Volume 2, Issue 6 June 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal Of Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.01

NAIRJC JOURNAL PUBLICATION

North Asian
International
Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.01

NEXT GENERATION ENCRYPTION DECRYPTION TECHNIQUE FOR FINGERPRINTING ON CLOUD COMPUTING ARCHITECTURE: IMPLEMENTATION

NISHA & ASTT. PROF. MS. POOJA DHANKHAR
CBS Group of Institutions, Maharshi Dayanand University, Haryana

ABSTRACT:

Cloud frameworks allude to the accumulation of interconnected servers that are provisioned powerfully on request, for execution of application, to the client like electricity grid. Distributed computing has increased incredible consideration from industry yet there are still numerous issues that are in their primitive stage fussing the development of Cloud. One of these issues is security of information put away in the servers of datacenters of Cloud computing suppliers. Numerous plans have been created. These plans have been contemplated, examined and new technique has been proposed which infix the parameters of security like recuperation of information and classification of information such that it guarantee security of information put away in the servers of Cloud frameworks. The proposed plan depends on two techniques – Information Dispersal Algorithm and producing key from the image. Data dispersal calculation helps in keeping up classification and uprightness of information and key produced from picture will helps in recuperation of information.

Keywords: ***Next Generation, Encryption Decryption Technique, Fingerprinting, Cloud Computing Implementation.***

1. INTRODUCTION

Big organizations like Google [1], Amazon [2], and Yahoo [3] give services to users throughout the world with the help of websites hosted on the servers of their datacenters. Many datacenters were established by them to handle requests from users throughout the world. These organizations bought and established servers according to the peak traffic for the website; but, most of the time during a day, these servers were idle. There are many small organizations which have innovative ideas; but, they do not have enough capital to build such infrastructures to turn their ideas into reality. This lead to the origin of Cloud computing. Big organizations allow these small organizations use their servers for their use. Small organizations give money for the amount of time and number of resources they use. This help both parties satisfy their needs and it benefited all.

2. OBJECTIVE

a) To avoid or decrease all such cost, complexities, services and wastage of resources.

b) To meet the demands of user requests during peak hours.

c) To give the freedom to access the stored data like videos, photos and documents wherever internet is available like Apple's iCloud [6].

3. ABOUT CLOUD COMPUTING:

Cloud Computing can be described as "a sort of parallel and appropriated framework involving an amassing of between associated and virtualized PCs that are powerfully provisioned, and presented as one or more brought together processing assets in light of organization level assentions developed through course of action between the organization supplier and the clients" [7].

Characteristics of Cloud Computing:

a) It is a sort of customer server model such that customers are administration requesters and servers are service providers.

b) There are heterogeneous sorts of servers accessible at service provider site to satisfy the differing requests of customers.

c) Cloud Computing is like utility Computing. The services are given because of the measure of assets utilized for the given time.

d) Location independent.

Types of Cloud:

Cloud systems are separated into classes on the premise of the sort of customers which will be taking its services. Distinctive sorts of Cloud accessible are as per the following:

a) Public Cloud

b) Private Cloud

c) Community Cloud

4. LITERATURE REVIEW

Security of data at rest in severs is the common topic of discussion among researchers. There are different mechanisms reported till date to ensure security of data at rest and selection of any one of these for any particular system depends on various parameters like:

- Architecture of system where security is to be enabled.
- Level of security required.
- Amount of loss that may occur on loss of data and many more.

Shamir's algorithm: In 1976, a simple (k,n) threshold scheme was explained and this scheme is reported in. According to this scheme data is divided into n pieces and up to k pieces are required to get data. This scheme is based on polynomial interpolation: given k points (x_i , y_i) with distinct x such that for each x, there is one and only one polynomial q(x) of degree k-1 such that $q(x_i) = y_i$ for all i. Suppose data D is a number (ASCII value). To divide it into pieces D_i, a random polynomial $a_0 + a_1 x + \ldots\ldots\ldots a_{k-1} x^{k-1}$ of k-1 degree is selected in which $a_0 = D$.

$D_1 = q(1), \ldots\ldots\ldots D_i = q(i)$. If any of these k values are known, then other coefficients of polynomial are interpolated with the help of polynomial interpolation. On knowing the coefficients, data that is hidden is calculated with x = 0. Knowledge of just k-1 values does not reveal any data about secret data that is hidden.

Cryptographic file system (CFS): In 1993, CFS was presented which empowers security of information very still in the system. CFS pushes encryption benefits into the record framework. CFS underpins secure capacity at the system level through a standard UNIX record framework interface to scrambled documents. Clients relate a cryptographic key with the indexes they wish to secure.

CFS gives a basic component to protect information kept in touch with plates and sent to organized record servers.

Rabin's efficient dispersal of information for security, load balancing, and fault tolerance: In [53], another scheme is explained for dividing data into pieces/shares. In this scheme, the way of dividing secret into pieces is different from [52]. Consider a file F consisting of string of characters. It is represented as $F = b_1, b_2$,……..b_N . The characters of file F can be considered as integers such that each character is represented as its ASCII value.

Choose an appropriate integer m so that n = m+k satisfies $n/m \leq 1+\varepsilon$ for a specified $\varepsilon > 0$. Choose n vectors $a_i =$

$(a_{i1}$, …… , $a_{im}) \in Z_p^n$, $1 \leq i \leq n$. The file is segmented into sequences of length m.

Thus F= (b_1 ,……. ,b_m), (b_{m+1} , ……. . b_{2m}) , …,Denote S_1= (b_1,…… , b_m). For i = 1, …, n,

Secure Network Attached Disks (SNAD) In [42], portrayal about SNAD is accounted for. SNAD is the framework for guaranteeing data on framework affixed circles. The fundamental framework behind SNAD is to scramble all data at the client and give the server satisfactory information to approve the writer and the peruser sufficient information to check the end-to-end uprightness of the data. SNAD relies on a couple of standard cryptographic gadgets for ensuring grouping of data. The client uses a standard count, for instance, RC5 [43] or Blowfish [43] to encode the data, ensuring that the data is disjointed by anyone until it is unscrambled by the client that comprehends it. Open key cryptography is used to allow circles to store information that can be used to unscramble their records; since open key encryption is hilter kilter, in any case, only a customer with the reasonable private key can use this information. In case the sender and beneficiary share a key, the key can be fused into the cryptographic hash, staying away from any person who obstructs the data from indistinctly transforming it unless they know the basic key. By then present three substitute security plots, every fitting for different levels of customer and server CPU execution.

Secure Group Key Management For Storage Area Networks In [45], secure gathering key administration strategy has been presented for capacity region systems. Capacity range systems resemble 'Dispersed Systems' the place for security, information honesty and information privacy ought to be accomplished. In this paper, an answer had been suggested that addresses these center security necessities.

Cryptographic Security For Distributed File System: In paper [47], encryption is tended to at the record framework level. Here, the outline and execution of cryptographic insurance strategies in elite conveyed record framework is accounted for. The objective of this plan is to give SAN.FS outline that gives end-to-end privacy and trustworthiness assurance for the information put away by the clients on the SAN.FS customers such that every cryptographic operation happen just once in the information way. It is expected that the meta-information server (MDS) is trusted to keep up cryptographic keys for encryption and reference values for respectability assurance, and does not open them to unapproved customers.

A Tree Based Recursive Information Hiding Scheme In [57], another plan for separating mystery into shares and recreating the mystery once again from its shares is clarified. In this plan, extra data is included the shares of the mystery. This extra data is a message and the message is recovered alongside document (mystery) on reproducing the record (mystery). Work has been done in a limited field Zp, where p is a prime and it is open information. It has been expected that a mystery S is spoken to as series of numbers S = s . . . s , where every s Zp and |S| = r = n , where |S| signifies the length of mystery S for some number h. For instance, in the event that we expect that the mystery is an instant message made out of ASCII characters, then it can be spoken to as a series of numbers not as much as p = 257 [efficient dispersal of information]. Moreover, it has been accepted that there is another string meant by M = m . . . m , m Z , where |M| = t = n −1/(n−1) , that is to be covered up inside the shares of the first mystery S.

5. IMPLEMENTATION ISSUES ON CLOUD COMPUTING:

There are diverse issues in Cloud that is keeping relationship from using Cloud. These issues are according to the accompanying:

a) Privacy: Cloud advantages process customers' data on machines that customers don't have or work, this presents security issues and essens clients' control.
b) Security: While driving Cloud administrations suppliers use information stockpiling and transmission encryption, customer confirmation etc.
c) Reliability
d) Ownership: Once information is committed to the Cloud, a couple people stretch that they would lose a couple or most of their privileges of their information.
e) Data versatility and change
f) Intellectual property: An association makes something new and it uses Cloud administration as a component of the innovation.

6. PROPOSED WORK:

Here a new data storage security scheme for Cloud systems has been proposed in this research viz. Images based recursive information hiding scheme. The proposed plan fulfills all the expressed goals. It depends on two techniques:

a) Data (Information) Dispersal Algorithm

b) Generating key from image using RSA algorithm.

In the wake of concentrating on different calculations reported by analysts and comprehension their favorable circumstances and burdens as for security prerequisites of information put away in servers of Cloud in writing audit part, a calculation has been proposed in this section which accomplishes the destinations of this exploration. The calculation has been exceptionally all around executed in Cloud utilizing CloudSim reproduction apparatus. A case study has been discussed in next chapter ‘Experimental results and Comparison’. Discussion on this case study and success of various tests applied indicate that objectives set for this research have been achieved by the proposed algorithm.

SPLASH WINDOW

7. MATERIAL AND TOOLS UTILIZED :

For mimicking Cloud applications, CloudSim is the best recreation apparatus accessible. CloudSim is an extensible reenactment toolbox that empowers displaying and recreation of Cloud registering frameworks and application provisioning situations [59]. It executes bland application provisioning strategies that can be reached out easily and constrained endeavors.

CloudSim propagation instrument take after Java. In this instrument, all components are classes and the limits that these substances can perform are selected as methods. In the wake of growing a component class, methods are called to play out the application.

8. IMPLEMENTATION:

For the simulation of experiment in CloudSim, certain parameters of Cloud have been set. These parameters are:

1) One user – There is only one user in this experiment who sends one file to the Cloud for data storage in its servers.
2) One Datacenter Broker – In this experiment, only one datacenter broker is included.
3) One Datacenter – Generally, there are many datacenters available with Cloud service provider and datacenter broker chooses one of these datacenters depending on the QOS requirements of the user. However, in this experiment, only one datacenter is included and it is assumed that this datacenter meets the QOS requirements of client's application.
4) Fifteen hosts – Generally, there are thousands of hosts available with each datacenter of Cloud service providers; but, in this experiment only fifteen hosts are taken considering the size of file.

Hardware characteristics of hosts – The hosts are of heterogeneous nature at Cloud service provider's organization. This feature is important in cases where compute service is provided by Cloud such that hosts are assigned according to the computing requirements of the application. But in storage servers, this feature is not important.

Table: Server Table in Cloud Monitor

Servers Information	Type_of_data	Description
Server_ID	Int	Unique Server ID
Server_IP	Character	Server IP Address

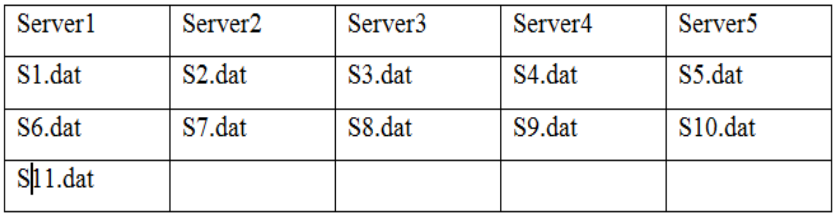
A database is maintained in the monitor of the cloud. Suppose there are five servers –Server1, Server2, Server3, Server4, and Server5 in the cloud. Information related to the storage are stored in Storage table in Cloud monitor.

Table: Storage Table in Cloud Monitor

Information Stored	Type_of_data	Description
Share_Name	Int	Share_Name
Server_IP	Character	Server IP Address
Key_value	Character	Key used for encyption
Filename	Character	Filename
FileNo	Int	Sequence of share

Data is stored in the form of decrypted files in the server

Table :4.3 Files stored in servers after encryption using image key:

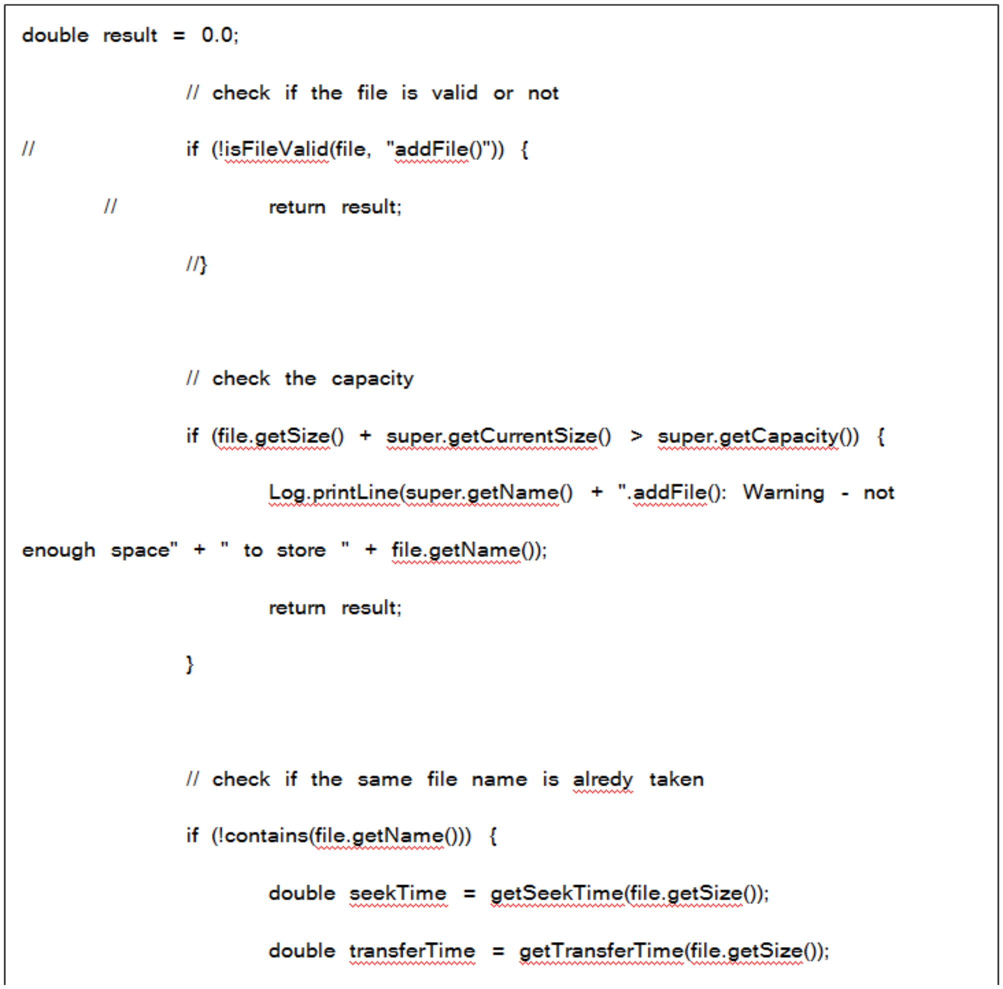


Server1	Server2	Server3	Server4	Server5
S1.dat	S2.dat	S3.dat	S4.dat	S5.dat
S6.dat	S7.dat	S8.dat	S9.dat	S10.dat
S11.dat				

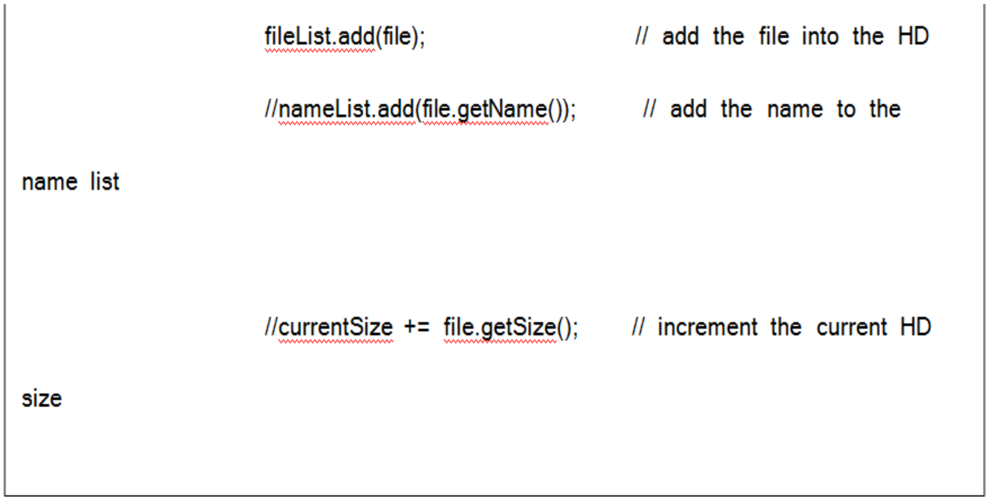
In Second Phase these shares are decoded to get S1.txt from S1.dat, S2.txt from S2.dat , S3.txt from S3.dat, S4.txt from S4.dat, S5.txt from S5.dat, S6.txt from S6.dat, S7.txt from S7.dat, S8.txt from S8.dat, S9.txt from S9.dat, S10.txt from S10.dat and S11.txt from S11.dat with same IMAGE key and joined to a solitary file S.

On Downloading ClousSim3.0, Hard storage Drive class is inherited by Cloud Hard drive Storage. Cloud Hard drive Storage Class is calling the constructors of Hard drive Storage Class. It is also using the functions of Hard Drive Storage Class to store the files on the cloud.

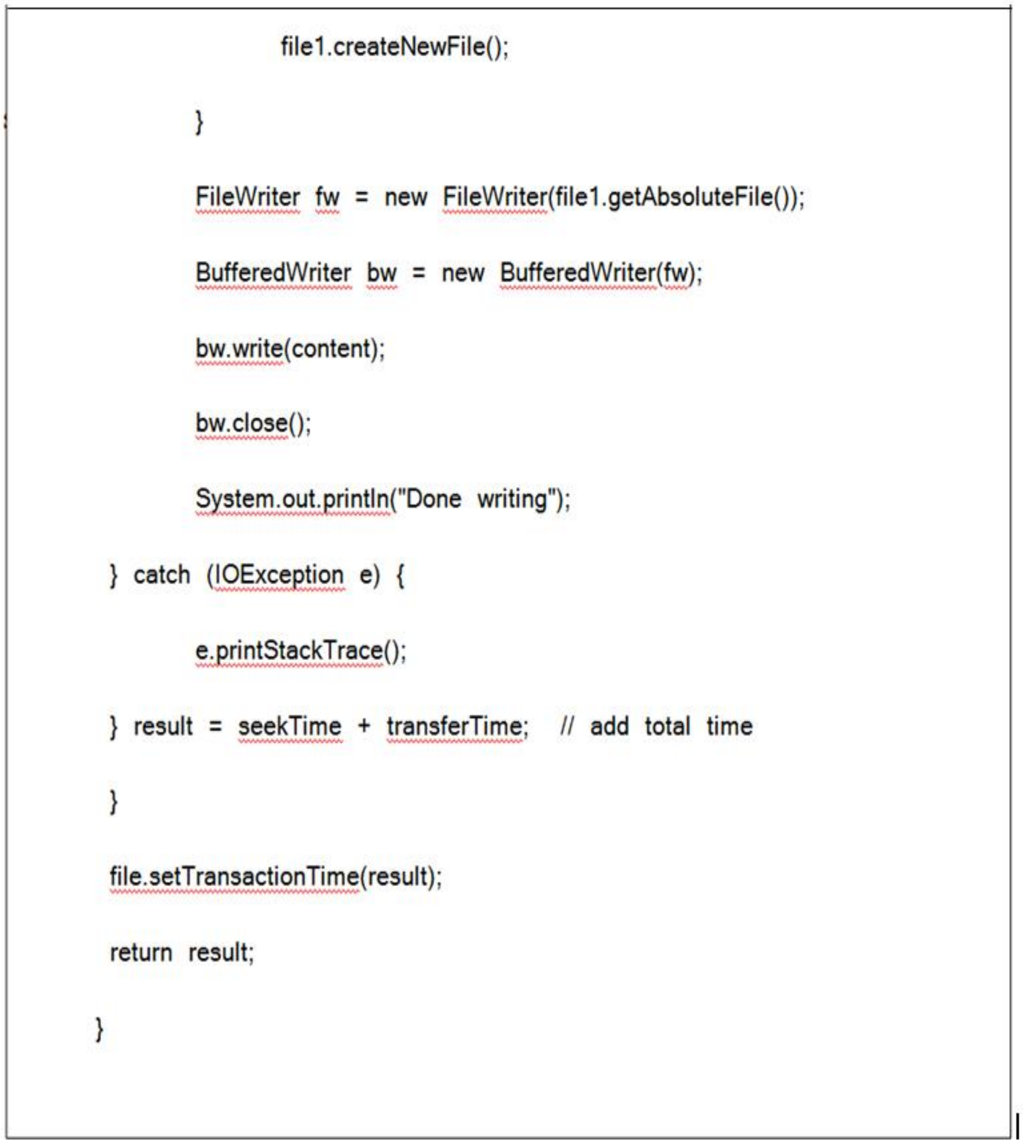
COMPLETE FILE USED:



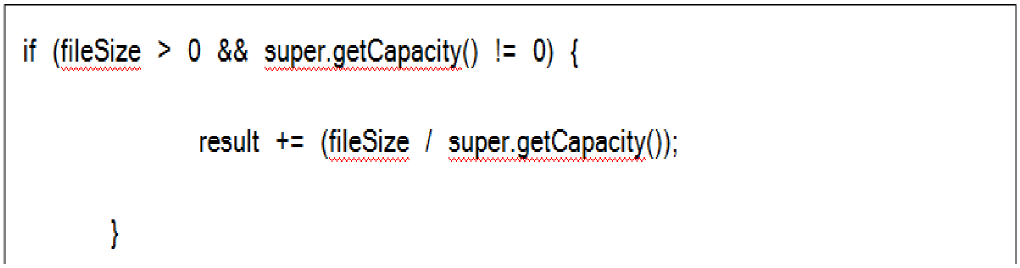
```
double result = 0.0;

                    // check if the file is valid or not

//                  if (!isFileValid(file, "addFile()")) {

          //                  return result;

                    //}


                    // check the capacity

                    if (file.getSize() + super.getCurrentSize() > super.getCapacity()) {

                              Log.printLine(super.getName() + ".addFile(): Warning - not

enough space" + " to store " + file.getName());

                              return result;

                    }


                    // check if the same file name is alredy taken

                    if (!contains(file.getName())) {

                              double seekTime = getSeekTime(file.getSize());

                              double transferTime = getTransferTime(file.getSize());
```



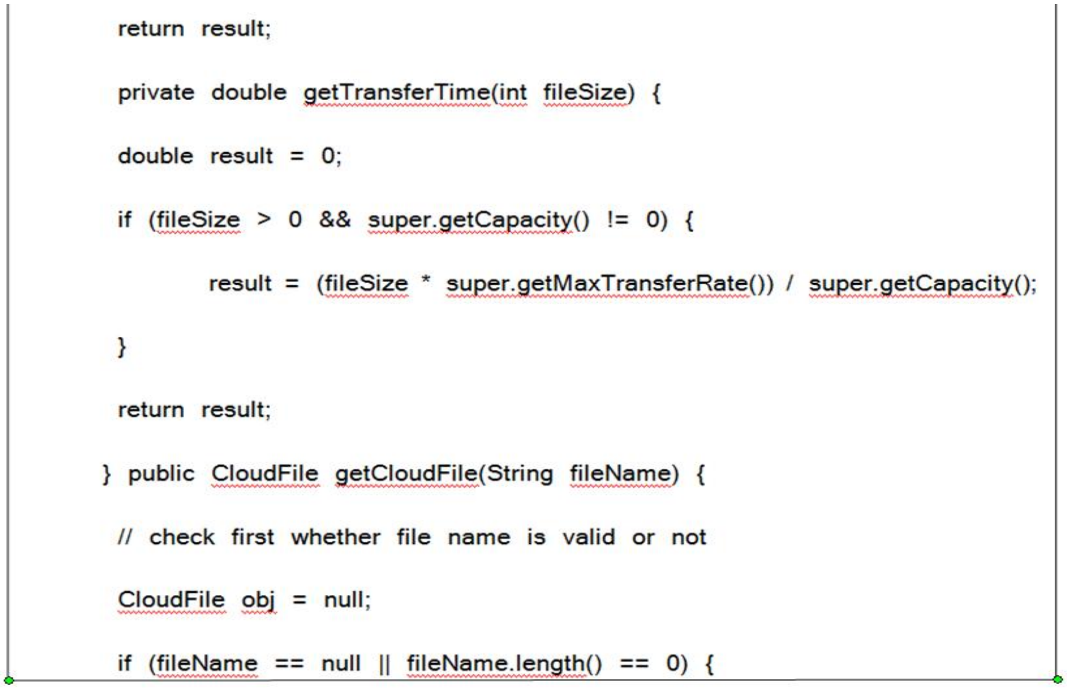
```
                              fileList.add(file);                   // add the file into the HD

                              //nameList.add(file.getName());        // add the name to the

name list


                              //currentSize += file.getSize();       // increment the current HD

size
```



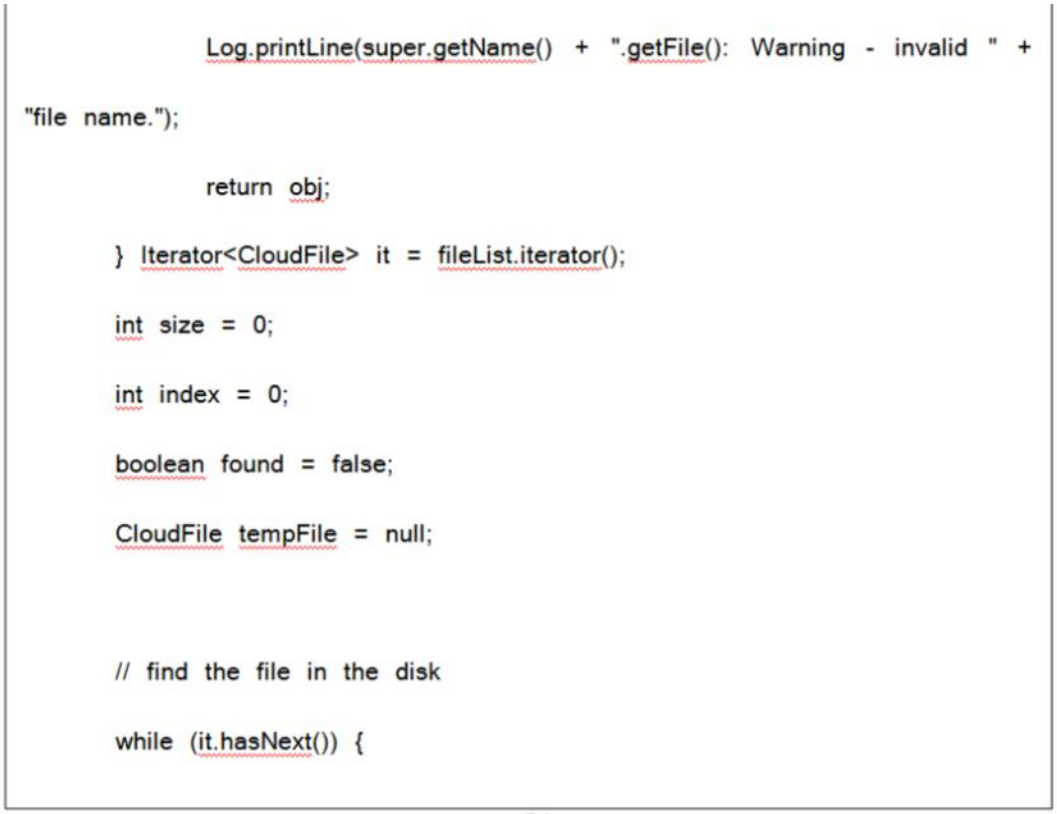
```
            file1.createNewFile();
        }
        FileWriter fw = new FileWriter(file1.getAbsoluteFile());
        BufferedWriter bw = new BufferedWriter(fw);
        bw.write(content);
        bw.close();
        System.out.println("Done writing");
    } catch (IOException e) {
        e.printStackTrace();
    } result = seekTime + transferTime;   // add total time
    }
    file.setTransactionTime(result);
    return result;
   }
```



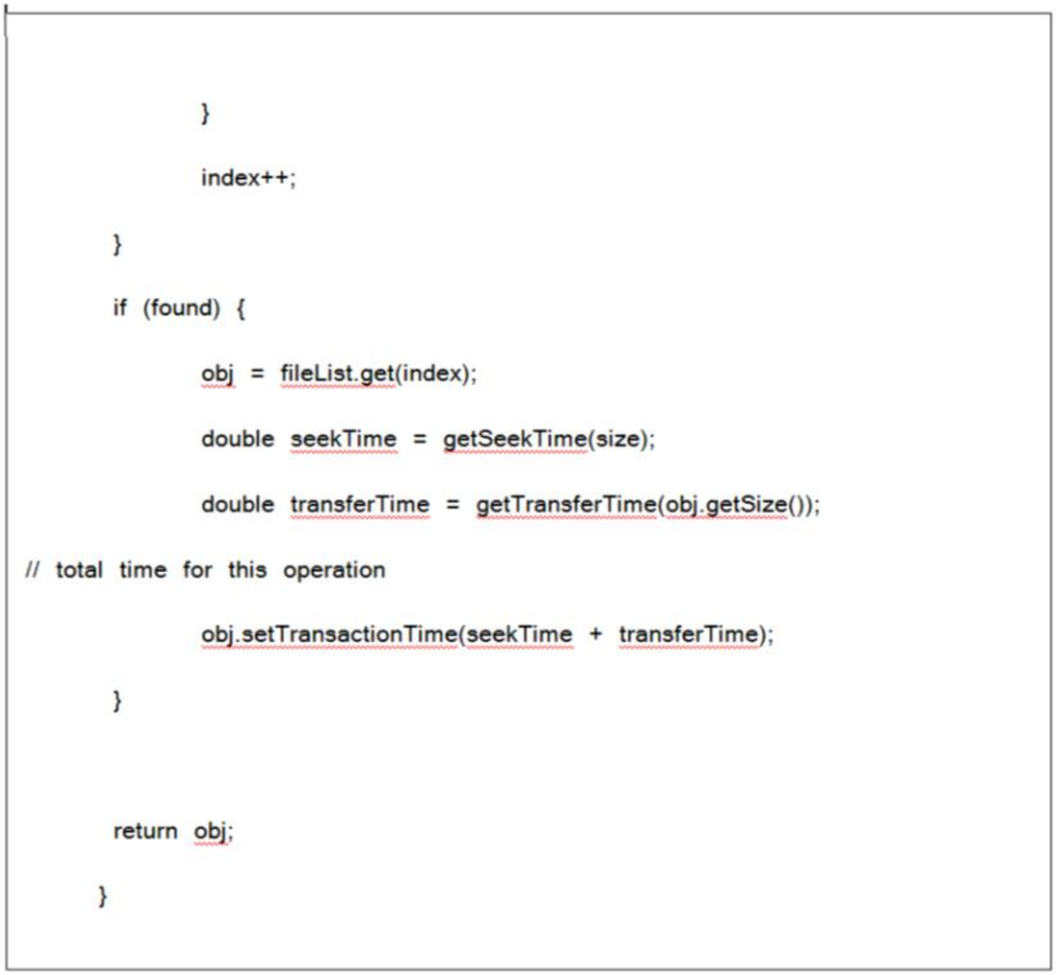
```
if (fileSize > 0 && super.getCapacity() != 0) {
        result += (fileSize / super.getCapacity());
    }
```



```
    return  result;

    private  double  getTransferTime(int  fileSize)  {

    double  result  =  0;

    if  (fileSize  >  0  &&  super.getCapacity()  !=  0)  {

          result  =  (fileSize  *  super.getMaxTransferRate())  /  super.getCapacity();

    }

    return  result;

  }  public  CloudFile  getCloudFile(String  fileName)  {

    //  check  first  whether  file  name  is  valid  or  not

    CloudFile  obj  =  null;

    if  (fileName  ==  null  ||  fileName.length()  ==  0)  {
```



```
            Log.printLine(super.getName()  +  ".getFile():  Warning  -  invalid  "  +
"file  name.");

            return  obj;

       }  Iterator<CloudFile>  it  =  fileList.iterator();

       int  size  =  0;

       int  index  =  0;

       boolean  found  =  false;

       CloudFile  tempFile  =  null;


       //  find  the  file  in  the  disk

       while  (it.hasNext())  {
```



```
                }
                index++;
            }
            if (found) {
                obj = fileList.get(index);
                double seekTime = getSeekTime(size);
                double transferTime = getTransferTime(obj.getSize());
// total time for this operation
                obj.setTransactionTime(seekTime + transferTime);
            }


            return obj;
        }
```

Input/output structure for proposed work:

Index Page to store data on the Cloud.

Inputs

Input the text file

Input an image file for key.

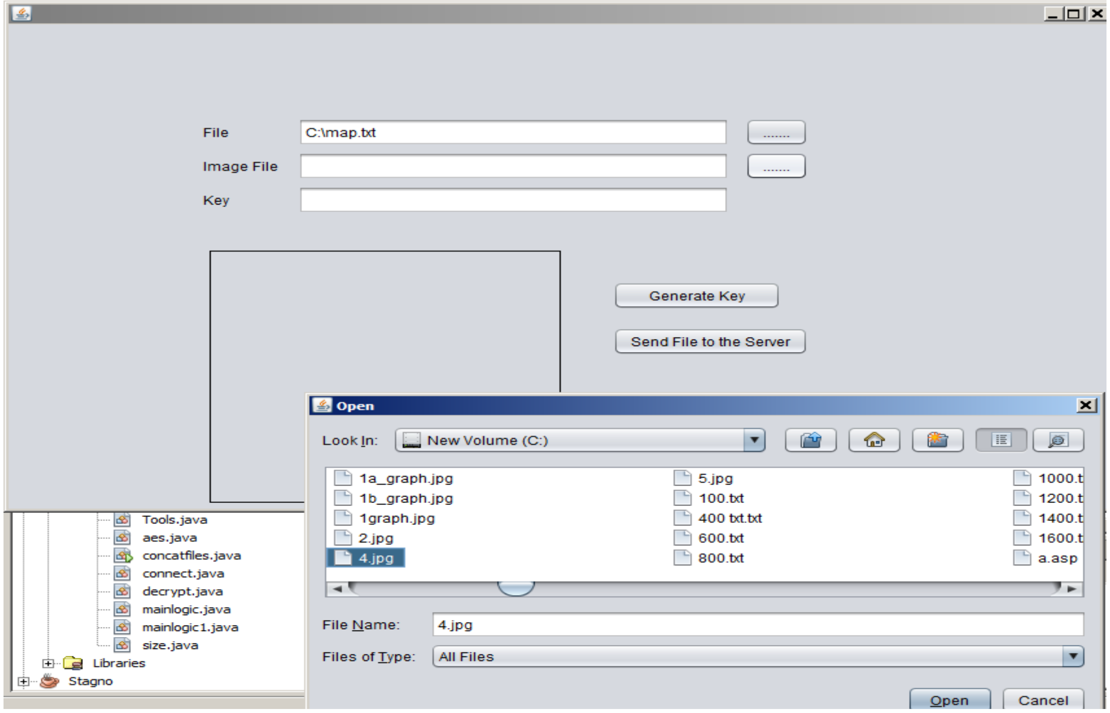
Processing

Text file is divided into several shares.

RSA Key is generated from the image for encryption of the shares.

All parts (shares) of the file are then encrypted using the key.

They are then stored in the Cloud having different servers.



File: C:\map.txt

Image File:

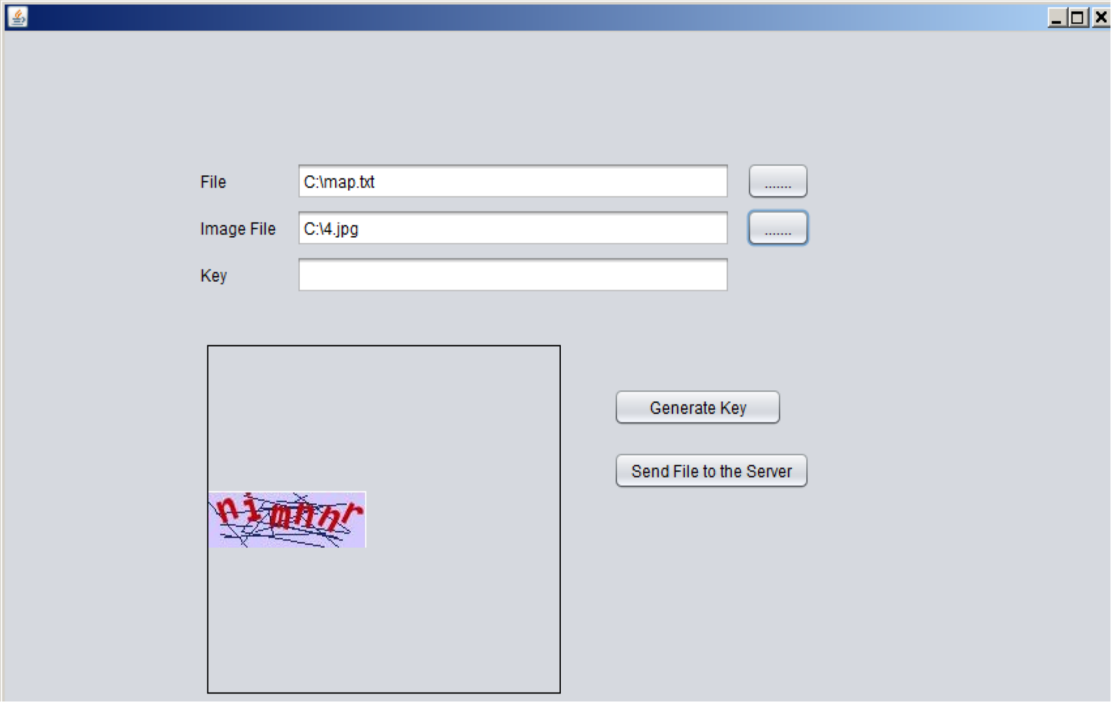
Key:

Look In: New Volume (C:)

File Name: 4.jpg

Files of Type: All Files

Figure: 1 Index Page



File: C:\map.txt

Image File: C:\4.jpg

Key:

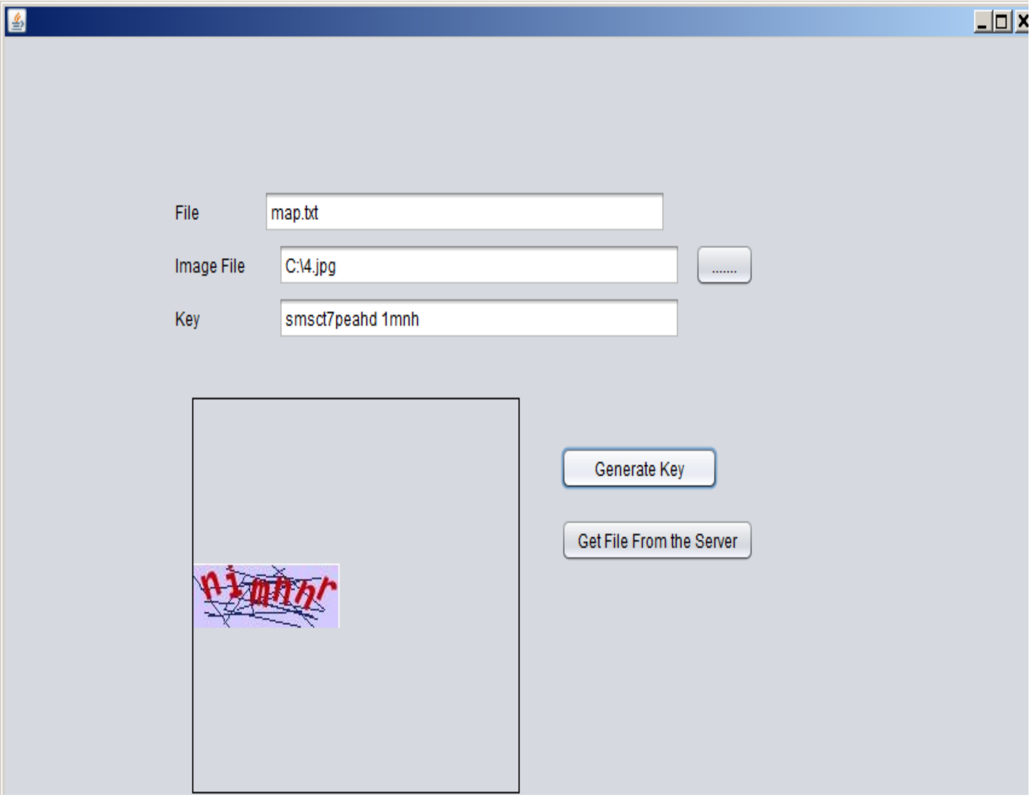
Figure 2: Index Page with Inputs

On Sending Files to the servers, System monitoring the cloud accesses its database and gives the information regarding the servers available in the Cloud. It contains IP Addresses of the servers. CloudSim3.0 library is used to create Virtual Cloud.

After getting the IP Addresses of the servers, file is divided into equal shares.

Image Files are used to create key for encryption process. Shares are then encrypted using this key. All these shares are stored in the cloud using the IP Addresses information. Information related to the encrypted share, their storage system IP address, key used in storage of shares are stored in the Cloud Monitor.

Index Page-2 .1to retrieve data from the Cloud



File map.txt

Image File C:\4.jpg

Key smsct7peahd 1mnh

Figure 3: Index Page-2 to retrieve data from the Cloud

Shares are decrypted using AES algorithm using Image key as a decryption key which is generated using RSA. After decryption, shares are combined to get the input file. If the image used for encryption matches with the image used for decryption then only the data can be retrieved.

9. FUTURE SCOPE:

This exploration is for online information stockpiling in a distributed computing environment. The proposed work portrays the utilization of an information apportioning plan called Information dispersal for actualizing such security. The chunks of data after encryption are put away on the servers.

Cloud information stockpiling has numerous focal points. It's not expensive, doesn't require establishment, needn't bother with supplanting, has reinforcement and recuperation frameworks, has no physical nearness, requires no faculty and doesn't require vitality for force or cooling.

Cloud information stockpiling however have a few noteworthy downsides, including execution, accessibility, contradictory interfaces and absence of gauges.

In this exploration work, servers are picked in the system and they should be recovered to reproduce the first information. Information reproduction obliges access to every server, and the learning of the servers on which the information or data are put away. This plan may likewise be utilized for information security as a part of sensor systems and web voting conventions, in armed force for sending private information's.

10. CONCLUSION

The recreation of the proposed work exhibits that is most suitable for those Cloud organization suppliers who are responsible for storing the client's information and where crucial focus is to give secured data stockpiling organizations. They provide confidentiality, easy recovery of the data as all computer operators are not literate regarding the internal process going on to maintain the security. Such type of user only knows how to upload the data.

11. REFERENCES

1) "About the Nebula Platform," http://nebula.nasa.gov/about/.
2) A Greenberg, "Distributed computing's Stormy Side," Forbes Magazine: http://www.forbes.com/2008/02/17/web-application-Cloud-tech-intel-cx_ag_0219Cloud.html, Feb 2008

3) "Amazon RDS for Oracle Database," http://aws.amazon.com/rds/prophet/?utm_source=OraclePR&utm_medium=RDSLandingPage&utm_campaign=Oracle

4) "Distributed computing versus Autonomic Computing," http://www.Cloudcomputingworld.org/Cloud-processing/Cloud-figuring versus autonomic computing.html

5) "Distributed computing issues," http://www.dataplex.com/blog/index.php/2010/01/07/Cloud-processing issues/

6) "Distributed computing," http://www.3tera.com/Cloud-registering/.

7) "Contextual investigations", http://aws.amazon.com/arrangements/contextual investigations/.

8) D. Chappell, "Presenting Windows Azure," http://www.microsoft.com/windowsazure/Whitepapers/IntroducingWindowsAzure/, October 2010.

9) Emily Maltby, "Little organizations hope to Cloud for funds in 2011," http://online.wsj.com/article/SB10001424052970203513204576047972349898048.html, December 29, 2010.

10) "Google App Engine," http://en.wikipedia.org/wiki/Google_App_Engine.

11) Robert McMillan, "Google to convey 'government Cloud' to feds in 2010," http://www.computerworld.com/s/article/9138075/Google_to_deliver_government_Cloud_to_feds_in_2010, Sept. 2009.

12) Sanjeev Aggarwal, Laurie McCabe, "The Compelling TCO Case for Cloud Computing in SMB and Mid-Market Enterprises," http://www.netsuite.com/entry/asset/collateral.shtml.

13) "What is iCloud," http://www.apple.com/iCloud/what-is.html.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com