**A MINI PROJECT ABSTRACT REPORT**

on

**Secure File Storage on Cloud Using Hybrid Cryptography**

Submitted to Jawaharlal Nehru Technological University for the partial

Fulfillment of the Requirement for the Award of the Degree of

**BACHELOR OF TECHNOLOGY**

**In**

**COMPUTER SCIENCE AND ENGINEERING**

By

**VYAS ANAND - 19Q91A05H9**

**GADDI KARTHIK REDDY - 19Q91A05E0**

**KOLIPAKA CHAITANYA RAJ - 20Q95A0509**

**SHAIK SAMEER - 18Q91A0555**

Under the guidance of

**Mrs. G.DEVI**

**ASSISTANT PROFESSOR**

****

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**MALLA REDDY COLLEGE OF ENGINEERING**

**(**Approved by AICTE-Permanently Affiliated to JNTU-Hyderabad)

Accredited by NBA & NAAC, Recognized section 2(f) & 12(B) of UGC New Delhi ISO 9001:2015 certified Institution

Maisammaguda, Dhulapally (Post via Kompally), Secunderabad- 500100

**2022 – 2023**

**ABSTRACT**

High-speed networks and ubiquitous Internet access become available to users for access anywhere at any time. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Cloud storage is a model of networked [online storage](http://en.wikipedia.org/wiki/Online_storage) where data is stored in virtualized pools of storage which are generally hosted by third parties. [Hosting](http://en.wikipedia.org/wiki/Internet_hosting_service) companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them.

The [data center](http://en.wikipedia.org/wiki/Data_center) operators, in the background, [virtualize](http://en.wikipedia.org/wiki/Storage_virtualization) the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers.

Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. A decentralized erasure code is suitable for use in a distributed storage system.

We construct a secure cloud storage system that supports the function of secure data forwarding by using an AES and Proxy re encryption. In this model initial phase owner will upload the data with AES Encryption. Next phase, inside of cloud again the data has divided into small pieces, for this process we will apply a dividing key. Data will place in different storage lactations. The information of data storage will monitor by a unique data distributors. If the valid user accessing the data cloud will retrieve the data as reversible manner.

**Keywords*:***

CLOUD COMPUTING,

AES ALGORITHM,

DATA SECURITY,

STORAGE,

CRYPTOGRAPHY.

**INDEX**

**CONTENTS PAGE NO**

1. **AIM 4**
2. **OBJECTIVES 4**
3. **INTRODUCTION 5**
4. **EXISTING SYSTEM 6**
   1. **EXISTING SYSTEM DRAWBACKS**
5. **PROPOSED SYSTEM 7**
   1. **PROPOSED SYSTEM ADVANTAGES**
6. **APPLICATIONS 8**
7. **SYSTEM ARCHITECTURE 9**
8. **MODULES 11**
   1. **MODULES DESCRIPTION**
9. **SYSTEM REQUIREMENTS 13**
   1. **SOFTWARE REQUIREMENTS**
   2. **HARDWARE REQUIREMENTS**

**REFERENCES**

**AIM**

Cloud has gained popularity in recent years with it being utilized in many fields such as military, health, industries, institutions, etc. in storage of bulk data. Cloud has an advantage as one can. access or retrieve the data on users request without necessarily accessing directly the server computer. However, security of the data stored online have raised concerns over the years, therefore, new techniques have been developed to secure the data stored online. One of the most used is the use of Hybrid Cryptography Algorithm. The system ensures total confidentiality because even if there is a security breach, the attacker will only access the encrypted data. Hybrid cryptography utilizes the AES and SHA algorithms, where key encryption is done by the SHA while data encryption is done by the AES. The aim of the project is to evaluate the security of online data under hybrid cryptography algorithm by analyzing the application of the system and exploring the direction of hybrid cryptography technology.

**OBJECTIVES**

* The propose an uprightness check plan for their framework to upgrade information strength against capacity server defilement, which returns altered cipher texts.
* More flexible adjustment between the number of storage servers and robustness.
* This hybrid approach when implemented in a cloud server makes the remote server more secure and thus, helps the cloud providers to do their work more securely
* For data security and privacy protection problems, the fundamental challenge of separation of sensitive data and access control is fulfilled
* only an authorized person can access data from the cloud server
* Ciphertext data is visible for all people. But for that again the decryption technique has to be used to translate it back into the original text.

**INTRODUCTION**

Cloud computing is originated from earlier large-scale distributed computing technology. NIST defines Cloud computing as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g.,networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. In Cloud computing, both files and software are not fully contained on the user’s computer. File security concerns arise because both user’s application and program are residing in provider premises. The cloud provider can solve this problem by encrypting the files by using encryption algorithm. This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid encryption is used where files are encrypted and secured communication between users and the servers.

Data Security Issues:

* Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:
* Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a particular resource that has a threat or has been compromised.
* According to service delivery models of Cloud computing, resources and cloud services may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.
* Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

**EXISTING SYSTEM**

In Existing System we use a straightforward integration method. In a straightforward integration method Storing data in a third party’s cloud system causes serious concern on data confidentiality. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages. When he wants to use a message, he needs to retrieve the

Codeword symbols from storage servers, decode them, and then decrypt them by using cryptographic keys. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. A Decentralized architecture for storage systems offers good scalability, because a storage server can join or leave without control of a central authority

**EXISTING SYSTEM DRAWBACKS**

* The user can perform more computation and communication traffic between the user and storage servers is high.
* The user has to manage his cryptographic keys otherwise the security has to be broken.
* The data storing and retrieving, it is hard for storage servers to directly support other functions.

**PROPOSED SYSTEM**

In our proposed systemwe address the problem of forwarding data to another user by storage servers directly under the command of the data owner. We consider the system model that consists of distributed storage servers and key servers. Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers that shall perform cryptographic functions on behalf of the user. These key servers are highly protected by security mechanisms.

Here Storage system has allocates by different data container. Once owner uploads the data with AES encryption mechanism, system again takes the data and makes Secure Data segregation process. All the data pieces will be save in different location in cloud storage. Here public distributor monitors all the data and corresponding positions where it is saved. When a proper client asking the data, cloud system will provide the data in reversible manner. So our system will prevent our data from both Inside and Outside attackers.

**PROPOSED SYSTEM ADVANTAGES**

* Tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.
* The storage servers independently perform encoding and re-encryption process and the key servers independently perform partial decryption process.
* More flexible adjustment between the number of storage servers and robustness.

**APPLICATIONS**

This study brings out the academic and theoretical aspect of data encryption and confidentiality into a real life working software. This project would result in the building of a software  that can be further used for research purposed for the function of improvement in data security.

The scope of the study would be contained and limited to relatively smaller file formats like texts, images, some small sized audio and videos. The reason for these limits placed on them is to ensure that the small cloud space budgeted is not exhausted in the course of testing and deployment. Large cloud space for storage also correlates with a large fee for the cloud service.

A more notable use of encryption is to encrypt the entire drive, and require correct credentials to access it. without the user logging in the data on the drive is completely opaque. If someone took the drive and tried to read it, they would not be able to access any data. This has the occasional side effect of locking the system, so some UCL readers may have had to request the recovery key.

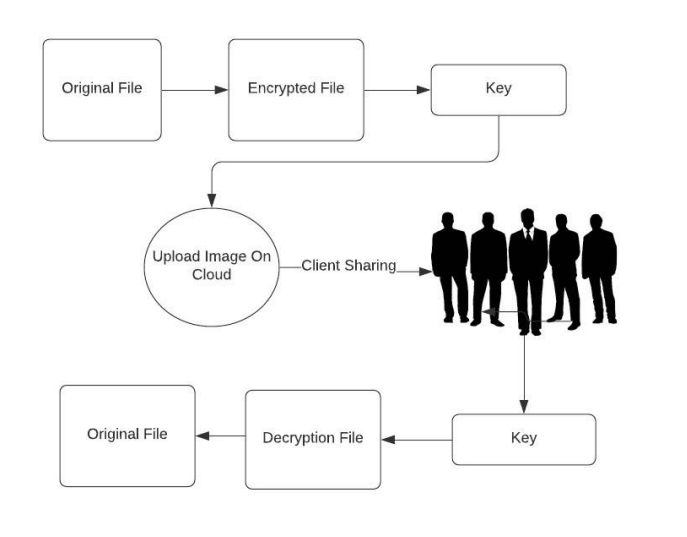
**SYSTEM ARCHITECTURE**

FILE UPLOAD TO SERVER

PROXY RE ENCRYPTION

DOWNLOAD THE DATA

ENCRYPT THE DATA



**MODULES**

1. Registration
2. Sharing Data
3. Secure Cloud Storage
4. Proxy re-encryption
5. Data retrieval

**MODULE DESCRIPTION**

**Registration:**

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.

**Sharing Data:**

The canonical application is data sharing. The public auditing property is especially useful when we expect the delegation to be efficient and flexible. The schemes enable a content provider to share her data in a confidential and selective way, with a fixed and small ciphertext expansion, by distributing to each authorized user a single and small aggregate key.

**Secure Cloud Storage:**

 Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. A decentralized erasure code is suitable for use in a distributed storage system.

**Proxy re-encryption:**

Proxy re-encryption schemes are crypto systems which allow third parties (proxies) to alter a cipher text which has been encrypted for one user, so that it may be decrypted by another user. By using proxy re-encryption technique the encrypted data (cipher text) in the cloud is again altered by the user. It provides highly secured information stored in the cloud. Every user will have a public key and private key. Public key of every user is known to everyone but private key is known only the particular user.

**Data retrieval:**

Reports and data are the two primary forms of the retrieved data from servers. There are some overlaps between them, but queries generally select a relatively small portion of the server, while reports show larger amounts of data. Queries also present the data in a standard format and usually display it on the monitor; whereas reports allow formatting of the output however you like and is normally retrieved.

**SYSTEM REQUIREMENTS**

**SOFTWARE REQUIREMENTS**

* Language (backend)         : Java, JSP
* Web Server       : Tomcat 6
* Operating System : Windows 7 32 Bit
* Front end :HTML,CSS, JS
* Storage software : SQLyog, MySQL
* IDE :Netbeans

**HARDWARE REQUIREMENTS**

* Main Processor               : 2GHz
* Ram                                : 512 MB (min)
* Hard Disk                       : 80 GB

**REFERENCES**

**IEEE, research\_gate Doc: Jan 2019**

Link:https://www.researchgate.net/publication/330326211Multiplex\_assay\_f\_or multiomics\_advances in personalized-precision medicine