A PROTECTED FILE ACCESS MECHANISM USING VISUAL CRYPTOGRAPHY

A PROJECT AND VIVA VOCE REPORT (ITB441)

Submitted by

S.RAJ KUMAR (0016134006)

SRUTHI CHANDRASEKARAN (0016132042)

Under the guidance of

Mr. B. V. Baiju

Assistant Professor

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING SCIENCES

DEPARTMENT OF INFORMATION TECHNOLOGY

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE

CHENNAI - 603 103

JUNE 2020

HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

BONAFIDE CERTIFICATE

Certified that this viva report on **"A PROTECTED FILE ACCESS MECHANISM USING VISUAL CRYPTOGRAPHY"** is the bonafide work of **"RAJ KUMAR(0016134006) AND SRUTHI C(001613042)"** who carried out the Viva-Voce Project work under my supervision during the academic year 2019-2020.

Signature:

Name: Dr. V. C. Sharmila

ASSOCIATE PROFESSOR

HEAD OF THE DEPARTMENT

DEPARTMENT OF IT

Signature:

Name: Mr. B. V. Baiju

ASSISTANT PROFESSOR

SUPERVISOR

DEPARTMENT OF IT

INTERNAL EXAMINER

Name:_____

Designation:_____

EXTERNAL EXAMINER

Name: _____

Designation: _____

A Viva- Voce Project conducted on _____

DEDICATION

I dedicate this project to God Almighty my creator, my source of inspiration, wisdom knowledge and understanding.

He has been the source of my strength throughout this problem and on his wings only have I soared; I also dedicate this to my Parents.

ACKNOWLEDGEMENT

The satisfaction that accompanies that the successful completion any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all effort with success. Our sincere thanks to our Chancellor **Dr. Elizabeth Varghese** and Vice Chancellor **Dr. Kuncheria P Isaac** for providing us with sufficient facilities which aided in the successful completion of project work.

We express our profound gratitude to Head of the Department, **Dr. V Ceronmani Sharmila** for her constant guidance and encouragement throughout the course of the project. We would like to thank our Faculty Incharge **Mr. B. V. Baiju,** Assistant Professor, Department of Information Technology, for giving valuable support and suggestion in finishing our project.

We thank all other teaching staff, supporting staff, of Department of Information Technology. It's a matter of pride and privilege for us to express our deep gratitude to the management of Hindustan Institute of Technology for providing us the necessary facilities and support. Last but not the least we would like to thank our Parents and Friends who encouraged and helped us in doing this project

ABSTRACT

In this era Cloud Computing has been used widely to bring more distributed data and resources together. The client can easily access the information from anywhere via internet at any time. As many data is introduced in each day, the insurance of information protection, delicate information typically needs to be scrambled before redistributing, which makes compelling information usage a difficult assignment. Here comes the need of client to protect the data that they store and accessing it wisely. The proposed system uses Advanced Encryption System (AES) for secure file uploading. Cloud provider upload the user file with secured image, that image should be splitting into two images like source and key image by using BVCS (Binocular Visual Cryptography schemes algorithm. Then, the key image and the password will be sent to the particular user and the necessary file can then be downloaded. The password is generated which is then splited into source image and key image and they are stored to the user and cloud server. Now the user has to send the key image to the cloud for accessing the files. The cloud matches the key image with the source image it already has. When both matches the file can be downloaded.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

According to NIST Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].The Cloud computing has cloud roots that can be tracked by several advanced technologies like web services, service-oriented architecture, cluster, grid, data center automation. Cloud applications are the combinations of different providers, such as Software as a service (SaaS) can provide services like e-mail, user authentication etc. The optimization of cloud is better than virtualization that it is easy to share and balance the loads across pools. There are no manual interventions needed to move or resize the resources for the applications that have built, moreover cloud provides a automatic provisioning within few hours from the requested time. Cloud infrastructure can be divided into three and that is Private, Public and Hybrid. Private cloud is preferred or most likely used by a private organization for a limited number of people thus the security is high and the data is not misused. In Public cloud, the service provided is for the general population. There is no need of initial investment and it less secure than public cloud. The Hybrid cloud is a combination of private and public cloud.

Cloud Computing is emerging very quickly in this era where there are lot of big industries like Facebook, Google etc have already show cased their best. As the cloud storage is a virtual space to store data and access via network. The user doesn't have any control over the data stored in the cloud, but the cloud provider has access to all information in stored in the cloud. Here comes the data protection in role. Security of information in cloud plays a major role when all data is being stored in it. Information Security [2] is the center of the cloud computing security problems. Data security [2] is mainly about the data confidentiality, integrity, availability.

CHAPTER 2

LITERATURE REVIEW

2.1 Review details

Paper 1:

A Secure cloud storage system

[3] Storing data in cloud has become a common in these days, thus it reduces the burden of user to oversee the data. The invisible part is data protection, which is a concern. To balance this issue, they have proposed a system with two authentication level that is Time-based One Time Password (TOTP) for cloud user's verification and Automatic Blocker Protocol (ABP). By introducing these techniques no third party could access the information.

Paper 2:

Secure Cloud Storage using AES Encryption

[4] As the resources stored in cloud are shared via internet, the user has access to the information anytime from anywhere. The security plays a curial such that the data stored by user is not misused or leaked by any third-party attack. Here comes secure cloud storage. Advanced Encryption Standard (AES) is used for high data security and keep it as a secret. The data is encrypted before it is being upload in the cloud and a Short Message Service (SMS) is implemented to avoid any unofficial access to the data.

Paper 3:

Efficient Cloud Storage Confidentiality to ensure Data Security

[5] All most every organization store the information in cloud, where they give the data to any outsourcing agent as they get large space to store data. By out sourcing the initial investments done by a small-scale industry would be less. It is important to encrypt the data before storing in cloud

to avoid data misuse and privacy. Here along with encryption, obfuscation technique is also performed to find out illicit users by performing particular mathematic functions.

Paper 4:

Secure Cloud Storage and File Storage

[6] Many industries store their data in cloud as that gives a plenty of virtual space. Once the data is uploaded in cloud the user does not have control over the uploaded file. Disintegration protocol (DIP) is performed for a secure file sharing.

CHAPTER 3

PROJECT DESCRIPTION

3.1 Existing system

Originally this type of systems was developed for operating systems. When the concept of multiple user operating system came, there came a need for mechanism which allowed users to create and manipulate files in this type of environment. In this type of operating system, each user doesn't get a separate environment, rather they get a common shared environment where all files created by all users are visible to all. To overcome this problem the concept of file access and file permissions came. A user creating a file becomes its owner and the operating won't allow other users to access it unless explicitly specified by the owner. These permissions are called meta data and stored along with the file and is used by operating system whenever anyone tries to open that file. over the years there were subtle changes to this mechanism such as user groups and so on as the operating system evolved. As the internet boomed, the need to share information became crucial and hence came file servers. They are internet connected computers whose purpose is to share files stored in them to whomever requested them via the internet. First security measures were similar to computer log in passwords. People who are trying to connect to the servers need to provide a username and password and if they are valid the person will be allowed to download content from the server. The current system evolved so much, the contents are now encrypted, sessions are authenticated. databases of suspicious IP address are stored and maintained and verified against incoming requests.

3.2 Limitations in existing system

Although existing systems are evolved so much, the security is still not impenetrable. username and passwords can be obtained by various methods. a simple sql injection allows an attacker to view the database of the system from there he can view the username and passwords of all the users and he can log in as whomever he pleases as some accounts have higher privileges. The attacker can also skip this step and directly gain access to this system and simply copy the files off as modern systems have multiple services running on the same system and not all of them are secure. Sometimes a single user using an weak password or compromised some other way locally

can compromise the entire server because security is implemented in the same way for all users and the attacker can study the system from inside and compromise the server to great extent.

3.3 Proposed system

The proposed system consists of various mechanisms to ensure protected data access. The data storing part consists of generating a random key for every file upload, it then uses that key to encrypt it with AES. During this process a separate image is generated using that key. This key image is then split into two images and one part of it is shared/stored along with user and other with the file itself. Anyone wanting to access a particular file puts in a request. The system then updates the owner of the particular file mentioning the person wanting to access that file. If he approves the request then the system will update the user that he can access the file now. This time when he access the file, the system will retrieve both images, merge it together and show it in the form of captcha, the user then identifies the key from the image and passes it back to the system, which will use that particular key to decrypt the file and send it to the user. Since this system uses different key for every file, the chances of system compromise is greatly reduced. Also since the system by itself doesn't store the decryption keys directly and authentication is done by visual means it further reduces the chances of system compromise.

3.4 Advantages of proposed system

While uploading the file is encrypted and key is separated and when a user is downloading, the encrypted file is downloaded and tried to decrypt in a sandboxed mode so that if it fails to decrypt, it will be destroyed. This ensures the security and integrity of data both in transit and idle. Since this system uses different keys for every file, the chances of system compromise are greatly reduced. Also, since the system by itself doesn't store the decryption keys directly and authentication is done by visual means it further reduces the chances of system compromise.

CHAPTER 4

SYSTEM REQUIREMENTS

4.1 Hardware requirements:

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It should what the system does and not how it should be implemented

- Processor - Pentium –III
- RAM - 4 GB
- Hard Disk - 260 GB
- Key Board, Mouse, Monitor

4.2 Software requirements:

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity.

- Operating System - Windows95/98/2000/XP
- Front End - HTML, Java, Jsp
- Scripts - JavaScript.
- Server side Script - Java Server Pages.
- Database - My Sql
- Database Connectivity- JDBC

CHAPTER 5

SYSTEM DESIGN

5.1 Architecture

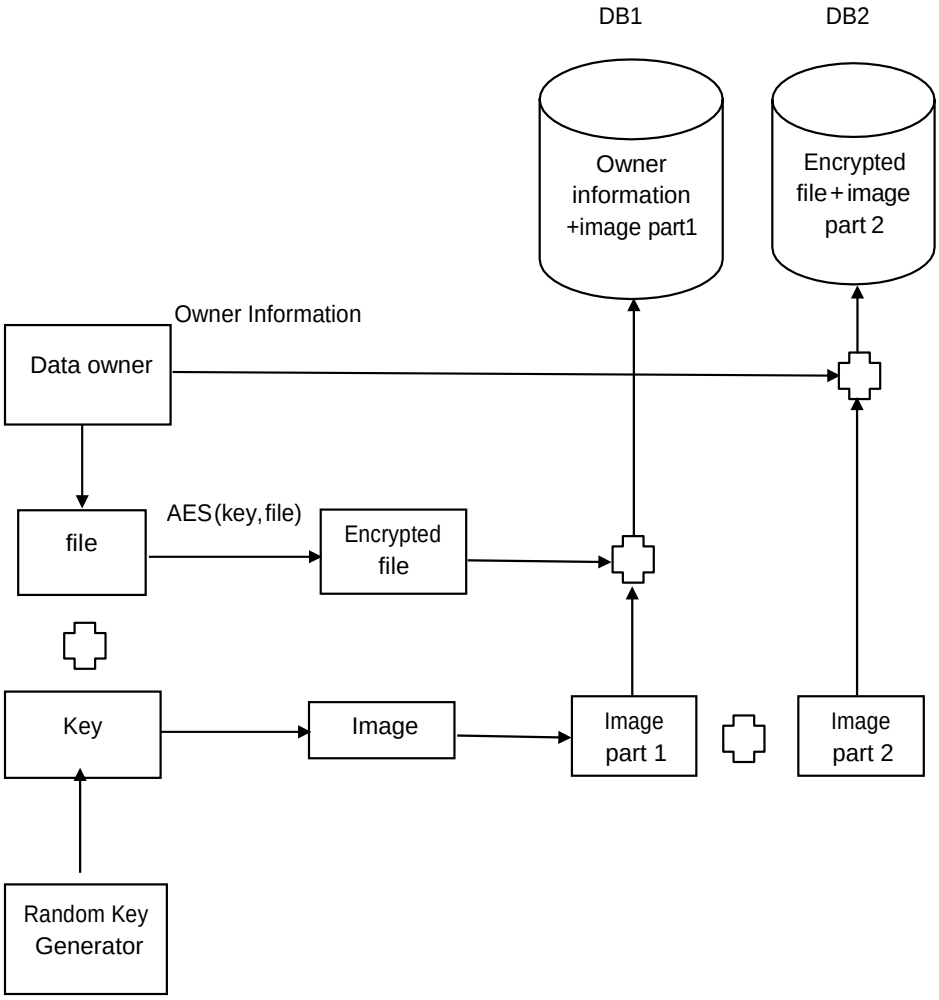


Fig.5.1 Data Upload

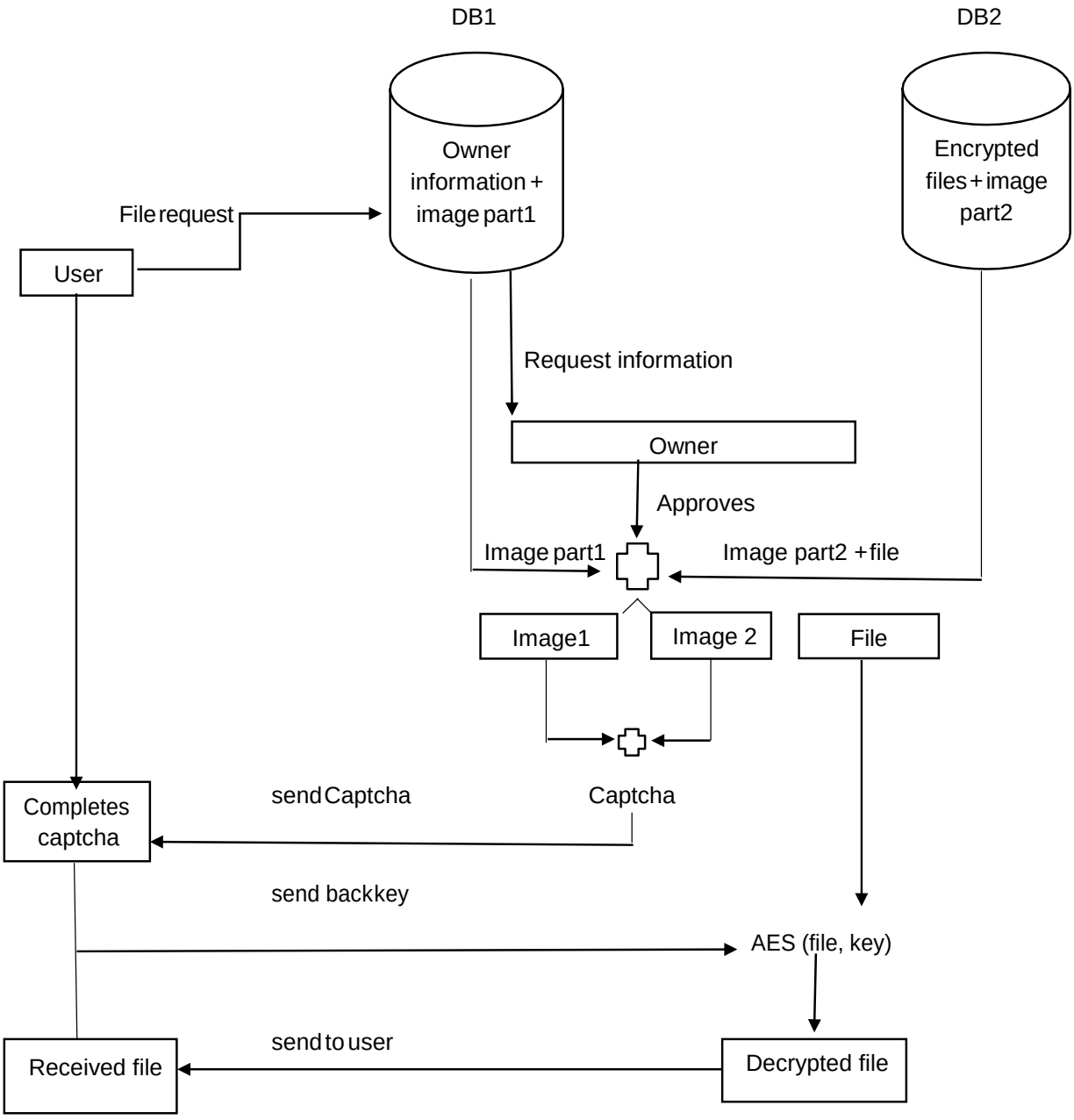


Fig.5.2 Data Retrieval

5.2 System design description

The software is implemented as web application and hence will reflect common web application pattern. An web interface for the users to interact with system. This web interface will also have a cryptographic module to encrypt and decrypt files. In the back end there will be two databases, one containing user profiles and part of meta datas needed to decrypt files of respective users, the other database containing the files and other part of meta datas. They are designed to be used asynchronously by the web application.

5.2.1 Input Design

The file upload part of the application is designed as a form. It also utilizes the cryptographic part of the application to produce a unique key whenever the form is opened. The form contains fields to gather file name and file upload and a check option to whether this file is to be stored securely or not. when the form is submitted and if the file is to be stored securely, the file is encrypted using AES using the generated random key and then an image is generated using the key and splitted into two and stored across the two databases along with the encrypted file as show in the diagram.

5.2.2 User Interface Design

The user interface has been designed using web technologies such as HTML, CSS, and JSP. It has profile pages for data owners, users and admin. Data owners have various pages to manage their uploaded files, form to upload new files and requests tab to view users who want to access files of the owner, he can accept or deny in this tab. Users have following pages, index page where they can view the list of documents and request for access to them, requests pages where the view the status of all the files requested by them and a page containing form to download the allowed files. A separate page for the admin to view and approve user profiles of data owner and users and file access requests and finally profile creation pages for data owners and users.

5.2.3 Procedural Design

The entire system has been designed to work asynchronously. Apart from the input/output system, the process from file request to user downloading the file works on event based. When an event occurs the response to it is executed by the system

5.2.4 Output Design

Once the request for the file is approved by the data owner and admin. The approved information is made available to the user via his requests page. The user now has to visit the portal where the verification using captcha occurs. After successful verification the file will be downloaded.

5.3 UML diagrams

5.3.1 Use case diagram:

Roles of the actors in the system can be depicted. In our use case diagram first user login into user window then if it is a valid user means then it can communicate with the cloud server.

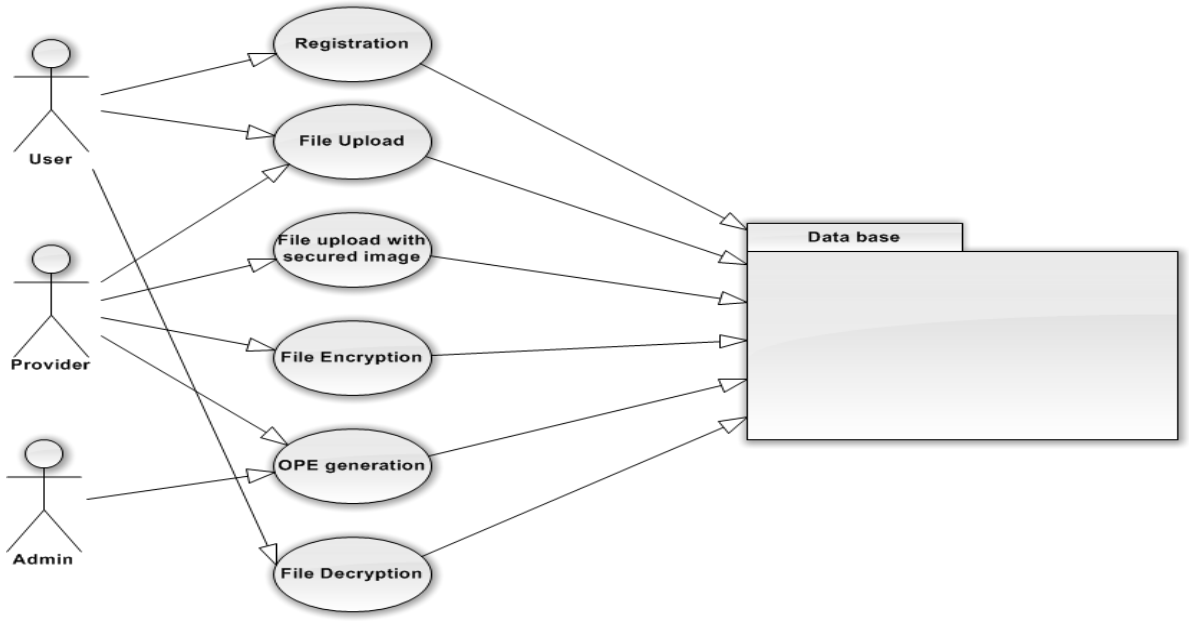


Fig. 5.3.1 Use Case Diagram

5.3.2 Class diagram:

In our class diagram we having the details about user, first user login into user window then if it is a valid user, then it can communicate with the cloud server. Here ranking function is involved in order to search the file in the order of ranking basis. The storage node contains the encrypted files and the user and provider has some of the particular registrations such as username and password.

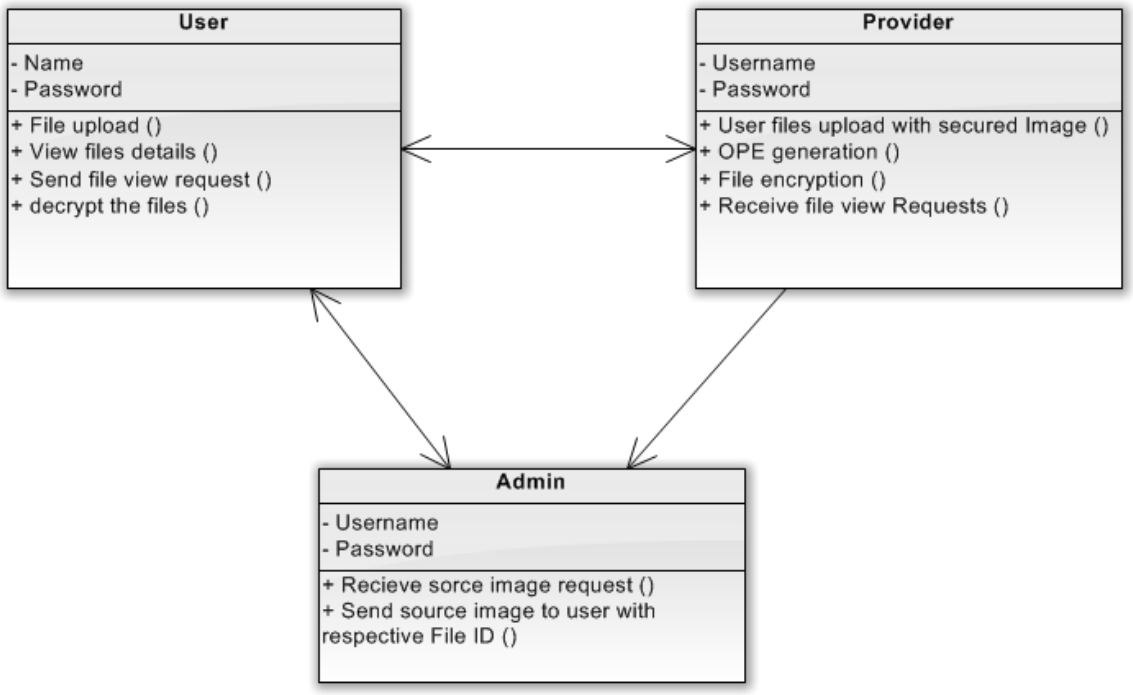


Fig. 5.3.2 Class diagram

5.3.3 Activity diagram:

The cloud storage contains the encrypted file and files can be retrieved from the user. The cloud server contains the respective keys and later entering the correct key the files will be downloaded.

After valid registration, user uploads the file and sends the file request. Similarly, provider performs the encryption and generates OPE password and admin verifies.

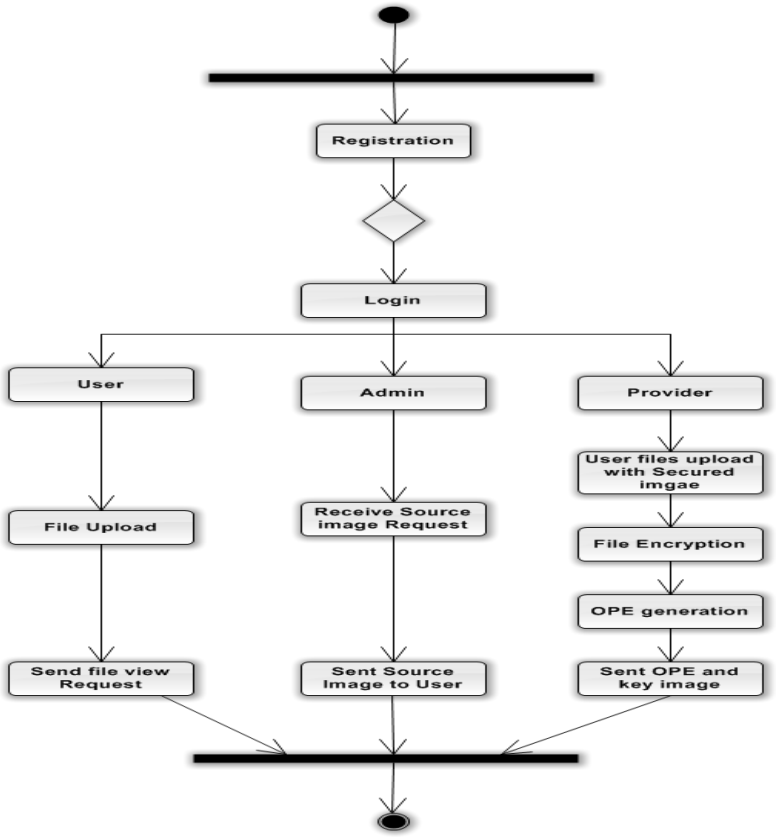


Fig. 5.3.3 Activity diagram

5.3.4 Sequence diagram:

In the sequence diagram, user enters into the cloud by performing certain authentication and user will retrieve the files available in the server. It explains about sending a file request to the provider and requesting for a OPE password and after verification the cloud server will provide the required source image to the user.

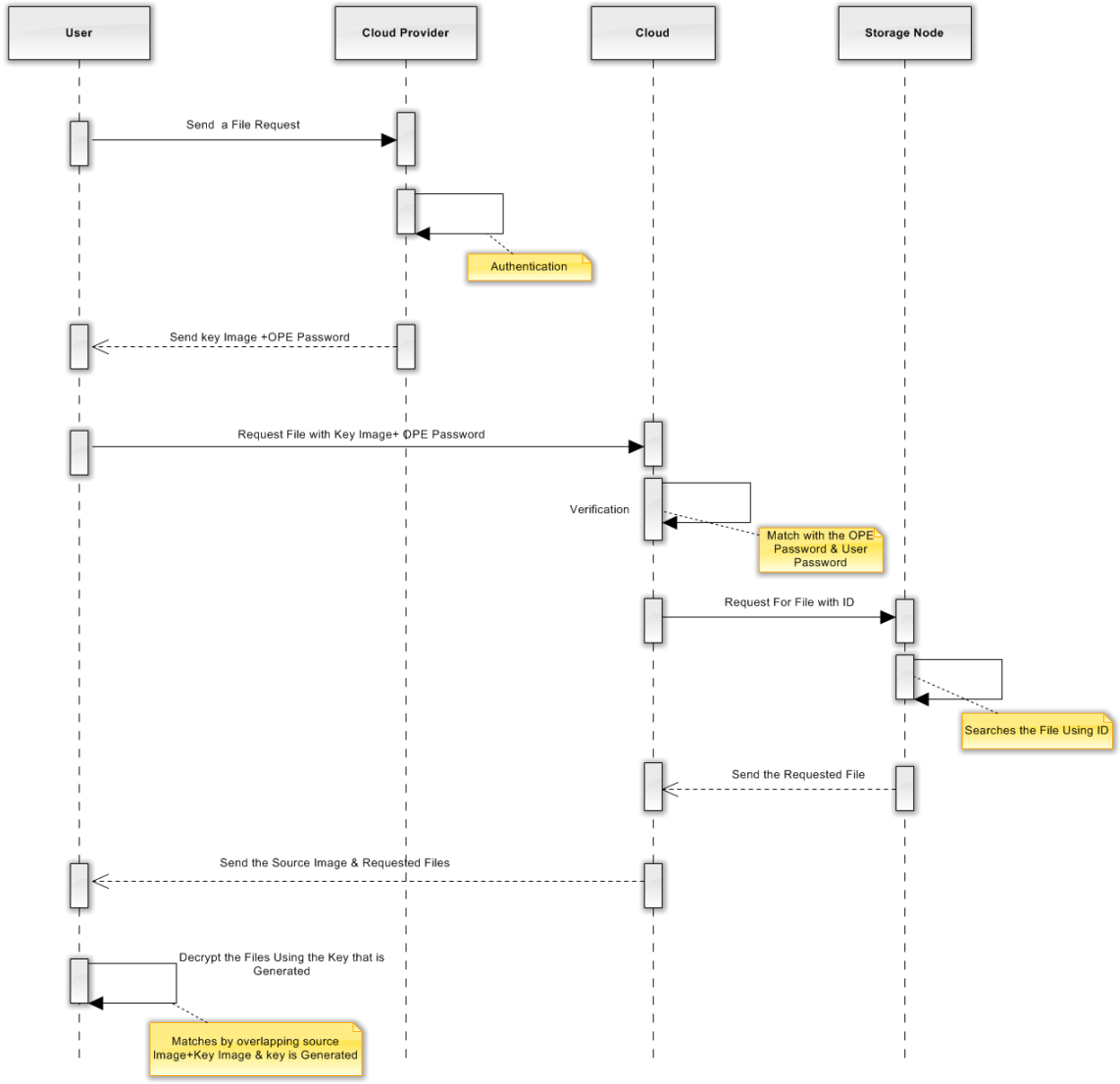


Fig. 5.3.4 Sequence diagram

5.3.5 Collaboration diagram:

A collaboration diagram describes interactions among objects in terms of sequenced messages it, explains about sending a file request to the provider and requesting for a OPE password and after verification the cloud server will provide the required source image to the user.

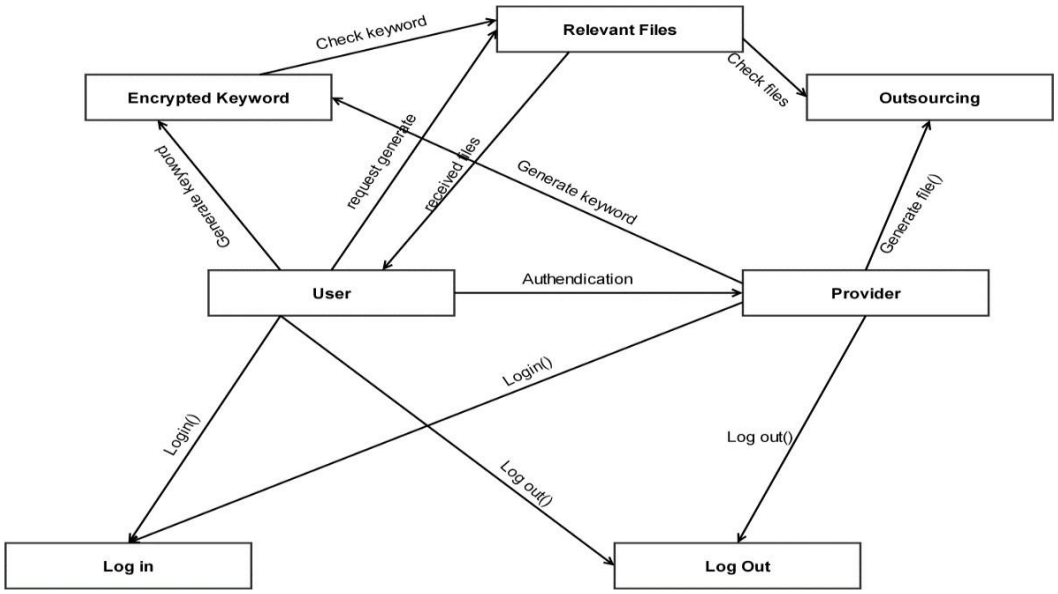


Fig. 5.3.5 Collaboration diagram

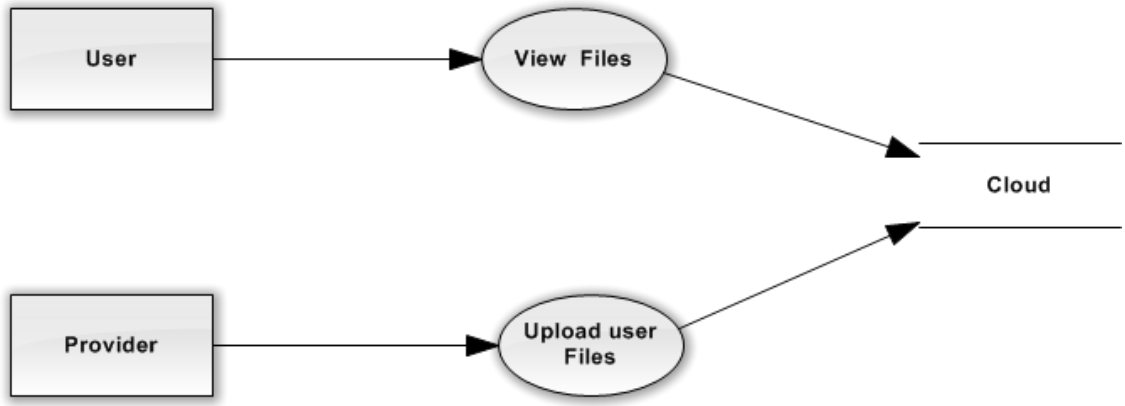
5.3.6 Data flow diagram:

User login into user window then if it is a valid user means then it can communicate with the cloud server. The registered users can publish and subscribe.

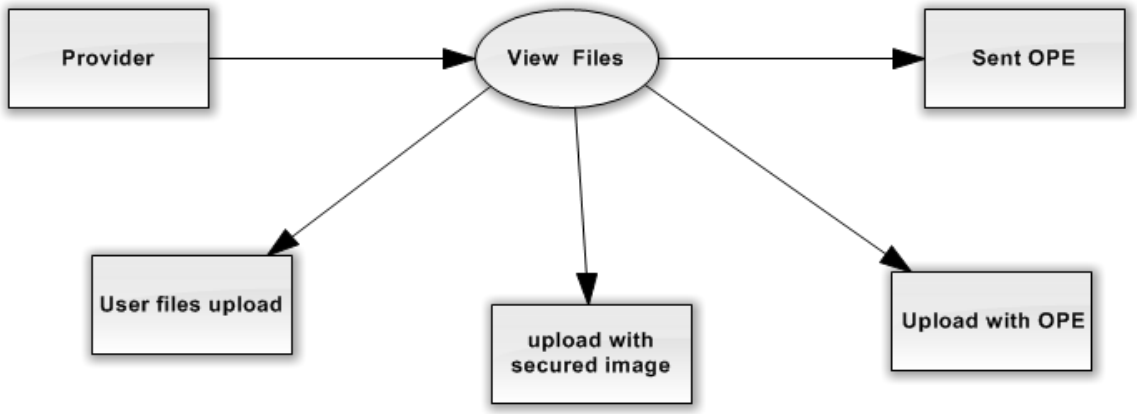
Level 0:

Level 1:

Level 2:



Level 3:



Overall:

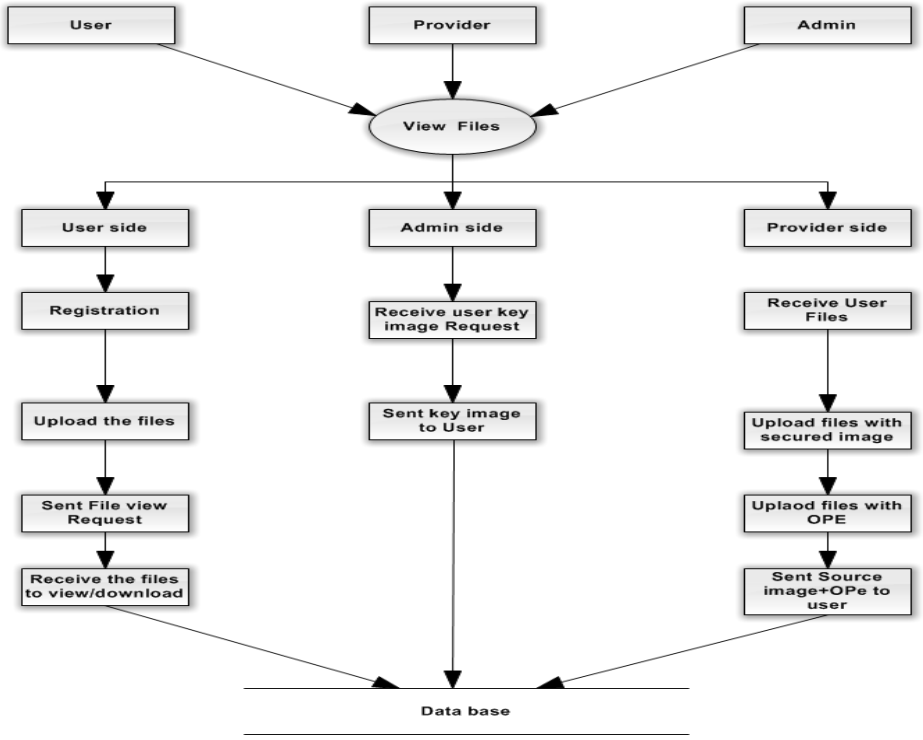


Fig.5.3.6 Data flow diagram

5.3.7 Entity Relationship Diagram

Entity-Relationship Model is an abstract and conceptual representation of data. Entity-relationship modelling is a database modelling method. It describes whether authentication between the user and server is performed correctly and the respective encrypted files and index are generated and then the image is displayed to the user.

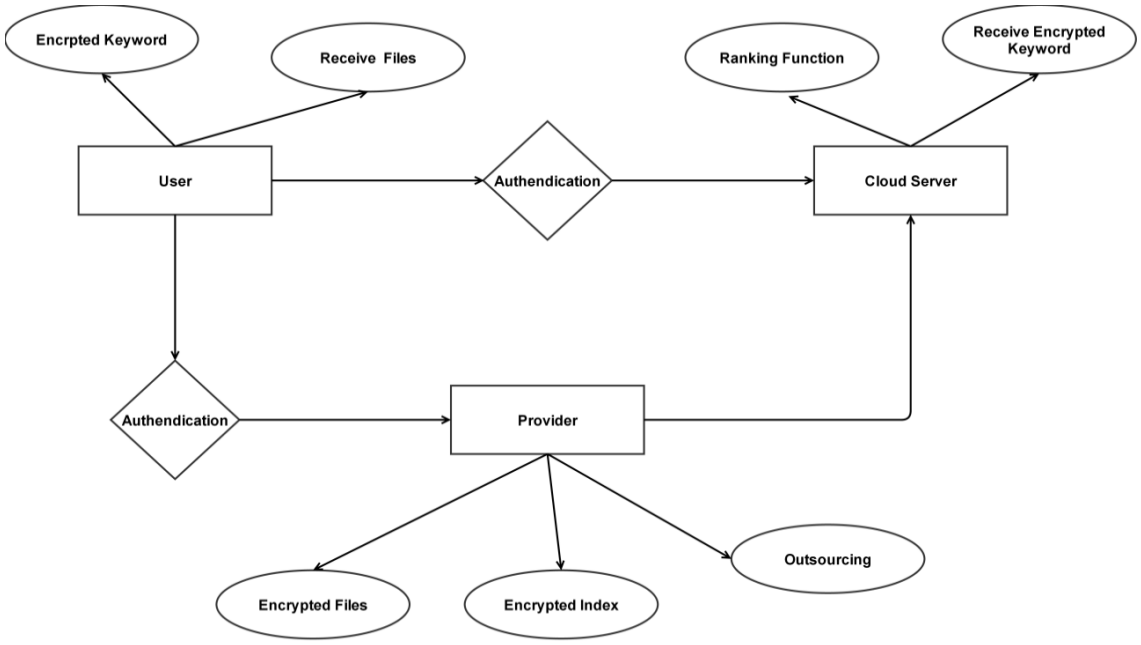


Fig.5.3.7 Entity Relationship Diagram

CHAPTER 6

MODULES

6.1 Secure file uploading

In the upload portal when the data owner uploads a file a random key is generated and the file is immediately encrypted using AES with that key. Along with this process visual cryptography takes place which is explained in detail below. By encrypting data before uploading to the server, MITM attacks (Man In The Middle) can be mitigated. An MITM attack is one where an attacker sets himself between a user and a server and all the interaction between them passes through the attacker. If the encryption occurs in the server side and if the attacker was able to obtain a copy of the data while it was being sent to the server then the entire process would be moot. Hence the file should be encrypted before sending it to the server.

6.2 Visual cryptography

Visual cryptography is a technique where confidential information is injected/transformed into an image after which it is split into n parts. Any one of the n parts or even n-1 parts couldn't be used to reproduce the original information injected into the image. Only when all the n parts are combined together the secret is revealed visually. We use this technique to inject the random key generated during upload into an image and split into two parts. One is stored along with data owner, other with the uploaded file. These two will be combined when another user wants to retrieve the file to reveal the decryption key.

6.3 Storing the uploaded files

The uploaded files are two images, and an AES encrypted file. One image along with encrypted file is stored together on a distribution server while the other image is stored along with the data owner's records/data. These two should be using separated servers and database so that even if one of the systems gets compromised, the data remains protected. We use AES because it's implementation in software is faster and it is highly secure, qualities due to which it has become an industry standard for data protection.

6.4 Verification and retrieval

When the user has been approved by the owner, the system will merge the images from both sources and send it in the form of captcha. The user then visually identifies the key and sends it back to the system. The system then creates a copy of that file and decrypts it, if the output is garbled (the output can be verified if garbled or not by checking the padding, for example in java BadPaddingException occurs) then it knows it’s not the correct key and informs the user and the file is not retrieved. If the output is not garbled the user is given a copy of the file.

CHAPTER 7

SYSTEM IMPLEMENTATION

7.1 System Implementation

Systems implementation is the construction of the new system and the delivery of that system into production the Construction Phase of Systems Implementation has two things: builds and tests a functional system that fulfills business or organizational design requirements, and implements the interface between the new system and the existing production system. The project team must construct the database, application programs, user and system interfaces, and networks. Some of these elements may already exist in the project or be subject to enhancement.

7.2 ALGORITHM

7.2.1 AES algorithm:

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

STEPS IN ADVANCED ENCRYPTION STANDARD:

Step 1: Derive the set of round keys from the cipher key

Step 2: Initialize the state array with the block data

Step 3: Add the initial round key to the starting state array

Step 4: Perform nine rounds of state manipulation

Step 5: Perform the tenth and final round of state manipulation

Step 6: Copy the final state array out as the encrypted data

7.2.2 File hashing splitting algorithm

The two encryption methods used in this work for encryption use different keys. Key splitting module generates two random keys from the main key. It divides the Key bits into half i.e. if key is of length n then the generated random two keys will be of length n/2. The pseudo code for key splitting is given below:

Step1: Input is n bit key

Step2: Set Key1 and Key2 as n/2 bit value and initialize it to 0

Step3: Initialize the random function with given seed value. 323

Step4: Initialize length as n, i=0, j=0, flag=0.

Step5: While (length != 0)

5.1: If Flag==0 then

Find a bit position randomly that has not been used.

Find out the value at that bit position in main key.

If value at that bit position is 1 then

Set the i'th bit of key1 as 1 and Increment i value

else

Set the i'th bit of key1 as 0 and Increment i value

Set Flag=1, Set the above found bit position is used.

Go to Step 5.3

5.2 : Else

Find a bit position randomly that has not been used.

Find out the value at that bit position in main key.

If value at that bit position is 1 then

Set the i’th bit of key2 as 1 and Increment j value

else

Set the i’th bit of key2 as 0 and Increment j value

Set Flag=0, Set the above found bit position is used.

Go to Step 5.3

5.3 : Decrement the Length;

5.4: Go to step 5

Step6: Return the keys key1 and key2 of size n/2.

CHAPTER 8

SYSTEM TESTING

8.1 Software testing

Software testing is the process used to help identify the correctness, completeness, security and quality of developed computer software. Testing is vital to the success of the system. System Testing makes logical assumption that if all the parts of the system are correct, the goal will be successfully achieved.

System Testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of developed system using various kinds of data.

There are many approaches to software testing, but effective testing of complex products is essentially a process of investigation, not merely a matter of creating and following rote procedure. One definition of testing is the "the process of questioning a product in order to evaluate it", where the" questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. The quality of the application can, and normally does, vary widely from system too system but some of the common quality attributes include reliability, stability, portability, maintainability and usability.

8.2 Testing objectives

A number of rules that can serve well as testing objectives:

1. Testing is a process of executing a program with the intent of finding an error.

2. A good test case is one that has a high probability of finding an as-yet undiscovered error.

3. A successful test is one that uncovers an as-yet-undiscovered error. These objectives imply a dramatic change in viewpoint. They move counter to the commonly held view that:- a successful test is one in which no errors are found. Our objective is to design tests that systematically uncover different classes of errors and to do so with a minimum amount

of time and effort. If testing is conducted successfully according to the objectives stated previously it will uncover errors in the software. As a secondary benefit, testing demonstrates that software functions appear to be working according to specification, that behavioral and performance requirements appear to have been met. In addition, data collected as testing is conducted provide a good indication of software reliability and some indication of software quality as a whole. But testing cannot show the absence of errors and defects, it can show only that software errors and defects are present. It is important to keep this statement in mind as testing is being conducted.

8.3 Test plan

A test plan can be defined as a document describing the scope, approach, resources, and schedule of intended testing activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. A test plan documents the strategy that will be used to verify and ensure that a product or system meets its design specifications and other requirements. A test plan is usually prepared by or with significant input from test engineers.

Depending on the product and the responsibility of the organization to which the test plan applies, a test plan may include a strategy for one or more of the following:

- Design Verification or Compliance test - to be performed during the development or approval stages of the product, typically on a small sample of units.
- Manufacturing or Production test - to be performed during preparation or assembly of the product in an ongoing manner for purposes of performance verification and quality control.
- Acceptance or Commissioning test - to be performed at the time of delivery or installation of the product.
- Service and Repair test - to be performed as required over the service life of the product.
- Regression test - to be performed on an existing operational product, to verify that existing functionality didn't get broken when other aspects of the environment are changed (e.g., upgrading the platform on which an existing application runs).

A complex system may have a high-level test plan to address the overall requirements and supporting test plans to address the design details of subsystems and components. Test plan document formats can be as varied as the products and organizations to which they apply. There are three major elements that should be described in the test plan: Test Coverage, Test Methods, and Test Responsibilities. These are also used in a formal test strategy.

CHAPTER 9

CONCLUSION

9.1 Conclusion

Thus, we have created a web application using JSP which functions as a file server which focuses on the security and safety of the data much more rigorously. Things such as profile approval by the admin and file requests approval by both admin and data owner increases security and helps remove possible security threats at a higher level (such as unwanted person even accessing the download portal). On a lower level using random key to encrypt file ensures that every file is encrypted using separate key and if the attacker manages to get access to a particular key only that file be affected leaving the rest of them secure (however the security checks at higher level will deter this). Next by using two different databases and by splitting data between those and making the decryption of file dependent on data in both databases, the security is enhanced significantly. Because even if the attackers gain access to one database the data available there will be useless without the data from the other database, and since each file is encrypted using different keys, security is compounded. By using visual cues to obtain decryption keys and the key never stored in any other form or made available to the system to be managed by the system scripts from the attacker will be useless. The only possible way for a script to decrypt the file (assuming the script has access to file for repeated processing) will be by brute forcing which will take even supercomputers hundreds of years which is not feasible

REFERENCES

[1] P. Mell, Grance, “The NIST definition of cloud computing”, Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011, pp. 800-145.

[2] Xiaojun Yu, Qiaoyan Wen, ”A View about Cloud Data Security from Data Life Cycle”, International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, Dec 2010, pp 1-4.

[3] Sangamesh, S. M., and S. S. Joshi. "A Survey on: A Secure Cloud Storage System: An Approach."

[4] Babitha, M. P., and KR Remesh Babu. "Secure cloud storage using AES encryption." 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT). IEEE, 2016.

[5] Arockiam, L., and S. Monikandan. "Efficient cloud storage confidentiality to ensure data security." 2014 International Conference on Computer Communication and Informatics. IEEE, 2014.

[6] Rawal, Bharat S., and S. Sree Vivek. "Secure cloud storage and file sharing." 2017 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2017.

[7] Q. Chai and G. Gong, “Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,” in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922.

[8] Ali, Fairouz Sher, and Songfeng Lu. "Searchable encryption with conjunctive field free keyword search scheme." 2016 International Conference on Network and Information Systems for Computers (ICNISC). IEEE, 2016.

[9] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, “Privacy preserving multiple keyword search for confidential investigation of remote forensics,” in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE, 2011, pp. 595–599.

APPENDIX

SAMPLE CODE

Encryption:

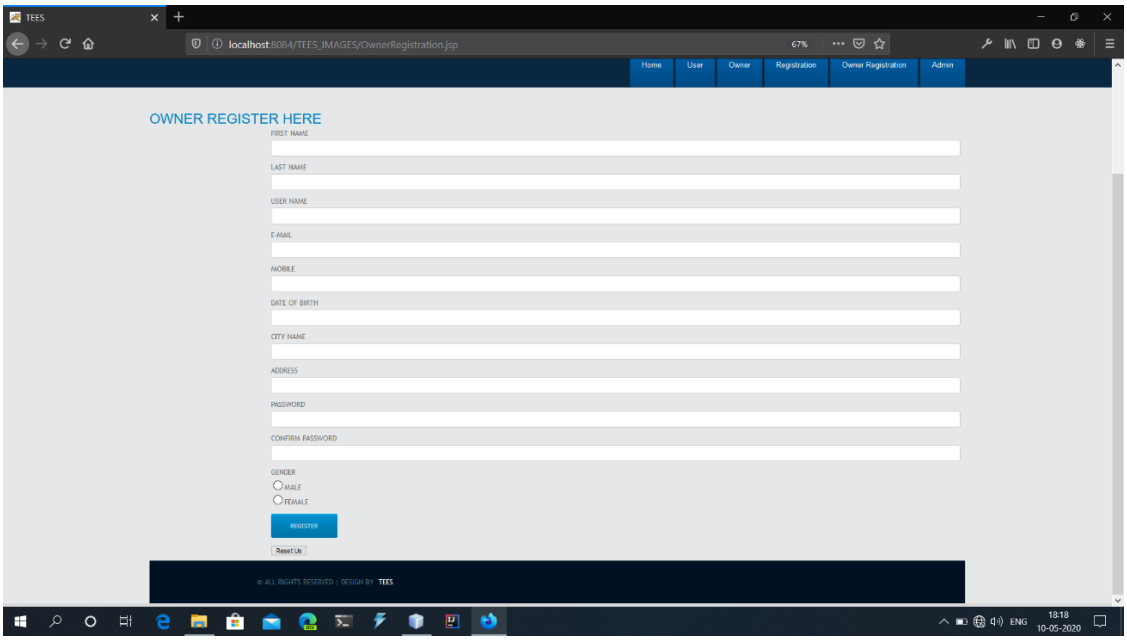
```
import java.security.InvalidAlgorithmParameterException;

import java.security.InvalidKeyException;

import java.security.NoSuchAlgorithmException;

import java.util.logging.Level;

import java.util.logging.Logger;

import javax.crypto.BadPaddingException;

import javax.crypto.Cipher;

import javax.crypto.IllegalBlockSizeException;

import javax.crypto.KeyGenerator;

import javax.crypto.NoSuchPaddingException;

import javax.crypto.SecretKey;

import sun.misc.BASE64Encoder;

public class Encryption {

  public String Encryption1(String value) throws InvalidKeyException, IllegalBlockSizeException, BadPaddingException

  {

    String Encry="";

    try {

      String plainData=value,decryptedText;
```

```
        KeyGenerator keyGen = KeyGenerator.getInstance("AES");
        keyGen.init(128);
        SecretKey secretKey = keyGen.generateKey();
        Cipher aesCipher=null;
        try {
           aesCipher = Cipher.getInstance("AES");
        } catch (NoSuchPaddingException ex) {
           Logger.getLogger(Encryption.class.getName()).log(Level.SEVERE, null, ex);
        }
        aesCipher.init(Cipher.ENCRYPT_MODE,secretKey);
        byte[] byteDataToEncrypt = plainData.getBytes();
        byte[] byteCipherText = aesCipher.doFinal(byteDataToEncrypt);
        Encry = new BASE64Encoder().encode(byteCipherText);
              try {
                 aesCipher.init(Cipher.DECRYPT_MODE,secretKey,aesCipher.getParameters());
              } catch (InvalidAlgorithmParameterException ex) {
              }
        byte[] byteDecryptedText = aesCipher.doFinal(byteCipherText);
        decryptedText = new String(byteDecryptedText);
        System.out.println("\n Plain Data : "+plainData+" \n Cipher Data : "+Encry+" \n Decrypted
Data : "+decryptedText);

      } catch (NoSuchAlgorithmException ex) {
```

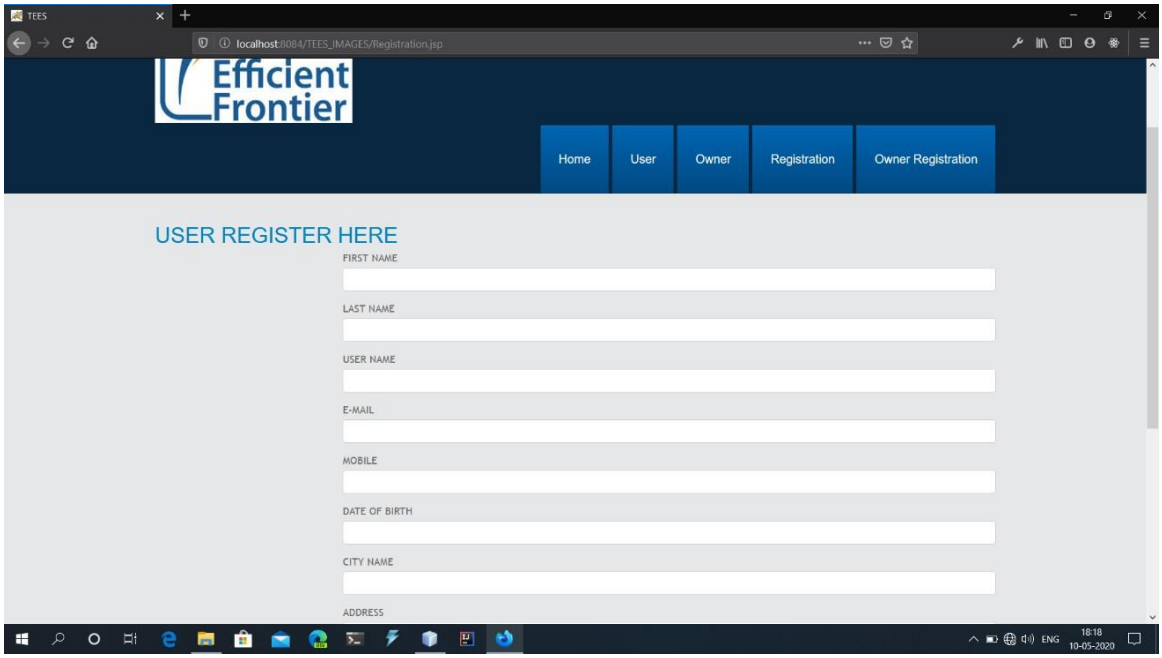
```
            Logger.getLogger(Encryption.class.getName()).log(Level.SEVERE, null, ex);
        }
        return Encry;
    }


}
            }
        }
        return "";
    }
}
```

SAMPLE SCREENSHOTS

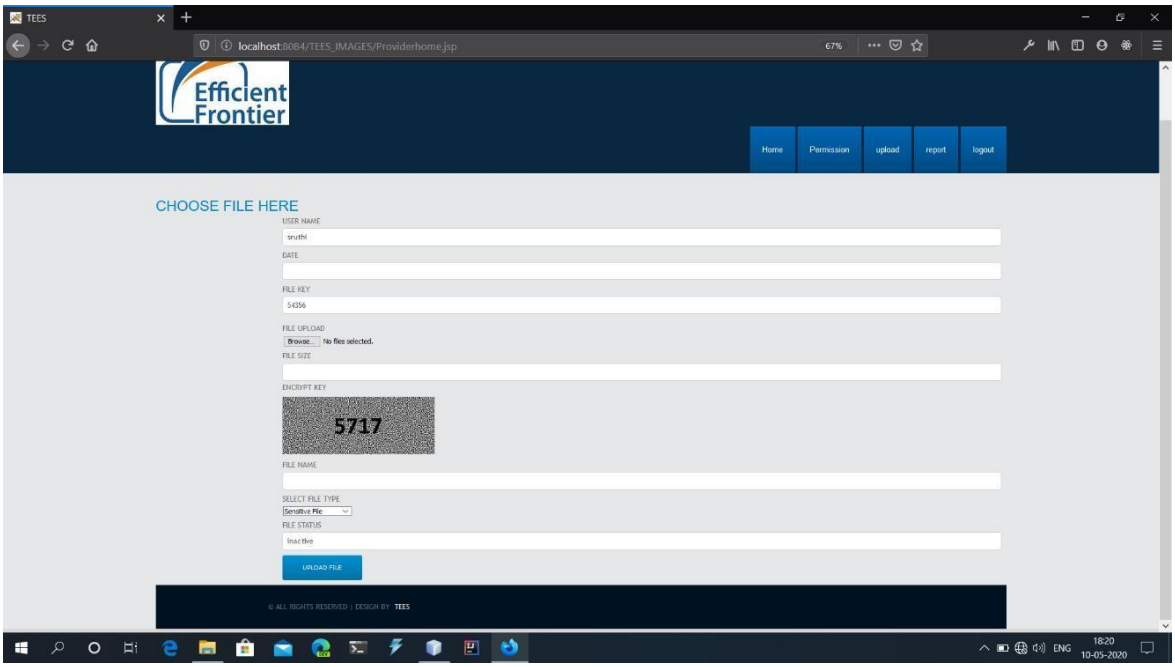
Home Page



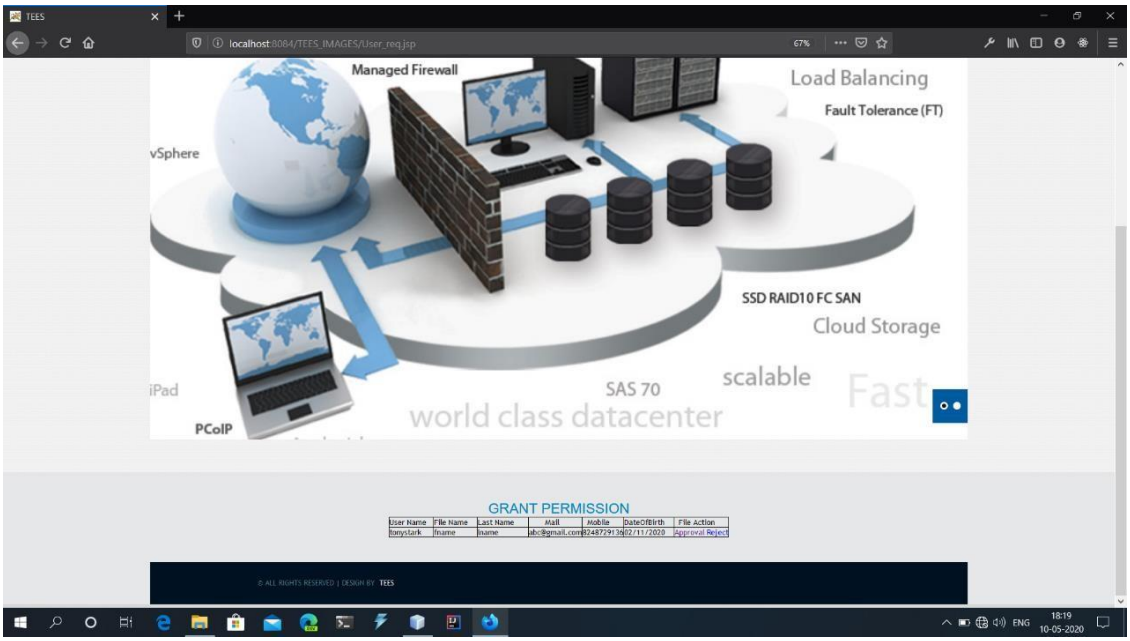
Owner Registration



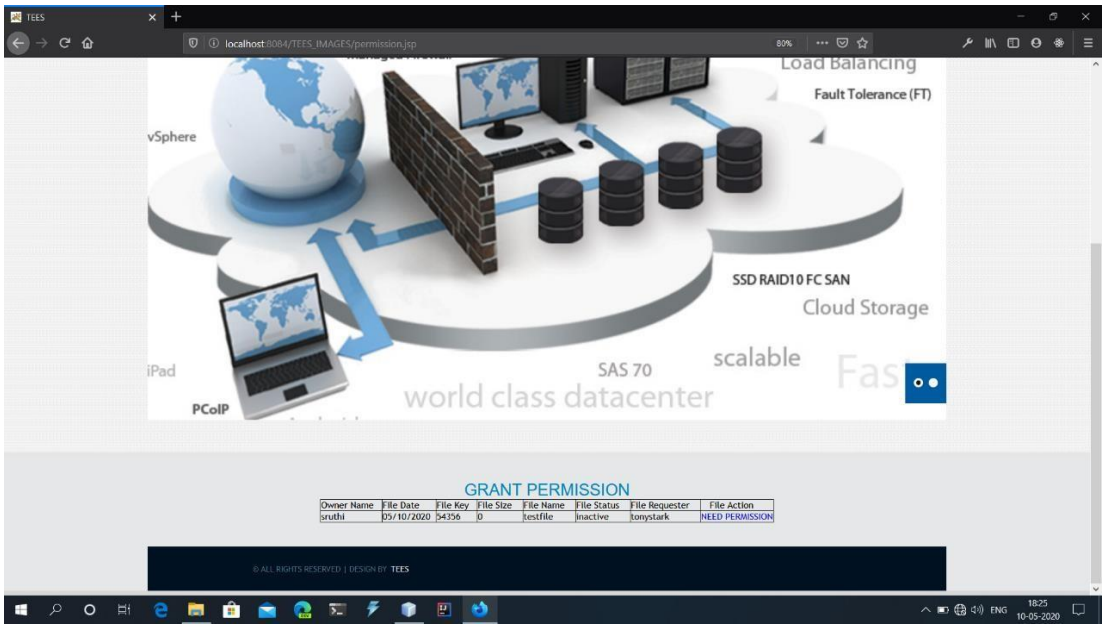
User Registration



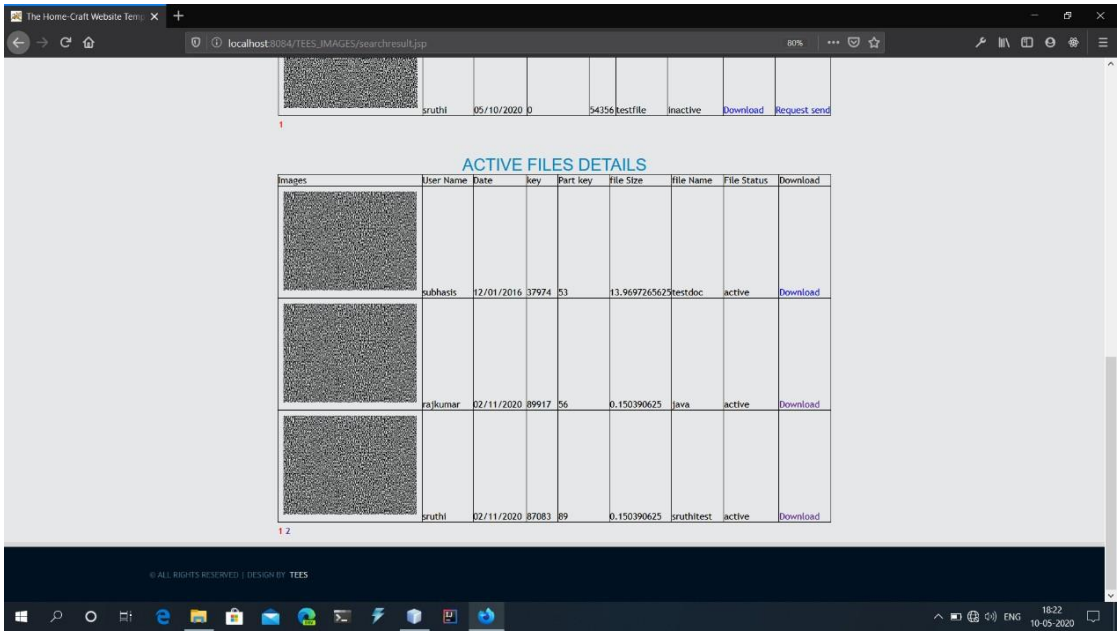
File Upload



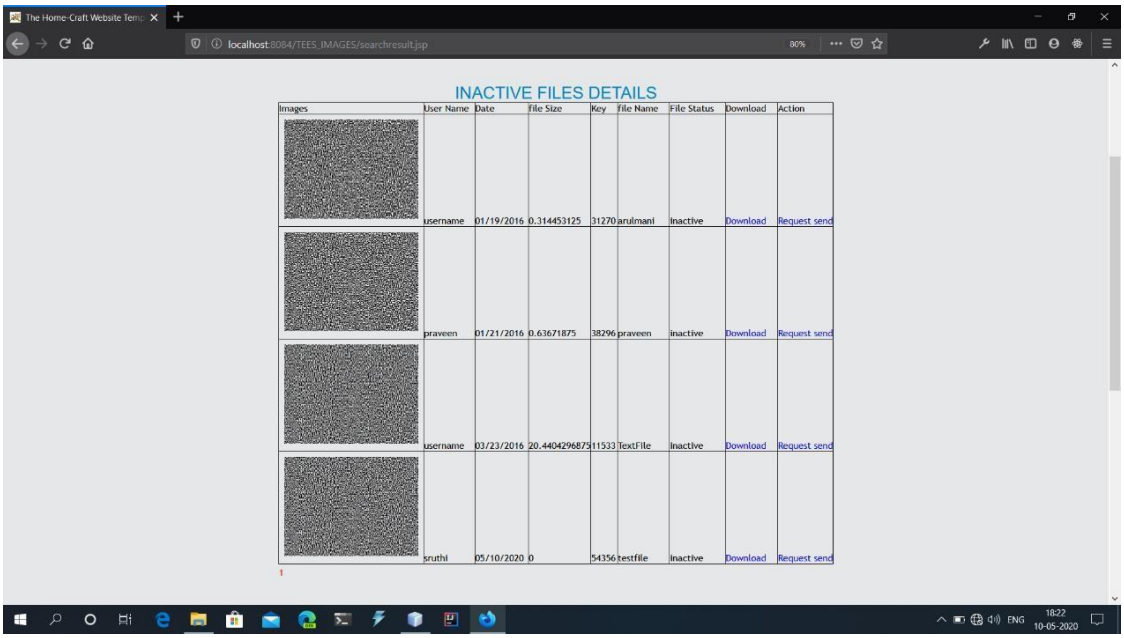
Data Owner File Request/Approve



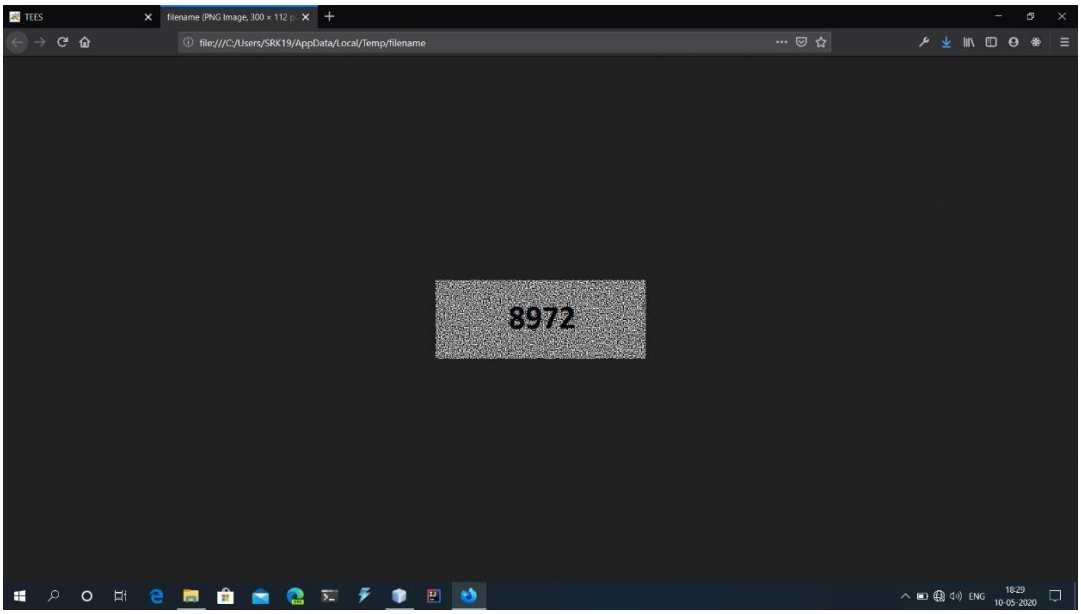
Admin File Request /Approve



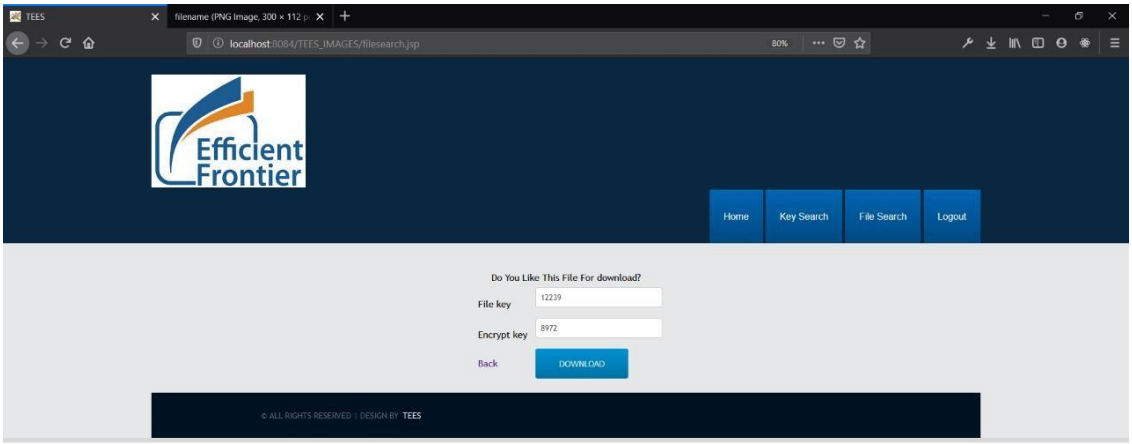
Approved files ready to be downloaded



Available files that can be requested for access



Captcha Image



Download Portal

Document Information

Analyzed document	Report content new.pdf (D70971271)
Submitted	5/12/2020 5:45:00 PM
Submitted by	Juvanna
Submitter email	ijuvanna@hindustanuniv.ac.in
Similarity	3%
Analysis address	ijuvanna.hits@analysis.urkund.com

Sources included in the report

W	URL: https://docplayer.net/4105394-Secure-storage-in-cloud-computing.html Fetched: 3/13/2020 6:05:50 AM	1
J	**Enrichment Of Security And Privacy In Cloud Over Outsourced Data** URL: a8de0ee8-2f29-4779-ab10-6fb055324757 Fetched: 3/16/2019 4:49:37 AM	2
W	URL: https://theintactone.com/2019/03/29/sad-u1-topic-6-system-development-life-cycle-i ... Fetched: 5/12/2020 5:48:00 PM	1
W	URL: https://www.ijresm.com/Vol.2_2019/Vol2_Iss3_March19/IJRESM_V2_I3_234.pdf Fetched: 3/30/2020 7:01:06 PM	2

Entire Document

1 CHAPTER 1 INTRODUCTION 1.1 Overview According to NIST

100% **MATCHING BLOCK 1/6** W https://docplayer.net/4105394-Secure-storage-i ...

Cloud computing is a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

The Cloud computing has cloud roots that can be tracked by several advanced technologies like web services, service-oriented architecture, cluster, grid, data center automation. Cloud applications are the combinations of different providers, such as Software as a service (SaaS) can provide services like e-mail, user authentication etc. The optimization of cloud is better than virtualization that it is easy to share and balance the loads across pools. There are no manual interventions needed to move or resize the resources for the applications that have built, moreover cloud provides a automatic provisioning within few hours from the requested time. Cloud infrastructure can be divided into three and that is Private, Public and Hybrid. Private cloud is preferred or most likely used by a private organization for a limited number of people thus the security is high and the data is not misused. In Public cloud, the service provided is for the general population. There is no need of initial investment and it less secure than public cloud. The Hybrid cloud is a combination of private and public cloud. Cloud Computing is emerging very quickly in this era where there are lot of big industries like Facebook, Google etc have already show cased their best. As the cloud storage is a virtual space to store data and access via network. The user doesn't have any control over the data stored in the cloud, but the cloud provider has access to all information in stored in the cloud. Here comes the data protection in role. Security of information in cloud plays a major role when all data is being stored in it. Information Security [2] is the center of the cloud computing security problems.
Data security [2] is mainly about the data confidentiality, integrity, availability.

2 CHAPTER 2 LITERATURE REVIEW 2.1 Review details Paper 1: A Secure cloud storage system [3] Storing data in cloud has become a common in these days, thus it reduces the burden of user to oversee the data. The invisible part is data protection, which is a concern. To balance this issue, they have proposed a system with two authentication level that is Time-based One Time Password (TOTP) for cloud user's verification and Automatic Blocker Protocol (ABP). By introducing these techniques no third party could access the information. Paper 2: Secure Cloud Storage using AES Encryption [4] As the resources stored in cloud are shared via internet, the user has access to the information anytime from anywhere. The security plays a curial such that the data stored by user is not misused or leaked by any third-party attack. Here comes secure cloud storage. Advanced Encryption Standard (AES) is used for high data security and keep it as a secret. The data is encrypted before it is being upload in the cloud and a Short Message Service (SMS) is implemented to avoid any unofficial access to the data. Paper 3: Efficient Cloud Storage Confidentiality to ensure Data Security [5] All most every organization store the information in cloud, where they give the data to any outsourcing agent as they get large space to store data. By out sourcing the initial investments

3 done by a small-scale industry would be less. It is important to encrypt the data before storing in cloud to avoid data misuse and privacy. Here along with encryption, obfuscation technique is also performed to find out illicit users by performing particular mathematic functions. Paper 4 : Secure Cloud Storage and File Storage [6] Many industries store their data in cloud as that gives a plenty of virtual space. Once the data is uploaded in cloud the user does not have control over the uploaded file. Disintegration protocol (DIP) is performed for a secure file sharing.

4 CHAPTER 3 PROJECT DESCRIPTION 3.1 Existing system Originally this type of systems was developed for operating systems. When the concept of multiple user operating system came, there came a need for mechanism which allowed users to create and manipulate files in this type of environment. In this type of operating system, each user doesn't get a separate environment, rather they get a common shared environment where all files created by all users are visible to all. To overcome this problem the concept of file access and file permissions came. A user creating a file becomes its owner and the operating won't allow other users to access it unless explicitly specified by the owner. These permissions are called meta data and stored along with the file and is used by operating system whenever anyone tries to open that file. over the years there were subtle changes to this mechanism such as user groups and so on as the operating system evolved. As the internet boomed, the need to share information became crucial and hence came file servers. They are internet connected computers whose purpose is to share files stored in them to whomever requested them via the

internet. First security measures were similar to computer log in passwords. people who are trying to connect to the servers need to provide a username and password and if they are valid the person will be allowed to download content from the server. the current system evolved so much, the contents are now encrypted, sessions are authenticated. databases of suspicious IP address are stored and maintained and verified against incoming requests. 3.2 Shortcomings found in existing system Although existing systems are evolved so much, the security is still not impenetrable. username and passwords can be obtained by various methods. a simple sql injection allows an attacker to view the database of the system from there he can view the username and passwords of all the users and he can log in as whomever he pleases as some accounts have higher privileges. The attacker can also skip this step and directly gain access to this system and simply copy the files off

5 as modern systems have multiple services running on the same system and not all of them are secure. sometimes a single user using an weak password or compromised some other way locally can compromise the entire server because security is implemented in the same way for all users and the attacker can study the system from inside and compromise the server to great extent. 3.3 Proposed system The proposed system consists of various mechanisms to ensure protected data access. The data storing part consists of generating a random key for every file upload, it then uses that key to encrypt it with AES. During this process a separate image is generated using that key. This key image is then split into two images and one part of it is shared/stored along with user and other with the file itself. Anyone wanting to access a particular file puts in a request. The system then updates the owner of the particular file mentioning the person wanting to access that file. If he approves the request then the system will update the user that he can access the file now. This time when he access the file, the system will retrieve both images, merge it together and show it in the form of captcha, the user then identifies the key from the image and passes it back to the system, which will use that particular key to decrypt the file and send it to the user. Since this system uses different key for every file, the chances of system compromise is greatly reduced. Also since the system by itself doesn't store the decryption keys directly and authentication is done by visual means it further reduces the chances of system compromise. 3.4 Benefits of proposed system While uploading the file is encrypted and key is separated and when an user is downloading, the encrypted file is downloaded and tried to decrypt in a sandboxed mode so that if it fails to decrypt, it will be destroyed. This ensures the security and integrity of data both in transit and idle. Since this system uses different keys for every file, the chances of system compromise is greatly reduced. Also, since the system by itself doesn't store the decryption keys directly and authentication is done by visual means it further reduces the chances of system compromise.

6 CHAPTER 4 SYSTEM REQUIREMENTS 4.1 Hardware requirements: The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It should what the system does and not how it should be implemented • Processor - Pentium –III • RAM - 4 GB • Hard Disk - 260 GB • Key Board, Mouse, Monitor 4.2 Software requirements: The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team’s progress throughout the development activity. • Operating System - Windows95/98/2000/XP • Front End - HTML, Java, Jsp • Scripts - JavaScript. • Server side Script - Java Server Pages. • Database - My Sql • Database Connectivity- JDBC

7 CHAPTER 5 SYSTEM DESIGN 5.1 Architecture Data Upload DB1 DB2 Owner Information AES (key, file) Data owner file Key Encrypted file Random Key Generator Image Image part 2 Image part 1 Owner information +image part1 Encrypted file + image part2

8 Data Retrieval DB1 DB2 File request Request information Approves Image part1 Image part2 + file send Captcha Captcha send back key AES (file, key) send to user User Image 2 Decrypted file Owner Image1 File Owner information + image part1 Encrypted files + image part2 Completes captcha Received file

9 5.2 System design description The software is implemented as web application and hence will reflect common web application pattern. An web interface for the users to interact with system. This web interface will also have a cryptographic module to encrypt and decrypt files. In the back end there will be two databases, one containing user profiles and part of meta datas needed to decrypt files of respective users, the other database containing the files and other part of meta datas. They are designed to be used asynchronously by the web application. 5.2.1 Input Design The file upload part of the application is designed as a form. It also utilizes the cryptographic part of the application to produce a unique key whenever the form is opened. The form contains fields to gather file name and file upload and a check option

to whether this file is to be stored securely or not. when the form is submitted and if the file is to be stored securely, the file is encrypted using AES using the generated random key and then an image is generated using the key and splitted into two and stored across the two databases along with the encrypted file as show in the diagram. 5.2.2 User Interface Design The user interface has been designed using web technologies such as HTML, CSS, and JSP. It has profile pages for data owners, users and admin. Data owners have various pages to manage their uploaded files, form to upload new files and requests tab to view users who want to access files of the owner, he can accept or deny in this tab. Users have following pages, index page where they can view the list of documents and request for access to them, requests pages where the view the status of all the files requested by them and a page containing form to download the allowed files. A separate page for the admin to view and approve user profiles of data owner and users and file access requests and finally profile creation pages for data owners and users. 5.2.3 Procedural Design The entire system has been designed to work asynchronously. Apart from the input/output system, the process from file request to user downloading the file works on event based. When an event occurs the response to it is executed by the system

10 5.2.4 Output Design Once the request for the file is approved by the data owner and admin. The approved information is made available to the user via his requests page. The user now has to visit the portal where the verification using captcha occurs. After successful verification the file will be downloaded. 5.3 UML diagrams 5.3.1 Use case diagram: Roles of the actors in the system can be depicted. In our use case diagram first user login into user window then if it is a valid user means then it can communicate with the cloud server.

11 5.3.2 Class diagram: In our class diagram we having the details about user, first user login into user window then if it is a valid user, then it can communicate with the cloud server. Here ranking function is involved in order to search the file in the order of ranking basis. The storage node contains the encrypted files and the user and provider has some of the particular registrations such as username andpassword.

12 5.3.3 Activity diagram: The cloud storage contains the encrypted file and files can be retrieved from the user. The cloud server contains the respective keys and later entering the correct key the files will be downloaded. After valid registration, user uploads the file and sends the file request. Similarly, provider performs the encryption and generates OPE password and admin verifies.

13 5.3.4 Sequence diagram: In the sequence diagram, user enters into the cloud by performing certain authentication and user will retrieve the files available in the server. It explains about sending a file request to the provider and requesting for a OPE password and after verification the cloud server will provide the required source image to the user.

14 5.3.5 Collaboration diagram: A collaboration diagram describes interactions among objects in terms of sequenced messages it, explains about sending a file request to the provider and requesting for a OPE password and after verification the cloud server will provide the required source image to the user.

15 5.3.6 Data flow diagram: User login into user window then if it is a valid user means then it can communicate with the cloud server. The registered users can publish and subscribe. Level 0: Level 1: Level 2:

16 Level 3: Overall:

17 5.3.7 Entity Relationship Diagram Entity-Relationship Model is an abstract and conceptual representation of data. Entity- relationship modelling is a database modelling method. It describes whether authentication between the user and server is performed correctly and the respective encrypted files and index are generated and then the image is displayed to the user.

18 CHAPTER 6 MODULES 6.1 Secure file uploading In the upload portal when the data owner uploads a file a random key is generated and the file is immediately encrypted using AES with that key. Along with this process visual cryptography takes place which is explained in detail below. By encrypting data before uploading to the server, MITM attacks (Man In The Middle) can be mitigated. An MITM attack is one where an attacker sets himself between a user and a server and all the interaction between them passes through the attacker. If the encryption occurs in the server side and if the attacker was able to obtain a copy of the data while it was being sent to the server then the entire process would be moot. Hence the file should be encrypted before sending it to the server. 6.2 Visual cryptography Visual cryptography is a technique where confidential information is injected/transformed into an image after which it is split into n parts. Any one of the n parts or even n-1 parts couldn't be used to reproduce the original information injected into the image. Only when all the n parts are combined together the secret is revealed visually. We use this technique to inject the random key generated during upload into an image and split into two parts. One is stored along with data owner, other with the uploaded file. These two will be combined when another user wants to retrieve the file to reveal the decryption key. 6.3 Storing the

uploaded files The to be uploaded files are two images, and an AES encrypted file. One image along with encrypted file is stored together on a distribution server while the other image is stored along with the data owner's records/data. These two should be using separated servers and database so that even if one of the systems gets compromised, the data remains protected. We use AES because it's implementation in software is faster and it is highly secure, qualities due to which it has become an industry standard for data protection.

19 6.4 Verification and retrieval When the user has been approved by the owner, the system will merge the images from both sources and send it in the form of captcha. The user then visually identifies the key and sends it back to the system. The system then creates a copy of that file and decrypts it, if the output is garbled (the output can be verified if garbled or not by checking the padding, for example in java BadPaddingException occurs)then it knows it's not the correct key and informs the user and the file is not retrieved. If the output is not garbled the user is given a copy of the file.

20 CHAPTER 7 SYSTEM IMPLEMENTATION 7.1 System Implementation Systems implementation is the construction of the new system and the delivery of that system into production the Construction Phase of Systems Implementation has two things: builds and tests a functional system that fulfills business or organizational design requirements, and implements the interface between the new system and the existing production system. The project team must construct the database, application programs, user and system interfaces, and networks. Some of these elements may already exist in the project or be subject to enhancement. 7.2 ALGORITHM 7.2.1 AES algorithm: AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits STEPS IN ADVANCED ENCRYPTION STANDARD : Step 1: Derive the set of round keys from the cipher key Step 2: Initialize the

Step 4: Perform nine rounds of state manipulation Step 5: Perform the tenth and final round of state manipulation Step 6:

File hashing splitting algorithm The two encryption methods used in this work for encryption use different keys. Key splitting module generates two random keys from the main key. It divides the Key bits into half i.e. if key is of length n then the generated random two keys will be of length n/2. The pseudo code for key splitting is given below: Step1: Input is n bit key Step2: Set Key1 and Key2 as n/2 bit value and initialize it to 0 Step3: Initialize the random function with given seed value. 323 Step4: Initialize length as n, i=0, j=0, flag=0. Step5: While (length != 0) 5.1: If Flag==0 then Find a bit position randomly that has not been used. Find out the value at that bit position in main key. If value at that bit position is 1 then Set the i'th bit of key1 as 1 and Increment i value else Set the i'th bit of key1 as 0 and Increment i value Set Flag=1, Set the above found bit position is used. Go to Step 5.3 5.2: Else Find a bit position randomly that has not been used. Find out the value at that bit position in main key.

22 If value at that bit position is 1 then Set the i'th bit of key2 as 1 and Increment j value else Set the i'th bit of key2 as 0 and Increment j value Set Flag=0, Set the above found bit position is used. Go to Step 5.3 5.3: Decrement the Length; 5.4: Go to step 5 Step6: Return the keys key1 and key2 of size n/2.

23 CHAPTER 8 SYSTEM TESTING 8.1 Software testing Software testing is the process used to help identify the correctness, completeness, security and quality of developed computer software.

a critical element of software quality assurance and represents the ultimate review of specification, design and coding. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of developed system using various kinds of data. There are many approaches to software testing, but effective testing of complex products is essentially a process of investigation, not merely a matter of creating and following rote procedure. One definition of testing is the “the process of questioning a product in order to evaluate it”, where the” questions” are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. The quality of the application can, and normally does, vary widely from system too system but some of the common quality attributes include reliability, stability, portability, maintainability and usability. 8.2 Testing objectives A number of rules that can serve well as testing objectives: • 1. Testing is a process of executing a program with the intent of finding an error. • 2. A good test case is one that has a high probability of finding an as-yet undiscovered error. • 3. A successful test is one that uncovers an as-yet-undiscovered error. These objectives imply a dramatic change in viewpoint. They move counter to the commonly held view

24 that:- a successful test is one in which no errors are found. Our objective is to design tests that systematically uncover different classes of errors and to do so with a minimum amount of time and effort. If testing is conducted successfully according to the objectives stated previously it will uncover errors in the software. As a secondary benefit, testing demonstrates that software functions appear to be working according to specification, that behavioral and performance requirements appear to have been met. In addition, data collected as testing is conducted provide a good indication of software reliability and some indication of software quality as a whole. But testing cannot show the absence of errors and defects, it can show only that software errors and defects are present. It is important to keep this statement in mind as testing is being conducted. 8.3 Test plan A test plan can be defined as a document describing the scope, approach, resources, and schedule of intended testing activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. A test plan documents the strategy that will be used to verify and ensure that a product or system meets its design specifications and other requirements. A test plan is usually prepared by or with significant input from test engineers. Depending on the product and the responsibility of the organization to which the test plan applies, a test plan may include a strategy for one or more of the following: • Design Verification or Compliance test - to be performed during the development or approval stages of the product, typically on a small sample of units. • Manufacturing or Production test - to be performed during preparation or assembly of the product in an ongoing manner for purposes of performance verification and quality control. • Acceptance or Commissioning test - to be performed at the time of delivery or installation of the product. • Service and Repair test - to be performed as required over the service life of the product.

Test engineer

25 • Regression test - to be performed on an existing operational product, to verify that existing functionality didn't get broken when other aspects of the environment are changed (e.g., upgrading the platform on which an existing application runs). A complex system may have a high-level test plan to address the overall requirements and supporting test plans to address the design details of subsystems and components. Test plan document formats can be as varied as the products and organizations to which they apply. There are three major elements that should be described in the test plan: Test Coverage, Test Methods, and Test Responsibilities. These are also used in a formal test strategy.

Test strategy

26 CHAPTER 9 CONCLUSION Thus we have created a web application using JSP which functions as a file server which focuses on the security and safety of the data much more rigorously.Things such as profile approval by the admin and file requests approval by both admin and data owner increases security and helps remove possible security threats at a higher level (such as unwanted person even accessing the download portal). On a lower level using random key to encrypt file ensures that every file is encrypted using separate key and if the attacker manages to get access to a particular key only that file be affected leaving the rest of them secure (however the security checks at higher level will deter this). Next by using two different databases and by splitting data between those and making the decryption of file dependant on data in both databases, the security is enhanced significantly. Because even if the attackers gain access to one database the data available there will be useless without the data from the other database, and since each file is encrypted using different keys, security is compounded. By using visual cues to obtain decryption keys and the key never stored in any other form or made available to the system to be managed by the system scripts from the attacker will be useless. The only possible way for an script to decrypt the file (assuming the script has access to file for repeated processing) will be by brute forcing which will take even supercomputers hundreds of years which is not feasible

27 REFERENCES [1]

pp. 800-145. [2] Xiaojun Yu, Qiaoyan Wen, ”A View about Cloud Data Security from Data Life Cycle”, International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, Dec 2010, pp 1-4. [3] Sangamesh, S. M., and S. S. Joshi. "A Survey on: A Secure Cloud Storage System: An Approach." [4]

IEEE, 2016. [5] Arockiam, L., and S. Monikandan. "Efficient cloud storage confidentiality to ensure data security." 2014 International Conference on Computer Communication and Informatics. IEEE, 2014. [6] Rawal, Bharat S., and S. Sree Vivek. "Secure cloud storage and file sharing." 2017 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2017. [7] Q. Chai and G. Gong, “Verifiable symmetric searchable encryption for semi-honest-but- curious cloud servers,” in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922. [8] Ali, Fairouz Sher, and Songfeng Lu. "Searchable encryption with conjunctive field free keyword search scheme." 2016 International Conference on Network and Information Systems for Computers (ICNISC). IEEE, 2016. [9] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, “Privacy preserving multiple keyword search for confidential investigation of remote forensics,” in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE, 2011, pp. 595–599.

28 APPENDIX SAMPLE CODE Encryption: import java.security.InvalidAlgorithmParameterException; import java.security.InvalidKeyException; import java.security.NoSuchAlgorithmException; import java.util.logging.Level; import java.util.logging.Logger; import javax.crypto.BadPaddingException; import javax.crypto.Cipher; import javax.crypto.IllegalBlockSizeException; import javax.crypto.KeyGenerator; import javax.crypto.NoSuchPaddingException; import javax.crypto.SecretKey; import sun.misc.BASE64Encoder; public class Encryption { public String Encryption1(String value) throws InvalidKeyException, IllegalBlockSizeException, BadPaddingException { String Encry="";

29 try { String plainData=value,decryptedText; KeyGenerator keyGen = KeyGenerator.getInstance("AES"); keyGen.init(128); SecretKey secretKey = keyGen.generateKey(); Cipher aesCipher=null; try { aesCipher = Cipher.getInstance("AES"); } catch (NoSuchPaddingException ex) { Logger.getLogger(Encryption.class.getName()).log(Level.SEVERE, null, ex); } aesCipher.init(Cipher.ENCRYPT_MODE,secretKey); byte[] byteDataToEncrypt = plainData.getBytes(); byte[] byteCipherText = aesCipher.doFinal(byteDataToEncrypt); Encry = new BASE64Encoder().encode(byteCipherText); try { aesCipher.init(Cipher.DECRYPT_MODE,secretKey,aesCipher.getParameters()); } catch (InvalidAlgorithmParameterException ex) { }

30 byte[] byteDecryptedText = aesCipher.doFinal(byteCipherText); decryptedText = new String(byteDecryptedText); System.out.println("\n Plain Data : "+plainData+" \n Cipher Data : "+Encry+" \n Decrypted Data : "+decryptedText); } catch (NoSuchAlgorithmException ex) { Logger.getLogger(Encryption.class.getName()).log(Level.SEVERE, null, ex); } return Encry; } } } } return ""; } }

31 SAMPLE SCREENSHOTS Home Page Owner Registration

32 User Registration File Upload

33 Data Owner File Request/Approve Admin File Request /Approve

34 Approved files ready to be downloaded Available files that can be requested for access

35 Captcha Image Download Portal

Hit and source - focused comparison, Side by Side

Submitted text As student entered the text in the submitted document.

Matching text As the text appears in the source.

1/6	SUBMITTED TEXT	42 WORDS	100%	MATCHING TEXT	42 WORDS

Cloud computing is a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

W https://docplayer.net/4105394-Secure-storage-in-cloud-computing.html

2/6	SUBMITTED TEXT	21 WORDS	70%	MATCHING TEXT	21 WORDS

state array with the block data Step 3: Add the initial round key to the starting state array

state array with the block data content (plaintext). ? Attach the initial round key to the initial state array. ?

J a8de0ee8-2f29-4779-ab10-6fb055324757

3/6	SUBMITTED TEXT	19 WORDS	100%	MATCHING TEXT	19 WORDS

Copy the final state array out as the encrypted data 21 7.2.2

Copy the final state array out as the encrypted data (

J a8de0ee8-2f29-4779-ab10-6fb055324757

4/6	SUBMITTED TEXT	34 WORDS	93%	MATCHING TEXT	34 WORDS

Testing is vital to the success of the system. System Testing makes logical assumption that if all the parts of the system are correct, the goal will be successfully achieved. System Testing is

Testing is vital to the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, the goal will be successfully achieved. Another reason for system testing is

W https://theintactone.com/2019/03/29/sad-u1-topic-6-system-development-life-cycle-implementation-p ...

5/6	SUBMITTED TEXT	25 WORDS	98% MATCHING TEXT	25 WORDS

P. Mell, Grance, “The NIST definition of cloud computing”, Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011,

P. Mell, Grance, “The NIST definition of cloud computing”, Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication, pp.800-145; Sep.2011. [12]

W https://www.ijresm.com/Vol.2_2019/Vol2_Iss3_March19/IJRESM_V2_I3_234.pdf

6/6	SUBMITTED TEXT	25 WORDS	84% MATCHING TEXT	25 WORDS

Babitha, M. P., and KR Remesh Babu. "Secure cloud storage using AES encryption." 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT).

Babitha M.P. and K. R. R. Babu, "Secure cloud storage using AES encryption," International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT),

W https://www.ijresm.com/Vol.2_2019/Vol2_Iss3_March19/IJRESM_V2_I3_234.pdf

A Protected File Access Mechanism using Visual Cryptography

S. Rajkumar
Department of Information Technology
Hindustan Institute of Technology and Science Chennai,India
srk1998007@gmail.com

B.V Baiju
Assistant Professor
Department of Information Technology
Hindustan Institute of Technology and Science Chennai,India
bvbaiju@hindustanuniv.ac.in

Sruthi Chandrasekaran
Department of Information Technology
Hindustan Institute of Technology and Science Chennai,India
chandrasekarsruthi123@gmail.com

***Abstract*— In this era Cloud Computing has been used widely to bring more distributed data and resources together. The client can easily access the information from anywhere via internet at any time. As many data is introduced in each day, the insurance of information protection, delicate information typically needs to be scrambled before redistributing, which makes compelling information usage a difficult assignment. Here comes the need of client to protect the data that they store and accessing it wisely. The proposed system uses Advanced Encryption System (AES) for secure file uploading. Cloud provider upload the user file with secured image, that image should be splitting into two images like source and key image by using BVCS (Binocular Visual Cryptography schemes algorithm. Then, the key image and the password will be sent to the particular user and the necessary file can then be downloaded. The password is generated which is then splited into source image and key image and they are stored to the user and cloud server. Now the user has to send the key image to the cloud for accessing the files. The cloud matches the key image with the source image it already has. When both matches the file can be downloaded.**

I. INTRODUCTION

According to NIST Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].The Cloud computing has cloud roots that can be tracked by several advanced technologies like web services, service-oriented architecture, cluster, grid, data center automation. Cloud applications are combinations of various technologies. Software as A Service (SAAS) is one such type of cloud application where multiple internet technologies are used to create an application which runs on the internet and is consumed through the internet. The cloud is based on multi-tenant policy, a vast amount of computing resources using virtualization technologies has been shared/leased to cloud users in the form of virtual Machines. These virtual machines although accessible only by that particular cloud user doesn't have a dedicated isolated hardware. Since the underlying hardware is shared among all users of the cloud, a breach from a single virtual machine can affect the entire infrastructure. Cloud providers have basic cloud user identification and authorization security policies and mechanisms in place; however, these are not failsafe and may not be ergonomic to all cloud users. Hence cloud providers came up with different cloud deployment models to accommodate various cloud users with varying levels of security mechanisms. There are three main cloud deployment models - private cloud, public cloud and hybrid cloud. A public cloud is where the cloud is made available to everyone. Here the security mechanisms are implemented in such a way that it is cost effective and not too tedious for a typical cloud user. The security measures implemented by a public cloud will always be less effective than the security measures implemented by the private cloud. The private cloud on the other hand incorporates state of the art security mechanisms which requires additional resources and mechanisms which will incur high costs. Private clouds are mostly used by organizations internally. Hybrid clouds are a combination of both private and public cloud where an organization can choose to use private part of the cloud to protect mission critical data while using public part of the cloud to reduce operational costs. Although the cloud provider has various security mechanisms in play, It's the responsible usage by the cloud user who understands the security implications will be the most effective. Hence came branches of computer security called information security and data security which focuses on the effective way of handling data respective to its security. Data security is the prevention of unauthorized access, use, disruption, modification or destruction of data in storage and a subset of information security. Information security on the other hand is a broader practice that encompasses security mechanisms to an end to end information flow. In this paper we propose a data-flow keeping information security and data security in mind for a typical data server.

II. RELATED WORKS

A. A Secure cloud storage system

[3] Storing data in cloud has become a common in these days, thus it reduces the burden of user to oversee the data. The invisible part is data protection, which is a concern. To balance this issue, they have proposed a system with two authentication level that is Time-based One Time Password (TOTP) for cloud user's verification and Automatic Blocker Protocol (ABP). By introducing these techniques no third party could access the information.

B. Secure Cloud Storage using AES Encryption

[4] As the resources stored in cloud are shared via internet, the user has access to the information anytime from anywhere. The security plays a curial such that the data stored by user is not misused or leaked by any third-party attack. Here comes secure cloud storage. Advanced Encryption Standard (AES) is used for high data security and keep it as a secret. The data is encrypted before it is being upload in the

cloud and a Short Message Service (SMS) is implemented to avoid any unofficial access to the data.

C. Efficient Cloud Storage Confidentiality to ensure Data Security

[5] All most every organization store the information in cloud, where they give the data to any outsourcing agent as they get large space to store data. By out sourcing the initial investments done by a small-scale industry would be less. It is important to encrypt the data before storing in cloud to avoid data misuse and privacy. Here along with encryption, obfuscation technique is also performed to find out illicit users by performing particular mathematic functions.

D. Secure Cloud Storage and File Storage

[6] Many industries store their data in cloud as that gives a plenty of virtual space. Once the data is uploaded in cloud the user does not have control over the uploaded file. Disintegration protocol (DIP) is performed for a secure file sharing.

III. METHODOLOGY

The proposed system consists of various mechanisms to ensure protected data access. The data storing part consists of generating a random key for every file upload, it then uses that key to encrypt it with AES. During this process a separate image is generated using that key. This key image is then split into two images and one part of it is shared/stored along with user and other with the file itself. Anyone wanting to access a particular file puts in a request. The system then updates the owner of the particular file mentioning the person wanting to access that file. If he approves the request then the system will update the user that he can access the file now. This time when he access the file, the system will retrieve both images, merge it together and show it in the form of captcha, the user then identifies the key from the image and passes it back to the system, which will use that particular key to decrypt the file and send it to the user. Since this system uses different key for every file, the chances of system compromise are greatly reduced. Also, since the system by itself doesn't store the decryption keys directly and authentication is done by visual means it further reduces the chances of system compromise.

MODULES

A. SECURE FILE UPLOADING

B. VISUAL CRYPTOGRAPHY

C. STORING THE UPLOADED FILES

D. VERIFICATION AND RETRIEVAL

A. Secure File Upload

In Fig. 1in the upload portal when the data owner uploads a file a random key is generated and the file is immediately encrypted using AES with that key. Along with this process visual cryptography takes place which is explained in detail below. By encrypting data before uploading to the server, MITM attacks (Man in The Middle) can be mitigated. An MITM attack is one where an attacker sets himself between a user and a server and all the interaction between them passes through the attacker. If the encryption occurs in the server side and if the attacker was able to obtain a copy of the data while it was being sent to the server then the entire process would be moot. Hence the file should be encrypted before sending it to the server.

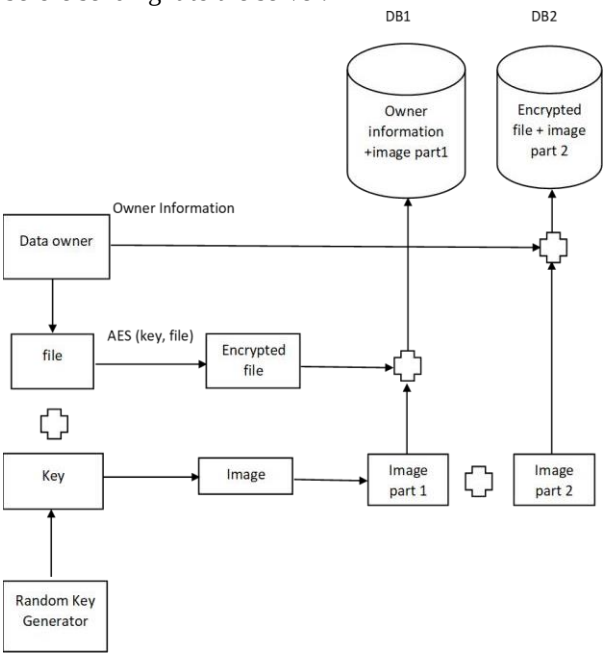


Fig1: Data Upload

B. Visual Cryptography

Visual cryptography is a technique where confidential information is injected/transformed into an image after which it is split into n parts. Any one of the n parts or even n-1 parts couldn't be used to reproduce the original information injected into the image. Only when all the n parts are combined together the secret is revealed visually. We use this technique to inject the random key generated during upload into an image and split into two parts. One is stored along with data owner, other with the uploaded file. These two will be combined when another user wants to retrieve the file to reveal the decryption key.

C. Storing the uploaded files

The to be uploaded files are two images, and an AES encrypted file. One image along with encrypted file is stored together on a distribution server while the other image is stored along with the data owner's records/data. These two should be using separated servers and database so that even if one of the systems gets compromised, the data remains protected. We use AES because it's implementation in software is faster and it is highly secure, qualities due to which it has become an industry standard for data protection.

D. verification and Retrieval

In Fig. 2 when the user has been approved by the owner, the system will merge the images from both sources and send it in the form of captcha. The user then visually identifies the key and sends it back to the system. The system then creates a copy of that file and decrypts it, if the output is garbled (the output can be verified if garbled or not by checking the padding, for example in java BadPaddingException occurs)then it knows it's not the correct key and informs the user and the file is not retrieved. If the output is not garbled the user is given a copy of the file.

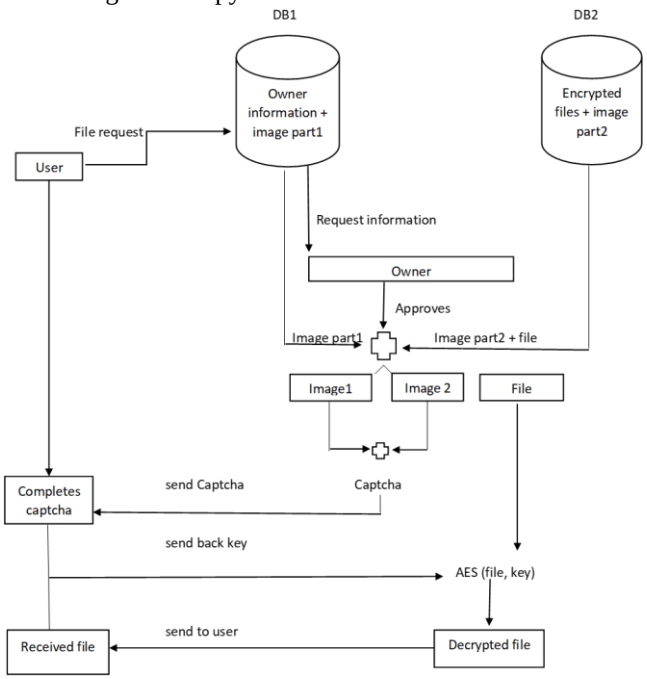


Fig. 2 Data Retrieval

IV CONCLUSION AND FUTURE WORK

In this paper we've have proposed a controlled file access Mechanism using visual cryptography. By splitting keys and storing it separately and never actually storing these keys directly decreases the attack surface significantly. Also, by having different keys for different files, the chances of entire system compromise from a single file is also reduced. Also, by using visual means to authenticate, the checkpoint of "prove you are not a robot" is implied. There are lot of future possibilities, one of which is: having user groups where files being accessed by someone who is in the same user group as owner need not wait for his/her approval and can immediately continue with the process, while someone outside the group undergoes the regular scrutiny.

REFERENCES

[1] P. Mell, Grance, "The NIST definition of cloud computing", Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011, pp. 800-145.

[2] Xiaojun Yu, Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle", International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, Dec 2010, pp 1-4.

[3] Sangamesh, S. M., and S. S. Joshi. "A Survey on: A Secure Cloud Storage System: An Approach."

[4] Babitha, M. P., and KR Remesh Babu. "Secure cloud storage using AES encryption." 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT). IEEE, 2016.

[5] Arockiam, L., and S. Monikandan. "Efficient cloud storage confidentiality to ensure data security." 2014 International Conference on Computer Communication and Informatics. IEEE, 2014.

[6] Rawal, Bharat S., and S. Sree Vivek. "Secure cloud storage and file sharing." 2017 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2017.

[7] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922.

[8] Ali, Fairouz Sher, and Songfeng Lu. "Searchable encryption with conjunctive field free keyword search scheme." 2016 International Conference on Network and Information Systems for Computers (ICNISC). IEEE, 2016.

[9] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy preserving multiple keyword search for confidential investigation of remote forensics," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE, 2011, pp. 595–599.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[11] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE.

[12] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[13] X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[14] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[15] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[16] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[17] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

Document Information

Analyzed document	Sruthi Raj Kumar Batch 4 3 2020 Edited paper new.docx (D64810131)
Submitted	3/4/2020 7:29:00 AM
Submitted by	Juvanna
Submitter email	ijuvanna@hindustanuniv.ac.in
Similarity	16%
Analysis address	ijuvanna.hits@analysis.urkund.com

Sources included in the report

W	URL: https://www.infotech.co.uk/understanding-technology/cloud-computing Fetched: 3/4/2020 7:31:00 AM	1
W	URL: https://www.ijert.org/a-survey-on-a-secure-cloud-storage-system-an-approach Fetched: 3/4/2020 7:31:00 AM	2
W	URL: https://www.ijarcs.info/index.php/Ijarcs/article/download/3966/3628 Fetched: 3/4/2020 7:31:00 AM	1
W	URL: https://www.ripublication.com/ijcir17/ijcirv13n5_55.pdf Fetched: 9/27/2019 7:10:16 PM	1
J	**Enrichment Of Security And Privacy In Cloud Over Outsourced Data** URL: a8de0ee8-2f29-4779-ab10-6fb055324757 Fetched: 3/16/2019 4:49:37 AM	1
W	URL: https://www.ijcseonline.org/pub_paper/299-IJCSE-07322-25.pdf Fetched: 10/5/2019 2:40:33 PM	1
W	URL: https://ijarcce.com/wp-content/uploads/2016/10/IJARCCE-88.pdf Fetched: 10/23/2019 9:43:24 AM	1

Entire Document

A Protected File Access Mechanism using Visual Cryptography Dr. S. Sivakumar Professor Department of Information Technology Hindustan Institute of Technology and Science Chennai,India ssivakumar@hindustanuniv.ac.in S. Rajkumar Department of Information Technology Hindustan Institute of Technology and Science Chennai,India srk1998007@gmail.com Sruthi Chandrasekaran Department of Information Technology Hindustan Institute of Technology and Science Chennai,India chandrasekarsruthi123@gmail.com

Abstract— In this era Cloud Computing has been used widely to bring more distributed data and resources together. The client can easily access the information from anywhere via internet at any time. As many data is introduced in each day, the insurance of information protection, delicate information typically needs to be scrambled before redistributing, which makes compelling information usage a difficult assignment. Here comes the need of client to protect the data that they store and accessing it wisely. The proposed system uses Advanced Encryption System (AES) for secure file uploading. Cloud provider upload the user file with secured image, that image should be splitting into two images like source and key image by using BVCS (Binocular Visual Cryptography schemes algorithm. Then, the key image and the password will be sent to the particular user and the necessary file can then be downloaded. The password is generated which is then splited into source image and key image and they are stored to the user and cloud server. Now the user has to send the key image to the cloud for accessing the files. The cloud matches the key image with the source image it already has. When both matches the file can be downloaded.

I. Introduction

According to

95%	MATCHING BLOCK 1/8	W	https://www.infotech.co.uk/understanding-techn ...

NIST Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

The

Cloud computing has cloud roots that can be tracked by several advanced technologies like web services, service-oriented architecture, cluster, grid, data center automation. Cloud applications are the combinations of different providers, such as Software as a service (SaaS) can provide services like e-mail, user authentication etc. The optimization of cloud is better than virtualization that it is easy to share and balance the loads across pools. There are no manual interventions needed to move or resize the resources for the applications that have built, moreover cloud provides a automatic provisioning within few hours from the requested time. Cloud infrastructure can be divided into three and that is Private, Public and Hybrid. Private cloud is preferred or most likely used by a private organization for a limited number of people thus the security is high and the data is not misused. In Public cloud, the service provided is for the general population. There is no need of initial investment and it less secure than public cloud. The Hybrid cloud is a combination of private and public cloud. Cloud Computing is emerging very quickly in this era where there are lot of big industries like Facebook, Google etc have already show cased their best. As the cloud storage is a virtual space to store data and access via network. The user doesn't have any control over the data stored in the cloud, but the cloud provider has access to all information in stored in the cloud. Here comes the data protection in role. Security of information in cloud plays a major role when all data is being stored in it. Information Security [2] is the center of the cloud computing security problems.
Data security [2] is mainly about the data confidentiality, integrity, availability. The proposed system consists of various mechanisms to ensure protected data access. The data storing part consists of generating a random key for every file upload, it then uses that key to encrypt it with AES. During this process a separate image is generated using that key. This key image is then split into two images and one part of it is shared/stored along with user and other with the file itself. Anyone wanting to access a particular file puts in a request. The system then updates the owner of the particular file mentioning the person wanting to access that file. If he approves the request then the system will update the user that he can access the file now. This time when he access the file, the system will retrieve both images, merge it together and show it in the form of captcha, the user then identifies the key from the image and passes it back to the system, which will use that particular key to decrypt the file and send it to the user. Since this system uses different key for every file, the

chances of system compromise is greatly reduced. Also since the system by itself doesn't store the decryption keys directly and authentication is done by visual means it further reduces the chances of system compromise

II. RELATED WORKS

A. A Secure cloud storage system [3] Storing data in cloud has become a common in these days, thus it reduces the burden of user to oversee the data. The invisible part is data protection, which is a concern. To balance this issue, they have proposed a system with two authentication level that is

By introducing these techniques no third party could access the information.

B. Secure Cloud Storage using AES Encryption [4] As the resources stored in cloud are shared via internet, the user has access to the information anytime from anywhere. The security plays a curial such that the data stored by user is not misused or leaked by any third-party attack. Here comes secure cloud storage. Advanced Encryption Standard (AES) is used for high data security and keep it as a secret. The data is encrypted before it is being upload in the cloud and a Short Message Service (SMS) is implemented to avoid any unofficial access to the data.

C. Efficient Cloud Storage Confidentiality to ensure Data Security [5] All most every organization store the information in cloud, where they give the data to any outsourcing agent as they get large space to store data. By out sourcing the initial investments done by a small-scale industry would be less. It is important to encrypt the data before storing in cloud to avoid data misuse and privacy. Here along with encryption, obfuscation technique is also performed to find out illicit users by performing particular mathematic functions.

D. Secure Cloud Storage and File Storage [6] Many industries store their data in cloud as that gives a plenty of virtual space. Once the data is uploaded in cloud the user does not have control over the uploaded file. Disintegration protocol (DIP) is performed for a secure file sharing.

III. METHODOLOGY

Fig1: Flow of operation for the proposed system

MODULES Secure File Uploading Visual Cryptography Storing the uploaded files Verification and retrieval

A. Secure File Upload In the upload portal when the data owner uploads a file a random key is generated and the file is immediately encrypted using AES with that key. Along with this process visual cryptography takes place which is explained in detail below. By encrypting data before uploading to the server, MITM attacks (Man In The Middle) can be mitigated. An MITM attack is one where an attacker sets himself between a user and a server and all the interaction between them passes through the attacker. If the encryption occurs in the server side and if the attacker was able to obtain a copy of the data while it was being sent to the server then the entire process would be moot. Hence the file should be encrypted before sending it to the server.

B. Visual Cryptography Visual cryptography is a technique where confidential information is injected/transformed into an image after which it is split into n parts. Any one of the n parts or even n-1 parts couldn't be used to reproduce the original information injected into the image. Only when all the n parts are combined together the secret is revealed visually. We use this technique to inject the random key generated during upload into an image and split into two parts. One is stored along with data owner, other with the uploaded file. These two will be combined when another user wants to retrieve the file to reveal the decryption key.

C. Storing the uploaded files The to be uploaded files are two images, and an AES encrypted file. One image along with encrypted file is stored together on a distribution server while the other image is stored along with the data owner's records/data. These two should be using separated servers and database so that even if one of the systems gets compromised , the data remains protected. We use AES because it's implementation in software is faster and it is highly secure, qualities due to which it has become an industry standard for data protection.

D. verification and Retrieval When the user has been approved by the owner, the system will merge the images from both sources and send it in the form of captcha. The user then visually identifies the key and sends it back to the system. The

system then creates a copy of that file and decrypts it, if the output is garbled (the output can be verified if garbled or not by checking the padding, for example in java BadPaddingException occurs)then it knows it's not the correct key and informs the user and the file is not retrieved. If the output is not garbled the user is given a copy of the file.

IV CONCLUSION and future work In this paper we've have proposed a controlled file access Mechanism using visual cryptography. By splitting keys and storing it separately and never actually storing these keys directly decreases the attack surface significantly. Also, by having different keys for different files, the chances of entire system compromise from a single file is also reduced. Also, by using visual means to authenticate, the checkpoint of "prove you are not a robot" is implied. There are lot of future possibilities, one of which is: having user groups where files being accessed by someone who is in the same user group as owner need not wait for his/her approval and can immediately continue with the process, while someone outside the group undergoes the regular scrutiny.

References

[1] P. Mell, Grance, "The NIST definition of cloud computing", Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011, pp. 800-145. [2] Xiaojun Yu, Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle", International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, Dec 2010, pp 1-4. [3]

International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT).

IEEE, 2016. [5] Arockiam, L., and S. Monikandan. "Efficient cloud storage confidentiality to ensure data security." 2014 International Conference on Computer Communication and Informatics. IEEE, 2014. [6] Rawal, Bharat S., and S. Sree Vivek. "Secure cloud storage and file sharing." 2017 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2017. [7] Q. Chai and G.

IEEE, 2012, pp. 917– 922. [8] Ali, Fairouz Sher, and Songfeng Lu. "Searchable encryption with conjunctive field free keyword search scheme." 2016 International Conference on Network and Information Systems for Computers (ICNISC). IEEE, 2016. [9] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy preserving multiple keyword search for confidential investigation of remote forensics," in Multimedia Information Networking and Security (MINES), 2011 Third

International Conference on.

IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014. [11]

88% MATCHING BLOCK 7/8 W https://www.ijcseonline.org/pub_paper/299-IJCS ...

B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE. [12]

99% MATCHING BLOCK 8/8 W https://ijarcce.com/wp-content/uploads/2016/10 ...

L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008. [13] X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263. [14] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011. [15] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653. [16] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35. [17] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

Hit and source - focused comparison, Side by Side

Submitted text As student entered the text in the submitted document.

Matching text As the text appears in the source.

1/8	SUBMITTED TEXT	43 WORDS	95%	MATCHING TEXT	43 WORDS

NIST Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

NIST) cloud computing   a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

W https://www.infotech.co.uk/understanding-technology/cloud-computing

2/8	SUBMITTED TEXT	15 WORDS	81%	MATCHING TEXT	15 WORDS

Time-based One Time Password (TOTP) for cloud user’s verification and Automatic Blocker Protocol (ABP).

Time-based One Time Password (TOTP) for cloud   users verification and Automatic Blocker Protocol (ABP)

W https://www.ijert.org/a-survey-on-a-secure-cloud-storage-system-an-approach

3/8	SUBMITTED TEXT	19 WORDS	91%	MATCHING TEXT	19 WORDS

Sangamesh, S. M., and S. S. Joshi. "A Survey on: A Secure Cloud Storage System: An Approach." [4]

Sangamesh S M,   S S Joshi, 2018, A Survey on: A Secure Cloud Storage System: An Approach,

W https://www.ijert.org/a-survey-on-a-secure-cloud-storage-system-an-approach

4/8	SUBMITTED TEXT	15 WORDS	84%	MATCHING TEXT	15 WORDS

Babitha, M. P., and KR Remesh Babu. "Secure cloud storage using AES encryption." 2016

Babitha.M.P and K.R. Remesh Babu, "Secure Cloud Storage Using AES Encryption,"

W https://www.ijarcs.info/index.php/Ijarcs/article/download/3966/3628

5/8	SUBMITTED TEXT	18 WORDS	78% MATCHING TEXT	18 WORDS

Gong, “Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,” in Communications (ICC), 2012 IEEE International Conference on.

Gong G. : “Verifiable Symmetric Searchable Encryption for Semi- Honest-but-Curious Cloud Servers” in the proceedings of IEEE International Conference on

W https://www.ripublication.com/ijcir17/ijcirv13n5_55.pdf

6/8	SUBMITTED TEXT	30 WORDS	88% MATCHING TEXT	30 WORDS

IEEE, 2011, pp. 595–599. [10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” Parallel and Distributed Systems,

IEEE INFOCOM, 25 (2011), 829-837. 79. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud IEEE Transactions Parallel and Distributed Systems, 25 (2014), 222-233. 80.

J a8de0ee8-2f29-4779-ab10-6fb055324757

7/8	SUBMITTED TEXT	28 WORDS	88% MATCHING TEXT	28 WORDS

B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in INFOCOM, 2014 Proceedings IEEE. [12]

B. Wang, S. Yu, W. Lou, and Y. T. Hou, —Privacy-preserving   multikeyword fuzzy search over encrypted data in the cloud,‖ in INFOCOM, 2014 Proceedings IEEE.

W https://www.ijcseonline.org/pub_paper/299-IJCSE-07322-25.pdf

URKUND

8/8	SUBMITTED TEXT	180 WORDS	99%	MATCHING TEXT	180 WORDS

L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008. [13] X. Yu and Q. Wen, “Design of security solution to mobile cloud storage,” in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263. [14] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011. [15] O. Mazhelis, G. Fazekas, and P. Tyrvainen, “Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage,” in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653. [16] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized in-cloud security services for mobile devices,” in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35. [17] J. Oberheide and F. Jahanian, “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008. [2] Yu and Q. Wen, “Design of security solution to mobile cloud storage,” in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263. [3] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011. [4] O. Mazhelis, G. Fazekas, and P. Tyrvainen, “Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage,” in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653. [5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized in-cloud security services for mobile devices,” in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35. [6] J. Oberheide and F. Jahanian, “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48. [7]

W https://ijarcce.com/wp-content/uploads/2016/10/IJARCCE-88.pdf

ICSIE 2020

Organized by **JAWAHAR ENGINEERING COLLEGE**

Venue - JAWAHAR ENGINEERING COLLEGE, Near AVM studio, Saligramam, Chennai- 93

PAPER ID – ICSIE20164

CONFERENCE ATTENDANCE:

Will you attend the conference (**YES/NO**)?

1. If No, give reason— Due to pandemic we cannot attend the conference and our team members are situated in different places. There are some network issues in the situated areas so we are choosing to submit through PPT document.

(INABSENTIA)

CHOOSE ANY ONE TYPE

SKYPE

SKYPE ID --_____

(OR)

PPT DOCUMENT (OFFLINE)

(NOTE- PPT SHOULD SEND ALONG REGISTRATION DETAILS)

2. If Yes, how many will attend—

NOTE – CERTIFICATES WILL BE *SEND* TO INABSENTIA AUTHORS THROUGH MAIL OR COURIER WITHIN 48 HOURS AFTER CONFERENCE

Declaration & Copyright transfer form for ICSIE 2020 TO BE SIGNED BY AUTHORS I/We, the undersigned author(s) of the manuscript entitled

_____

_____

_____

_____

I hereby declare that (a) the above manuscript which is submitted for publication in the ICSIE 2020 is not under consideration elsewhere. (b) The manuscript is not published already in part or whole (except in the form of abstract) in any journal or magazine for private or public circulation. The work described in the manuscript is my/our own and my/our individual contribution to this work is significant enough to qualify authorship. (c) No one who has contributed significantly to the work has been denied authorship and those who helped have been duly acknowledged. (d) Free journal category for publication will be considered only if the article meets the journal requirement. (e) Indexing of articles will be sole responsible of respective author/s once published (f) All conference & Journal payment received are inclusive of tax, any refund once paid will be refunded with tax deduction. (g) Paper can be rejected if it doesn't meet the journal standard or not in scope. (h) I/we also agree to the authorship of the article in the following sequence:

Authors Name(s) 1. _____

2. _____

3. _____

4. _____

5._____

NOTE: 1.Authors is required to sign this form. Signature (s) _____

_____ _____ _____

2. No addition, deletion or change in the sequence of authors is allowed at the later stage without valid reasons.

CONFERENCE FEE

CHOOSE YOUR CATEGORY:

Note: **Tick mark** your category (CHOOSE ANY ONE)

Category 1 – UG/PG student / Faculty/Research scholar/Industry Participant (Individual Participant - **1 certificate only**)
(Conference Fee- **2000** INR) ☐

Category 2- UG/PG students (**Group of 2 or 6 members – 2 or 6 certificates**)
(Combination of Student/Faculty/Research Scholar/Industry Participant)
(Conference Fee - **2950** INR) ☑

3. **PAYMENT DETAILS**:

- CONFERENCE PAYMENT ALONE to be paid to the below account.

Payment mode (INTERNET BANKING OR CHALLAN (DEPOSITING MONEY IN BANK)) –

Account Name – ORGANISATION OF SCIENCE AND INNOVATIVE ENGINEERING AND TECHNOLOGY OR OSIET
Account number – 966510402
Name of the Bank – INDIAN BANK, Vadapalani branch IFSC Code – IDIB000V001
Type – Current Account

Journal Payment

(INTERNET BANKING OR CHALLAN (DEPOSITING MONEY IN BANK)) -

Account Name – M Swaminathan Account number – 714327120
Name of the Bank - INDIAN BANK, KODAMBAKKAM branch IFSC Code - IDIB000K040
Type – Savings Account

Please pay the amount and send us the screen shot of the Statement/Payment copy.

Payment details: Online: online

Details of **Challan / Online** Transaction: **Acct name – Sruthi Chandrasekaran**
Acct no.- 0056053000014810 IFSC – SIBL0000056
Amount Paid: **14,900** (both conference-**Rs 2950** and journal- **Rs 11,950**)
Bank & Branch: **South Indian Bank, Nemmara**

JOURNAL CATEGORY (Please tick one Option):

For Publication purpose, we do "PUBLICATION FROM HOME*" *(ICSIE 2020 WILL START THE PUBLICATION PROCESS IMMEDIATELY AFTER THE PAPER SUBMISSION & REGISTRATION)*
*(applicable only for * For paid SCOPUS, SCIE, WEB OF SCIENCE, ANNEXURE 1 journal only)

S.no	Journal Name	ISSN	Indexing	Price	Please tick anyone
1	Not interested in Journal Publication.			N/A	
2	International Journal of Science and Innovative Engineering & Technology(IJSIET)		Google Scholar	Free	
3	International Journal of Innovative Research in Applied Sciences and Engineering(IJIRASE)	ISSN:2456-8910	Google Scholar	Free	
4	International Journal of Advanced Research in Basic Engineering Sciences and Technology(IJARBEST)	E-ISSN:2456-5717	Google Scholar, Thomson Reuter	600	

5	Journal of Engineering Science and Technology Review	ISSN: 1791-2377	SCOPUS	Issue closed	

6	Journal of Electronic Science and Technology	ISSN:1674-862X	SCOPUS	Issue closed	
7	Journal of Information and Communication Convergence Engineering	ISSN:2234-8255 E-ISSN:2234-8883	SCOPUS	Issue closed	
8	Periodica polytechnica Electrical engineering and computer science	ISSN:2064-5260 E-ISSN:2064-5279	SCOPUS	Issue closed	
9	Internet of Things and Machine Learning in Agriculture		SCOPUS BOOK CHAPTER	Free	
10	Integrating Robotics with AI and IoT		SCOPUS BOOK CHAPTER	Free	
11	Our Heritage https://www.ourheritagejournal.com/# https://ugccare.unipune.ac.in/Apps1/User/WebA/SearchList	ISSN- 0474-9030	UGC Care	1950	
12	Parishodh https://ugccare.unipune.ac.in/Apps1/User/WebA/SearchList http://www.parishodhpu.com/	ISSN: 2347-6648	UGC Care	1950	
13	International Journal of Psychosocial Rehabilitation https://www.scopus.com/sourceid/17700156008#tabs=3 https://www.psychosocial.com/	ISSN:1475-7192	SCOPUS (Multi-disciplinary – All engineering stream)	6150	
14	Indian Journal of Science and Technology(INDJST) http://mjl.clarivate.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&Full=*Indian%20Journal%20of%20Science%20and%20Technology	ISSN:0974-6846 E-ISSN: 0974-5645	Web of Science (Multi-disciplinary – All engineering stream)	8000	
15	International Journal Of Pharmaceutical Research	ISSN:0975-2366	SCOPUS/UGC IJPR - Scopus indexing confirmation (Multi-disciplinary – All engineering stream)	8500	
16	Open Biomedical Engineering Journal https://www.scopus.com/sourceid/19700175072?origin=resultslist#tabs=3	ISSN:1874-1207	SCOPUS	Issue closed	
17	The IIOAB Journal	ISSN: 0976-3104	ESCI/Web of Science	10000	
18	Journal of Critical Reviews https://www.scopus.com/sourceid/21100920227	E-ISSN:2394-5125	SCOPUS	11500	

19	Journal of Advanced Research in Dynamical and Control Systems(JARDCS)	ISSN:1943-023X	SCOPUS/UGC (Multi-disciplinary – All engineering stream)	11950	**yes**
20	Journal of Research on the Lepidoptera http://mjl.clarivate.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&Full=*Journal%20of%20Research%20on%20the%20Lepidoptera https://www2.scopus.com/sourceid/21100372632	ISSN: 0022-4324 E-ISSN: 2156-5457	SCOPUS/Web of Science (Multi-disciplinary – All engineering stream)	12500	
21	International Journal on Emerging Technologies https://www.scopus.com/sourceid/21100901133?origin=resultslist#tabs=1	ISSN:0975-8364 E-ISSN:2249-3255	SCOPUS * Based on scope coverage	Issue closed	
22	International Journal of Advanced Trends in Computer Science and Engineering(IJATCSE) https://www.scopus.com/sourceid/21100896268#tabs=1 http://www.warse.org/IJATCSE/	E-ISSN:2278-3091	SCOPUS * Based on scope coverage	Issue closed	
23	International Journal of Mechanical and Production Engineering Research and Development(IJPMERD)	ISSN:2249-6890 E-ISSN:2249-8001	SCOPUS	13000	
24	Environmental Technology & Innovation	ISSN: 2352-1864	SCIE	69000	
25	NeuroQuantology	ISSN: 1303-5150	A1 Regular issue/SCOPUS	98000	
26	JOURNAL OF ADVANCED OXIDATION TECHNOLOGIES	ISSN 2371-1175	A1 Regular issue	125000	
27	COMPUTATIONAL INTELLIGENCE -WILEY BLACKWELL	ISSN: 0824-7935 E-ISSN: 1467-8640	SCIE/A1 Regular issue	130000	
28	*INTERDISCIPLINARY SCIENCES-COMPUTATIONAL LIFE SCIENCES*	ISSN: 0824-7935 E-ISSN: 1467-8640	Springer/SCIE/A1 Regular issue	130000	
29	POLYMER COMPOSITES	ISSN: 0272-8397 E-ISSN: 1548-0569	SCIE/A1 Regular issue	130000	
30	*Journal of Ambient Intelligence and Humanized Computing*	ISSN: 1868-5137 E-ISSN: 1868-5145	Springer/SCIE/A1 Regular issue	130000	
31	*COMPUTER COMMUNICATIONS*	ISSN: 0140-3664 E-ISSN: 1873-703X	Springer/SCIE/A1 Regular issue	130000	
32	*BIOSYSTEMS*	ISSN: 0303-2647	SCIE/A1 Regular issue/Elsevier	130000	
33	WORK-A Journal of Prevention Assessment & Rehabilitation	ISSN: 1051-9815	SCIE/A1 Regular issue	130000	
34	*DESIGN AUTOMATION FOR EMBEDDED SYSTEMS* http://mjl.clarivate.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&Full=*Indian%20Journal%20of%20Science%20and%20Technology	ISSN: 0929-5585 E-ISSN: 1572-8080	Springer/SCIE/ A1 Regular issue	130000	
35	MATERIALS AND MANUFACTURING PROCESSES	ISSN: 1042-6914 E-ISSN: 1532-2475	SCIE/A1 Regular issue	130000	
36	ENERGY SOURCES PART A	ISSN: 1556-7036 E-ISSN: 1556-7230	SCIE/A1 Regular issue	130000	

37	THERMAL SCIENCE	ISSN: 0354-9836 E-ISSN: 2334-7163	SCIE/A1 Regular issue	130000	
38	MATERIALS SCIENCE - MEDZIAGOTYRA	ISSN: 1392-1320 E-ISSN: 2029-7289	SCIE/A1 Regular issue	130000	
39	*MICROPROCESSORS AND MICROSYSTEMS*	ISSN: 0141-9331 E-ISSN: 1872-9436	SCIE/A1 Regular issue/Elsevier	130000	
40	MECHANIKA	ISSN: 1392-1207 E-ISSN: 2029-6983	SCIE/A1 Regular issue	130000	
41	JOURNAL OF INTELLIGENT & FUZZY SYSTEMS	ISSN: 1064-1246 E-ISSN: 1875-8967	SCIE	135000	
42	INTERNATIONAL JOURNAL OF UNCERTAINTY FUZZINESS AND KNOWLEDGE-BASED SYSTEMS	ISSN: 0218-4885 E-ISSN: 1793-6411	SCIE/A1 Regular issue	135000	
43	CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE	ISSN: 1532-0626 E-ISSN: 1532-0634	SCIE/A1 Regular issue	140000	
44	IET SOFTWARE	ISSN: 1751-8806 E-ISSN: 1751-8814	SCIE/A1 Regular issue	145000	
45	JOURNAL OF MEDICAL IMAGING AND HEALTH INFORMATICS	ISSN: 2156-7018 E-ISSN: 2156-7026	SCIE/A1 Regular issue	145000	

Articles meets the journal requirement will be considered for publication in Free journals category.

Please send all the details (**Softcopy of research papers, filled Registration form, Declaration form, Journal, Conference attendance, Payment details(scanned copy of Challan and online transaction),** to our mail ID – **icsieconference@gmail.com**.

Note: **Please always user the paper ID in the subject for any communication.**

PAYMENT PROOF