Visvesvaraya Technological University
Jnana Sangama, Belagavi

A PROJECT REPORT ON

Secure File Storage On Cloud Using Hybrid Cryptography

Submitted by

Chandana K S	:	**4PM17CS025**
Deepa Kajjera	:	**4PM17CS028**
Meghana S Bhat	:	**4PM17CS046**
Monali S Patel	:	**4PM17CS049**

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

Under the Guidance of

Mrs. Thara K L

(Asst. Prof., Dept. of CSE)

PES INSTITUTE OF TECHNOLOGY AND MANAGEMENT,SHIVAMOGGA

(Approved by AICTE, New Delhi, Affiliated to VTU, Belagavi, ISO 9001 Certified)

NH 204, Sagar Road, Shivamogga - 577 204

August 2, 2021

PESITM, NH 206, Sagar Road, Shivamogga, Karnataka 577204
Department of Computer Science & Engineering

CERTIFICATE

Certified that the project work entitled **"Secure File Storage On Cloud Using Hybrid Cryptography"** carried out by Chandana K S (4PM17CS025), Deepa Kajjera (4PM17CS028), Meghana S Bhat (4PM17CS046) and Monali S Patel (4PM17CS049), a bonafide student of PESITM, Shivamogga in partial fulfillment for the award of Bachelor of Engineering in Computer Science & Engineering of the Visvesvaraya Technological University, Belagavi during the year 2020-21. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the departmental library.

The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

Mrs Thara K L	**Prof Chatrapathy K**	**Prof Chaitanya Kumar M V**
Project Supervisor	HOD, CSE	Principal, PESITM

External Viva

Name of the Examiner	**Signature with Date**
1.	
2.	

PESITM, NH 206, Sagar Road, Shivamogga, Karnataka 577204
Department of Computer Science & Engineering

DECLARATION

We, Chandana K S (4PM17CS025), Deepa Kajjera (4PM17CS028), Meghana S Bhat (4PM17CS046) and Monali S Patel (4PM17CS049) students of 8^{th} semester B.E. in Computer Science & Engineering, PESITM, Shivamogga hereby **declare** that the final year B.E. major project report entitled **Secure File Storage On Cloud Using Hybrid Cryptography** which is being submitted to the **PESITM, Shivamogga** during the year 2020-21 is a record of an original work done by us under the supervision of Mrs Thara K L, Asst. Prof., Dept. of CSE, PESITM, Shivamogga. This Project work is submitted in partial fulfilment of the requirements for the award of the Degree of **Bachelor of Engineering** in **Computer Science and Engineering**. The material contained in this report has not been submitted to any University or Institution for the award of any degree.

(**Chandana K S, 4PM17CS025**) (**Deepa Kajjera, 4PM17CS028**)

(**Meghana S Bhat, 4PM17CS046**) (**Monali S Patel, 4PM17CS049**)

Place: PESITM, Shivamogga.
Date: August 2, 2021

Acknowledgements

It's our pleasure to express our heartfelt thanks to Mrs.Thara K L, Asst Professor, Department of Computer Science and Engineering, for his supervision and guidance which enabled us to understand and develop this project.
We remain thankful to the co-operation and the help rendered Dr.Likewin Thomas, Assoc prof.,Department of Computer Science and Engineerring, for their advice and suggestions at various stages of the work.
We are indebted to Dr.Chatrapathy K, Head of the Department, CSE and Dr.Chaitanya Kumar M V, Principal, for their advice and suggestions at various stages of the work.
We are thankful to all teaching and non-teaching staff of the department. We also extend our thanks to the management of PES Institute od Technology and Management for providing us with the good study environment and laboratories facilities.
Lastly, we take this opportunity to offer our regards to all those who have supported us directly ot indirectly in the successfull completion of this project work.

Chandana K S
Deepa Kajjera
Meghana S Bhat
Monali S Patel

Place: PESITM, Shivamogga
Date: August 2, 2021

Abstract

The cloud computing distributed resources are shared via network in open environment. As a result, users can access their data from anywhere. At the same time there exist privacy and security issues due to many reasons. The first is the development of higher of network technologies. Another component is the rising demand for computing resources, prompting many companies to outsource their data storage. In a public cloud environment where the provider is not trusted, a secure cloud storage service is provided. This addresses different data security and privacy protection issues in a cloud computing environment and proposes a method for providing different security services like authentication, authorization and confidentiality along with monitoring in delay. To increase data security and confidentiality, the 128-bit Advanced Encryption Standard (AES) is used. The hosted services are offered to limited number of people this minimizes the security concern. The infrastructure in a public cloud is owned and managed by the cloud provider. Hence security and confidentiality of data is an important concern. In this proposed approach data is encrypted using AES for file encryption and Data Encryption Standard (DES) is used for key encryption and there are 16 rounds of encryption in the algorithm, and a different key is used for each round and then uploaded on a cloud. For preventing unauthorised access to user data,the proposed model uses an SMS alert mechanism.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Histroy of cloud computing

The cloud computing model integrates several technological advancements such as virtualization, web services, and Service Level Agreement (SLA) management for enterprise application. Due to rapid development in technologies more and more service providers and customers moving towards cloud environment. Today military, government and commercial enterprise systems are using different cloud services to provide network connectivity and high service availability to the end users. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three basic models used by cloud providers (SaaS). Even though cloud computing has many advantages when compared with the traditional data storage mechanisms; security concern is a barrier for choosing cloud computing from the consumers view point. The researchers are done several studies related to security issues in cloud. The most of cloud infrastructure is available in both public and private methods. A private cloud is one that is dedicated to a single customer or company. The hosted services are offered to limited number of people this minimizes the security concern. The infrastructure in a public cloud is owned and managed by the cloud provider. As a result, data security and confidentiality is a major concern. As the number of cloud users increases day by day, the Quality of Service (QoS) management is another important issue. QoS management in cloud computing environment refers to the activities in QoS specification such as evaluation, prediction, aggregation and control of resources to meet end-to-end user and application requirements. With the emergence in technologies a large number of organizations like IBM, Google, Yahoo, eBay etc., have already invested in cloud computing. Large number users share huge amount of data at high speeds from geographically dispersed locations. But in real cloud com-

puting environment existing solutions are prone to failure and security compromise in many areas: computing performance, cloud reliability and information security. Present approaches are not sufficient to ensure data security for end user.
Some of the advantages of Cloud Computing are:

- Potentially cheaper - It can be cheaper than paying to maintain existing IT companies.
- Sharing information is quick and efficient
- Variety of services - They are able to provide wide variety of services.
- Provides high security because files are stored in different blocks.

Some of the disadvantages:

- Less confidentiality and reliability of user data
- RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer
- It requires a third party to verify the reliability of public keys

Some of the challenges:

- Security: Security is the protection of data stored via cloud computing platforms from theft,leakage and deletion.
- Performance: Performance includes cloud services,reliability and scalability.
- Cloud Compliance: When transferring data from on-premises local storage into cloud storage it can be difficult to manage compliance with industry regulations.

1.2 Problem Statement

Main aim is to securely store the information on cloud by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality,integrity and ensures availability.

1.3 objectives

The objectives of the project can be summarized with the points below:

- To achieve a secure platform for storing files on cloud using hybrid cryptography.
- To achieve storage reliability that is a significant metric to measure the quality of service of a storage strategy.
- To achieve reduced key size and encryption time.
- To achieve integrity and data confidentiality.

1.4 Outline of the Project

The Project Report encompassed with seven chapters in total and it is organised as follows:

- Chapter 1 includes the introduction about the problem and the method used to solve the problem.
- Chapter 2 includes Literature survey which includes the works related to the project and the notable works prevailing prior to this project development with their results.
- Chapter 3 includes methodology and technology used for the development of the project.
- Chapter 4 includes system design techniques along with the use case, activity diagram used for the development of the system.
- Chapter 5 about results and future scope.

Chapter 2

Literature Survey

Swarna, Marrynal S. Eastaff(march 2018)[1]"Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm", in their proposed resources are shared among all servers, users, and individuals in a cloud environment[1]. As a result, ensuring file security is difficult for the cloud provider. As a result, an attacker can easily access, misuse, and destroy data in its original form. The paper describes a file security model that uses a hybrid encryption scheme to meet security controls. This problem can be solved by the cloud provider encrypting the files with an encryption algorithm. This paper presents a file security model that provides a practical solution to the major problem of cloud security[1].

Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam(31 jan 2019)[2]"Secure File Storage on Cloud using Hybrid Cryptography", in their proposed cloud computing is now used in a variety of fields, including industry, the military, colleges, and others, for a variety of services and the storage of large amounts of data. Without direct access to the server computer, data stored in this cloud can be accessed or retrieved at the user's request. However, security is the primary concern when it comes to data storage in the cloud. This security issue can be discussed in a variety of ways, the most common of which is cryptography. However, there's many times when a single technique or algorithm is incomplete to provide high-level security. As a result, we've introduced a new security mechanism that combines multiple symmetric key cryptographic algorithms. AES (Advanced Encryption Standard) algorithms are used to secure data in this proposed system. 128-bit keys are used in the algorithms. During encryption, the file is divided into three parts. Different encryption algorithms will be used to encrypt these individual parts of the file[2].

S. Hesham[2] in her research proposed an algorithm that increases the efficiency of the Advanced Encryption Algorithm. The proposed method reduces the critical path delay of the original algorithm. Compared to the original AES encryption/decryption

algorithm the proposed algorithm provides an efficiency improvement of 61 and 29 respectively. Taufik Hidayat, Rahutomo Mahardiko(1 june 2020)[3]"A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing", in their proposed the AES algorithm for secure cloud data sharing can be thoroughly investigated and then well implemented. AES algorithm for cloud data security, according to the authors. These papers discussed how cloud data security could affect data authenticity as well as prevent any unauthorised access[3]. Cloud computing is an information technology (IT) revolution that allows users to share resources, services, and data over a network. Because all users on the network have the same authorizations to transfer data, data is vulnerable to unauthorised access. Because security is considered as a serious issue, a proposed encryption-based system for data transfer security is presented. Advanced Encryption Standard (AES) will be proposed to secure data transmission and storage in cloud computing to prevent an attack by an unauthorised person[3].

In [4] proposed cloud storage scheme, The data requested by end users is served to them using over-encryption by the cloud storage provider after proper authentication from the data owner, where the data owner had already sent the data to the cloud storage provider in encrypted form. The data owner generates all of the required secret keys and distributes them to the right client. B. Rakesh, K. Lalitha, M. Ismail and H. Parveen Sultana(6 december 2017)[5] , In [5] proposed a distributed scheme to authenticate data, Cloud Computing is the next-generation IT enterprise's revolution. Database and application software are being reduced to large data centres as a result of cloud computing. This aspect attribute, on the other hand, includes a variety of security challenges that aren't well understood. It focuses on cloud data storage security, which has always been a critical aspect of service quality (QOS). As a result, cloud providers charged on a pay-per-use basis. As a result, supporters attempt computing resources through Outsourcing. As a result, users' hardware and software maintenance costs are reduced. The introduction of Cloud Computing reduces the need for direct hardware management and provides great convenience to users. The best examples for Cloud Computing example are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

In [6] Vinita Keer, Dr. Syed Imran Ali, and Prof. Neeraj Sharma, [7] "Hybrid Approach of Cryptographic Algorithms in Cloud Computing," the main objective of their research is to secure data files stored in the cloud[7]. In [6] Priyajaiswal, Randeepkaur, and Ashok Verma, "Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique,"[8] their proposed model, classical encryption technique is used in their algorithm. The main goal of their work is to make data in

cloud storage more complex in terms of space. In [9] The cloud is a term that refers to the storage, processing, and management of data over a network. The cloud primarily offers three services: storage as a service, platform as a service, and software as a service, all of which are produced via the internet and are based on the needs of the user. Many businesses are expanding their infrastructure as it has become a critical platform. They focused on issues and challenges in the existing system of single-level encryption techniques in [10]. A number of symmetric and asymmetric encryption algorithms, such as DES and AES, are also available.

In [11] The Author had proposed consumers to store their personal files or data on a cloud server, which they can access whenever they need it. Because many consumers store or send personal data to the cloud, security and privacy are important issues. The data is encrypted using the Modify advanced encryption standard, resulting in successful and secure cloud storage. The proposed system is very effective against malicious data and provides a high level of security as well as a maximum execution time. In [12] their proposed, on the cloud, AES is used to send and receive data messages. For message file upload, the cloud user must first secure the data message or file before sending it to the Cloud Service Provider. The data message or file with the public key is then encrypted with the AES encryption algorithm and sent to the cloud service provider, during which the encrypted data or file is stored in the corresponding cloud server. The cloud user must request the cloud service provider to download his or her stored secure data message or file for the message file download. Cryptography is a key component of information security. Cryptography is a form of data encryption that plays an important role in data security. The process of converting ordinary plain text into unintelligible text, and vice versa, is known as cryptography. Subramanian and Jeyaraj [13] analyse the security issues that cloud entities face (i.e. Cloud Service Provider, the Data Owner and Cloud User).

In [14] proposed Secured user authentication using a hybrid of AES for encryption/decryption has the potential to impact not only authentication but also file access control mechanisms in the cloud.

In [15] It has three levels of services, each with its own number of resources. Infrastructure as a service (IaaS) (ii) Platform as a service (PaaS) (iii) Software as a service (SaaS) (SaaS). Hardware assets, such as hard disk drives, memory, and networking resources, are included in the rent and charged based on usage in IaaS. PaaS includes not only all of the features found in IaaS, but also operating system features, updates, and other services. As a result, make everything work properly. Finally, the SaaS, which is the most flexible and simple to use. The various layers of cloud infrastructure

are related to each layer of cloud computing. In [16] their proposed today, encryption of data at rest is considered to be one of the most important issues in cloud computing, especially cloud storage, according to many research findings. Based on the results of the survey and the need for enterprise-wide data encryption strategies. One of the most important aspects of security in cloud computing, particularly cloud storage, is data encryption at rest [17,18]. Cloud Provider (CP), which is an important part of this security, is a problem with older technologies that is currently occurring. In [19] The proposed system shows that using hybrid algorithms improves the encryption level of encrypted mobile data while also reducing the time it takes to encrypt and decrypt it. In [20] We looked at various cryptographic techniques for data sharing security in this survey. One simple way to achieve secure data sharing in the cloud is for the data owner to encrypt his data before storing it in the cloud, ensuring that the data is information-theoretically secure against the Cloud provider and other malicious users.

In [21] Aditya SadanandGhadi, "Secure File Storage Using Hybrid Cryptography" 2020 Nowadays, increase of mobile devices and technologies in networking technology, now we have the ability to securely store files over the network. Cryptography is the most important technology for data security of all types. This paper provides a broad overview of the various methods for securely storing and sharing files over the network. This proposed scheme will also mean that the correct model is secured by confidentiality, integrity, and availability methods. In [22] Author - Punam V. Maitri, Aruna Verma, Year 2016 The paper focuses on how files are stored on a cloud platform in a secure way. It also discusses the issue of encrypting a file with only one algorithm and how ineffective this will be in the cloud. This paper divides the file into blocks and encrypts each block with AES. The paper focuses on allowing users to securely store and share data in a group setting using cloud technology. The paper's method employs group signature and encryption techniques. The advantages of this proposed method is that data owners can store files in the cloud without showing their true identity to others. The proposed security mechanisms will prevent the misuse of confidential data, making the system more reliable. High speed: The proposed method will make proper key encryption and decryption much faster than before. Cryptographic Algorithms for Cloud Computing Security.

In [23] aim to securely store information in the cloud in this paper by splitting data into several chunks and storing parts of it on the cloud in a way that maintains data confidentiality, integrity, and availability. Many institutions and IT industries are rapidly adopting cloud computing, which provides new software at a low cost. Cloud computing is useful in terms of cost and data accessibility. Cloud computing offers

many advantages, including low costs and data accessibility via the Internet. Users often store sensitive information with cloud storage providers, but these providers may be unreliable. Ensuring the security of cloud computing is a major factor in the cloud computing environment. The main goal is to securely store and access data that is not under the control of the data owner in the cloud. In [24] The most difficult component of cloud computing security is decrypted by well-known security experts. Cloud computing allows both large and small businesses to take advantage of Internet-based services. so that they can reduce start-up costs and capital expenditures, access applications only when necessary, use services on a fee basis, and quickly reduce or increase ability. One of the most regular and mostly symmetric block cypher algorithms is Advanced Encryption Standard. This algorithm is implemented in all hardware and software and has a specific form for encrypting and decrypting sensitive data. AES is able to deal with three different key sizes: 128, 192, and 256 bits. Its codes are each 128 bits in length. AES encryption is a quick, flexible, and simple method of encrypting data. In [25] Cloud computing allows for the storage and management of large amounts of data. It has a large capacity for storing a large number of users and individual data at the same time, as well as the ability to retrieve it at any time and from any place. Data security and privacy are main goals. proposed a new security model for cloud data storage that uses the concept of hybrid encryption and decryption to provide a secure and protected environment. In the proposed model, the data owner sends encrypted data to a cloud server to keep it safe from intruders, and only authorised users are given the decryption key to retrieve its original data.

In [26] The data that the owner wanted to store in the cloud may contain sensitive data or information that requires extra safety measures before being stored on an untrusted network. Before migrating any confidential data to the cloud, security becomes a must. It allows the user to access their data at any time and from any location by easily connecting to the network.This hybrid approach secures data and protects it from any malicious activity taken out by intruders. Using this proposed method, a brute force attack is also provided impossible. Symmetric encryption also improves processing ability because it is faster and more efficient than asymmetric encryption.

In [27] To make a cloud system more secure, all of the general Cryptography Algorithms are used. While they perform this task excellently, clients must have confidence in the cloud service provider's data security. This dependency reduces the use of a cloud system by clients who need to store sensitive data. In [28] Cloud computing security refers to the use of policies, controls, and technologies to protect data in the

cloud, its applications, and the underlying infrastructure. Information security, also known as secure data storage, is a component of cloud security that aims to prevent unauthorised users from accessing data and to prevent data destruction or modification. Because it generates a unique key for the encryption process in each round, AES takes up more space. Privacy and security are more important in cloud computing because large amounts of data are transferred, increasing the risk of data attack day by day. In [29] today's world, users want to keep their data in both storage and the cloud, so they use cloud storage. Instead of using a single encryption algorithm, users use hybrid encryption to secure cloud storage. The user can protect data confidentiality, privacy, and integrity from hackers by implementing this method. Users learn more about how this approach works by having a look at the flow chart and algorithm in the methodology section of this paper.

In [30] Cloud computing is now used in many areas, such as industry and military colleges, to store large amounts of data. On the user's request, we can retrieve data from the cloud. Many issues must be resolve in order to store data in the cloud. There are a number of different approaches that can be used to address these issues. All algorithm key size is 128 bit. Which part of the file is encrypted with which algorithm and key is contained in key information. The file is divided into eight sections. Each section of the file is encrypted with a different algorithm. Advantages of security model are integrity, security and confidentiality.

Chapter 3

Proposed Methodology

System Analysis is a collection of components that work together to realize same objective from a system. It will have some of the objectives of a system like, an easy approach to solve a problem and managerial skills to slove such problems if the same problem is repeatedly occuring also maintenance and reuse of proposed systems. Input, processing and output are the major components in the system. In a system, the different components are connected with each other and they are

Figure 3.1: System Behaviour.

mutually supporting each other. The objective of the system demands that some output is produced because of processing the suitable inputs. A well designed system also includes an additional element referred to as 'control' that provides a feedback to achieve desired objective of the system. The systems are created to solve many problems. The system can be called an organized way of dealing with problems. They teach us understanding about problems and solve those problems easily.

3.1 Functional Requirements of the project

In one sentence "What the system should do", how the system should react to particular inputs and how the system should behave in the particular situations. In some cases, the functional requirements may also explicitly state what the system should not do. This is the list of the actual services which a system should provide. This is the list of the services or functions that a user desires from the software.
The functional requirements for the system describe what the system should do. These requirements depend on the type of software being developed, the expected users of the software and the general approach taken by the organization when writing requirements. When expressed as user requirements, the requirements are usually described in a fairly abstract way. However, functional system requirements describe the system function in detail, its inputs and outputs, exceptions, and so on. Functional requirements for a software system may be expressed in a number of ways.
Description of service which software will provide to the end user. Constraint which we will imposed on the services are also part of the requirements.

3.2 Non Functional Requirements of the project

Non-functional requirements are requirements that are not directly concerned with specific functions delivered by the system. They may relate to emergent system properties such as reliability, response time and store occupancy. Alternatively, they may define constraints on the system such as the capabilities of I/O devices and the data representations used in the system interfaces. The plan for implementing functional requirements is detailed in the system design. The plan for implementing non-functional requirements is detailed in the system architecture. The non-functional requirement of the system can be summarized as follows:

- Usability : Application is designed with usability in mind so that users will find it very easy to use an application.
- Reliability : Reliability refers to the consistency of a measure. A test is considered reliable if we get the same result repeatedly. In general reliability systemic definition is the ability of a person or system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances.
- Availability : The system should be available to user anytime.
- Performance : The system have a quick, accurate and reliable results.

- Recovery : In case of malfunctioning, the system should be able to recover and prevent any data loss or redundancy.

3.3 Use Case Diagram

3.3.1 Use Case Diagram of Owner

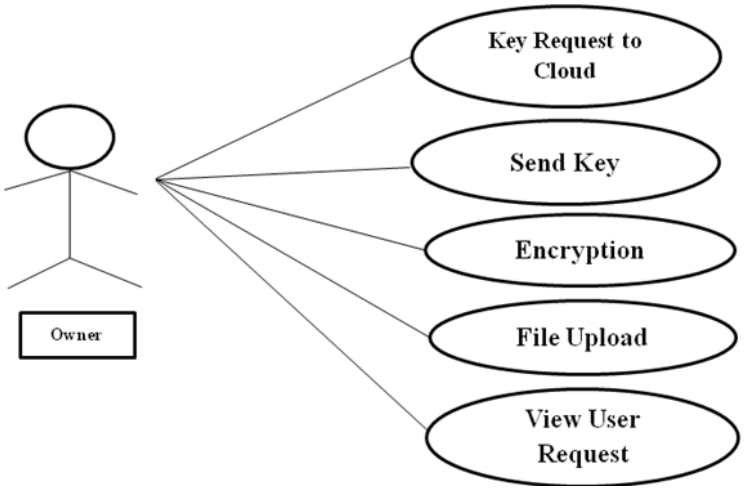

Figure 3.2: Use Case Diagram of Owner

- The data owner has the authority to edit, modify, create, share, and restrict cloud data access.
- Data user sends a key request to data owner and return to the cloud.
- File upload section is where the user can upload their files. The file that is encrypted, using AES algorithm.
- View user request section of this module is a page to view key requests sent by the data user.

3.3.2 Use Case Diagram of User

- Data user uses the cloud to store and access it at any point of time.
- Registration module is present for new users to register by providing details such as username and password.
- Login module allows user to login to one's cloud data segment.

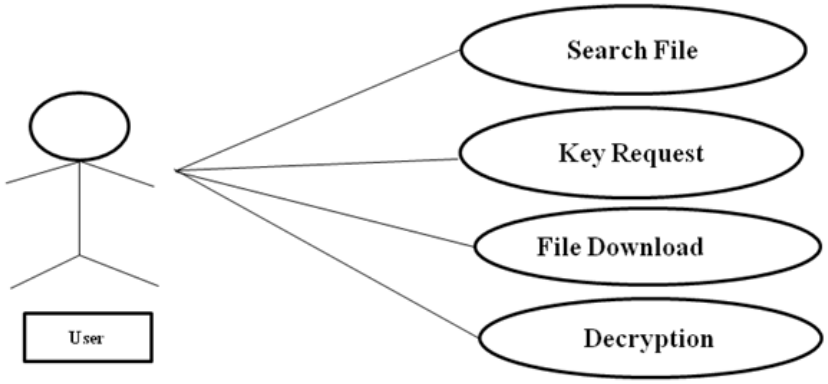

Figure 3.3: Use Case Diagram of User

- The user can search the required files present in the cloud storage. These files are uploaded by the data owner. They are present in encrypted format Hence, data user must request data owner for key to decrypt the file and download it.
- The request for key can be sent in the key request module.
- Using the key sent by data owner, the data user can decrypt the file and download it.

3.4 System Architecture

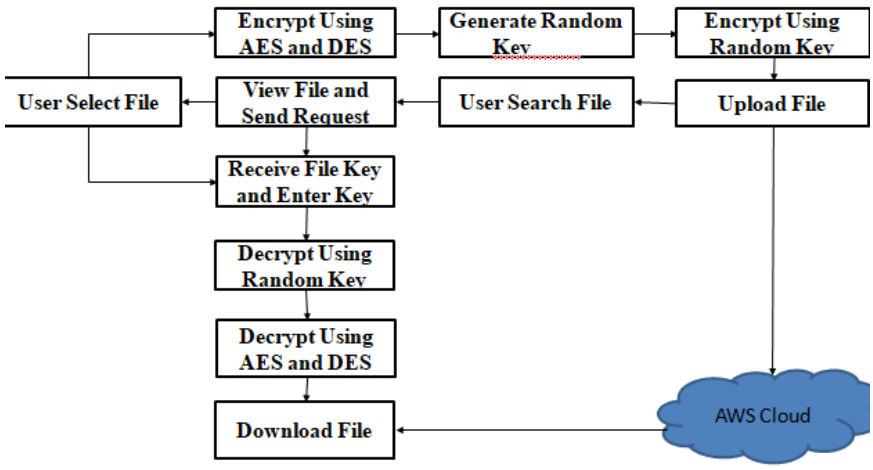

Figure 3.4: System Architecture

The proposed system built on a prototype of an online file processing application. One important application of this system is secure sharing of confidential data like medical record, personal information, financial information etc. Suppose a user wants to access our application for uploading their confidential data, she/he must register with their valid email id and mobile number with our system. The username and password for their account is user defined and not system defined. After successful registration they can login as a user. Then user can upload the confidential file through file upload module. Before uploading file to cloud, the user gets a window for encrypting their file as individual blocks. Then click the save button after setting a secret file ID for future accessing and sharing. The file will be uploaded to the database on the server. In the case of medical record, user can share record with their doctor anytime from anywhere, there is no need for keeping their files with them always as hard copy or soft copy. All they have to do now is remember their secret file ID. The file ID may be numbers, alphanumeric characters or special characters anything as user wish or they can use a combination of these as file ID. The length of a file id is uncontrolled. The user can see how long it took to upload their file. The proposed model uses AES encryption with a key length of 128 bits. For 128-bit keys, there are ten rounds of encryption. For 128-bit keys, there are ten rounds of encryption. In this model, the file was split into different blocks depending on file size. Then individual blocks are encrypted separately. Regarding block-by-block encryption, each block was uploaded to the cloud at different locations, each with its own file id and block id. If anybody like cloud provider, try to access a file directly from the server, they cant get whole data, since it stored at different locations and also in encrypted form. Hence the person who knows secret file id can retrieve data.

The proposed system allows users to edit their data online and then upload it to the cloud without having to download it to their desktop. This facility is only available to the actual user, while others can only view data. User authentication is performed through password verification. For their account, each user has a unique user id and password. During registration user sets his/her own user id and password by which they can access their account for uploading their text files. When uploading file, each user has a unique file id for future access to their data. The user gains access to their account if he or she enters the correct user name and password. Otherwise error message will be generated.

Authorization is the process of verifying users privilege to access something. An SMS alert system is used in the proposed system to inform the actual owner of

unauthorised access to a specific file. Each file uploaded in cloud has a unique file id. This ID can be used by authorised users to download and edit their uploaded data. If somebody tries to access another persons file, an alert SMS will send to the actual owners mobile number which he/she provided during the time of registration.

3.5 Methodology

3.5.1 AES algorithm:

AES steps of encryption for 128 bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data(plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data(ciphertext).
- Each round of the encryption process requires a series of steps to alter the state array. These steps invlove 4 types of operations called: Sub Bytes, Shift Rows, Mix Columns and XOR Round key.

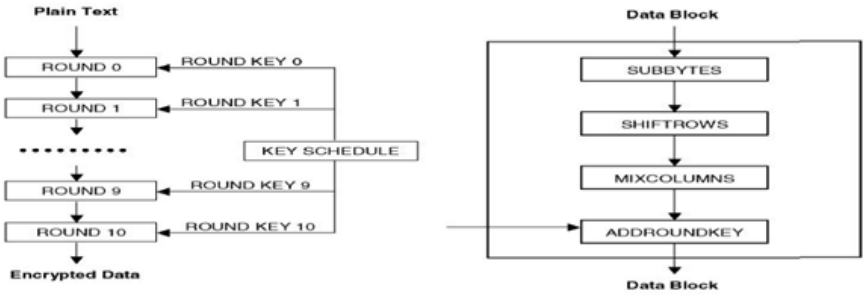

Figure 3.5: Steps in AES algorithm

- Decryption involves reversing all the steps taken in encryption using inverse functions:Inverse Sub Bytes, Inverse Shift Rows, Inverse Mix Columns.
- XOR Round key doesn't need an inverse function because XORing twice gives the original value.

Implementation of AES algorithm:
The state array is a 4x4 matrix that contains 128 bytes of input data. The encryption process is divided into four stages: mix, columns, sub bytes, add round key, and shift rows.

- Sub Bytes-It's referred to as a "substitution step." It's not a straight line. According to S-box, each byte is replaced with another. In cypher, the operation provides an indirect proportion. There are four columns and four rows in the resulting matrix.

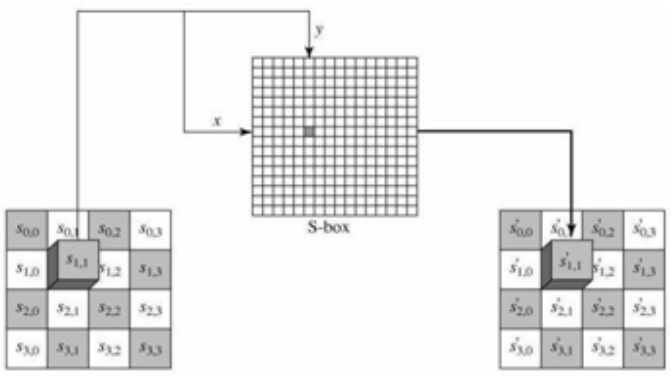

Figure 3.6: Byte Substitutuin

- Shift Rows- It is a stage in which each row is rotated a set number of times. Permutation is another name for it. The matrix's four rows are rotated accordingly. Rows have been shifted to the left. Shift is done because Row 1 isn't rotated. Row2 has been shifted one byte to the left. Row 3 has been moved two positions to the left. Row 4 has been moved three positions to the left.The resulting matrix is made up of the 16 bytes that have been rotated in relation to each other.

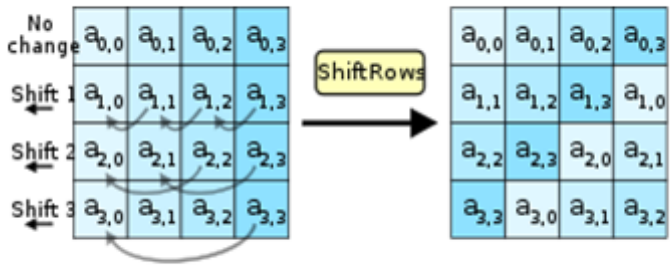

Figure 3.7: Shift Rows

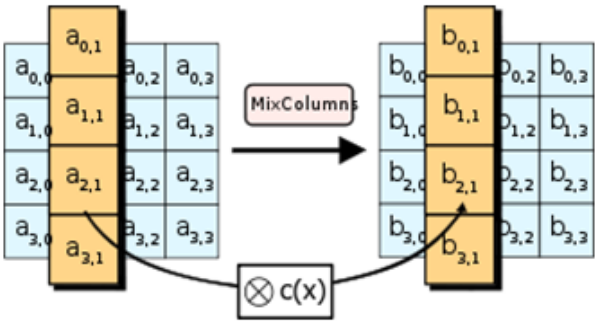

Figure 3.8: Mix Columns

- Mix Columns- In this step, matrix multiplication is used to change each column. There are four bytes in each column. The resulting matrix is 16 bytes long. For each column, the input is taken. It takes four bytes to use it. The output produces four bytes that are not the same as the four bytes provided as input.

- Add Round Key- Each byte of state is bound by the round key. The XO-Red matrix with the round key is used in this step. The original key is represented by a 4x4 matrix. It has a 128-bit key. This four-word key, each of which is four bytes long, is converted to a 43-word key. W[0], W[1], W[2], and W[3] are represented by the first four words.

3.5.2 DES algorithm:

DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.

Steps in DES algorithm:

- In the first steps, the 64 bit plain text block is handed over to an initial permutation function.
- The initial permutation performed on plain text.
- Next the initial permutation produces 2 halves of the permuted block: says Left Plain Text(LPT) and Right Plain Text(RPT).
- Now each LPT and RPT go through 16 rounds of encryption process.
- In the end, LPT and RPT are re-joined and a Final Permutation(FP) is performed on the combined block.
- The result of this process produces 64 bit cipher text.

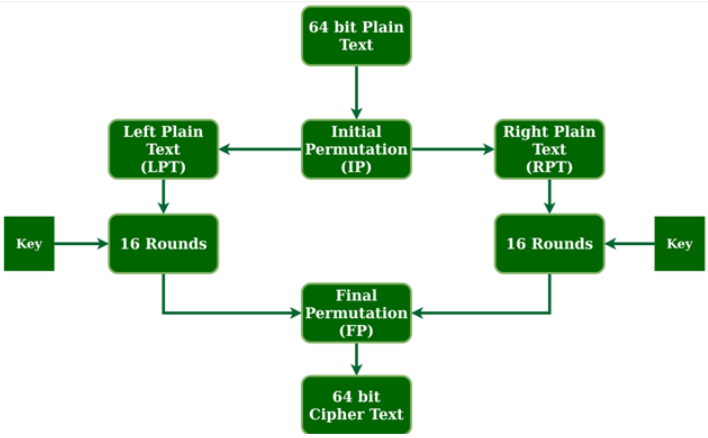

Figure 3.9: Steps in DES algorithm

Chapter 4

Implementation

In this chapter, we are going to discuss a brief idea about the implementation of the Secure File Storage on Cloud Using Hybrid Cryptography. We also discuss about the different components used in our project.

4.1 Software Requirements of the Project

The software requirements specification is a description of a software system to be developed. The software requirements are:

4.1.1 Netbeans IDE

Netbeans is an open-source integrated development environment (IDE) for developing with Java, PHP, C++, and other programming languages. It allows for integration of various component, support various scripting languages and advanced text editor. It also provides a GUI to create and design the project and also sup- ports databases. Rapid application development thus enables quality products to be developed faster, saving valuable resources.

IDE is basically a software category in which can write program and run the program their only. IDE helps to identify an errors in proper manner even before running the program. Netbeans framework reusability simplifies Java Swing desktop application development, which provides platform extension capabilities to developers.

Netbeans uses components, also known as modules, to enable software development. Netbeans dynamically installs modules and allows users to download updated features and digitally authenticated upgrades.

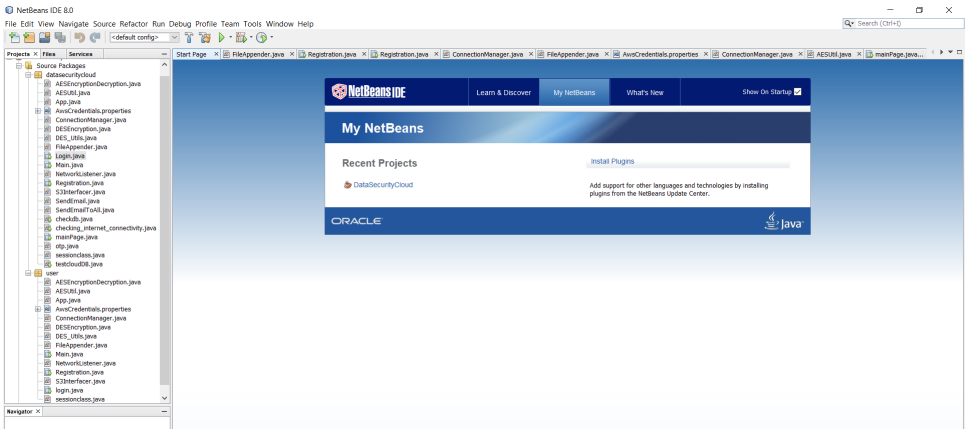

Figure 4.1: Netbeans IDE

4.1.2 Amazon S3 Cloud

The Amazon Simple Storage Service (Amazon S3) is an online storage service. Its goal is to make web-scale computing more available. You may use Amazon S3's basic web services interface to store and retrieve any amount of data, at any time, from any location on the internet.It provides any developer with access to the same highly scalable, reliable, fast, and low-cost data storage infrastructure that Amazon uses to run its global network of web sites. The service aims to maximise scaling benefits and pass them on to developers.

It explains how to make requests to create buckets, store and retrieve objects, and manage resource permissions. It also describes the authentication and access control processes. Access control determines who has access to Amazon S3 objects and buckets, as well as the type of access (for example, READ and WRITE).The authentication process ensures that a user attempting to access Amazon Web Services is who they say they are (AWS).

Advantages of using Amazon S3: Amazon S3 was developed with a small feature set in mind, focusing on simplicity and reliability. Some of the benefits of using Amazon S3 are as follows:

- Creating buckets– Create a data bucket and give it a name. Buckets are the most simple data storage containers in Amazon S3.
- Storing data- A bucket can hold an infinite amount of data. You can fill an Amazon S3 bucket with as many objects as you want. Each object can hold up to 5 TB of data. A developer-assigned key is used to store and retrieve each object.

- Downloading data– You can either download your data or allow others to do so. You can download your data whenever you want, or you can give others permission to do so.
- Permissions- Allow or disallow others from uploading or downloading data to your Amazon S3 bucket. Allow three different types of users to upload and download files. Authentication mechanisms can help in preventing unauthorised access to data.
- Standard interfaces– Use REST and SOAP interfaces that are standards-based and designed to work with any internet-development toolkit.

Figure 4.2: Amazon S3 Cloud

4.2 Hardware Requirements of the Project

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware. Following are the hardware requirements of this project:

Table 4.1: Basic hardware requirement of a project

Processor	Intel i3 and above
RAM	4GB
HardDisk	500GB

Chapter 5

Results-Analysis

5.1 Test Analysis

- Design Philosophy Of The AESAVS.
  The AESAVS is designed to test conformance to FIPS197, Advanced Encryption Standard, rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.
  The AESAVS has the following design philosophy:
  - The AESAVS is designed to allow the testing of an IUT at locations remote to the AESAVS. The AESAVS and the IUT communicate data via REQUEST and RESPONSE files.
  - The testing performed within the AESAVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100 percent conformance with the standard. The AESAVS Tests Description:
    The AESVS is designed to test the following Modes of Operation:
    - o ECB
    - o CBC
    - o OFB
    - o CFB1 (CFB where the length of the data segment is 1 bit, s=1)
    - o CFB8 (CFB where the length of the data segment is 8 bits, s=8)
    - o CFB128 (CFB where the length of the data segment is 128 bits, s=128)
    - o Counter (Counter mode is tested by selecting the ECB mode)

For each mode implemented, selections are available for the key sizes (i.e., 128-bit, 192- bit, and 256-bit) supported as well as the ciphering direction (i.e., encryption and decryption). It is not necessary for every mode implemented to support the same key sizes and ciphering directions. For example, an implementation may support all three key sizes for CBC for both encryption and decryption, but only the 128-bit key size for CFB1 for decryption only.

Once configuration information has been provided, appropriate REQUEST files will be generated. REQUEST files are the means by which test data is communicated to the Implementation Under Test (IUT). The IUT is used to process the data in the REQUEST file, and the resulting data is placed in a RESPONSE file. The data in the RESPONSE file is then verified.

- Testing Philosophy For DES

  The DES has been implemented by many vendors using many different techniques. To be most useful a test for the DES should be applicable to all DES devices without regard to implementation. The maintenance tests are therefore designed only to test the functionality of the algorithm itself at the well defined interfaces, such as input, key and output. While the NBS validation test could be used for maintenance, it does not meet the desirable criterion of a maintenance test for minimizing the amount of data stored. It was also desired to minimize the total number of encipherments and decipherments during the test to make the test more practical in an on-line environment during intervals between transmissions.

  Stuck-faults in Cipher Feedback Mode:

  One of the modes of operation of the DES is cipher feedback, where the output of the DES is added mod 2 to the plaintext to produce ciphertext. If the output of the DES is subject to stuck-faults, either at one or at zero, then some part of the plaintext, or its complement, is being transmitted in the clear. It is therefore desirable that the device be tested for stuck-faults, preferably during all encipherment operations, while being used in cipher feedback mode.

5.2 Test Cases

- Confidentiality: Confidentiality covers a spectrum of access controls and measures that protect your information from getting misused by any unauthorized access. The ideal way to keep your data confidential and prevent a data breach

is to implement safeguards. Every piece of information a company holds has value, especially in today's world. Whether it's financial data, credit card numbers, trade secrets, or legal documents, everything requires proper confidentiality. In other words, only the people who are authorized to do so should be able to gain access to sensitive data.

A failure to maintain confidentiality means that someone who shouldn't have access has managed to get access to private information. Through intentional behavior or by accident, a failure in confidentiality can cause some serious devastation.

Some information security basics to keep your data confidential are:

Encryption

Password

- Integrity: Integrity refers to the accuracy and completeness of data. Security controls focused on integrity are designed to prevent data from being modified or misused by an unauthorized party. Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and precautionary steps must be taken to ensure that data cannot be altered by unauthorized people.

  For example, in a data breach that compromises integrity, a hacker may seize data and modify it before sending it on to the intended recipient.

  Some security controls designed to maintain the integrity of information include:

  1. Encryption
  2. User access controls
  3. Backup and recovery procedures

- Availability: Data availability means that information is accessible to authorized users. It provides an assurance that your system and data can be accessed by authenticated users whenever they're needed. Similar to confidentiality and integrity, availability also holds great value.

  Availability is typically associated with reliability and system uptime, which can be impacted by non-malicious issues like hardware failures, unscheduled software downtime, and human error, or malicious issues like cyberattacks and insider threats. If the network goes down unexpectedly, users will not be able to access essential data and applications. Information security policies and security controls address availability concerns by putting various backups and redundancies in place to ensure continuous uptime and business continuity.

Your information is more vulnerable to data availability threats than the other two components in the CIA model. Making regular off-site backups can limit the damage caused to hard drives by natural disasters or server failure. Information only has value if the right people can access it at the right time.

Information security measures for mitigating threats to data availability include:

1. Off-site backups
2. Disaster recovery
3. Redundancy
4. Failover
5. Proper monitoring

5.3 Outcomes

Figure 5.1: Admin Login Page

Figure 5.2: Main Page

In this page we can perform the actions like viewing user's information, upload the files, send the messages and key encryption.Search buttom is used to find the user's details using employee ID.

Figure 5.3: status drop down menu

In this we are using the status drop down menu.This is used in order to know whether the user is authorized or not.If the user is authorized, then he will be accepted else it will be in the pending state.

Figure 5.4: Updated successfully

Modification done in any user's information like changing the user's email ID, password or phone number can be updated.

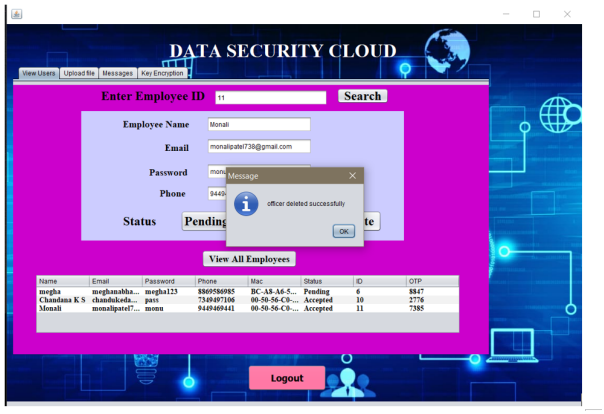

Figure 5.5: Any user's information like user's email ID, password or phone number can be deleted successfully

Figure 5.6: When otp is deactivated this message mechanism is used by the user to resend the otp

Figure 5.7: Overview of message mechanism

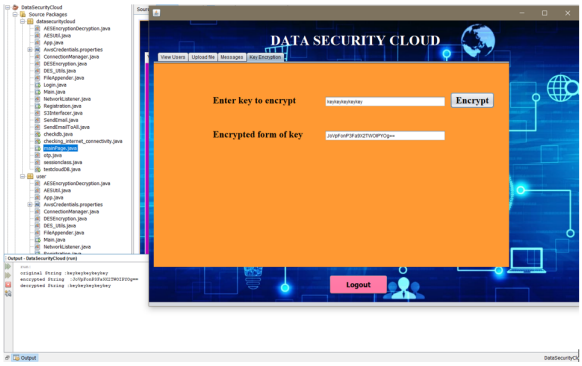

Figure 5.8: Encryption mechanism

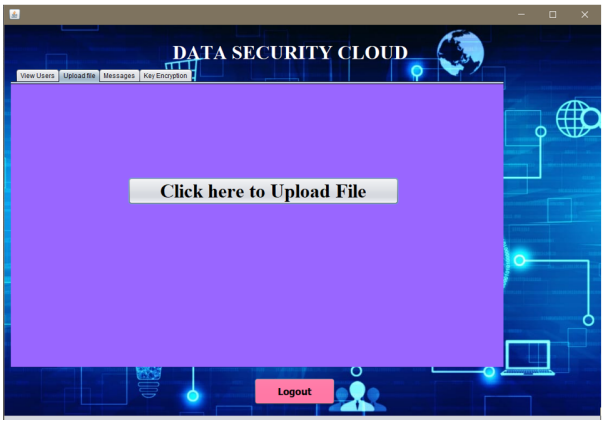

Figure 5.9: By clicking are redirected to the uploading page

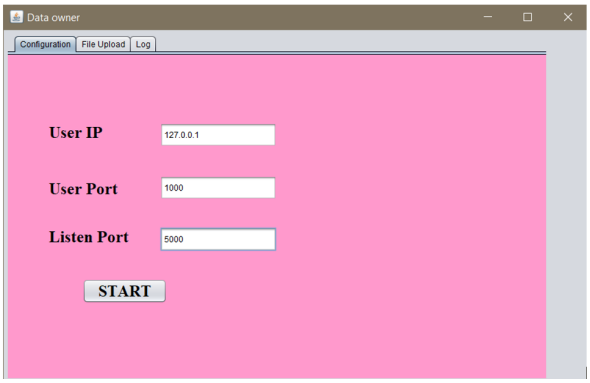

Figure 5.10: An IP address is a numerical label such as 123.0.0.1 that is connected to computer network that uses the Internet Protocol for communication. User Port is a registered port which is used for the communication with the cloud.

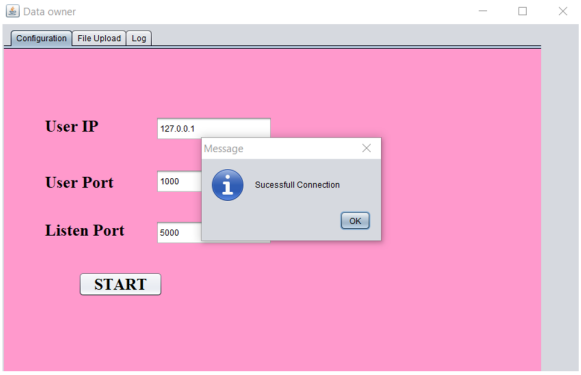

Figure 5.11: Listen port is used to establish communication between cloud and user's. By clicking on start button we will establish a successful connection.

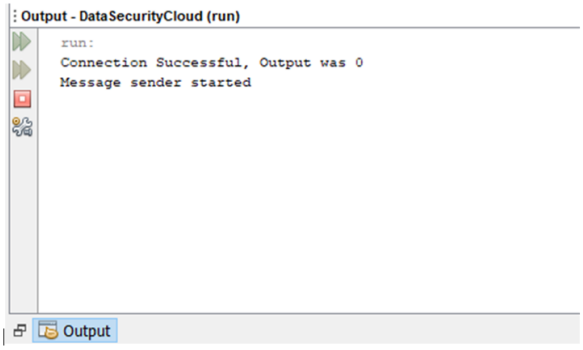

Figure 5.12: This successful connection is shown in NetBeans IDE.

Figure 5.13: After successful connection we are ready to upload to file to the cloud.

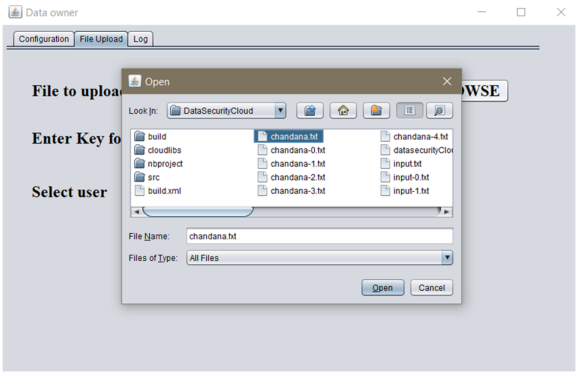

Figure 5.14: By clicking on button we browse the file which has to be uploaded to the cloud.

Figure 5.15: In this page we will specify the key and select the user to whom the details of the file has to be mailed.

Figure 5.16: By clicking on button it will generate a random otp number that has to mailed to a particular user.

Figure 5.17: In this page the otp of a particular person has been updated to the database.

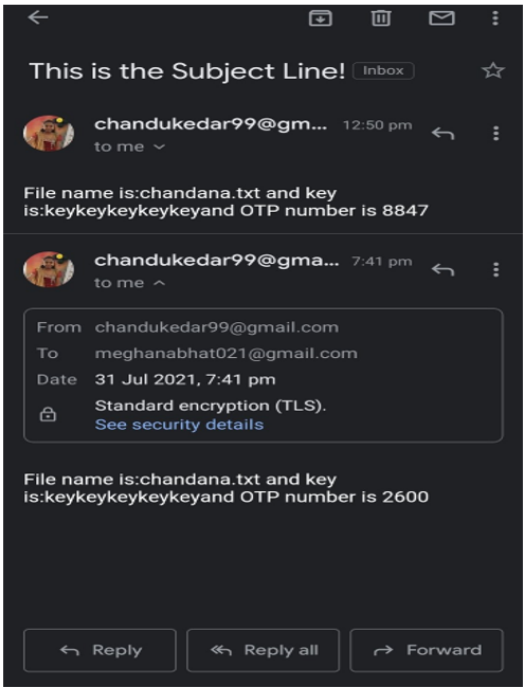

Figure 5.18: otp send by the user email ID.

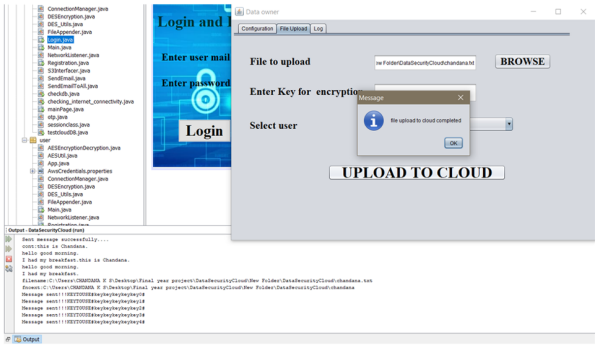

Figure 5.19: File has been uploaded to cloud successfully by dividing the file into five fragments.

Figure 5.20: User Login and Registration Page.

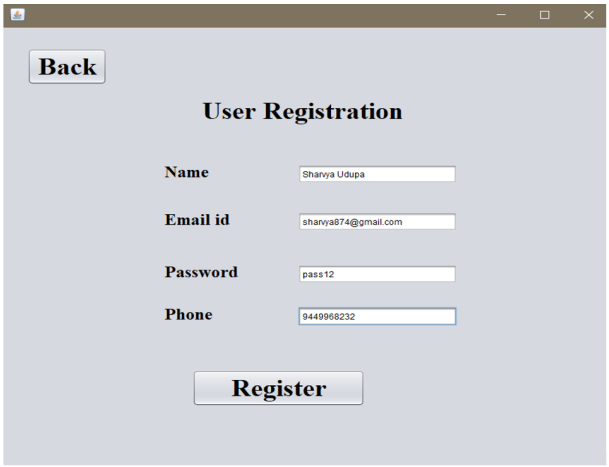

Figure 5.21: In this registration page users are allowed to enter their details.

Figure 5.22: The details of the users have been updated.

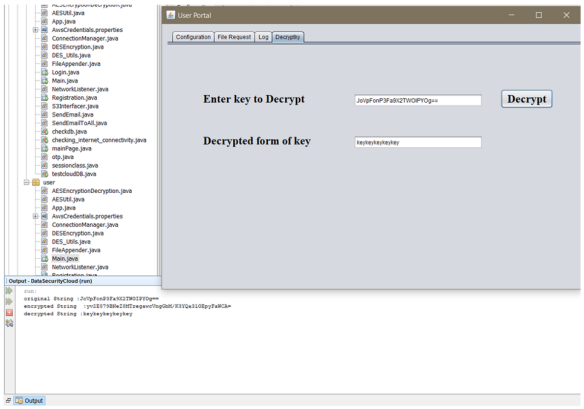

Figure 5.23: Decryption mechanism.

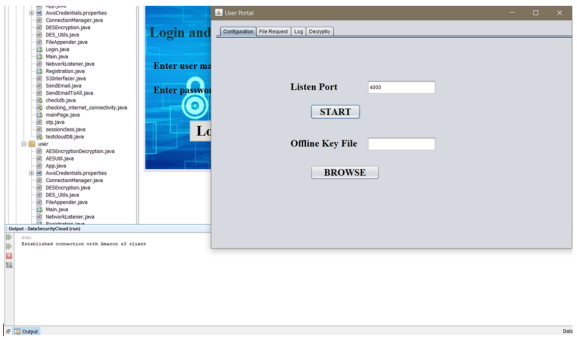

Figure 5.24: Listen port is used to establish the communication between the user's and the Amazon S3 cloud.

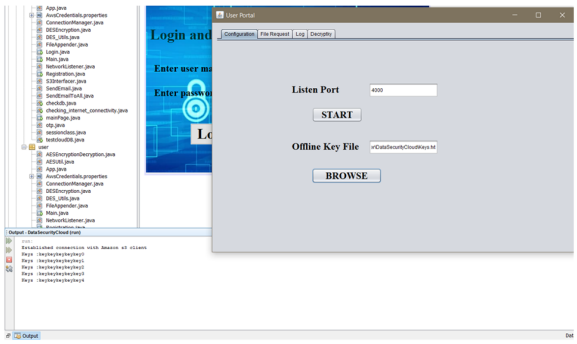

Figure 5.25: Keys text file has to be uploaded.

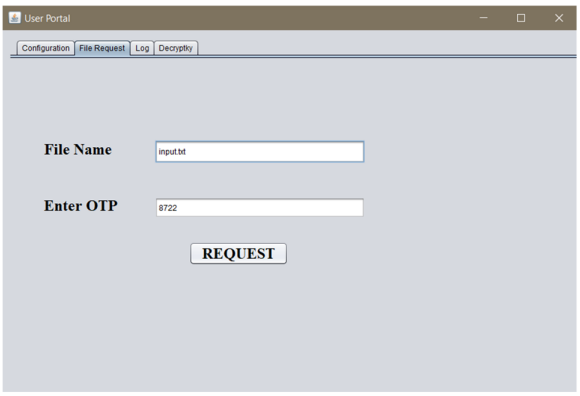

Figure 5.26: In this page we have to specify the file name and otp number that has been mailed by the admin for download purpose.

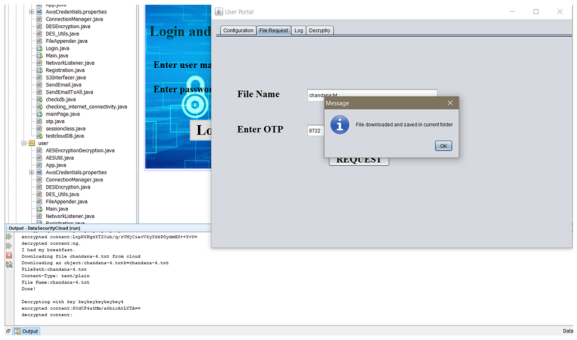

Figure 5.27: We are successfully downloaded the file from the cloud.

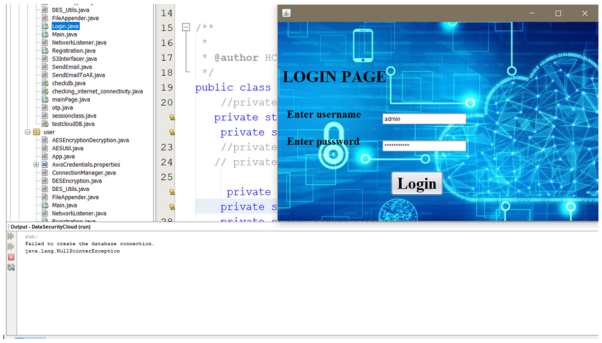

Figure 5.28: We will get this exception when it will fail to connect with the cloud or database.

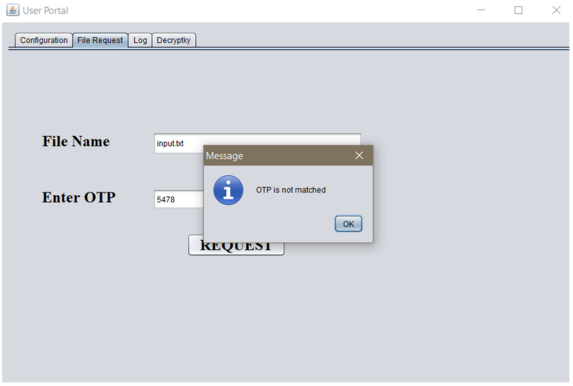

Figure 5.29: If otp is deactivated or the entered otp number is different with respect to the user and the file name, we will get the above figure.

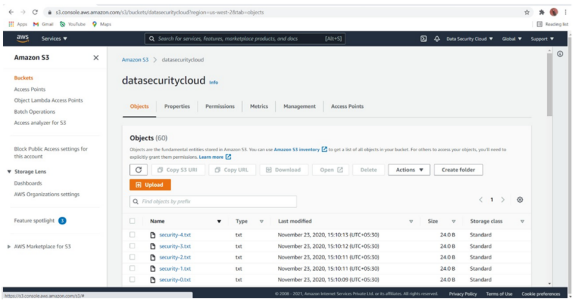

Figure 5.30: Data security cloud is the name of the bucket in amazon S3 cloud. The files we upload will be stored in this bucket..

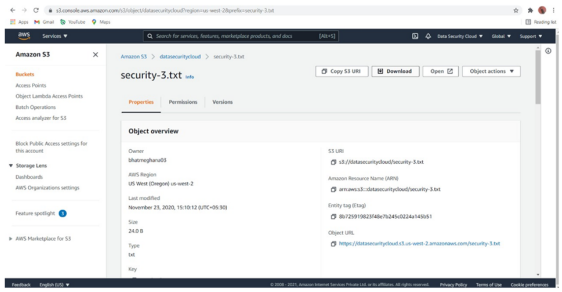

Figure 5.31: When we click on a particular file we will receive this window.

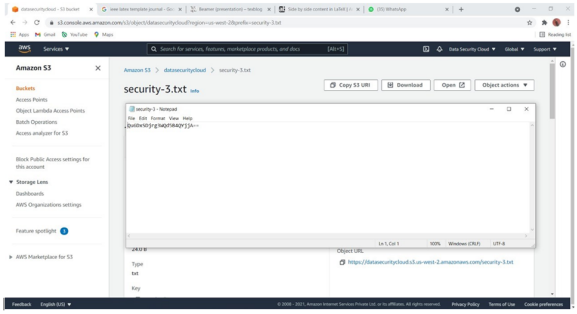

Figure 5.32: We have option to download the file from the cloud but we will get that file in fragment form. The content of the file is shown in the above figure which is in the encrypted form.

Chapter 6

Conclusions

Security of data while migrating it towards cloud computing become a major requirement before forwarding and storing any confidential data over cloud. Cloud provides flexible and accessible data storage which increases the chances of any intruder attack.To reduce this problem hybrid cryptography is the only technqiue, which allows encrypting sensitive data before storing it over cloud and only authorized users are provided with corresponding decryption key.Use of hybrid cryptography increases the complexity of data and makes it impossible to perform brute force attack.

6.1 Future Work

In future,more advanced symmetric or asymmetric cryptographic algorithm can be implemented to ensure more data security from malicious activity.Apart from this,some access control techniques can also be included to perform the access control and authenticate the user before data transmission.The future work of the proposed system will be extended by improving the speed of decryption process.

Bibliography

[1] Swarna C1, Marrynal S. Eastaff2 Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES ISSN NO: 2394-8442 VOLUME 5, ISSUE 3, MAR 2018 http: iaetsdjaras.org

[2] Aditya Poduval1, Abhijeet Doke2, Hitesh Nemade3, Rohan Nikam4 Secure File Storage on Cloud using Hybrid Cryptography

[3] Taufik Hidayata,1, Rahutomo Mahardikob,2 "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing", International Journal Of Artificial Intelegence Research ISSN: 2579-7298 Vol 4, No 1, June 2020, pp. 49 – 57 DOI: 10.29099 ijair.v4i1.154

[4] Atanu Basu, "Secure Cloud Storage Scheme Based On Hybrid Cryptosystem"

[5] B. Rakesh1, K. Lalitha1, M. Ismail1 and H. Parveen Sultana2 "DISTRIBUTED SCHEME TO AUTHENTICATE DATA STORAGE SECURITY IN CLOUD COMPUTING" International Journal of Computer Science and Information Technology (IJCSIT) Vol 9, No 6, December 2017 DOI:10.5121 ijcsit.2017.9606

[6] Kranthi Kumar K[1], Devi T[2] "Secured Data Transmissionin Cloud Using Hybrid Cryptography" volume 119 No. 16 2018,3257-3262 ISSN: 1314-3395 (on-line version) url: http://www.acadpubl.eu hub

[7]Vinita Keer, Dr. Syed Imran Ali, Prof. Neeraj Sharma, "Hybrid Approach of Cryptographic Algorithms in Cloud Computing",International Journal of Emerging Technology and Advanced Engineering.

[8]Priyajaiswal, Randeepkaur, Ashok Verma, "Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 1, January 2014)

[9] PERFORMANCE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS FOR CLOUD SECURITY Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018) IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

[10] Shakeeba S. Khanand Prof.R.R. Tuteja, "Security in Cloud Computing using

Cryptographic Algorithms" Vol. 3,Issue 1, January 2015.
[11] Bhale Pradeepkumar Gajendra, Vinay Kumar Singh, More Sujeet "Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption"IEEE(2016) DOI: 10.1109/CCAA.2016.7813920 PP 1304-1309
[12]V.K Soman and V. Natarajan, "An enhanced hybrid data security algorithm for cloud", International Conference on Networks and Advances in Computational Technologies, pp. 416-419. doi: 10.1109/NETACT.2017.8076807, 2017.
[13] N. Subramanian and A. Jeyaraj. "Recent security challenges in cloud computing"' Computers and Electrical Engineering,28(42). Doi:10.1016/j.compeleceng.2018.06.006, 2018.
[14] Nikhil Gajra. "Private Cloud Security: Secured user Authentication by using Enhance Hybrid Algorithm" 2014 International Conference on Advances in Communication and Computing Technologies 978-1-4799-7319-4/14/ 2014 IEEE
[15] S.V.N.Srivalli, Ben SwarupMedikonda, "Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019 Retrieval Number F2947037619/19 BEIESP
[16] Dhuratë Hyseni and Besnik Selimi," The Strategy of Cryptography for the Proposed Model of Security in Cloud Computing" IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017) 978-1-5386-0814-2/17/ 2017 IEEE
[17] Chauhan, N. S., and Saxena, A. (2013). Cryptography and Cloud Security Challenges. CSI Communications.
[18] Puzio, P., Molva, R., Onen, M., and Loureiro, S. (2013, December). ClouDedup: secure deduplication with encrypted data for cloud storage.
[19] Ali Abdulridha Taha, 2 Dr. Diaa Salama AbdElminaam, 3 Prof.. Khalid M Hosny "Enhancement the Security of Cloud Computing using Hybrid Cryptography Algorithms" International Journal of Advancements in Computing Technology(IJACT) Volume9, Number3, Dec. 2017
[20] B. M. Kore 1, Archana Jadhav 2 "A Literature Survey on Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem", B. M. Kore et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1511-1513
[21] Aditya SadanandGhadi," Secure File Storage Using Hybrid Cryptography", Volume 5, Issue 12, December – 2020 IJISRT20DEC144
[22]Maitri, P. V., and Verma, A. (2016). Secure file storage in cloud computing using a hybrid cryptography algorithm. 2016 International Conference on Wireless

Communications, Signal Processing and Networking (WiSPNET), 1635–1638. https://doi.org/10.1109/wispnet.2016.7566416
[23] Joseph Selvanayagam1, Akash Singh2, Joans Michael3, Jaya Jeswani4 "SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY", Volume: 05 Issue: 03 2018, IRJET
[24] S. Delfin1, Rachana Sai. B2, Meghana J.V3, Kundana Lakshmi. Y4, Sushmita Sharma5 "CLOUD DATA SECURITY USING AES ALGORITHM", Volume: 05 Issue: 10 — Oct 2018
[25] Shweta Kaushik, "Cloud data security with hybrid symmetric encryption", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT) 978-1-5090-0082-1/16/ 2016 IEEE
[26] Shweta Kaushik, Ashish Patel, "Secure Cloud Data Using Hybrid Cryptographic Scheme", 978-1-7281-1253-4/19/2019 IEEE
[27] Mohit Manoj Vinchoo, Suhas Sudhir Kadam, "Grey Immune : Security in Hybrid Cloud", Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS 2017) IEEE Xplore Compliant - Part Number:CFP17M19-ART, ISBN:978-1-5386-1959-9 978-1-5386-1959-9/17/ 2017 IEEE
[28] Nagasai Lohitha Kodumru, Supriya M, "Secure Data Storage in Cloud using Cryptographic Algorithms", 978-1-5386-5257-2/18/ 2018 IEEE
[29] Lalit Kumar, Dr. Neelendra Badal, "A REVIEW ON HYBRID ENCRYPTION IN CLOUD COMPUTING", 978-1-7281-1253-4/19/ 019 IEEE
[30] Punam V. Maitri, "Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm", This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference 978-1-4673-9338-6/16/ 2016 IEEE

Brief Bio-Data

Chandana K S

4PM17CS025

Department of Computer Science and Engineering

PESITM, Shivamogga

Phone: +91 8618308717

Email: kschandana197@gmail.com

Permanent Address

Chandana K S

D/o N S Kedarnath and Nagarathna

Chandana Opticals, Near LIC office, S S Road,

Shikaripura

Shivamogga (dist), 577427.

Karnataka, INDIA.

Father Phone: +91 9449968232

Mother Phone: +91 9448873760

Qualification

B.E in Computer Science and Engineering, Visvesvaraya Technological University,

Achievements

Attended IEEE workshops and competition. Being IEEE member organized many events. Coursera certification in cloud computing domain.

Deepa Kajjera

4PM17CS028

Department of Computer Science and Engineering

PESITM, Shivamogga

Phone: +91 9591849122

Email: deepalkajjera@gmail.com

Permanent Address

Deepa Kajjera,

D/o Lingamurthi and Sharada

Doddikoppa, moddy- post,

Soraba -tq, Shivamogga- dist, pincode-577413

Shivamogga (dist), 577427.

Karnataka, INDIA.

Father Phone: +91 9611246564

Mother Phone: +91 6363555680

Qualification

B.E in Computer Science and Engineering, Visvesvaraya Technological University, Belgaum Karnataka 2021.

Achievements

Attended IEEE workshops and competition. Coursera certification in cloud computing domain and NPTEL course.

Meghana Shrinivas Bhat

4PM17CS046

Department of Computer Science and Engineering

PESITM, Shivamogga

Phone: +91 9686342518

Email: bhatmeghana03@gmail.com

Permanent Address

Meghana Shrinivas Bhat

D/o A B Shrinivas Bhat and Jayashree S Bhat

K C Circle, Haliyal Road, Dandeli 581325

Karnataka, INDIA.

Father Phone: +91 8148286616

Mother Phone: +91 7204526628

Qualification

B.E in Computer Science and Engineering, Visvesvaraya Technological University, Belgaum Karnataka 2021.

Achievements

Attended IEEE workshops and competition. Being IEEE member organized many events. Completed Cloud Computing course in Coursera. Placed in Prolifics.

Monali S Patel

4PM17CS049

Department of Computer Science and Engineering

PESITM, Shivamogga

Phone: +91 9449469441

Email: monalipatel738@gmail.com

Permanent Address

Monali S Patel

D/o Sanjay G Patel and Hiteshri S Patel

Sri Hari Nivas, opposite Guptha General Store, near Manjunath Talkies,

MKK road, Shivamogga-577202

Karnataka, INDIA.

Father Phone: +91 9480023151

Mother Phone: +91 9481950927

Qualification

B.E in Computer Science and Engineering, Visvesvaraya Technological University, Belgaum Karnataka 2021.

Achievements

Attended IEEE workshops. Completed Cloud Computing course and UX/UI Design in Coursera. Attended online Cyber Security Workshop.

Guide profile

Mrs. Thara K L

Assistant Professor

Computer Science and Engineering

PESITM, Shivamogga

Email id: thara@pestrust.edu.in

Qualifications

B.E in CSE

M.Tech in CSE

Experience

Assistant Professor, Dept. of CS&E at PESITM, Shivamogga from August 2012 till date.

Workshops Attended

Four days Faculty Development Program on Teaching and Learning held at PESITM, Shivamogga on 20th to 23rd July 2015.

Five days Faculty Development Program on Research Methodologies held at PESITM, Shivamogga on 19th to 23rd January 2015.

Courses Taught

Data Structure with C, Object-Oriented Programming with C++, Unix System/Shell Programming, System Software, Cloud Computing, Operating System and many more.