A project report on

COMPUTATION OPTIMIZATION OUTSOURCING SECURELY IN CLOUD COMPUTING

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

MASTER OF COMPUTER APPLICATIONS

Of

Visvesvaraya Technological University
Belgaum, Karnataka
By

CHANDAN S

1CR16MCA09

CMR INSTITUTE OF TECHNOLOGY
132, IT Park Road, Kundalahalli, Bengaluru-560037
2019-2020

A project report on

COMPUTATION OPTIMIZATION OUTSOURCING SECURELY IN CLOUD COMPUTING

Submitted in partial fulfillment of the requirement
for the award of the degree

MASTER OF COMPUTER APPLICATIONS

Of

Visvesvaraya Technological University
Belgaum, Karnataka
By

CHANDAN S

1CR16MCA09

CMR INSTITUTE OF TECHNOLOGY
132, IT Park Road,Kundalahalli,Bangalore-560037
2019-2020

A project report on

COMPUTATION OPTIMIZATION OUTSOURCING SECURELY IN CLOUD COMPUTING

Submitted in partial fulfillment of the requirement
for the award of the degree

MASTER OF COMPUTER APPLICATIONS
Of
Visvesvaraya Technological University
Belgaum, Karnataka

By

CHANDAN S

1CR16MCA09

Under the guidance of

Internal Guide

Ms. Gomathi T
Asst Professor & HOD
Department of MCA
CMRIT, Bangalore

External Guide

Mr.T Nagamalleswara Rao
Technical Lead
MPower Global Pvt Ltd
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 - 560037

CERTIFICATE

This is to certify that the project work entitled

COMPUTATION OPTIMIZATION OUTSOURCING SECURELY IN CLOUD COMPUTING

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
is a result of the bonafide work carried out by

CHANDAN S
1CR16MCA09

during the academic year 2019-2020.

Signature of the Guide	**Signature of the HOD**	**Signature of the Principal**
Ms. Gomathi T	**Ms. Gomathi T**	**Dr. Sanjay Jain**
HOD, MCA	HOD, MCA	PRINCIPAL, CMRIT

External Viva

Name of the Examiners — Signature with date

1.

2.

DECLARATION

I, **CHANDAN S,** student of 6th MCA, **CMR Institute of Technology**, bearing the USN **1CR16MCA09**, hereby declare that the project entitled **"Computation Optimization Outsourcing Securely in Cloud Computing"** has been carried out by me under the supervision of External Guide **Mr. T Nagamalleswara Rao,** Technical Lead, MPower Global Pvt Ltd , Bangalore and Internal Guide **Ms. Gomathi T**, **Asst Professor & HOD**, **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 2019-2020.The reports has not been submitted to any other University or Institute for the award of any degree or certificate.

Place: Bangalore Chandan S

Date: (1CR16MCA09)

ACKNOWLEDGMENT

I would like to thank all those who are involved in this endeavour 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. T Nagamalleswara Rao, Technical Lead, MPower Global Pvt Ltd., Bangalore, and to my Internal Project guide Ms.Gomathi T, Asst Professor & HOD, Department of MCA, CMRIT, Bangalore without whose help and support throughout this project would not have been this success.

I am thankful to Dr. SANJAY JAIN, Principal, CMRIT, Bangalore for his kind support in all respect during my study. I would like to thank Mr. T Nagamalleswara Rao, Technical Lead, MPower Global Pvt Ltd., Bangalore, who gave opportunity to do this project at an extreme organization Most of all and more than ever, I would like to thanks 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.

Chandan S
(1CR16MCA09)

Certificate of Completion

Is hereby granted to

CHANDAN S

Reg No: 1CR16MCA09

We are glad to inform you that **Mr. CHANDAN S** of **CMR INSTITUTE OF TECHNOLOGY, Bangalore** has successfully completed his Internship and Project work at Trans mPower Global Pvt Ltd from **26th DECEMBER 2019** to **29th MAY 2020**.

During his internship, he was exposed to the activities related to **JAVA Web Application Development.**

He has worked on a project titled "**COMPUTATION-OPTIMIZATION OUTSOURCING SECURELY IN CLOUD COMPUTING**".

We found him extremely inquisitive and hard working. He was very much interested to learn the functions of Java Technology and also willing to put his best efforts and get in to depth of the subject to understand it better.

His association with us was very fruitful and we wish him all the best in the future endeavours.

For Trans mPower Global Pvt Ltd

Authorized Signatory.

CHAPTER 1

INTRODUCTION

1.1 Project Description:

Cloud Infrastructure makes on-demand feasible Connection to the network through a common device pool Tools which can be implemented easily Performance and low cost control easily through good productivity and limited supervision above. Above, overhead. When the task is externalized into the cloud, absolutely infinite software should be used by customers Pay-per-use services without any obligations significant expenditure in both equipment and acquisitions Overhead applications and/or running. Computing outsourced to the public cloud deprive even consumers with automatic device power consume and produce their data during Computing that eventually produces new protection concerns and problems for this machine Development that can be applied easily with high productivity and low overhead control.

Berechnungs Workloads typically contain sensitive data such as Financial reports for companies, advanced analysis or Identifiable details on personal wellbeing etc. Say Combating unwanted leaks, classified details Until outsourcing, data must be authenticated in order to Ensure the protection of end-to - end details Over and over the ground. The web operating data Customers are not fully clear. In turn, There are common cloud service reasons behave unfaithfully and offer fake findings This could be more than an truthful semi classical pattern.

Online infrastructure gives the business an outstanding opportunity to provide reliable machine resources at low prices. It allows consumers with minimal machine infrastructure to outsource massive cloud computing workloads Enjoy the great machine capacity, bandwidth, garage or even correct tools that you can use economically Be paid-per-use posted. Exchange it. While blessing is of a very high standard, safety is the number one boundary forestalls the far reaching reception of this promising adaptation of processing, especially for customers while holding individual information at some phase of the calculation they are ate up and created.

The Cloud is regarded as a totally insecure device From the cloud customers ' point of view, we need structures that are not most responsive to the defense Records make encrypted

statistical calculations but also shield customers from them Malicious conduct by requiring the finding to be confirmed.

One system of this type in theory, fashionable and comfortable code outsourcing proved feasible these days, but Practically effective systems remain a rather difficult issue. This document seems relaxed Outsourcing of linear (lp) equations which are commonly available. In an effort to achieve substantial performance, our method clearly decomposes the outsourcing of the lp calculation into the freely accessible lp solvers Cloud parameters and individual device lp parameters. The versatility of tests enable one to find adequate security / performance balance via the abstraction at the higher stage of lp measurements than the general circuit Identity. Identity.

Externalization is a common technique used in world of company when the customer decides to farm an agent has certain mission. The Customer's explanations There can be many to outsource the agent to the task lack of money to achieve the mission locally Conscious financial or response time choice That is why. Distributed computing gives simple access to a mutual pool on request Processing assets configurable which can be rapidly Utilizing with superior and restricted Overhead administration. Its goal is a real-life affinity feature This polyhedron is described. A linear algorithm of programming must consider a place in the polyhedron where this function has if there is such a point, a smallest (or largest) value. Given the great benefits, others are inaccessible health issues and consumer problems and the cloud isn't within the same domain of trust[1].

The data processed and generated during the processing Cloud computing is usually confidential. Furthermore, because inside the cloud operating data Customers are not sufficiently transparent, so no Quality of the computed is guaranteed The cloud results. This paper discusses stable large-scale outsourcing. Linear equation systems (LE) within the systems most popular computer and algorithmic tools related areas in engineering that examine and Optimize systems in the real-world. The volume requires The coefficient matrix of the system can easily exceed Customer computer device memory available 50,000 to 50,000 system matrix of typical double accuracy, which can result Electromagnetic devices can be conveniently involve up to 20 GB of extra room, which Low-end registering gadgets computational force.

The time a PC program is running additionally not simply depends on how many tasks it needs to perform Race, but also on the data position in the Hierarchy of memory

1.2 Problem Statement:

Two separate procurement systems As seen in the Fig, individuals. 1: who's the cloud client has a great deal of computer-cost LP Cloud service issues to be externalized; (CS) has considerable capital and estimates provides facilities such as managing computer resources Pay-per-use shared LP solvers. The company Has to solve a major problem with linear programming. But, because of the shortage of electronic tools, such as Control, power, data etc. encoding. Unable to do so Locally carry out these expensive measurements. Therefore, the For addressing the LP and CS Business resorts CS and Calculation power is leveraged in a pay-per-use way. The consumer will not give the initial question right away. Next use a hidden map key for any edition encrypted And the problem with CS outsources. Linear Programmable History The question of optimization is generally developed as a Issue of mathematical programming with values for reducing (or maximizing) a collection of judgment variables Objective attribute that describes a collection of costs limits. limits. The goal function is an association with the judgment variables for linear programming and the Limits are a linear equation scheme and Unfairness. Because of a limit of linear form Unfairness can be spoken to as a numerical condition Usage of a non-negative leeway and free vector The element of judgment may be represented as two The auxiliary variables are non-negative.

CHAPTER 2

LITERATURE SURVEY

2.1 Existing System:

The new work has made consistent progress on "free externalization of costly calculations" in both cryptography and theoretical machine scients societies. In principle a general outcome of protected computation outsourcing was proved feasible in view of Yao's troubled circuits and on Upper class' historic research on a totally homomorphic encryption (FHE) technique, in which computation is described by a combined cryptographic booline circuit that can be evaluated by cryptographic personal inputs. Frikken offers a provenly secure technique to add hidden outsourcing matrix anonymously. Although this research executes the previous work in the context of the presumption and reliability of a single server (not expensive cryptographic primitives), the downside is the broad overall contact. According to the secret sharing technique, all scalar operations are extended to polynomials with the original matrix multiplication which implies considerable overhead.

2.2 Objective of the work:

The problem of stable outsourcing of Cloud Computing LP computations is formalized, and have such a realistic system architecture that ensures safety , stability and quality of input / output. Explicitly breaking down LP computation into private data and public LP solvers, our system engineering can Investigating worthy security/effectiveness forfeits by more elevated level LP calculation than the general circuit depiction. We set up issue unraveling procedures which can furtively transform the underlying lP into certain clients Self-assertive while protecting touchy data input/yield.

Frikken offers a provenly secure technique to add hidden outsourcing matrix anonymously. Although this research executes the previous work in the context of the presumption and reliability of a single server (not expensive cryptographic primitives), the downside is the broad overall contact. According to the secret sharing technique, all scalar operations are extended to polynomials with the original matrix multiplication which implies considerable overhead.

Straight line scheming is obviously an analysis and measurement technique which catches what appears to be some process parameters, which need to be improved further so it makes sense to construct inflation. Inflation. It was primarily used in various architecture areas, such as packer sorting, flow administering, power administering over data centers, etc., to analyze and modify existing techniques / models. Nonetheless, whether you can retain the independent data collected and produced by prospects from beginning to end has become the principal trouble of democracy.

This script is focused on metallurgical computing and inflation activities and explores the accurate externalization of publicly available straight as computation for arrow programming (LP). To explain the rise in figures, the basic fallacy postulate of LP must be addressed and the required and tolerable conflicts must be resolved.

2.3 Proposed System with Methodology:

In this article, the effective methods for stable linear programming (LP) outsourcing are discussed. Linear programming is a computational and algorithmic technique that catches first order effects of specific machine parameters that require optimization and is important for the optimization of engineering.

The customer's public LP solver and private LP criteria are clearly decomposing the LP computation outsourcing.

In particular, we first create customer-owned private data as a collection of matrices and vectors for LP problems. These higher degree of representation helps one to apply a variety of powerful strategies of data security issue change, including framework increase and propelled mapping, to randomize the underlying LP question while saving basic info and yield subtleties.

This was utilized widely across various fields, for example, parcel preparing, stream guideline, power the executives of server farms, and more, in analysing and optimising real-life systems / models.

The versatility of these breakdown helps one to analyze higher degrees of complexity of LP calculations for functional utility than general circuit representation. For the first time, the question of safe LP calculations is formalized and a clear, realistic mechanism design is generated which meets safety, durability and efficiency input / output.

The system saves the customers a ton of cloud computing from stable LP outsourcing, as it just takes a little time to solve a typical LP problem. The cloud service computations bear the difficulty of functional algorithms presently in use to address linear programming challenges, which guarantees an commercially feasible usage of the computer. This trial shows that our instrument can generally spare clients more than 50 percent when the size of the first LP issues (whose arrangements are achievable) isn't excessively little, without presenting a huge cloud overhead.

2.4 FEASIBILITY STUDY

The feasibility study is to reference the requirement which is feasible for undertaking the proposed project different types of fractions are divided and each perfection will be discussed where the important considerations taken are in terms of : -

- Operational feasibility
- Technical feasibility
- Economic feasibility
- Scheduling feasibility

2.4.1 Operational feasibility

The operation’s are required to be guided has different types of design and implementation features are added so different types of steps will be taken to make understand about the real usability of the system.

The ease of use of the framework will be furnished with the assistance of definite preparing that will be given in house and even the references that will be direct as documentation.

The operations are well performed with the references off automated notification also making it very much useful when multiple users are using it in real time.

2.4.2 Technical feasibility

Operational considerations of the component which has to be included in multiple references for example when different types of perception are acknowledged the components will be automatically different so each reference is required to be provided in a compatible working manner.

All types of reference pages included will be checked for multi incorporated working which have associated to have detailed reference workability.

The technical aspects of incorporated sharing of the stages will be also undertaken as it is required that according to the scenario the perfection can be matched.

Reference of the sharing will be checked for the conversion and for the security based transfer.

Multiple templates and project undertaking with the concerned objectification will be also checked as it is needed that each perception should be perfect for the references and understanding.

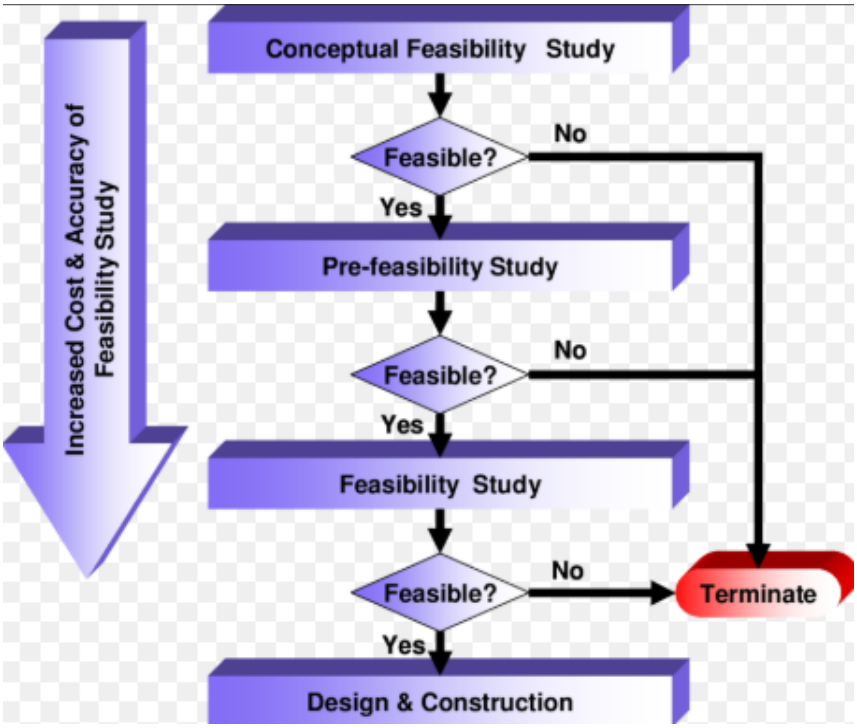


Figure 2 :-Shows the feasibility consideration.

2.4.3 Economic feasibility

The economic consideration that are proposed should be based on a proper mechanism of statistics that has to be generated to get an idea that how much money is required to undertake the overall development and implementation work.

Return on investment calculations will be performed so that will be having a clear understanding about how much money is required and for what.

Economic understanding is required for successful implementation of project.

2.4.4 Scheduling Feasibility:

This evaluation is the most critical one for project success after all, if not finished on schedule, a project would collapse. An company determines in the complexity of arranging how much time the project would take to finish.

2.5 Tools and technologies used

2.5.1 Technology

Java

It is an unadulterated article situated programming or language and that is comparative like c++ and is, autonomous stage in plan. Java is. Likewise an elevated level programming and language which was created by or James Gosling in., 1991. Because of this nature it can run on various stages like Unix, Macintosh, Windows. Java provides its own programming framework that contains JVM, Core Classes and Libraries, and is responsible for operating the computer's java software. JVM transforms the mysterious byte code into machine code and executes it.

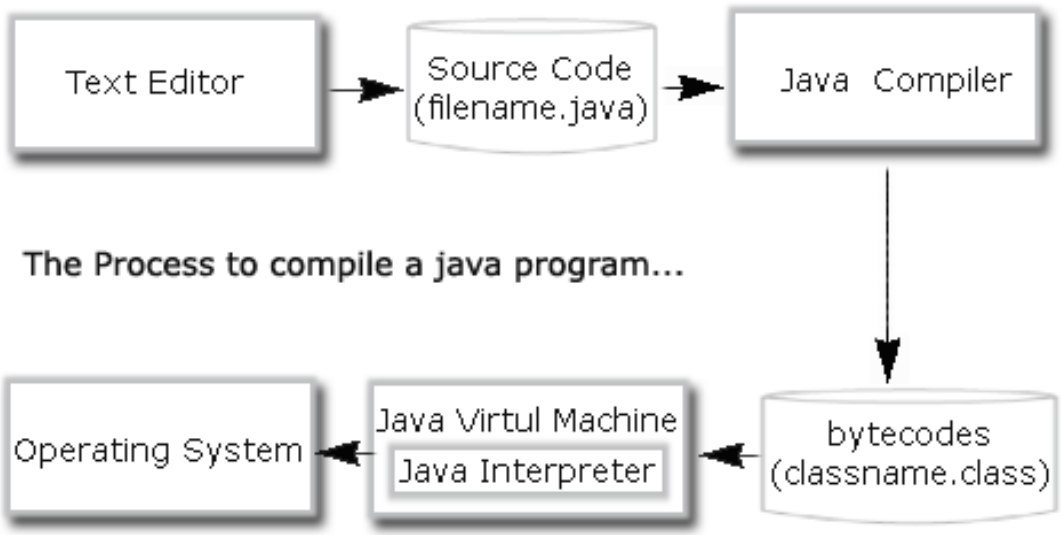


Fig : process to compile a java program

J2EE

The infrastructure on the server side is already an new technology in the creation of J2EE's web applications. Safe , efficient and flexible market applications. It enables developers to develop multi-stage apps. Both server and customer sides are possible for applications.

To perform the following tasks, the company application was developed:

1.Create a good gui for consumers.

2.To process data under some client laws

3.Through network contact

4. To save details.

Servlet technologies in java:

A servlet is an instrument for creating Programming applications on the Server side. Is utilized to make site pages that are dynamic. It is sturdy and robust. Servlet is an API that contains the classes and interfaces of serve, serve, service serve, service request and service reply. Servlet is an application. It provides better performance, portability and protection.

Java server pages

Servlets that are used in built Web applications are similar technologies. There are jsp tags and html tags there. Compared to servlets, it is simpler to manage and build. It is used mainly for redirecting, i.e. from one page to the next.

JSP benefits:

1.JSP design and maintenance are easy.

2.No computer recompilation necessity.

3.Code ambiguity is minimized by JSP.

JDBC Drivers

To interface java-program to database a JDBC driver is utilized JDBC drivers are 4 structures

1. JDBC ODBC driver for bridge Driver

2. Native API (Java part)

3. Driver of the Network Protocol

4. Thin driver (completely java)

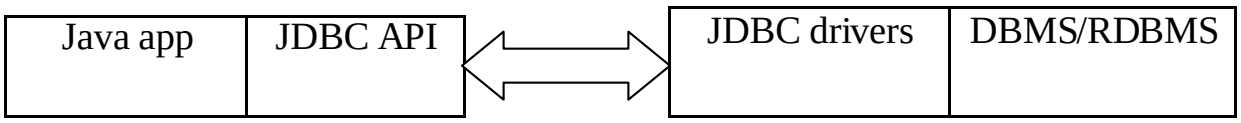


Fig : Data base with driver

JDBC driver-Manager:-

The jdbc driver-director is the spine for the Jdbc design. This manager manages a set of drivers generated for different DBs and the Java App link to a Java application user.

Apache POI

Apache POI has been developed with the aid of Java programs to handle Microsoft Excel sheets. The Apache Foundation is an open source API. "Bad Obfuscation Design" implies POI.

XSSFWorkbook − The module in Apache POI includes the methods for reading and writing excel sheets in the format.xls and.xlsx. Yet it is preferred only while operating with MS-Office edition 2007 and later.

2.6 Hardware Requirements:

- System : Pentium IV 2.4 GHz. (min)
- Hard Disk : 40 GB. (min)
- Ram : 512 Mb. (min)

2.7 Software Requirements:

- Operating System : Windows XP/7/8/10.
- Coding Language : JAVA/J2EE
- IDE : Netbeans 7/8
- Database : MYSQL
- Scripting : Java Script
- Front end : Jsp/html
- Web technologies : css/xml/html

CHAPTER 3

SOFTWARE REQUIREMENT SPECIFICATIONS

3.1 Customer:

We build the software of the Customer in this module. First, consumer signs and logins the information. Using a linear programming technique, customers will outsource critical and useful data to the cloud through multiplications in the ProbEnc issue encryption and automatically deliver hidden file key to their mail ID. You will access the file information uploaded. If the recipient is involved in retrieving the file from a server by utilizing the file's hidden key. When the software doesn't suit, consumer can't open the script.

3.2 Cloud:

We build the cloud functionality in this module. All user records, file upload data, and installation details can be accessed by the Cloud agency. We use and build the DriveHQ Cloud Service API in this module for cloud integration.

3.3 Analysis of I/O Privacy:

In the previously mentioned ciphertext format, we presently assess input/yield security ensure. In particular, the main data got by the cloud server is that both A and B of the original LP issue are generic matrices in full rank. Please notice that no hidden transition key is used twice in our layout. Offline guesses on issue input/yield don't give any profit to cloud servers because the truth of speculation can not be explained. We presume that our method uses finite floating precision numbers, with the entry xi of the original x solution in the extend L with k as our assurance parameter and poly as a polynomial capacity.

3.4 Linear Programming Methodology:

The decay of LP calculation into open LP solvers working on cloud and private information kept up by the shopper will give stable LP outsourcing via cloud. As specific LP decompositions typically create multiple trade-offs between performance and protection assurances, it is therefore of vital importance to choose the best approach that is most suited for our design goals.

To research this disparity systematically, we arrange the multiple decomposition into a hierarchy that incorporates the standard manner in which a function is specified: the higher abstractive approximation is composed of calculations at the lower levels of abstraction. At a larger degree of complexity further knowledge about the computations can be rendered accessible to the public, meaning that protection assurances are weaker. The architectures are similar at lower complexity stages, although the cloud may provide fewer details usable in order to obtain better protection assurances at the expense of performance.

We are focused on the top level of the hierarchy since we want to develop technically effective processes of secure LP outsourcing. We will discuss strategies of issue transformation that allow customers to secretly convert the initial LP to spontaneously develop the protected LP outsourcing.

3.5 Non-Functional Requirements:

According to the incredibly difficulty of the FHE process as well as to negative circuit sizes, which can not be addressed with the creation of initial and shielded circuits, implementation of the current system to our everyday computations is far from realistic. Either strong cloud-side cryptographic computations or dynamic implementations of multi-round protocols, or large connectivity complications, require current strategies. In short, essentially productive frameworks for safe cloud storage with immediate activities remain. The system saves the customers a ton of cloud computing from stable LP outsourcing, as it just takes a little time to solve a typical LP problem. The cloud service computations bear the difficulty of functional algorithms presently in use to address linear programming challenges, which guarantees an commercially feasible usage of the computer. This investigation shows that our component can generally spare clients more than 50 percent when the size of the first LP issues (whose arrangements are doable) isn't excessively little, without presenting a critical cloud overhead.

3.6 Functional Requirements:

The customer's public LP solver and private LP criteria are clearly decomposing the LP computation outsourcing. In particular, we first create customer-owned private data as a collection of matrices and vectors for LP problems. These higher degree of representation helps one to apply a variety of powerful strategies of data security issue change, including network increase and propelled mapping, to randomize the underlying LP question while safeguarding basic information and yield subtleties.

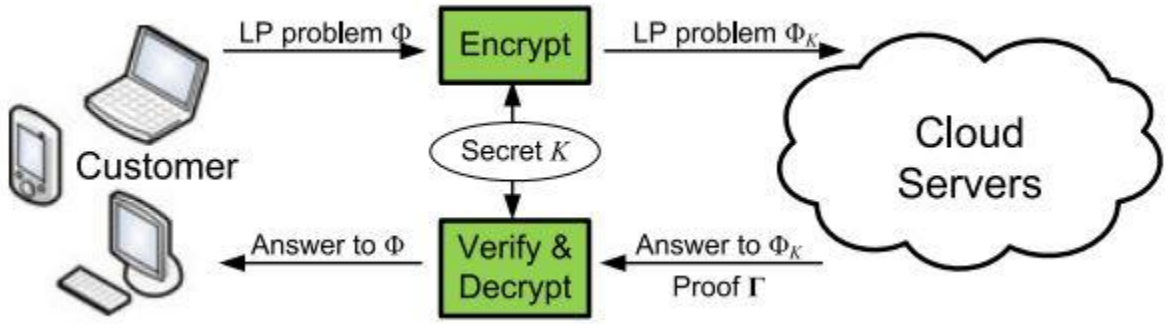
This was utilized broadly across various fields, for example, bundle handling, stream guideline, power the board of server farms, and more, in analysing and optimising real-life systems / models. The versatility of these breakdown helps one to analyze higher degrees of complexity of LP calculations for functional utility than general circuit representation. For the first time, the question of safe LP calculations is formalized and a clear , realistic mechanism design is generated which meets safety, durability and efficiency input / output.

The system saves the customers a ton of cloud computing from stable LP outsourcing, as it just takes a little time to solve a typical LP problem. The cloud service computations bear the difficulty of functional algorithms presently in use to address linear programming challenges, which guarantees an commercially feasible usage of the computer. This examination shows that our instrument can generally spare clients more than 50 percent when the size of the first LP issues (whose arrangements are attainable) isn't excessively little, without presenting a huge cloud overhead.

CHAPTER 4

SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE:

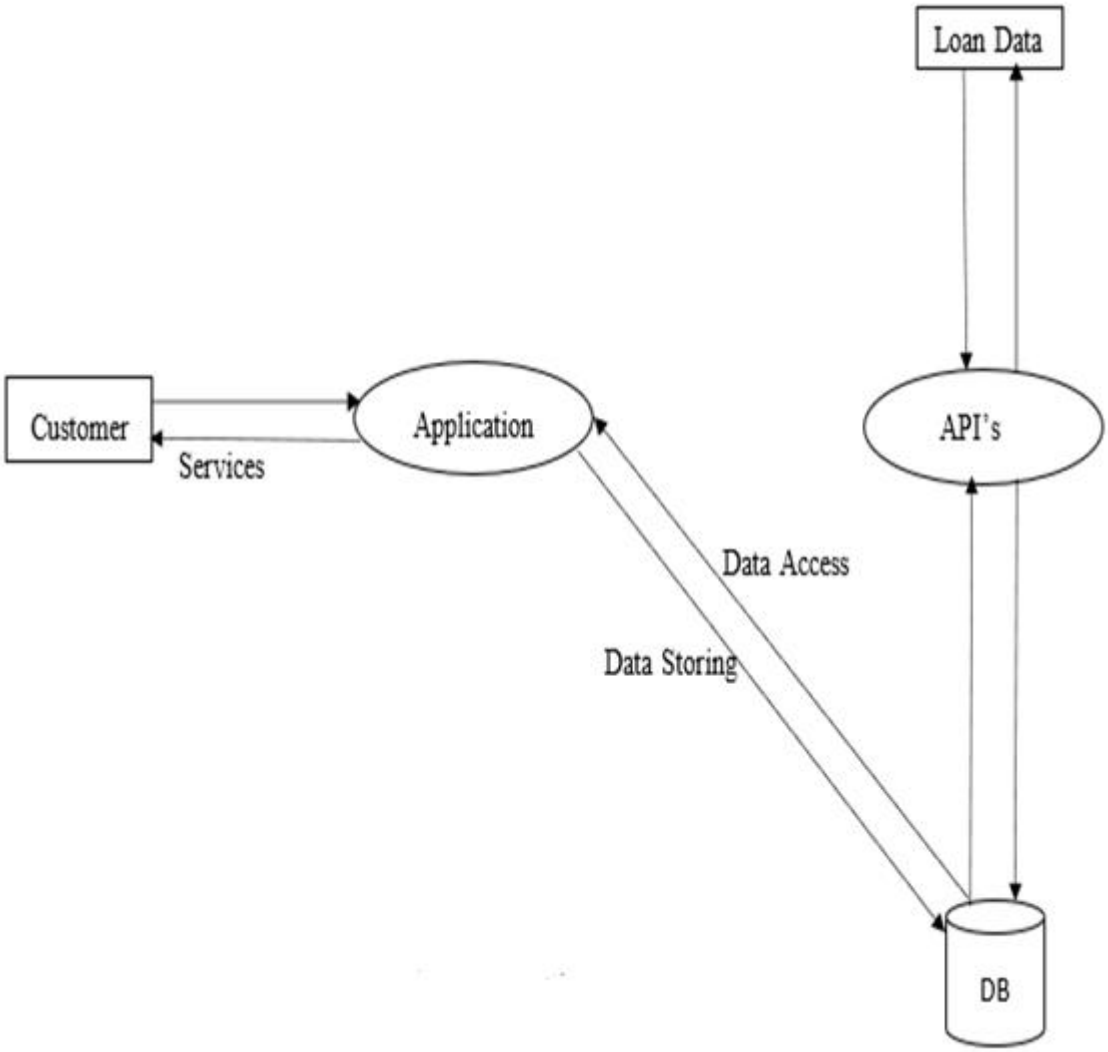


The customer has a wide linear schedule The problem is to be solved (later to be formally defined). Because of the lack of computer resources, such as Could not process power , storage, memory, etc. Perform local computing of this costly kind. Furthermore, the For solving LP computation, customer resorts to CS and leverages its pay-per-use computing capability The path. The path. Rather than submitting the initial question right away, The client uses the elusive K to visualize the entire thing in the first place. Encrypted edition oscillate K and trouble with outsources oscillate between K and CS.

The health risks to the machine platform The malicious activity of CS comes mainly. We Suppose that the CS is above the "honest butcurious" type , i.e. semi-honest expected type. either through a lot of previous research Whether it wants to or is unable to do so. The CS will be involved persistently in the study Encrypted and authenticated data submitted by the consumer Machine produced output to obtain knowledge important, as in the semi-legitimate model. An issue of improvement is commonly defined as an issue of scientific programming which looks to decrease the qualities for an assortment of choice factors (or Expand) (the objective hazard work The limitations are dependent upon a determination. For sequential strategy, The target function is the decision's affine function Variables and limits are a linear framework Inequalities and statistics.

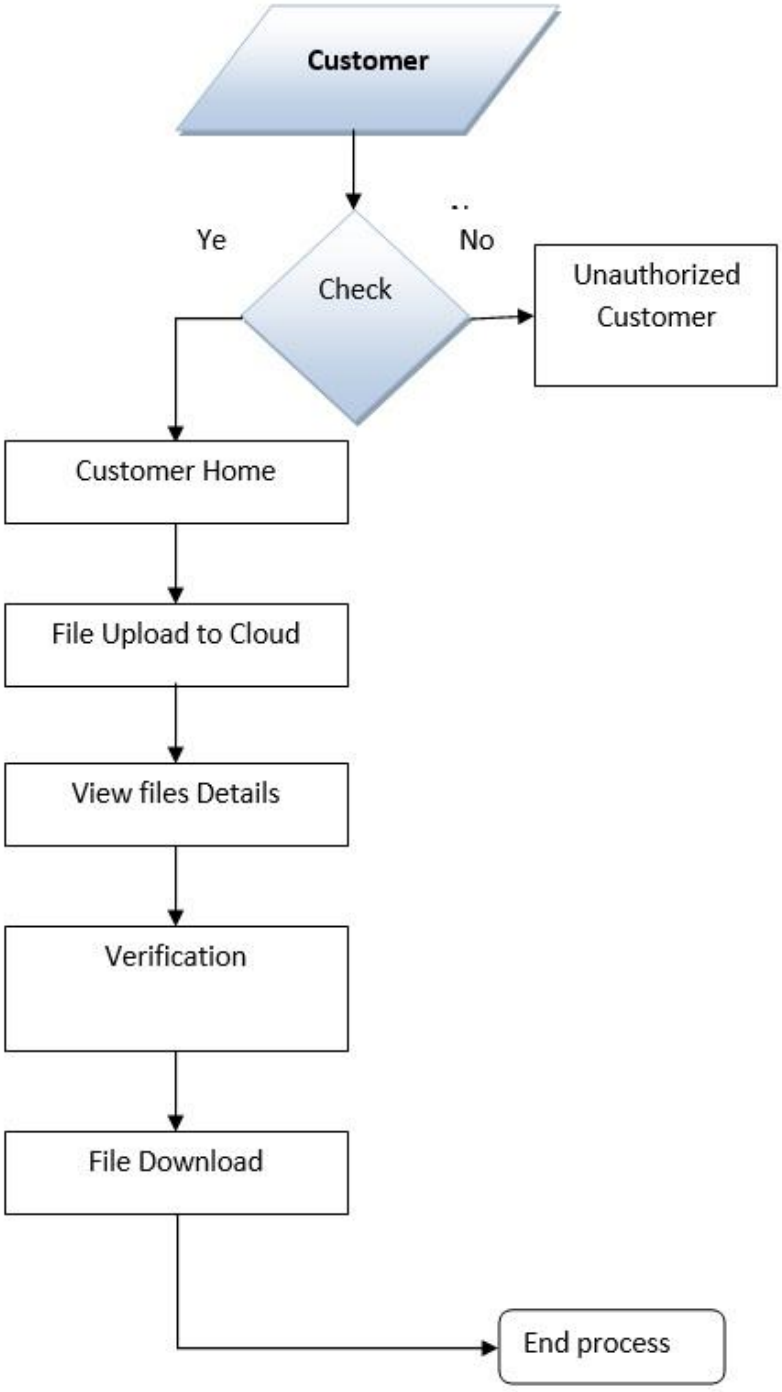
4.2 CONTEXT DIAGRAM:

Context diagrams will be used to represent boundaries between the system, entities and showing how they interact with each other in the system.

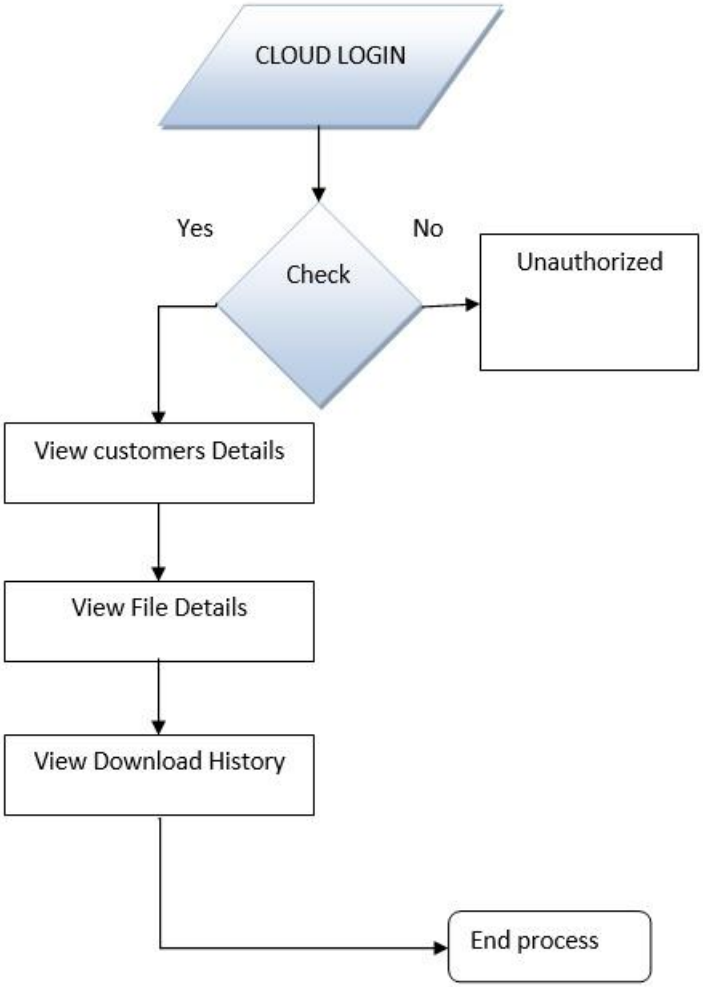


4.3 Data Flow Diagram:

4.3.1 Customer Flow Diagram:



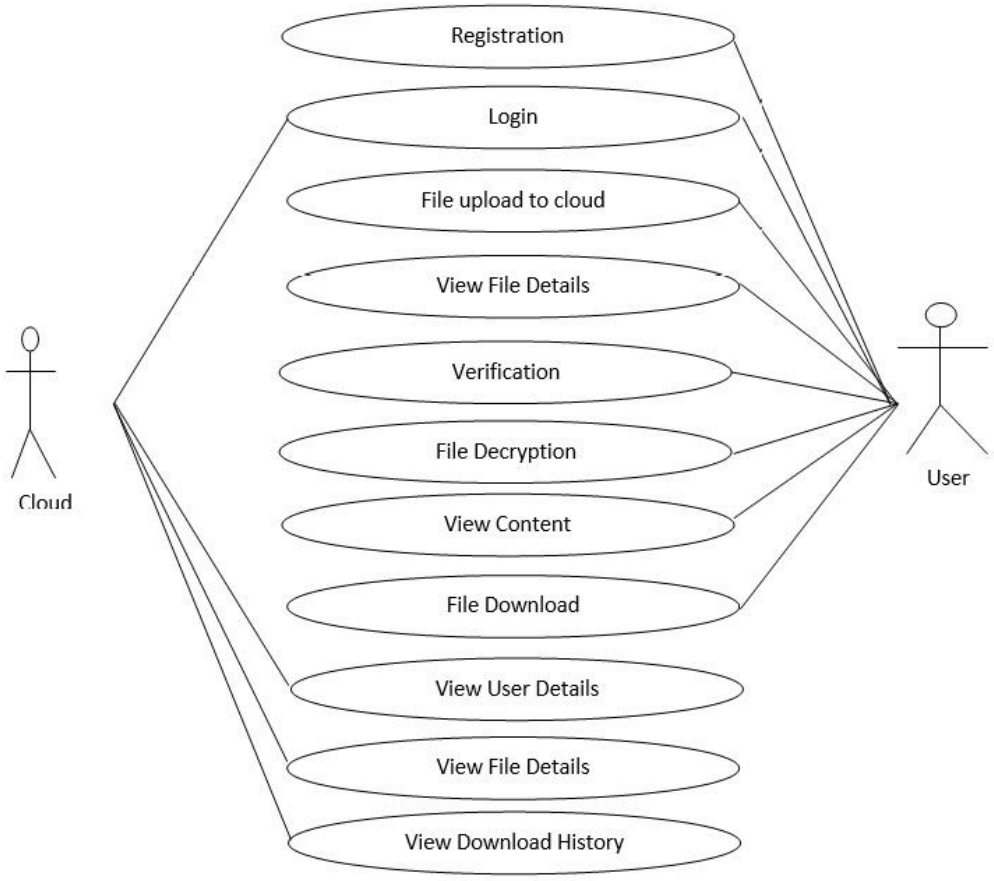
4.3.2 Cloud Flow Diagram:



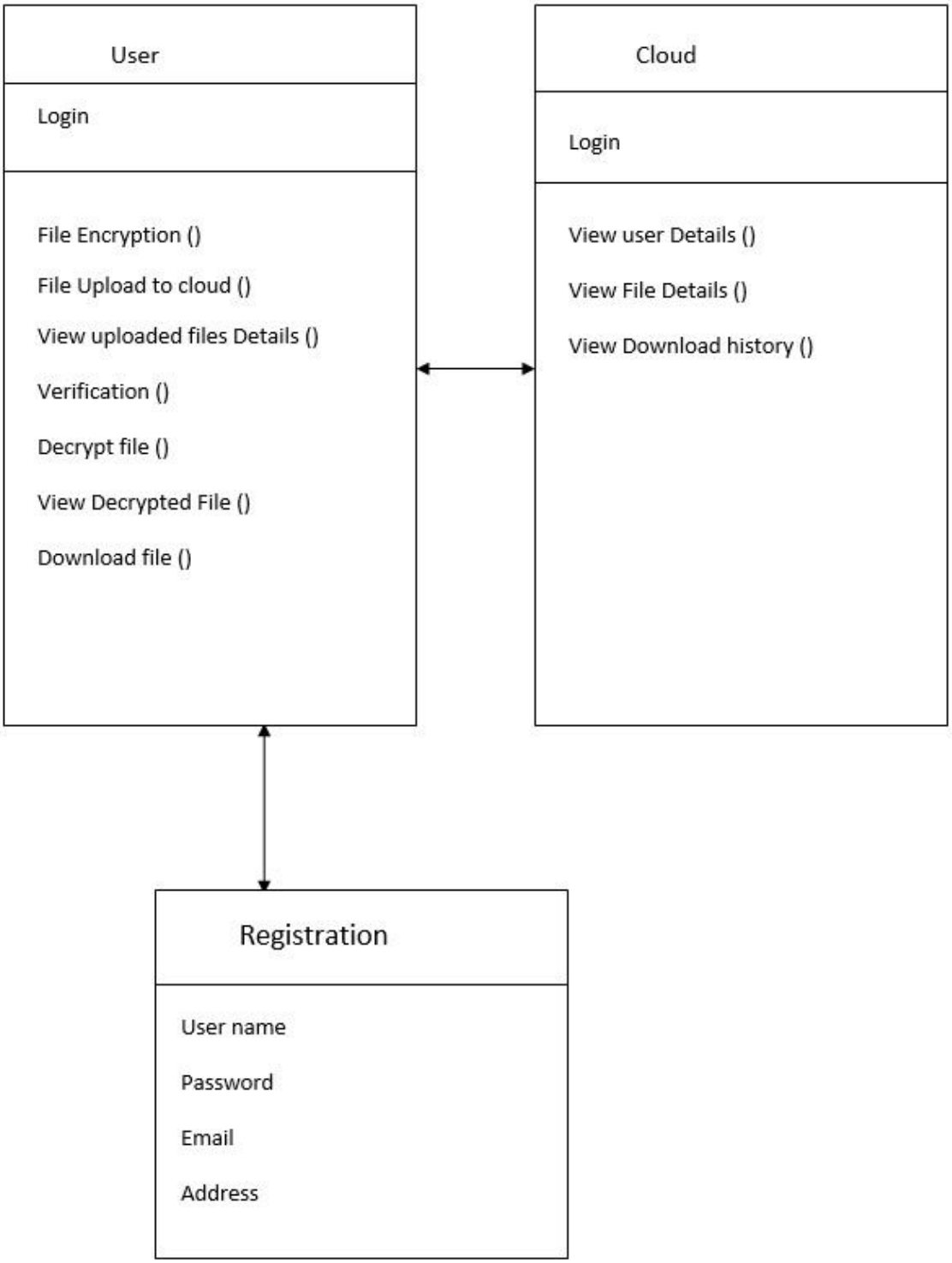
CHAPTER 5

DETAILED DESIGN

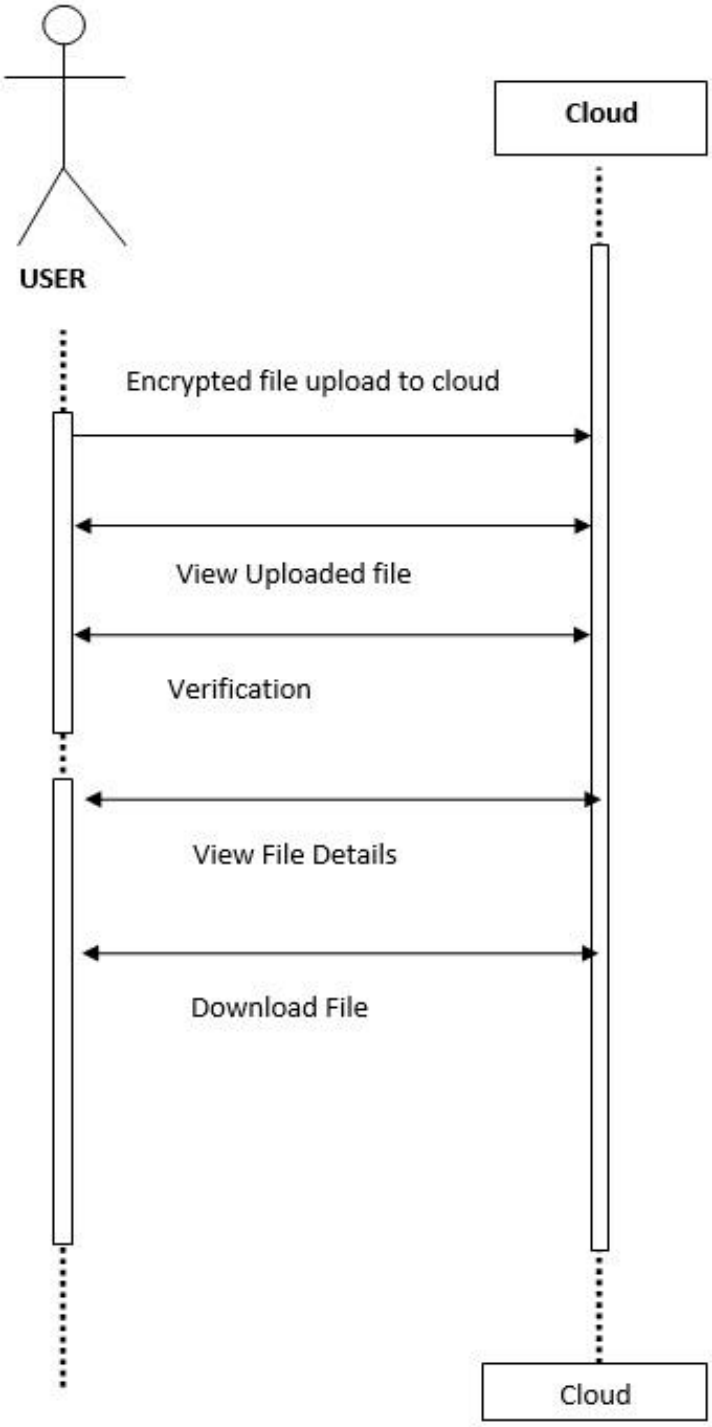
5.1 Use Case Diagram:



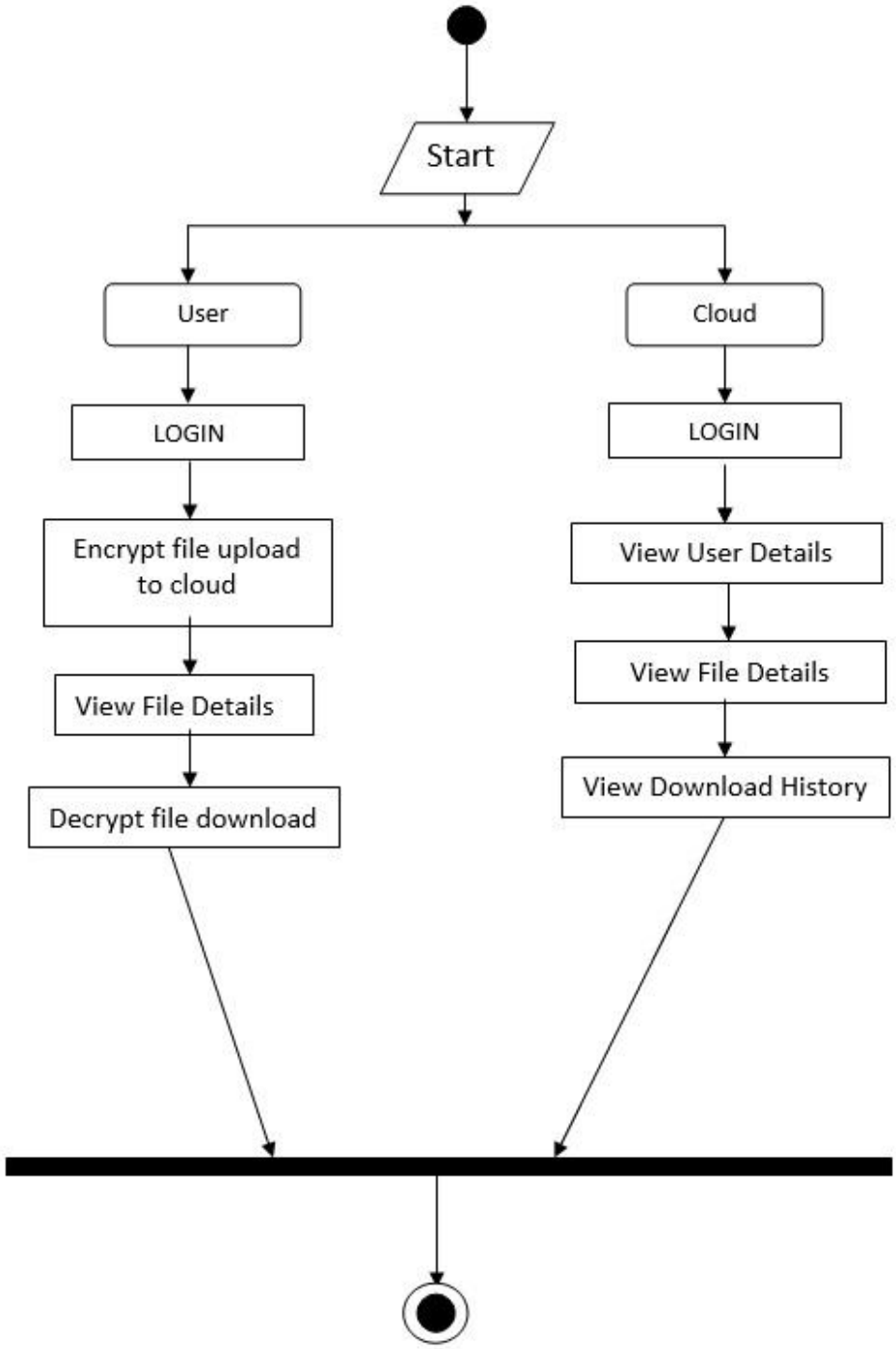
5.2 Class Diagram:



5.3 Sequence Diagram:



5.4 Activity Diagram:



CHAPTER 6

SYSTEM IMPLEMENTATION

6.1 Implementation:

6.1.1 Hiding Equality Constraints (A, b):

First and foremost, the secret key k may be a randomly generated m x m non-singular matrix Q. You may question the consumer The initial requirement matrix for the following transition restrictions,

Ax = b A x = b

Where A′ = QA and b′ = Qb. Where A′ Because A has full-line coverage, A′ requires full-line rating. It is not possible without knowing Q One for exact elements of A to be defined. The null spaces of A and A are, though, the same that may breach Certain applications' security requirements. The vector b is completely protected, since it can be converted to a Arbitrary b′ of the right Q range.

6.1.2 Proposed Algorithm:

Step 1: Extract the output from the cloud server say(a)

Step 2: Compute an output at client end say (b)

Step 4: if (a==b) then

Step 5: Cloud server will perform honestly else

Step 6: Cloud will given an incorrect result

Step7: If both the values will be match that is produce by client and server then our algorithm will give a robustness of output.

6.1.3 Linear Results:

Equation	Benchmark		Original Problem	Encrypted Problem	Cloud Efficiency
	M	N			
1	3	7	0.67	0.7	0.957142857
2	109	200	0.127	0.134	0.947761194
3	45	198	0.2	0.27	0.740740741
4	300	200	0.321	0.324	0.990740741
5	233	700	0.544	0.566	0.961130742
6	1500	3	0.666	0.7	0.951428571
7	2344	2000	0.899	0.92	0.977173913

Table :- Linear Results

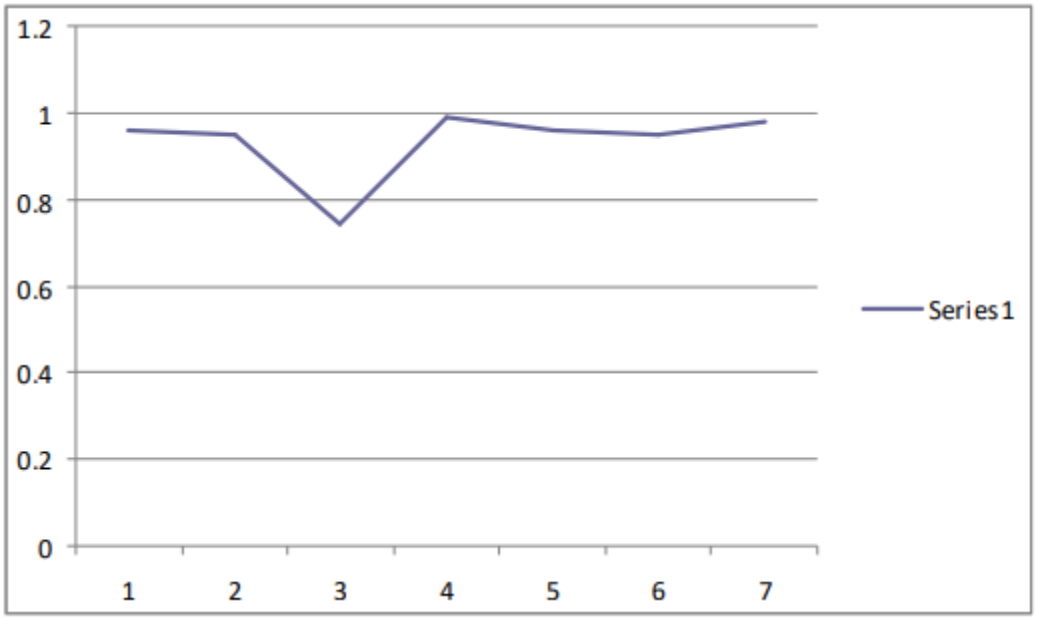


Fig. : Graph of Linear results

Equation	Benchmark		Original Problem	Encrypted Problem	Cloud Efficiency
	M	N			
1	1.66	18.59	0.245	0.27	0.907407
2	39.45	89.99	0.297	0.3	0.99
3	39.54	89.99	0.432	0.478	0.903766
4	90.00037	90.00082	0.544	0.567	0.959436
5	-116.11	106.43	0.788	0.798	0.987469
6	1887.7	899	0.9	0.912	0.986842
7	2787.7	89.99	1.2	1.233	0.973236

Table : Nonlinear Results

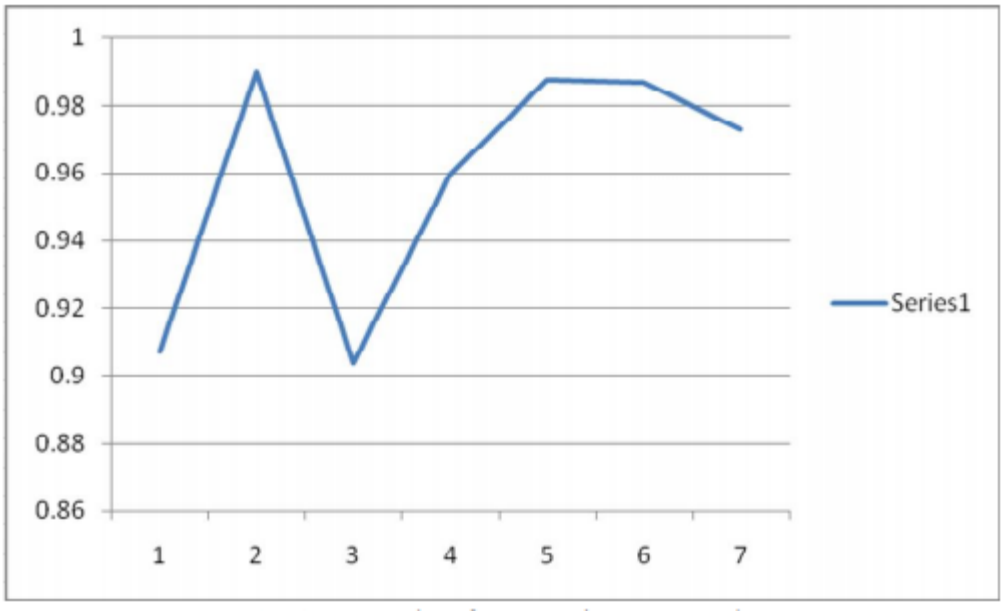


Fig.: Graph of Non Linear results

The problem is developed in this paper The Jacobi iterative outsourcing of linear equations Method and designs mechanisms that Privacy, flexibility and performance of input / output. Computational savings are achieved under the proposed mechanism. It involves O(n) measurement within every iteration. Customer burden and does not require unreal IO Harm is involved locally when solving linear equations O(n2) O(n2)) both in terms of period and rate of iteration The need for information. It also enables clients to Check all results of previous cloud iterations Just one batch. One batch. It guarantees both the advantage of efficiency and The design's robustness.

6.1.4 Pre-Implementation Technique:

We also discuss theorem of duality and create a sufficient and adequate condition to validate the findings. The ultimate system is able to integrate such a hacking resistance architecture with an extra near to zero overhead. The immediate practicality of the suggested system is shown by both health evaluations and test tests.

We are hoping to explore some fascinating potential work:

1. To obtain numerical consistency, formulate good algorithms

2. To further boost the performance, investigate the sparsely organized question

3. Set up the structured structure for defense

4. Extending our results to non-linear cloud programming.

6.1.5 Post-Implementation Technique:

The program is challenged by a huge range of data sets and mining functions! Requires a well-conceived process in framework. The application is data-intensive with a large amount and number of distributed data set! Needs connectivity and storage expenses to be reduced . Costs for calculation and data transfer (Classification / Discovery) rise as the number of iterations / data sets increases! Minimizing repetitive data mining expenses is necessary

6.2 Screenshots

Fig: Home Page

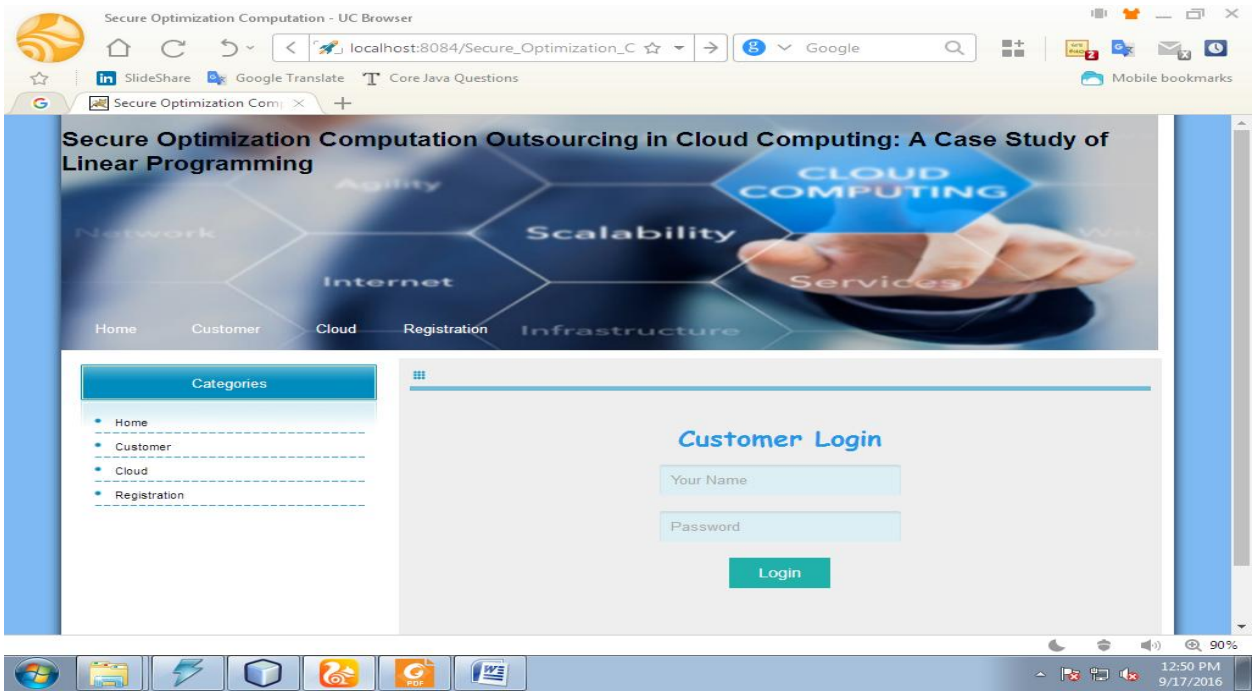


Fig:- Customer login page

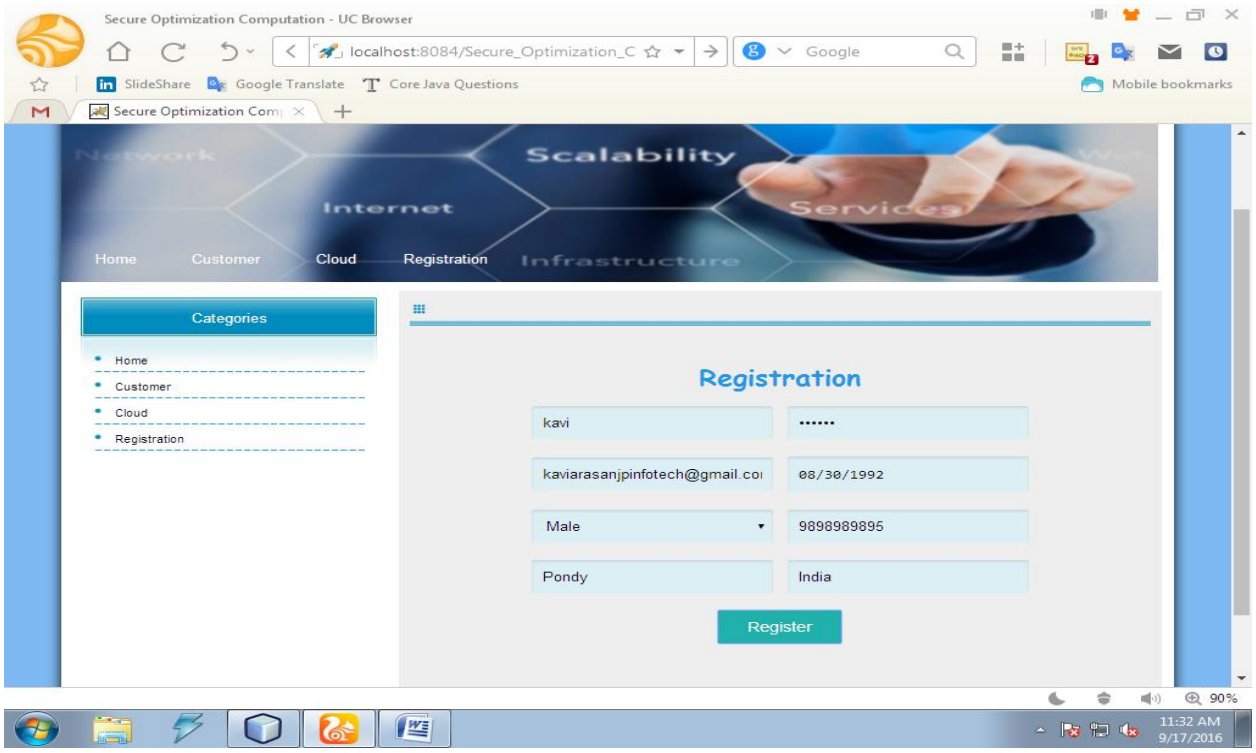


Fig:- Registration page

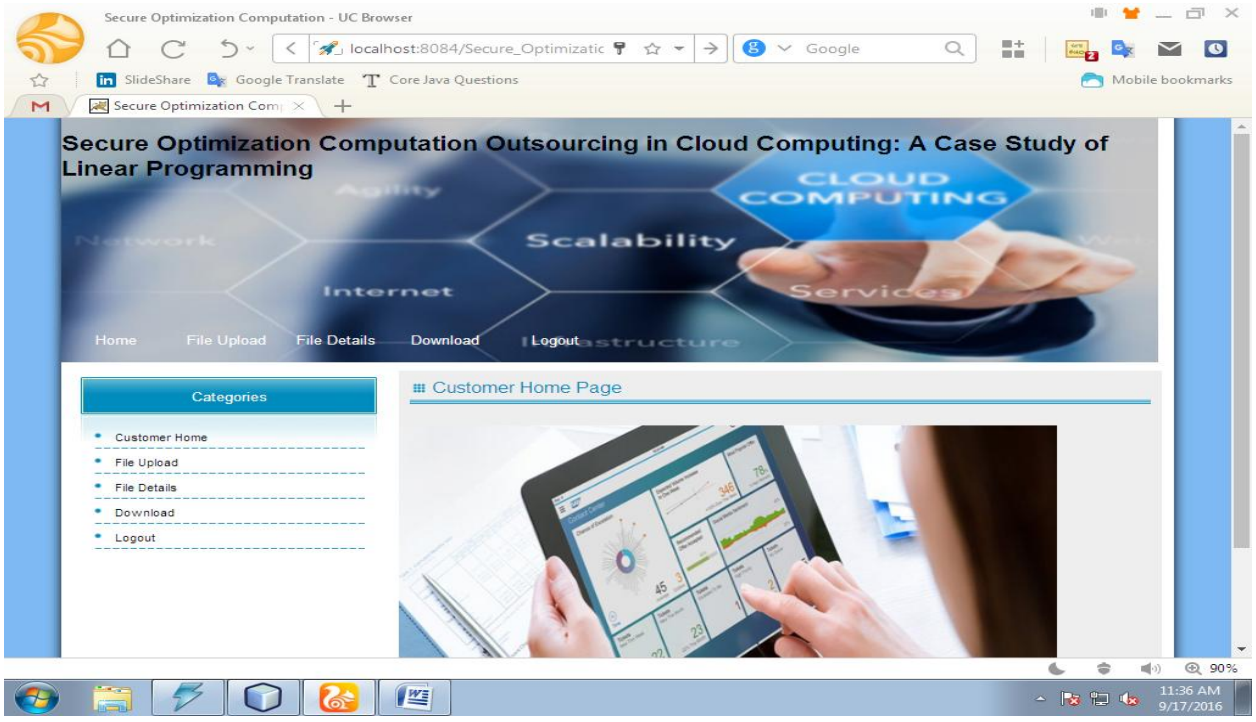


Fig:- Customer Home Page

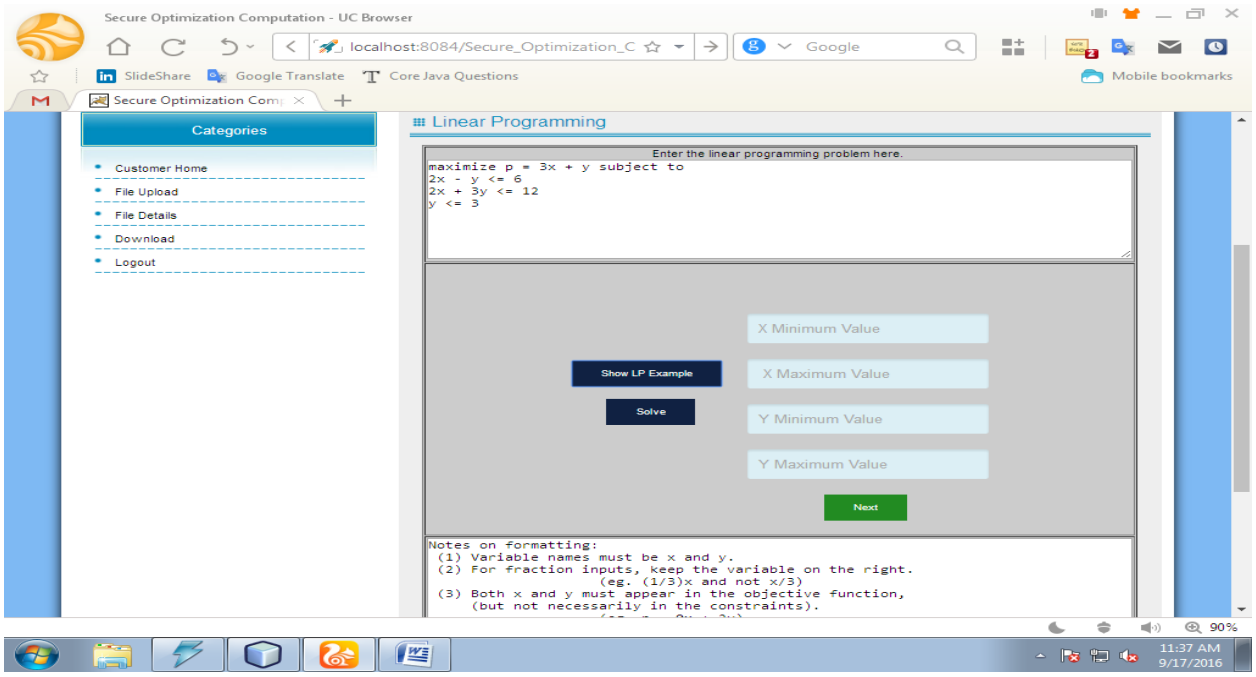


Fig:- Linear Calculation page

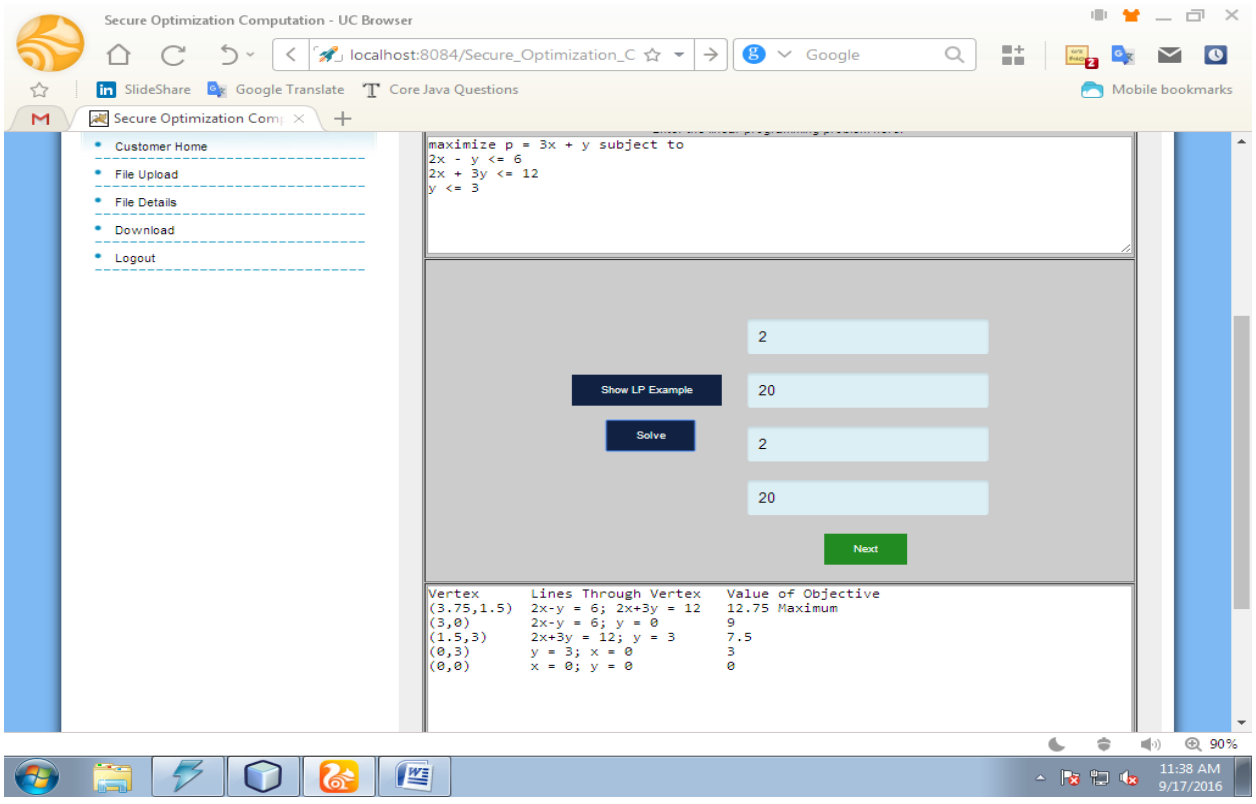


Fig:- Enter Linear Values in edit fields

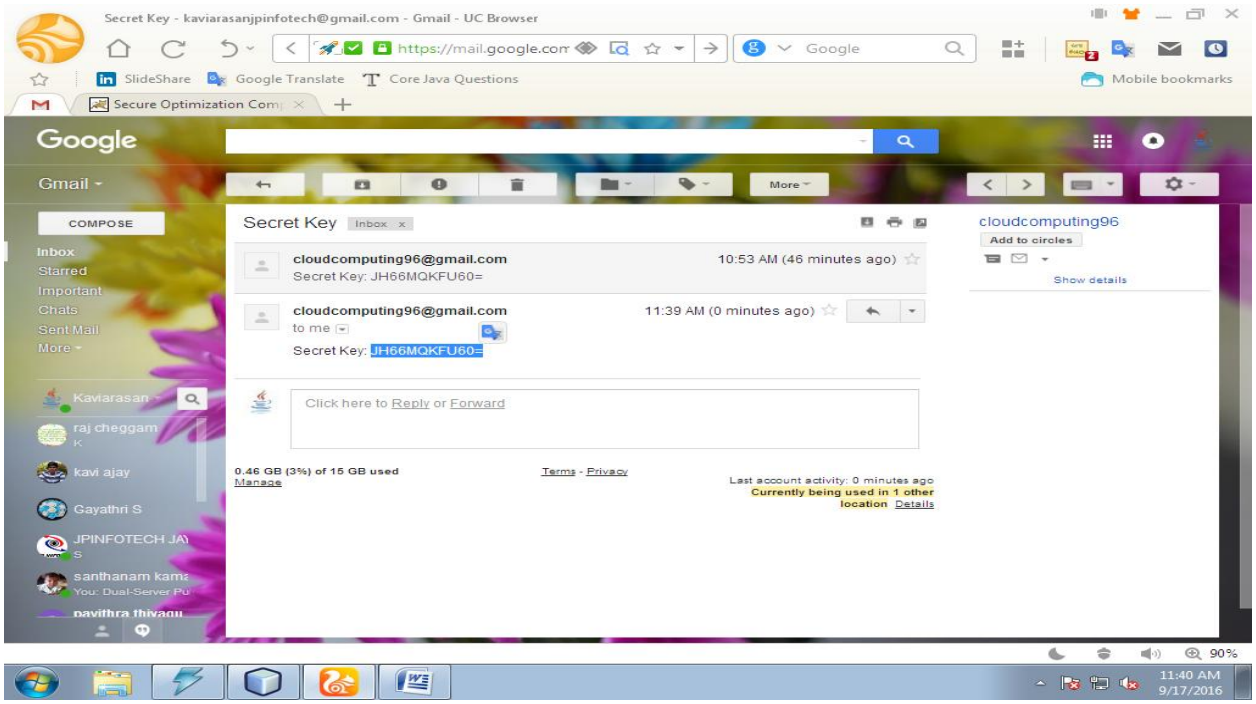


Fig:- Secure key in Gmail account

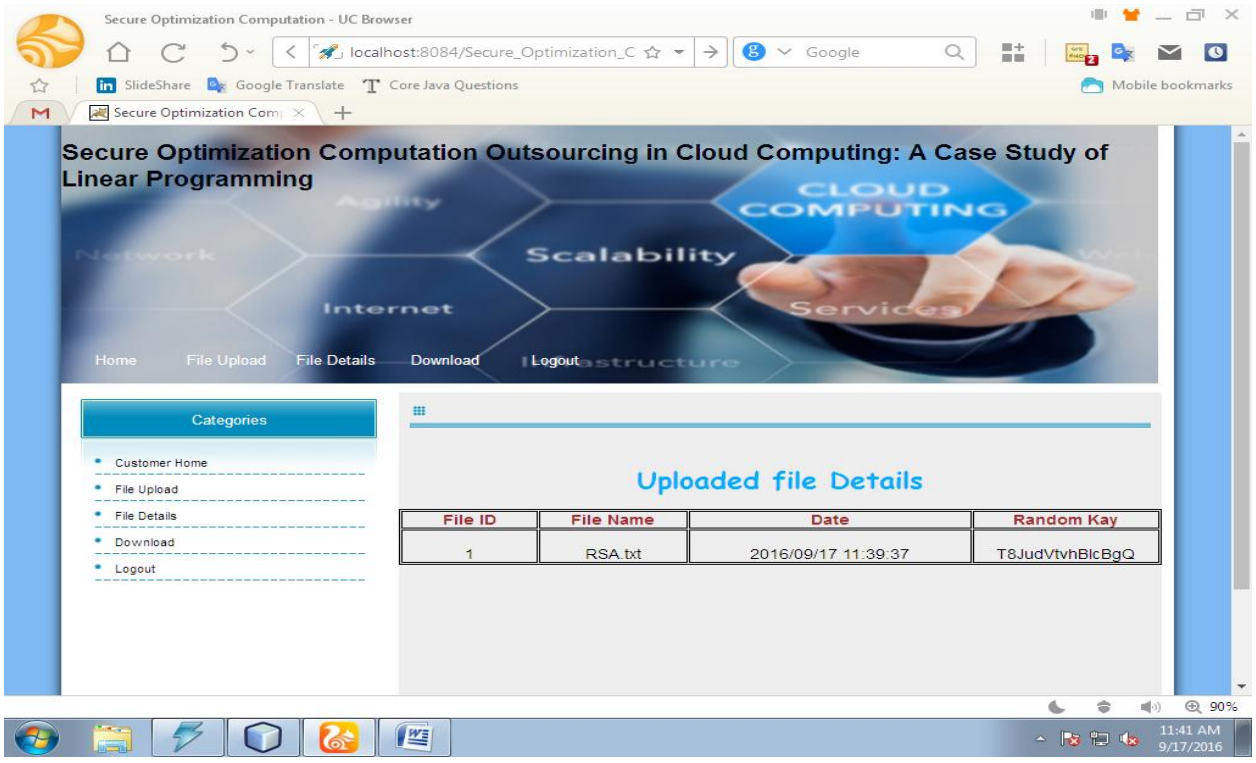


Fig:- Uploaded file details

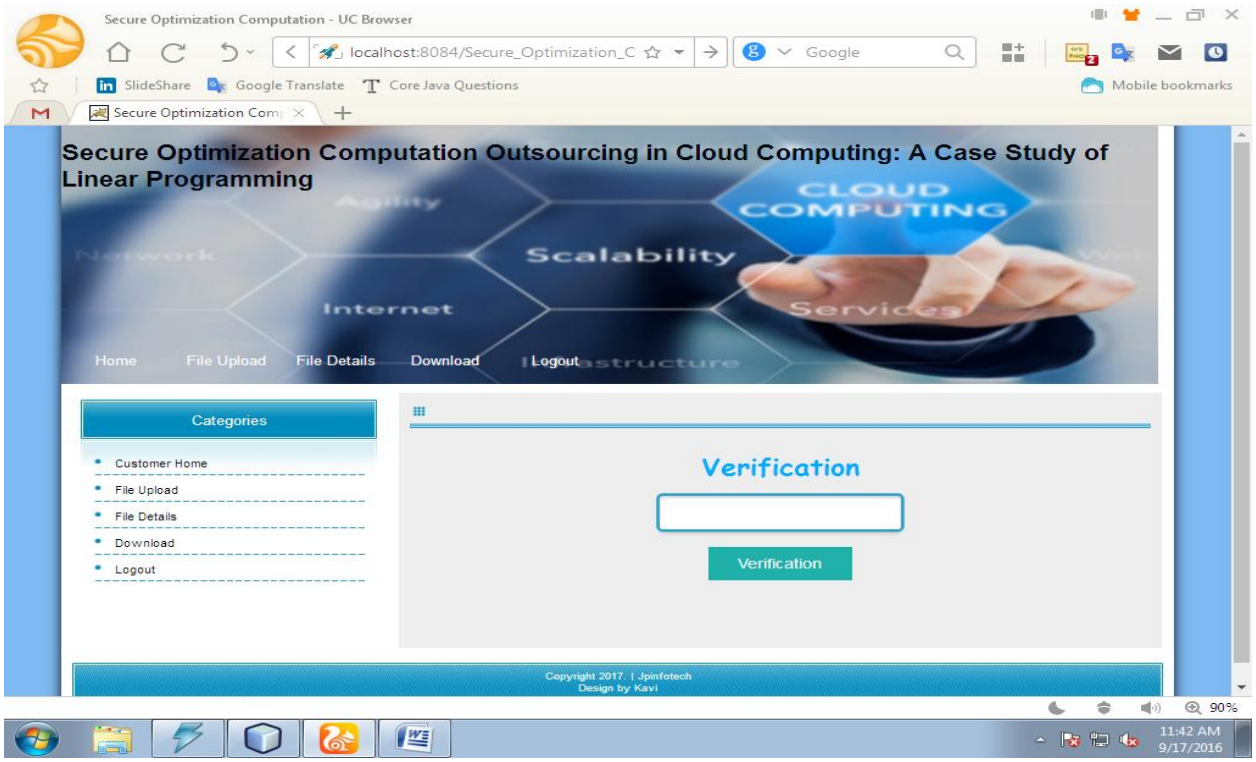


Fig:- Sk Verification page

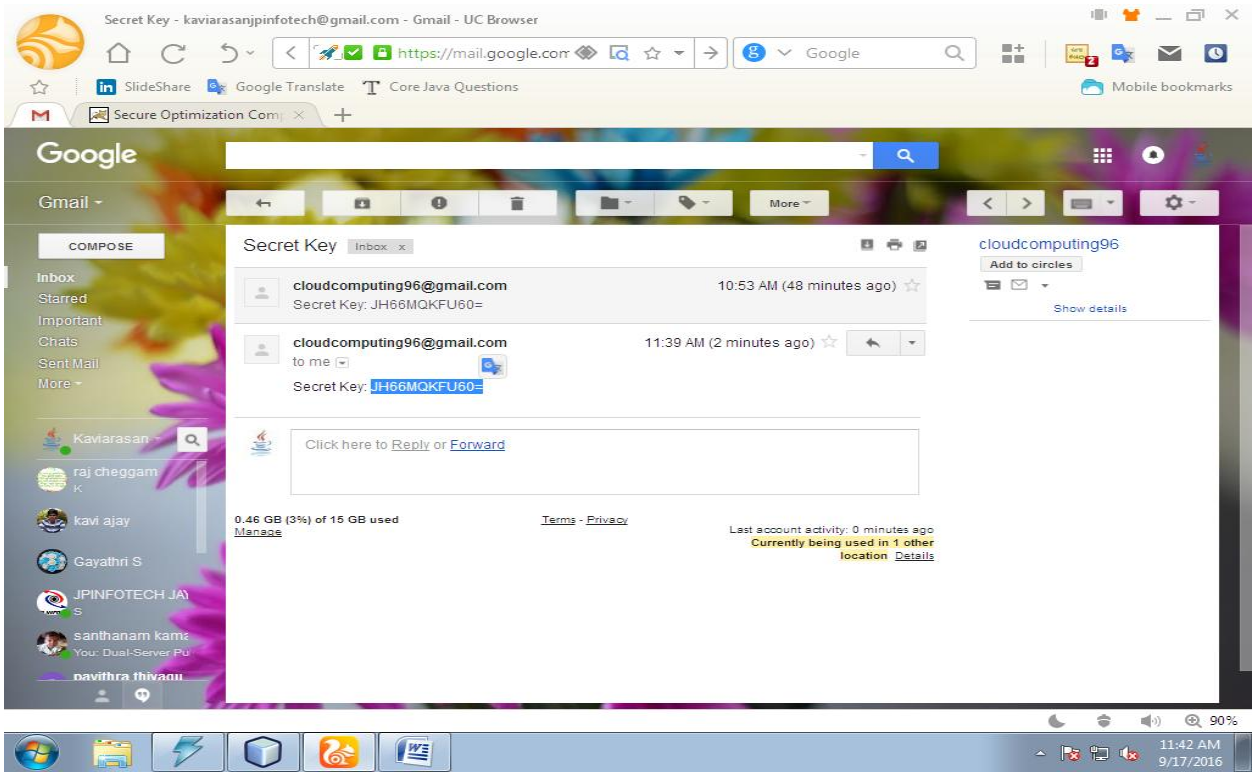


Fig:- get Key from mail

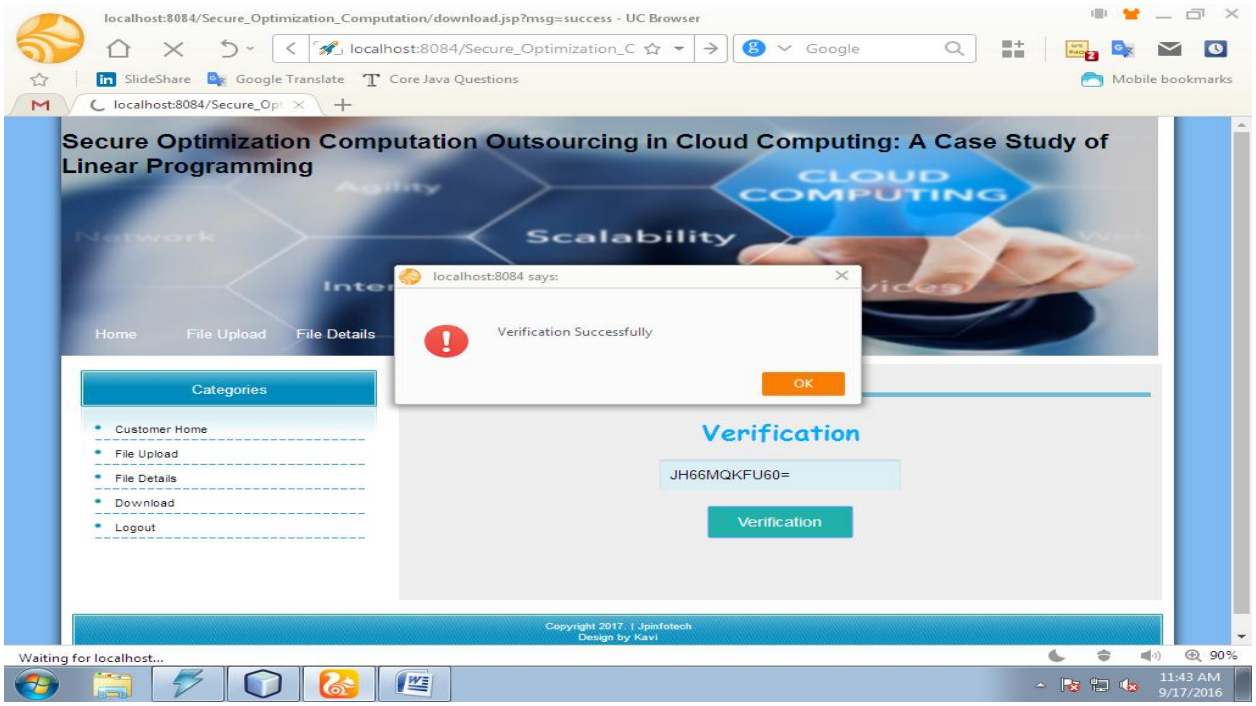


Fig:- Success page

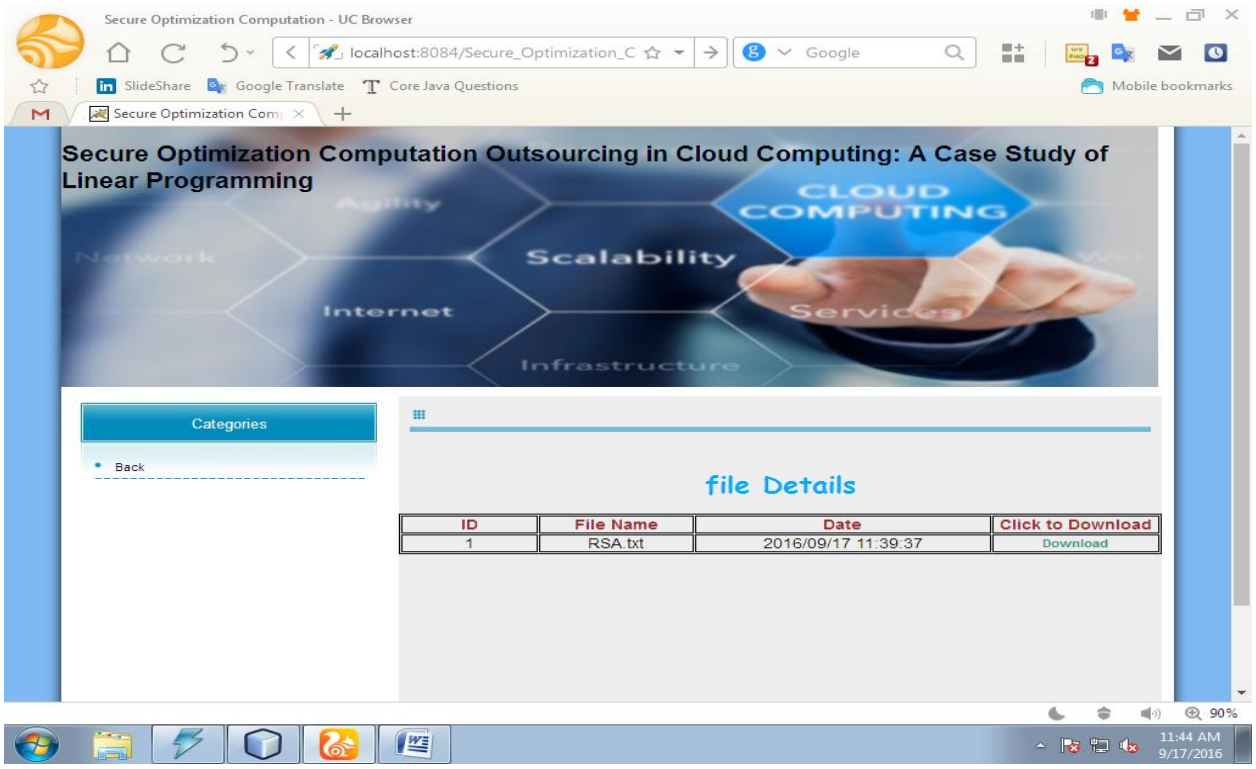


Fig:- file page

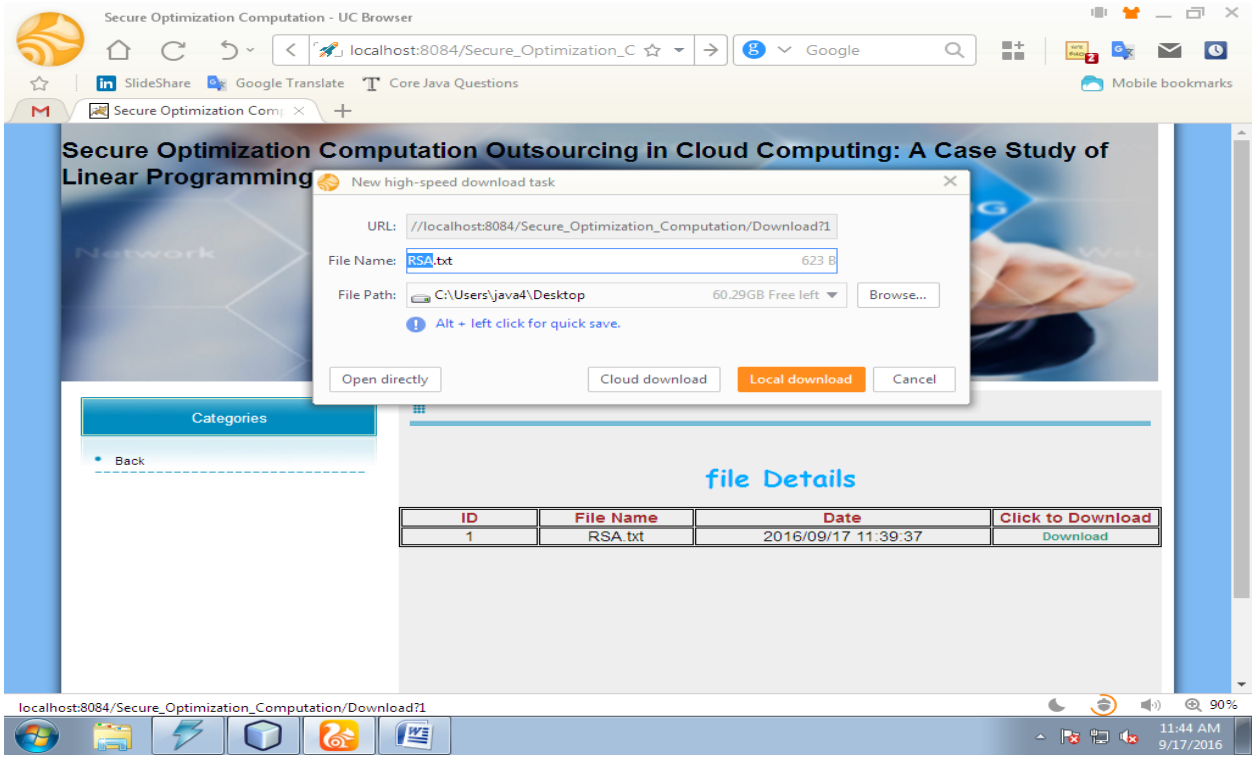


Fig:- file name page

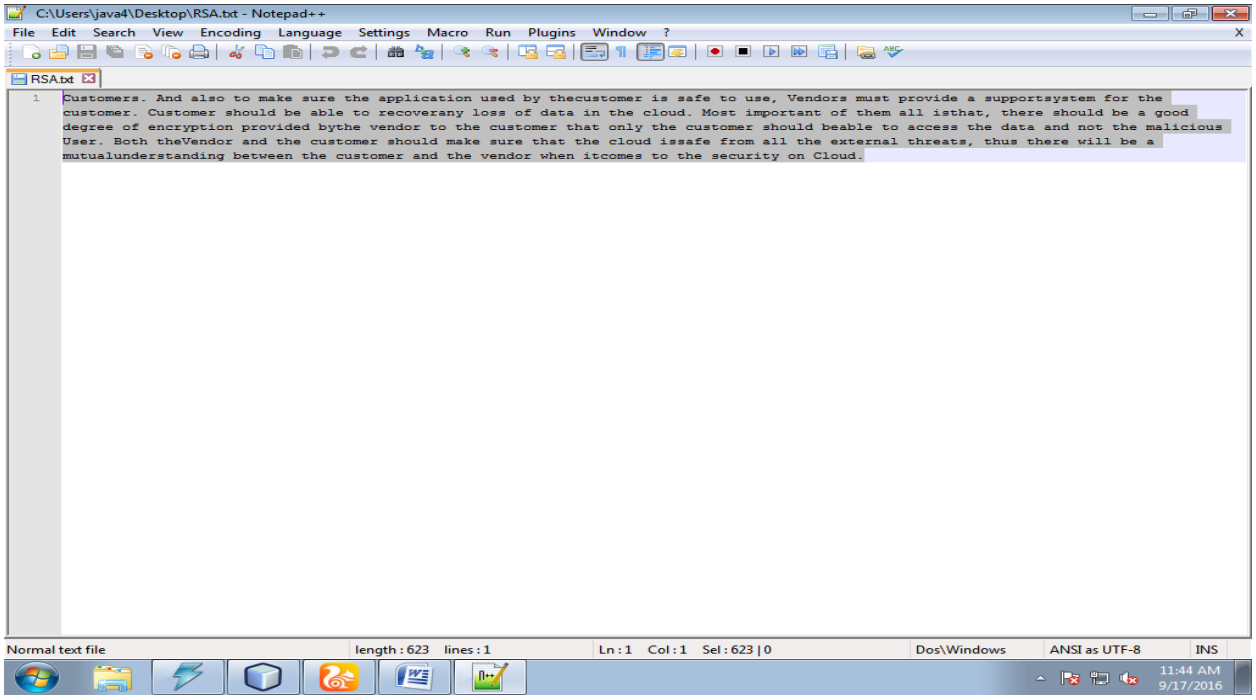


Fig:- original file

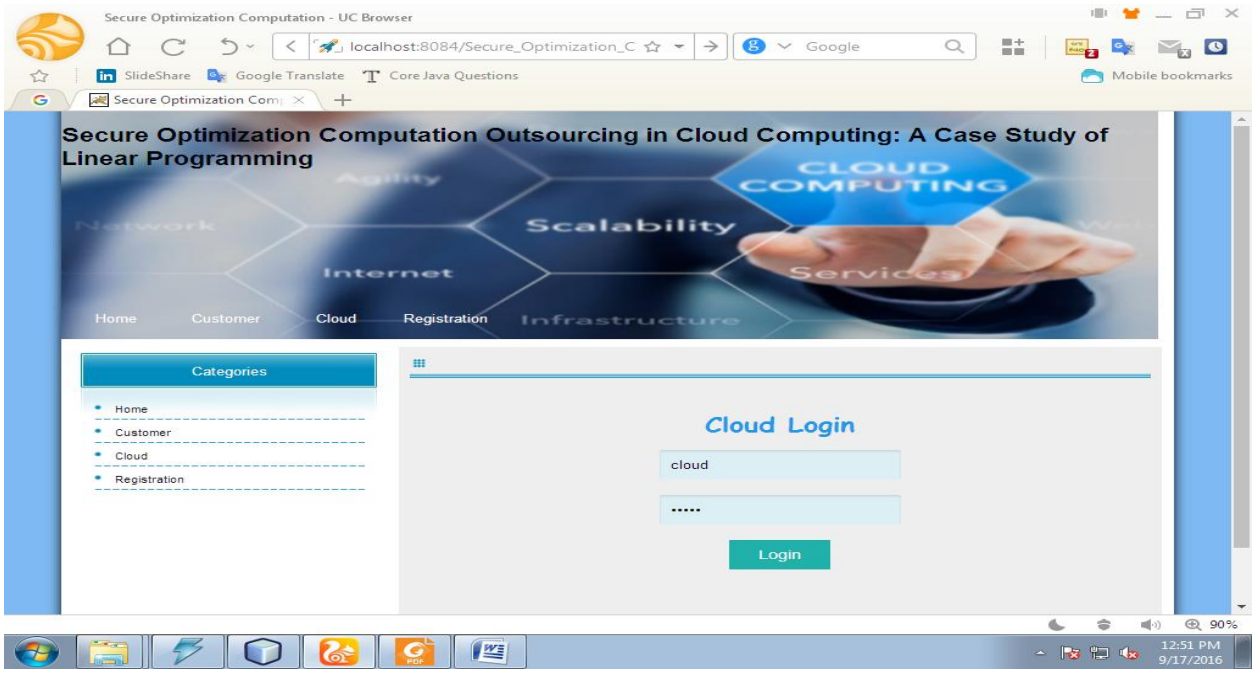


Fig:- cloud login page

Fig:- Cloud Home page

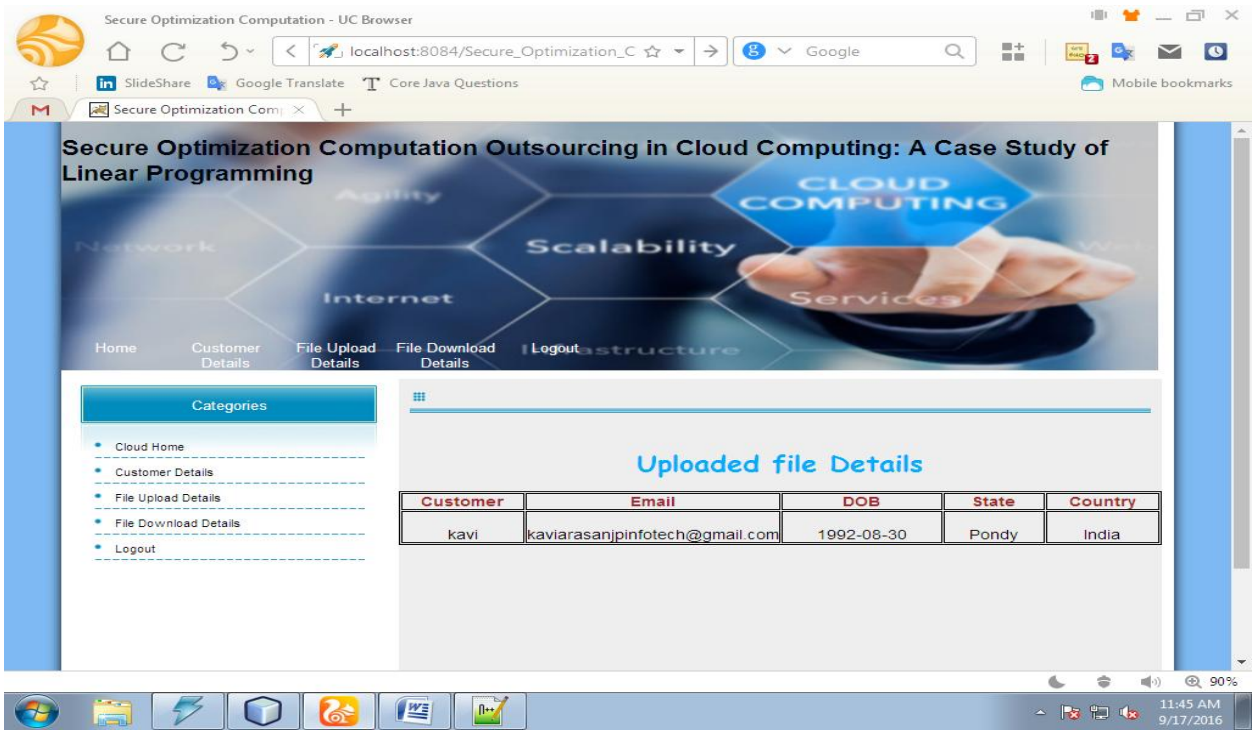


Fig:- Uploaded files in cloud page

Fig:- file with created date

CHAPTER 7

SOFTWARE TESTING

Test Cases:-

Test Case : Login	**Priority(H,L) :** High
Test Objective : Login Page	
Test Description : To check whether the user's user id and password are valid or not	
Requirements Verified : Yes	
Test Environment : jdk 1.7 version is installed and class path is set, sqlyog is installed	
Test Setup/Pre-conditions : Java and NetBeans IDE 7.0 should be installed and class path should be set to execute	
Actions	**Expected Results**
The User enters the valid user id and Password then he logins to home page. He/She enters the invalid user id and Password then the error message will Be displayed	Successful
Pass : Yes **Conditional Pass : Yes** **Fail : No**	
Problem/Issue : NIL	
Notes : Successfully Executed	

Fig:- Login Page Test case

Test Case : Registration	**Priority(H,L) :** High
Test Objective : Registration	
Test Description : To check whether all the details are entered are correct of a citizen	
Requirements Verified : Yes	
Test Environment : jdk 1.7 version is installed and class path is set, sqlyog is installed	
Test Setup/Pre-conditions : Java and NetBeans IDE 7.0 should be installed and class path should be set to execute	
Actions	**Expected Results**
The entered details are valid then Registration is successful else invalid Will be displayed	Successful
Pass : Yes **Conditional Pass : Yes** **Fail : No**	
Problem/Issue : NIL	
Notes : Successfully Executed	

Fig- Registration Page Test page

Test Case : Upload File	**Priority(H,L) :** High
Test Objective : Add File	
Test Description : To check whether content file along with data is done successfully.	
Requirements Verified : Yes	
Test Environment : jdk 1.7 version is installed and class path is set, sqlyog is installed	
Test Setup/Pre-conditions : Java and NetBeans IDE 7.0 should be installed and class path should be set to execute	
Actions	**Expected Results**
The User enters all the details in the Specified fields then website will be entered. He/She order for more than The available quantity then his order Can be denied.	Successful
Pass : Yes **Conditional Pass : Yes** **Fail : No**	
Problem/Issue : NIL	
Notes : Successfully Executed	

Fig- Upload Page Test page

Test Case : Using File Name	**Priority(H,L) :** High
Test Objective : File Name	
Test Description : To check whether the query related details displayed successfully.	
Requirements Verified : Yes	
Test Environment : jdk 1.7 version is installed and class path is set, sqlyog is installed	
Test Setup/Pre-conditions : Java and NetBeans IDE 7.0 should be installed and class path should be set to execute	
Actions	**Expected Results**
The User click the link in the specified Fields then websites will be redirected. The redirection will be fast as the and In less time.	Successful
Pass : Yes **Conditional Pass : Yes** **Fail : No**	
Problem/Issue : NIL	
Notes : Successfully Executed	

Fig:- Test Case for search file

7.1 SOFTWARE TESTING

Software testing is elaborated form of checking all types of options that are included within the system and it has to be done before the system is being provided to the users. Testing will be based on targeting the differences in such a way that all the client requirements are properly arranged and fulfilled. All sides of requirements will be associated and it is needed that the concepts should be clear so that each conceptualization can be properly represent his to the clients in the real time working. The software testing will be important to get the acknowledgement of work processes in a variation.

All types of software testing mechanism you will be implied by selecting the right process required and this will be done with the help of proper discretion and variations of working. Proper co-ordination is required so that understanding can be achieved for the processing that has to be acknowledged. Software testing will be also done to have proper primary labelling of the activities which will be even documented for more understanding.

7.2 TYPES OF TESTING

Unit testing

Unit Relations are best to get the references on individual scale so we are including the unit testing which will be referred in such a way that we will be taking each consideration and we will be testing it in different scenarios after which it will be even document.

The Data integrity option that is important to get the reference is also associated in the unit test and this will be done by checking that each data reference can be individually organized by the administrate for detailed references of security.

The components that are provided will be also check as we have to get the reference for different types of modifications rules and properties that will be included.

The modification types and the simulation references are also required to be checked and it is required that each relation works according or we can say that each reference should be substituted with proper reference add at the time of design.

Multiple users will be associated and we have to check that they can have the proper accessibility control and even the sharing platforms and we check for the accuracy and security.

White-box testing-Methodology

White-box testing will be set up by the users in terms of checking the codes that are written individually or we can say that the developers and the tester will check it and every code of the system to get the reference of work.

Proper knowledge is required to conduct the white box testing as it will be done internally and each reference is required to be checked by the associated users taking the charge.

7.3 MAINTANCE

There therefore a comprehensive array previous knowledge that we will use. Experience in the context of procedures and instructions is coordinated. Without software engineering concepts, a small program can be written. But if a broad software product is to be created then the concepts of software engineering become important to produce a highly productive quality program. It will be impossible to build massive systems without the usage of information development concepts. In business, wide systems for multiple functions are usually needed. The challenge with designing these major business systems is that their growth is rising exponentially in the sophistication and intensity of the initiatives. Computer development leads to raising the difficult programming.

The concepts of information engineering contribute to rising sophistication of problems by two essential techniques: abstraction and decomposition. The abstraction theory means the lack of trivial information that may render a question clearer. This implies that only the facets of the question applicable to a specific target must be taken into consideration and certain facets not important to the provided purpose must be omitted. The object of abstraction is paramount. After the easier problems are overcome, the incomplete information may be taken into consideration to address the lower complexity of the next level, etc. Abstraction is an effective approach to reduce the problem's difficulty. A complicated problem in this strategy is separated

into many smaller problems and the smaller ones are overcome. However, any spontaneous collapse of smaller sections of a question does not aid with this technique.

The problem must be decomposed in order to address each portion of the decomposed problem separately, and then to integrate a solution for the different components in order to obtain the complete solution. A successful issue analysis will eliminate conflicts between specific components. If the numerous subcomponents are entangled, then the respective components can not be independently solved and no decrease in complexity is required. For general, software development starts in the first phase as an implementation of a user request for a certain job or production. He sends his application to an agency of the service provider.

The product engineering department segregates customer requirements, program expectations and technical requirements. The criteria are obtained by customer interviews, a comparison to a database, an analysis of the current program etc. After demand compilation, the team must evaluate how the app fulfils any of the user's requirements.

A roadmap of his strategy is determined by the planner. Application design also requires an appreciation of the shortcomings of electronic devices. A program design is generated according to the necessity and review. Computer Development is applied in a compatible programming language in spite of the composition of application text. Software reviews are carried out through software development and comprehensive checking by research professionals at various stages of the application, such as framework checking, system testing, product testing, in-house testing and customer input

CHAPTER 8

CONCLUSION

8.1 Introduction:

The question of stable outsourcing of LP is formalized computations in cloud computing, to have such a Convenient process configuration that satisfies input / output Confidentiality, deception and performance. Generated directly Generated LP outsourcing via public LP decomposition Our system architecture is capable of solvers and private data Exploring adequate trade in security / efficiency through higher Calculation stage LP as a general circuit Democracy.-Representation. It causes transition issues techniques to easily turn consumers The original LP became an artificial one Details concerning critical input / output. Such a trick The ultimate process can be paired with durability architecture Additional overhead close-to-null. Security in The findings of the study and tests demonstrate the immediate The suggested mechanism's practicality.

The Strategy Investigate the following important research in the future:

- Build reliable numerical stability algorithms.
- Exploring the problem's sparsity composition.
- Develop structured security.
- Increase efficiency.
- Expand our outcome to non-linear Online outsourcing in computer resources.

8.2 Limitations:

Computing outsourcing usually stable that satisfies all Specifications above, such as anonymity of input / output The pledge was seen for correctness / soundness In theory feasible. This is not realistic at present, though. In the immense level in computing. The modified edition Solutions would be more successful than the general Why the circuits are built. A number of

problems The strategies for specific based disguises are suggested Applications such as linear algebra, collection, list Matching template, and so on. Such cover-up strategies nevertheless To some degree expressly permit the disclosure of details. Therefore, the relevant outcome case is not discussed tests, which are built into the architecture of our work And there is a supplementary cost close to nil. But both protocols are cryptographically powerful. Primitive encryptions and/or homomorphic versions Oblivion and not good for big question Move Set set Furthermore, both designs are based on the presumption two non-contaminating and thus open servers Attempts of colluding. On the basis of the same supposition Modular efficient externalization protocols Exponentiation found to be prohibitive Most public-key encryption operations are costly.

CHAPTER 9

FUTURE ENHANCEMENTS

In addition to the popularity of cloud infrastructure, expensive data or computations on cloud services may be easily outsourced. Recently, more and more focus was given to safe outsourcing processes. In this paper we concentrate on the secure Outsourcing of Linear Equations (LEs) systems for storage and calculation. Firstly, a new , effective matrix encryption system is being developed. We instead use this encoding scheme to construct a new algorithm that can outsource storage and computation in semi-honest conditions for massive linear equations. The new method needs fewer overhead capacity and is efficient in competition with previous practice.

CHAPTER 10

REFERENCES

[1] D. M. and K. McGrath. Bunny. Hindsight: a phisher mod operandi review. In preparation of the 1st Usenix Vulnerabilities and Emergent Threats Laboratory (LEET), 2008. 2008.

[2] hphosts, a hosting group file controlled. http:/hphosts.gt500.org.

[3] Domain Inventory of Malware. http:/files / files / domains.txt. microcommunication files.

[4] Reputation support for phone pindrop. The prs/ phone credibility facilities of http:/pindropsecurity.com.

[5] Scrapie — a framework for open source web python scraping. The details remain at the same moment.

[6] Le, A. M. and A. M. • M. Skinned. Skinned. Phishdef: The names of Url mean everything. International Computer Communications Conference (INFOCOM), IEEE Proceedings 2011.

[7] Alexa, the online news service. The top-sites of http:/www.alexa.com,2013.

[8] Dotmobi. Rendered available via twitter. Any device anywhere. Anywhere. , 2013. http:/dotmobi.com/.

[9] D. Boneh and X. Boneh and X. Boyen.-Boyen. Encryption based on a secure identity with no random oracles. Efficient Selective-ID In Cryptology Advances – Eurocrypt, LNCS series 3027, pages 223–238. June, 2004. July.

[10] D. Boneh, R. Ostrovsky, and G.D. Crescenzo. Persian. Persian. Eurocrypt Public-Key Encryption, LNCS version 3027, sections 506–522. 2004 Springer

Web Reference

[1] http.blogs.idc.com / ie/? P=210 P=22

[2] http:/160.wheeresmyserver.co.nz / storage / mediat-faq / cloud-def-v15.pdf

[3] https:/doi.org/10.12764.063.

[4] HostNewsletter /10.125/2503210.250326