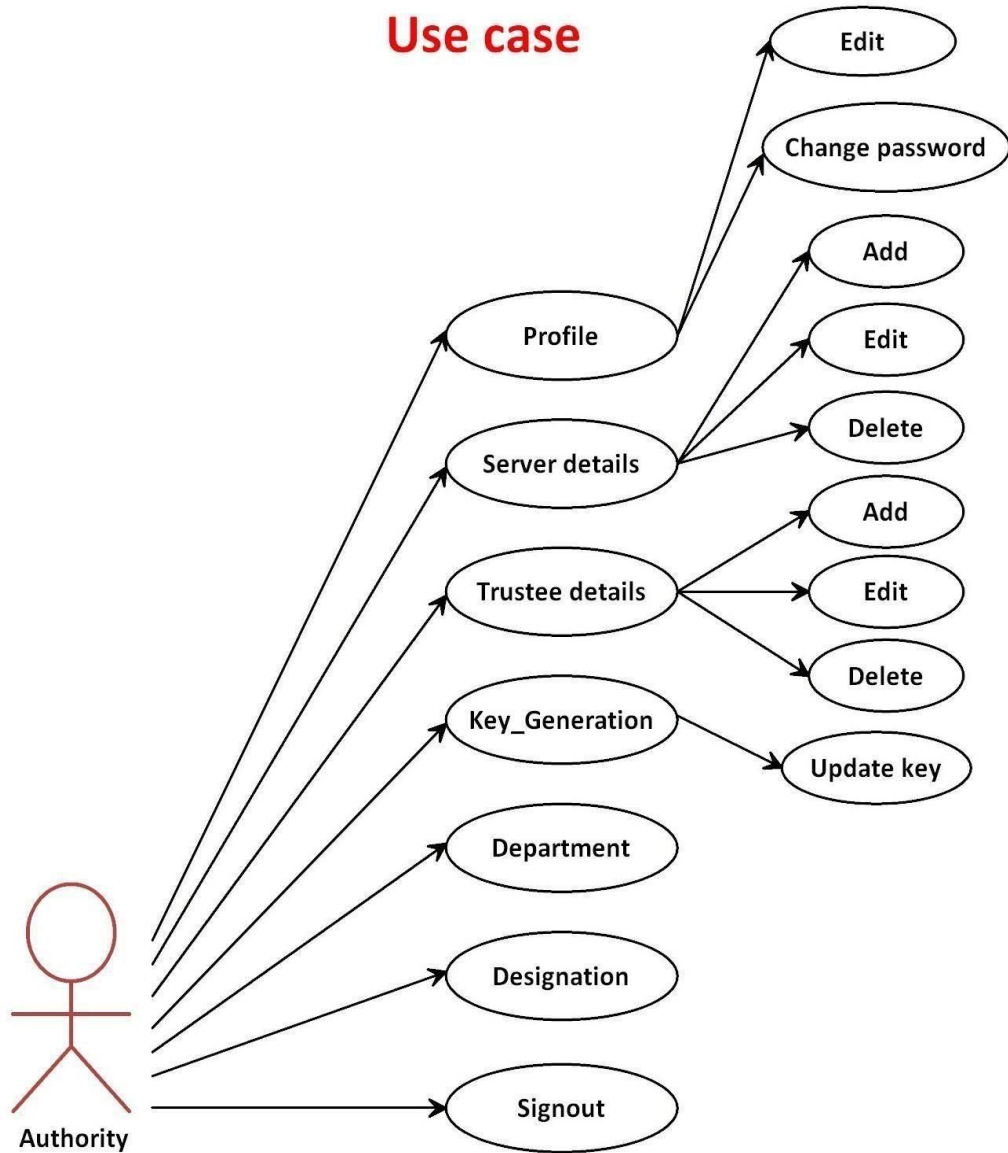


Figure 4.2.3 User Data Flow Diagram

In the domain trustee session the trustee can login to the module using the user id if the trustee fails to login the session will be terminated, if it is successfully logged in then it enters to the user page within the user id the user file details can be viewed from file upload, files can be downloaded, decryption and transaction takes place within the traction of the user. The user can change password if required.

CHAPTER 5

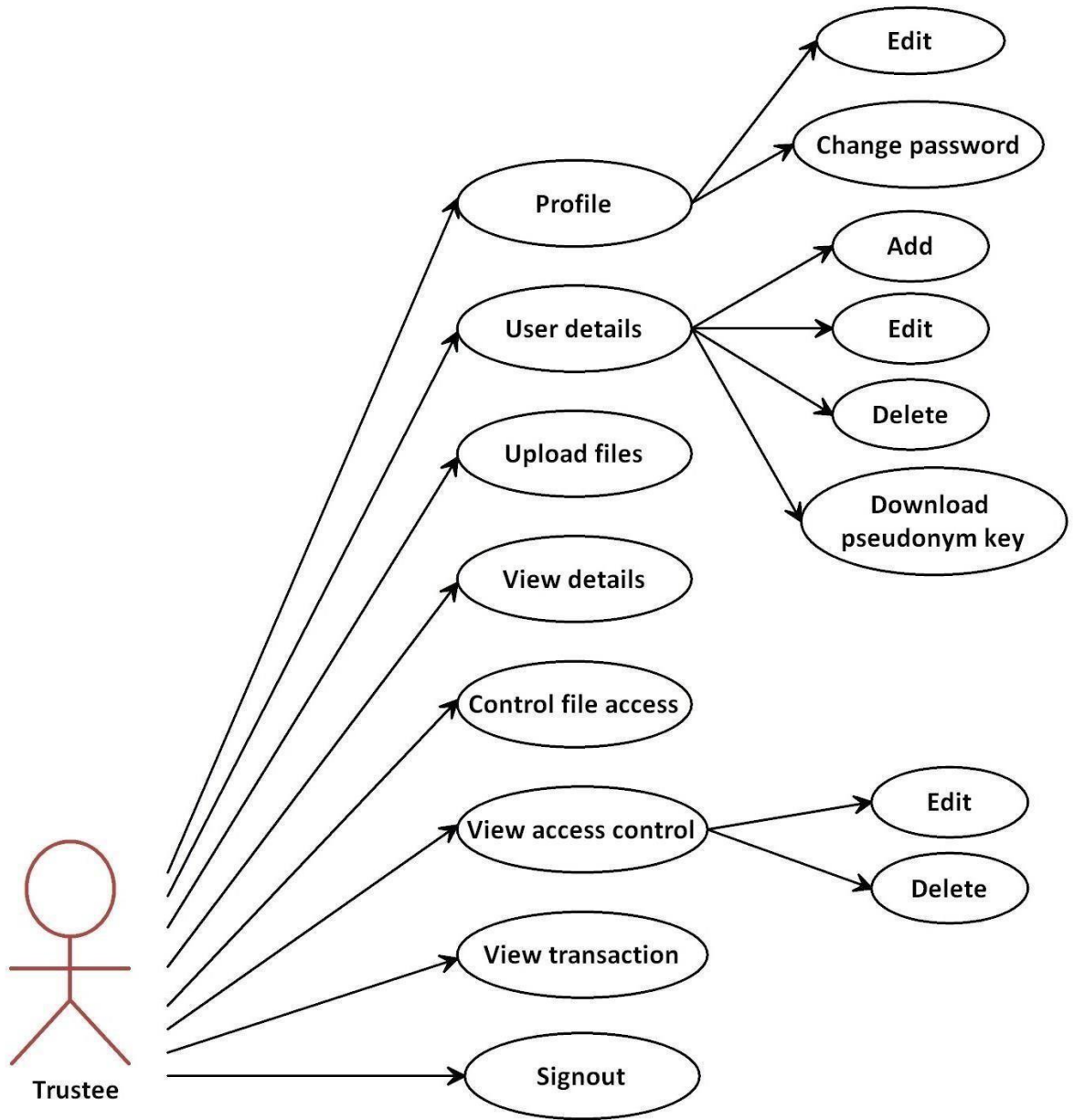
DETAILED DESIGN



5.1.1 Authority Use Case Diagram

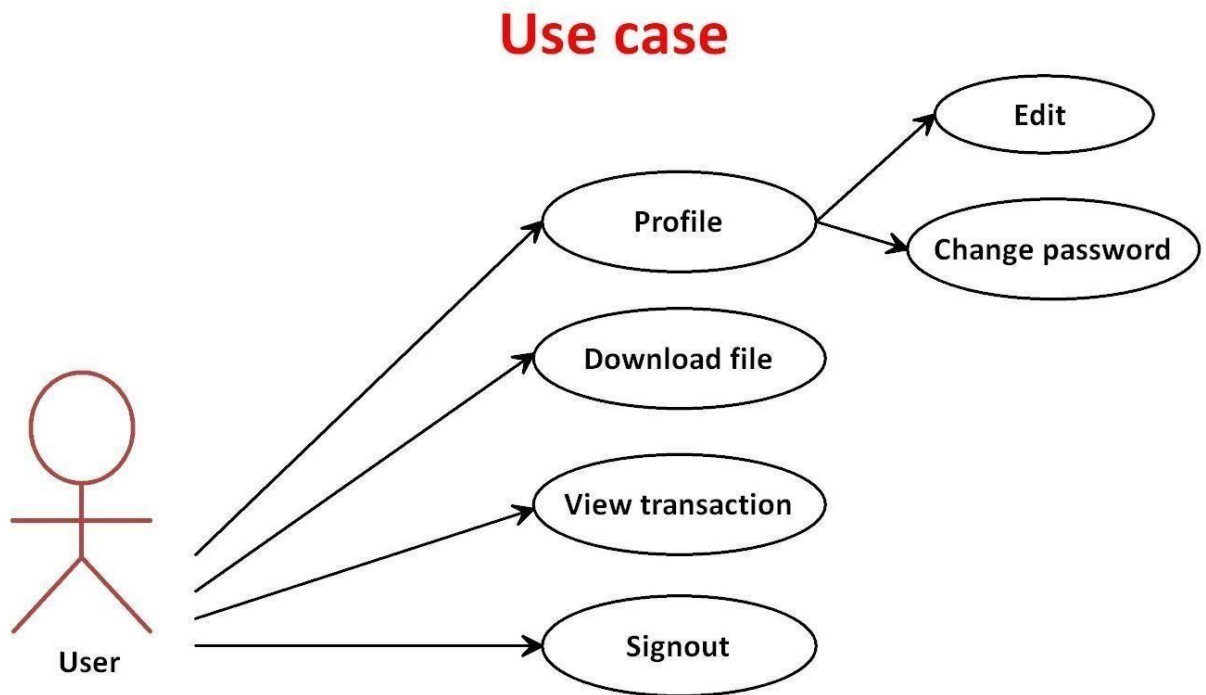
Domain authority can login using id provided by authority and password. Once he gets login authority can add data trusty. The working process of authority is who can login to the system details of the server. The key is generated by the domain authority, details about the trustee and the designation is known by the authority.

Use case



5.1.2 Trustee Use Case Diagram

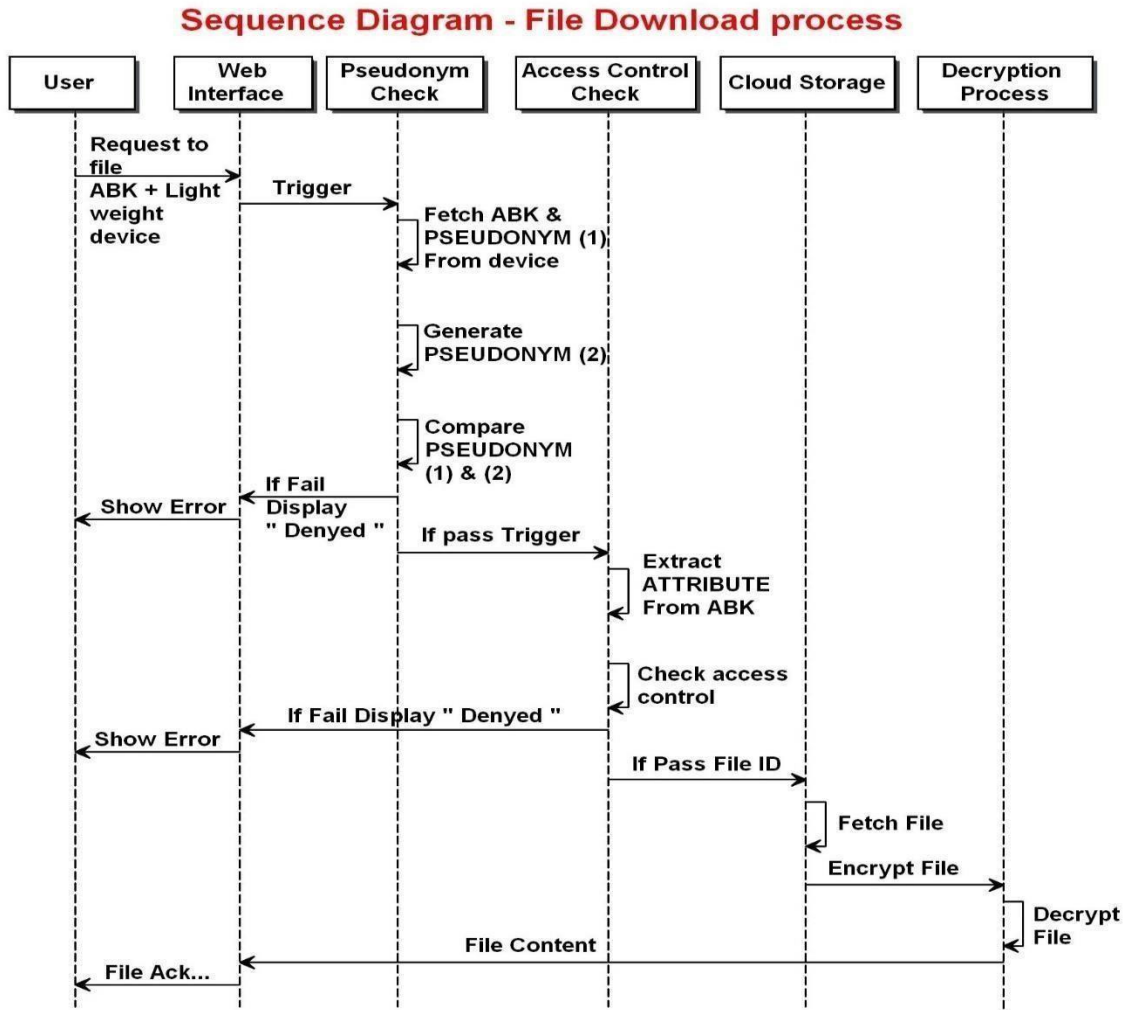
Domain Trustee is person who is appointed by the domain authority he as the access of knowing who is accessing to the server and the transactions that are taking place within the data server. Trustee can edit or delete the access control of the user, he as the access to download the pseudonym key with will be accessed by users.



5.1.3 User use case diagram

A user is the person who can store the data to the cloud service to share the data, he / she can view the transaction that took place. The user can download file. The user can anytime change the password so that it can be prevented without hacked by some hackers or profile can be edited if required. The user can only send the request so that the domain trustee checks for the request and process the data.

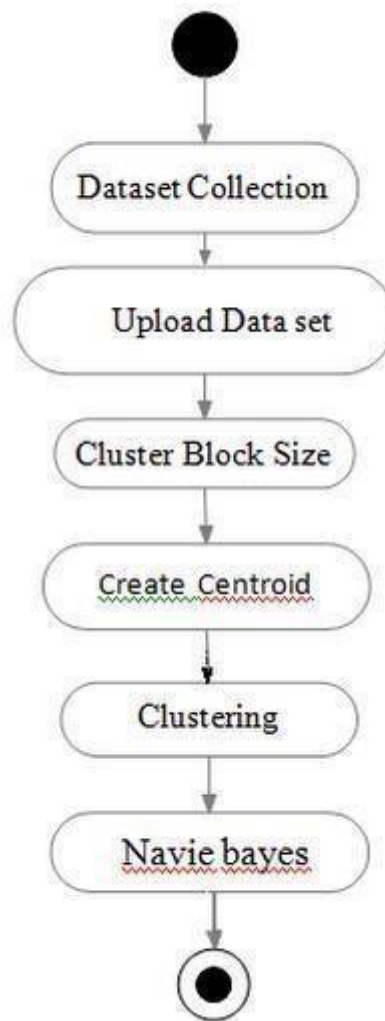
5.2 Sequence Diagram



5.2 Sequence file download

User request file to the web interface it triggers pseudonym check it fetches ABK from device then generate pseudonym 2 and then compare pseudonym 1 and 2, if it fails displays “Denied”, and user gets error. If the compared pseudonym 1 and 2 is passed then trigger to access control check it extract attribute from ABK, then check access control even if it denied it again shows error to the user. If there is no error it continues and provide file ID to cloud storage. The cloud storage fetches the file and encrypts the file and send to decrypt process and the decrypted file is shared to user.

5.3 Activity Diagram



5.3 Activity diagram

In activity starts data is collected by the user, inserted data set is uploaded and checks for the block size of the cluster. After the creation it creates centroid the data will be shared among different nodes into the cluster this process is known as clustering, and it goes to the naviebayes then the process stops.

5.4 CLASS DIAGRAM

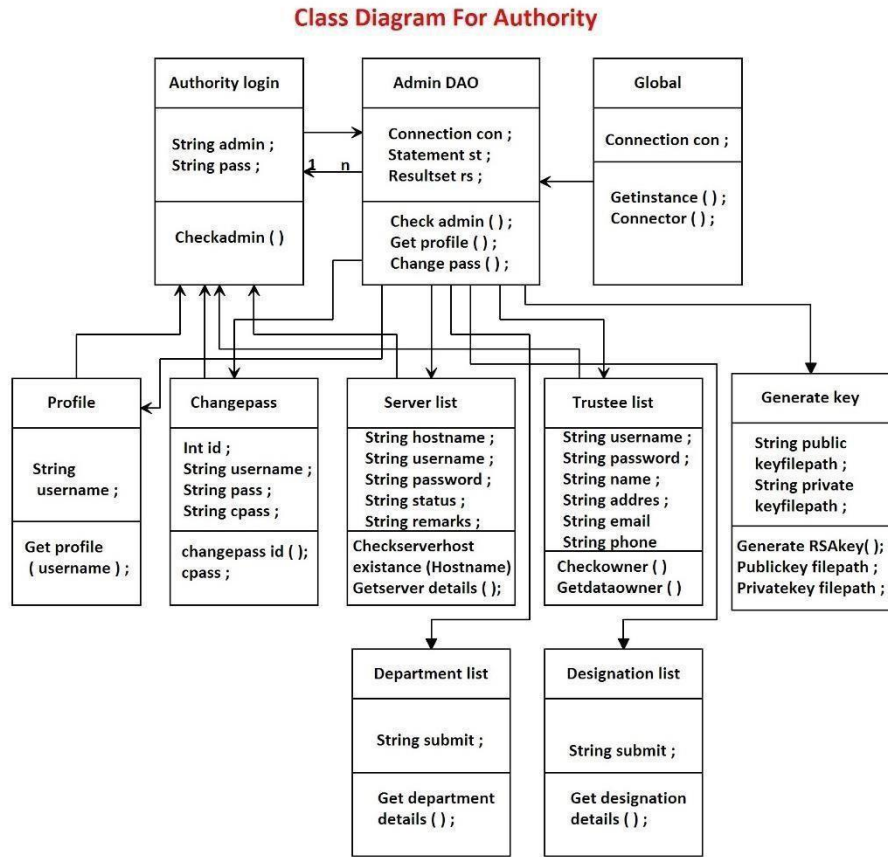


Figure 5.4.1 Authority Class diagram

Domain authority class diagram consists of authority login where admin and password is provided and checked, username is provided to access. Admin DAO is used to connect the connection between the admin using the profile in which the username and password id is checked to verify then checks for the server host to get permission for the details of the department and designation of the trustee, then the global connects to connector for key access the public and private file path is establish.

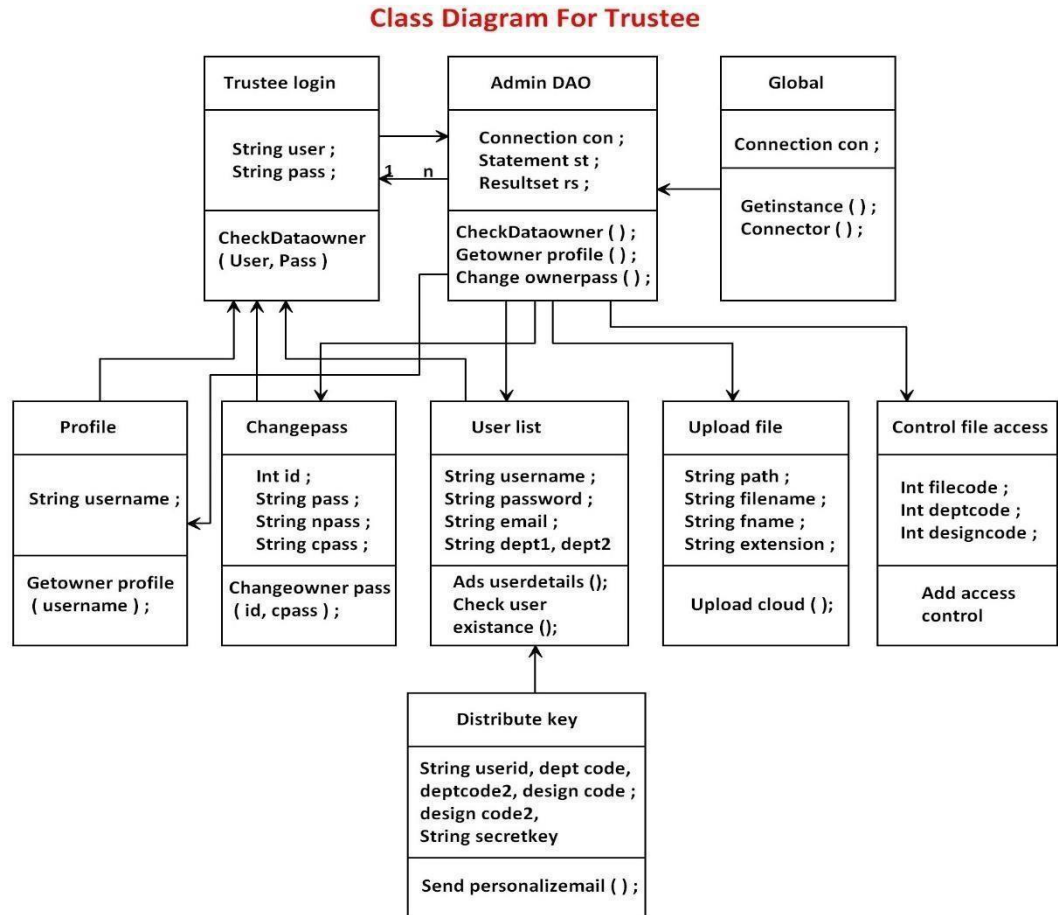


Figure 5.4.2 Trustee Class Diagram

When trustee needs to login to the server, he / she needs to provide username and password where the profile checks for the username if username is correct then proceeds to check the password if trustee requests to change the password it can be changed. Then admin DAO checks for the connection the owner password and profile to access. Trustee can check for the user list according to the department and modifies the profile if requested. The files can be uploaded to cloud by providing file name, path and the details of the file. Then the global connection takes place within the connector using the department code, designation of the user. The trustee gets the distributed key which is sent threwh the personal mail which is secure with the trustee.

Class Diagram For User

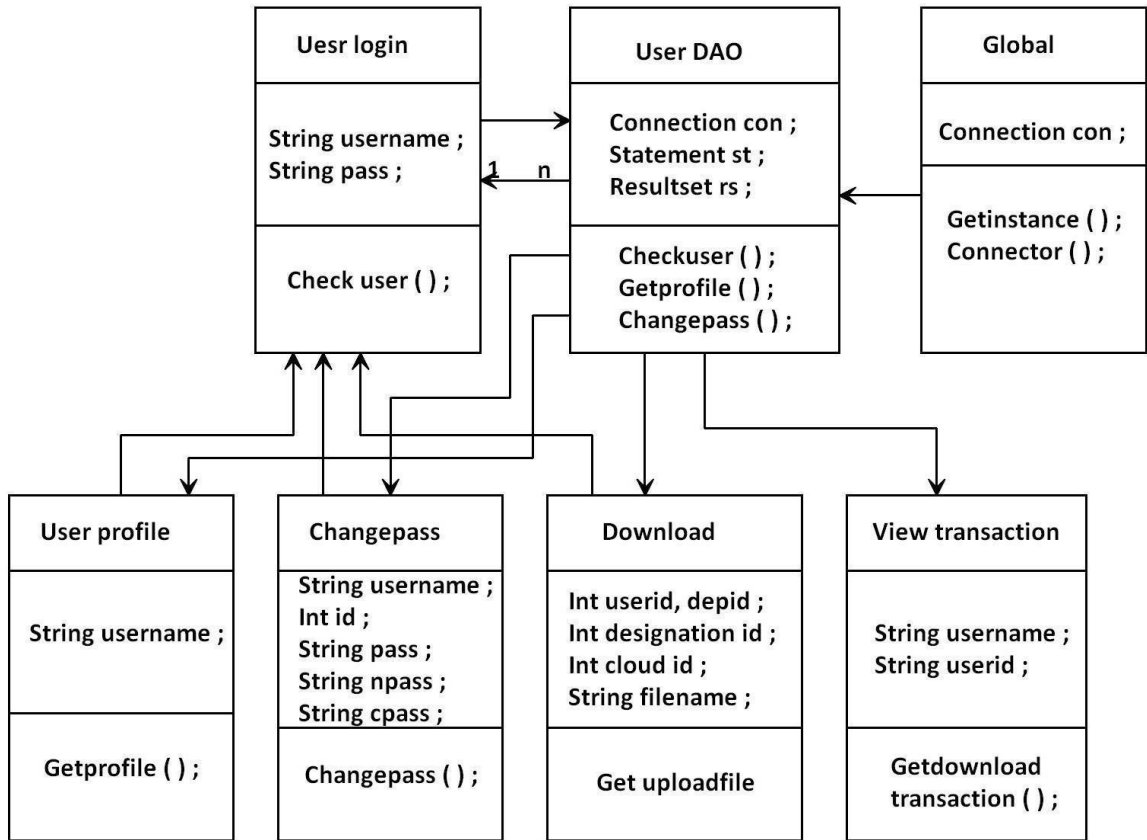


Figure 5.4.3 User Class Diagram

Domain user class diagram consists of user login where username and password provided and checked, username is provided to access. Admin DAO is used to connect the connection between the admin using the profile in which the username and password id, then the global connects to connector and provide file which need to be downloaded. The file can be downloaded by providing the designation id and cloud id with the file name to upload file.

CHAPTER 6

IMPLEMENTATION

6.1 SCREENSHOTS



6.1.1 Authority Login

Space authority can login to the site page utilizing client id and secret word. On the off chance that the authority gives right login certifications, at that point he can get to the profile page. The page will be reCOORDINATED to login page if the username or secret key isn't right.



6.1.2 Admin Profile Page

Once the domain authority enters correct username and password then the web page re-directs to authority profile details in which authority id number, name of the authority, mail id, address details are displayed. The domain authority can modify the password.

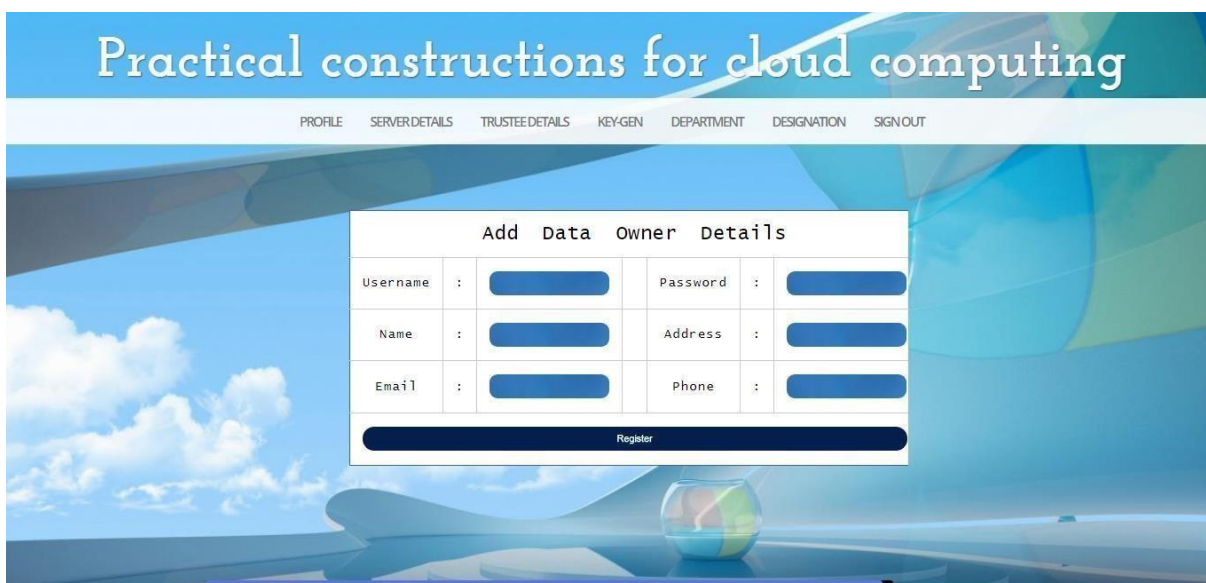


Figure 6.1.3 New Data Owner Entry

In this web page the domain authority can add data owner details which contains the details of the owner who have shared the data to the cloud storage for transaction. The data owner details are provided by the authority entered.



6.1.4 Key generation

Key generation process when the data is entered by the owner, when data is shared it is encrypted by generating the key which is access by domain authority person, the key can be known by the trustee to provide the data access to the user.



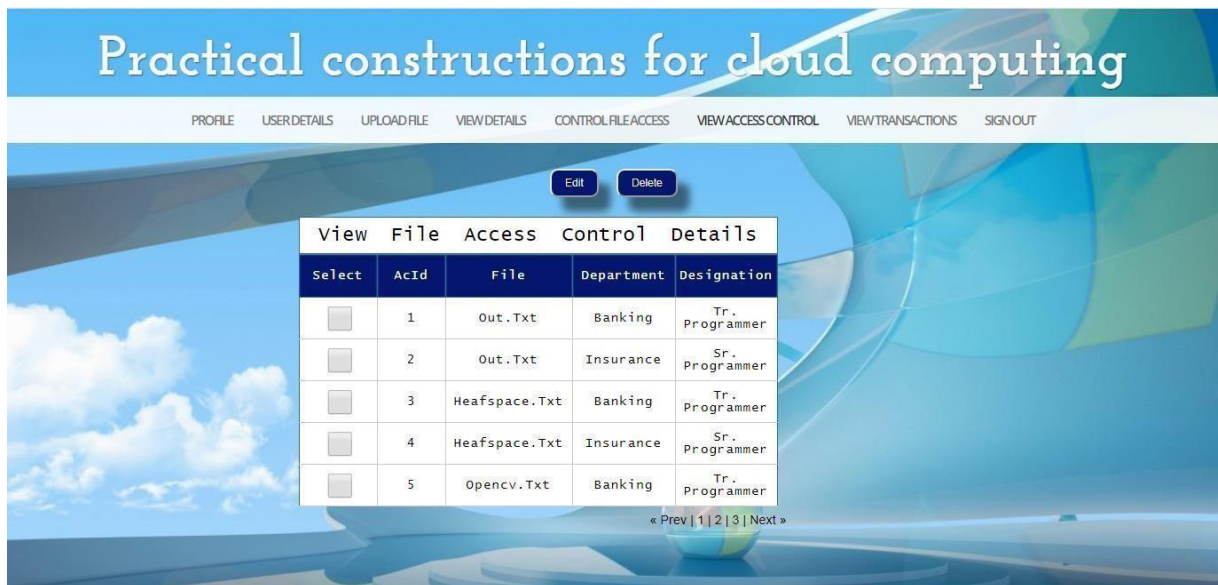
6.1.5 Department Details

Details of department are viewed by domain authority and trustee, who can even modify the contents of the department, the department contains department id and department name which is enters by the user while registering to the cloud service.



6.1.6 Authority file access page

The domain authority can check for file details within the web page of file access control. In this web page details of file in which file name, content of the file, name of the data share, department in which the file is stored and designation from where the file needs to be accessed.



6.1.7 File access details

Authority file access page re-directs the page to file access details where all the details about the file is stored. All the file which is been stored threw cloud stored is maintained in this file access, in which authority can check or edit if there need to be any changes within the file or can understand if any of the file is been misplaced.

Practical constructions for cloud computing

PROFILE USER DETAILS UPLOAD FILE VIEW DETAILS CONTROL FILE ACCESS VIEW ACCESS CONTROL VIEW TRANSACTIONS SIGN OUT

Edit Delete

View	File	Access	Control	Details
Select	AcId	File	Department	Designation
<input type="checkbox"/>	1	Out.Txt	Banking	Tr. Programmer
<input type="checkbox"/>	2	Out.Txt	Insurance	Sr. Programmer
<input type="checkbox"/>	3	Heafspace.Txt	Banking	Tr. Programmer
<input type="checkbox"/>	4	Heafspace.Txt	Insurance	Sr. Programmer
<input type="checkbox"/>	5	Opencv.Txt	Banking	Tr. Programmer

« Prev | 1 | 2 | 3 | Next »

6.1.8 User file access page

User file access page can contain only the details of the user who has logged in to the page, the file contains the filename, file id, designation and destination of the file is mentioned with the file access and can download the file which is necessary for the user.

CHAPTER 7

SOFTWARE TESTING

Definition

Software tester is the person test code according to modules in different stages during the implementation of the code. The first stage of testing is known as unit testing where each and every single module in a project is tested one after the another so that fault in the program can be identified in a class or function

The libraries used to test the source code is cunit oppunit test which issues can be fathomed rapidly and naturally.

Programming testing life cycle is an action which is performed in a steady progression during programming testing. It contains arrangement of movement with must be followed during testing.

Requirement specification

Supervisor will have an agenda which contains question and answer agenda choice where it indicates what all the means must be taken.

Business investigator can include more question however can lessen questions just inside a breaking point.

The report called Software necessity detail or client prerequisite particular is sent to administrator.

Two-way examination is finished by administrator, I) Size ii) need

As indicated by examination they separate SRS into little sub SRS, these sub SRS is known as client story.

When investigation is done supervisor has arrangement of client stories.

Acceptances it is important so we have to check that system works in different scenarios properly and it is accepted by different types of companies in different types of domain provisions. The references of the working should be acknowledged with proper consolidated provision so we will be checking all the control variations and setting variations. Software testing will help us even to maintain the quality because when properly checked it will provide optimal working to the clients. Different types of testing mechanism are incorporated this will be helpful to us all the features properly and more quality references can be checked and this will help us to affiliate the scope of the system in more advances way. Inclusive references are undertaken

and even it will be documented. Software testing will help us to check in real time the factorial references that are provided and this will help us to have a more comprehensive design for the service provision.

7.1 Testing Approaches:

There are three kinds of programming testing draws near.

1. White-Box Testing:

Is otherwise called Glass-Box. This depends on application's inner code structure. In this method, an internal viewpoint of the framework, just as encoding aptitudes, are used to configurate. This test will be usually Carried out in unit-level of development.

2. Discovery-Testing:

Known as Behavioural/ Specification-Based. It is thing taking a gander at framework in which the gathering reviews the support of the improvement under test without taking a gander at the information code structure.

3. Dark-Box Testing:

Dark box is the mix of both previously mentioned forms. The test group who goes after this kind of provocative needs to move toward compliance reports. This helps with improving analyses in this technique.

Principles of Software Testing are as per the following:

- ❖ Early testing.
- ❖ It shows the nearness of deformities.
- ❖ Thorough scanning is incomprehensible.
- ❖ Imperfection bunching,
- ❖ This sets the subordinate.
- ❖ Nonattendance of blunder-false notion

Program Testing Types:

1. Manual Testing

It is the course towards testing UI arrangement by hand to get settled with it, to discover what is and isn't working. This all things considered breakers avowing all the highlights appeared in essentials report, yet customarily correspondingly combine the analysers attempting the thing with the viewpoint of their end clients at the most elevated purpose of the need list. Manual test plans sway from completely scripted examinations, giving point by point steps and anticipated outcomes, through to raised level partners that steer exploratory get-togethers. There are stacks of complex contraptions open to help with this, at any rate on the off chance that it needs a crucial and flexible spot to begin, investigate test pad.

2. Computerization Testing

Motorization assessment is the way towards taking a gander at the creation utilizing a robotization instrument to discover the inadequacy. In this method, analysers execute the substance attempted what's more, make the aftereffects of the fundamental ordinarily by using the mechanized gadgets.

Diverse Testing Procedures:

- Static Testing
- Dynamic Testing

Static-Testing: For any situation called as Check. Insistence is a consistent system for checking reports and records. This is a strategy to guarantee that whether the item gathered is right i.e., to check the fundamentals which we have and to insist on account of working up of thing is in the manner or not. Exercise required here are Examinations, overviews, Walkthroughs.

Dynamic-Testing: Also called as an approval. Backing is an extraordinary method of looking at the veritable nature of the item. Assent is a presentation, independent of whether the development is in exact piece i.e., to endorse the creation is great or no.

Unit Testing

We have to established the unit testing because system is divided and is related with different types of structuring so that each and every frame and each and every option that is provided will be checked first individually.

Each modules of the project are tested to make sure that all modules work according to the functional requirements. The result obtained with correct input value and the results obtained with wrong input values are verified and validated according to the requirements. By checking each of modules form login to logout process. Here username and password are important to check whether user is using correct username and password.

The considerations of different types of related accomplishments will be undertaken where we have to revise that each and every option that is selected is redirected with detailed work understanding.

Automation testing

Automation references are important because we have to check the policy formulations in different scenarios so we will be established in a detail environment reference so that acknowledgments of the working can be properly referenced.

Integration Testing

The link between all modules is tested for the correct execution to provide to the desired output. Navigation through all the modules are necessary and which are performed in integration testing. Where in the project all modules are interred connected to each other to login to different page. Here once user succeed in login process then only user can enter into the next page where page providing to the user.

System Testing

Once all the modules are connected, it is tested as a single system. This testing is done many times as a process of verification and validation. The connectivity check after the integration is tested accordingly. Project is the combination of all different modules together to work properly. So, this tests the whole system whether all are running properly or not.

7.1 Tables:

m_access_control					
Fields					
Field	Type	Null	Key	Default	Extra
ac_code	int(5)	NO	PRI	(NULL)	auto_increment
f_code	int(5)	NO			
dept_code	int(5)	NO			
desig_code	int(5)	NO			

Figure 7.1.1 access control

The access control table consists of the access code which is auto increments within the database. File code is the secret code provided for every file with is uploaded to the cloud server. Department code and designation code is the code which is inserted by the trustee for during the user sign in.

m_authority					
Fields					
Field	Type	Null	Key	Default	Extra
id	int(5)	NO	PRI	(NULL)	auto_increment
name	varchar(50)	YES		(NULL)	
password	varchar(50)	YES		(NULL)	
adminid	varchar(20)	NO	PRI		
address	varchar(50)	YES		(NULL)	
phone	varchar(15)	YES		(NULL)	
email	varchar(50)	YES		(NULL)	

Figure 7.1.2 Authority

Domain authority is the person who has the control over all the users and trustee. The fields that are provided within authority is domain id, name and password, Admin id with contains special key with address, phone number and email id of the domain authority.

m_cloud					
Fields					
Field	Type	Null	Key	Default	Extra
c_id	int(10)	NO	PRI	(NULL)	auto_increment
c_url	varchar(200)	NO			
c_username	varchar(200)	NO			
c_password	varchar(200)	NO			
c_status	varchar(50)	YES		(NULL)	
c_remarks	varchar(200)	YES		(NULL)	

Figure 7.1.3 Cloud table

The cloud table is used to provide the file details of the user with the remarks and status of the data which is stored, the cloud contains id of each data which will be automatically inserted when the new file is created. Each and every field of file contains url of the respective field with its name and password.

m_config					
Fields					
Field	Type	Null	Key	Default	Extra
key_id	int(10)	NO	PRI	(NULL)	auto_increment
key_date	varchar(100)	NO			
public_key	blob	NO			
master_s_key	blob	NO			
des_secrete_key	blob	YES		(NULL)	
no_of_clouds	int(10)	YES		(NULL)	

Figure 7.1.4 Configuration

Configuration is the process which takes place when a file is loaded to the cloud. To transfer the file, it generates a key with different fields, the date when the key was generated with the public key which is access by every user within the cloud platform. A master key which will be available only to the admin. The number of cloud platform created by single user with its secret key.

m_file_upload					
Fields					
Field	Type	Null	Key	Default	Extra
f_code	int(5)	NO	PRI	(NULL)	auto_increment
f_name	varchar(100)	NO			
f_type	varchar(50)	NO			
f_upload_date	varchar(50)	NO			
f_subject	varchar(200)	NO			
cloud_id	int(5)	NO			
owner_id	int(10)	NO			

Figure 7.1.5 File upload

When a file is uploading file within the data table, the file contains auto generated code even each file is loaded. File name, type of the file which contains the designation and the department. Date of which the file was uploaded, which subject the file type, name of the file owner with the cloud id.

m_transaction					
Fields					
Field	Type	Null	Key	Default	Extra
t_no	int(10)	NO	PRI	(NULL)	auto_increment
t_date	varchar(100)	NO			
t_time	varchar(100)	NO			
u_code	int(10)	NO			
f_code	int(10)	NO			
dept_code	int(10)	NO			
design_code	int(10)	NO			
t_status	varchar(50)	YES		(NULL)	

Figure 7.1.6 Transaction

Transaction status can be viewed by the user and the trustee who checks for the transaction which is taken place by a single use at a time and what are the files which are uploaded or downloaded by the user. The trustee can view the date, time, status of the transaction using the file code, department code and designation code.

m_trustee					
Fields					
Field	Type	Null	Key	Default	Extra
id	int(5)	NO	PRI	(NULL)	auto_increment
name	varchar(50)	YES		(NULL)	
password	varchar(50)	YES		(NULL)	
ownerid	varchar(20)	NO	PRI		
address	varchar(50)	YES		(NULL)	
phone	varchar(15)	YES		(NULL)	
email	varchar(50)	YES		(NULL)	

Figure 7.1.7 Domain Trustee

Trustee within the profile the trustee can enter name, edit password, contains owner id, address and phone of the trustee who is authorized by the domain authority.

7.2 TEST CASES

TESTCASES ID	NAME OF TEST	ITEMS BIENG TESTED	SAMPLE INPUT	EXPECTED OUT	ACTUAL OUTPUT	REMARK
TCA01	Authority Login	Admin module	Invalid Authority-id Wong Password	Depending upon correct input its login's in as Admin	Admin invalid id and password login failed	PASS
TCA02	Authority Login	Admin module	Valid Authority-id Wong Password	Depending upon correct input it's login as Admin	Admin Login Failed	PASS
TCA03	Authority Login	Admin module	Unique Trusty ID	Depending upon unique Trusty-id user has to get registered.	Registered Failed	PASS
TCA04	Trusty Creation	Admin Module	Unique Trusty ID	Depending Upon unique Trusty-id user has to get registered.	Registered Success	PASS

Authority login test case it checks for the admin module the expected output depends on the correct input as login admin. The system checks depending on the unique user password it has to register, if correct password is entered then enters to the home page. The authority login can create trustee by using the unique trusty id and register successfully.

TCT01	Trusty Login	Trusty module	Invalid Trusty -id Wong Password	Depending upon correct input it must login as Trusty	Login Fail	Pass
TCT02	Trusty Login	Trusty module	Valid Trusty -id Wong Password	Depending upon correct input it must login as trusty	Login Fail	Pass
TCT03	Trusty Login	Trusty module	Valid Trusty -id Correct Password	Depending upon correct input it must login as Trusty	Login Success	Pass
TCT04	User Registration	Trusty module	Existing User-id	Depending Upon unique User-id user has to get registered send mail	Registration fail	Pass
TCT05	User Registration	Trusty module	Unique User-id	Depending Upon unique User-id user has to get registered send private key to mail	Registration success	Pass

TCu01	User Login	User module	Invalid Uer -id Wong Password	Depending upon correct input it must login as User	Login Fail	Pass
-------	------------	-------------	-------------------------------------	--	------------	------

TCU02	User Login	User module	Valid User - id Wong Password	Depending upon correct input it must login as User	Login Fail	Pass
TCU03	User Login	User module	Valid User - id Correct Password	Depending upon correct input it must login as User	Login Success	Pass
TCU04	Download file	User Module	Invalid private key and Invalid pseudo key	Private key and pseudo key are valid Download then download file if access is provided	Download fail	Pass
TCU05	Download file	User Module	Valid private key and Invalid pseudo key	Private key and pseudo key are valid Download then download	Download fail	Pass

The trustee logs in through the login id if the id which is provided by trustee is true then it checks for the other operation if the trustee enters wrong password then it will be re-directed to the previous page. Then checked for the password provided by the trustee during the login if password matches the requirement then the trustee can perform the operation. Trustee logs in to the module and can add or delete the user who have registered into the cloud check for the modification if required. The trustee can upload file to the cloud authority when a user needs to upload and send the files to the user if the user request for the file download. User logs in to the system to request for file needs to be downloaded, user can login to system by providing username or id which is saved in the software while registering to the cloud service.

CHAPTER 8

Conclusion

In our task, we have a constructor instrument for improvement of distributed computing framework where the client of the cloud stage can do the information sharing secure and there is no danger of dangers or hacking should be possible while moving the document or during the record download. In this venture we have proposed three principle areas, they are space authority, area trustee and the client.

Information sharing is accepting considerable consideration in distributed storage for data correspondence innovation, distributed storage is giving proficient and successful stockpiling administrations. Overseen, worked and kept up on a capacity server that are based on virtualization strategies. Information that must be classified those are touchy must be ensured by cryptographic procedures are generally applied.

In which the authority is the leader of the cloud administration who is the administrator to the exchanges which happens and who monitors the trustee and the client in each phase of record getting to. The authority makes trustee who checks for the client conduct and furthermore administrator the expel the trustee from the administrator board.

Trustee is the individual who keeps up the document and he is the person who can see or keep up the client subtleties. Trustee stores documents in cloud which is gotten to by the information buyers. As indicated by the information size cloud stage and programming can be scaled up and downsize utilizing the framework administrations. As the quantity of clients increments and diminishes the presentation is estimated. Normalized nature of distributed computing administration is utilized to make cloud interoperable among various suppliers.

Information figured procedure and capacity and programming conveyance is moved away from work areas and neighbourhood servers towards server farms over the web. Suppliers provided cloud benefits by marking SLA's with customers and end clients. The administration must be effective, a cloud stage administration must be scaled up or downsized its presentation as the quantity of clients increment and lessening.

CHAPTER 9

Future Enhancement

The record present in the cloud stage the information is forestalled by utilizing the key and sent to the space client by exchange. The encryption key is given to information while information should be sent to information sharer which is put away and during the information is secured by an extra insurance which is the extra layer. Driven by the highlights and focal points of the distributed computing administrations, the distributed computing-based application in industry and examination network they are increasing more force on improvement and sending. Distributed computing is a utility figuring, since it shares immense information the information sharing interest is high. The gigantic information that are shared on the double is cost expending task, the assets can be concentrated or a conveyed PC framework. The mutual information cost could be decreased with assistance of distributed storage, secure information the board activities.

In cloud information sharer can transfer the information and afterward get to one side. In the wake of transferring the document information sharer can get the information. Not just sharing of information is done tossed distributed storage It as likewise presented the odds of sharing the information without approval. Cryptographic plans are constantly utilized secrecy of the mutual information.

Bibliography

Appendix A

Review through Books

Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.

Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology. Upper Saddle River, NJ: PrenticeHall, 2001

Hoffstein, Jeffery, Pipher, Jill and Silverman, Joseph H. NTRU: A Public Key Crypto
<http://grouper.ieee.org/gatherings/1363/lattPK/submissions.html#NTRU1>

Kurose, James F., Ross, Keith W., Computer Networking: A top Down Approach Featuring the Internet. second release. Addison Wesley 2002.

Audit through Web Reference:

www.codenotes.com

www.dotnetspider.com

www.gotdotnet.com

msdn.microsoft.com

www.dotnet247.com

www.cs.columbia.edu

www.cdt.luth.se/~peppar/docs/lic/html/node66.html