2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

# SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

[1,2,3,4] **Pavan Kuthuru, Avula Shiva Prasad Yadav, Sowmya Sri Abisetty, Eran Sai Rishitha,** [5]**DR Radha Devi**

[1,2,3,4] Ug scholars, MallaReddy college Of Engineering , Hyderabad - 500100
[5] Assistant Professor, MallaReddy college Of Engineering , Hyderabad – 500100

## 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 where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them.

## CHAPTER - 1

## INTRODUCTION

### 1.1INTRODUCTION

Cloud storage is a service model in which data in maintained, managed and backed up remotely and made available to user over a network. Having your data stored offsite in the cloud makes it accessible from anywhere without the hassle of maintaining your own local storage and file- serving systems. It makes all the difference in a disaster, too.

This cloud storage system, having collection of storage servers these are providing long term storage service over the internet. Storing the data into third party’s cloud system causes concern over data confidentiality. In this cloud some general encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data.

## CHAPTER - 2

## LITERATURE SURVEY

### 2.1 LITERATURE SURVEY

**Literature survey 1:-**

**Title:-** On the impact of erasure coding parameters to the reliability of distributed brick storage systems

**Year:-** 2009

**Authors:-** Xiangyu Luo Yun Wang Zhuowei Shen

**Abstract:-**

The amount of storage overhead, erasure coding offers a higher degree of survivability than pure replication. They propose a method that can quantitatively evaluate these effects. Besides relationships among other reliability-affecting factors such as storage overhead, repair bandwidth and single brick's properties are also investigated**.**

**Literature survey 2:-**

**Title:-** On the speedup of recovery in large-sale erasure-coded storage system

**Year:-** 2014

**Authors:-** Y. ZHU, P. P. C. LEE, Y. XU, Y. HU, AND L. XIANG

**Abstract:-**

- Modern storage systems stripe redundant data across multiple nodes to provide availability guarantees against node failures.

- One form of data redundancy is based on XOR-based erasure code.

# CHAPTER - 3

# SYSTEM ANALYSIS

## 3.1 EXISTING SYSTEM

In Existing System we use a straightforward integration method. In 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.

## 3.2 DRAWBACKS

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

## 3.3 PROPOSED SYSTEM

In our proposed system we 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.

### 3.4 ADVANTAGES

1. Tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.
2. The storage servers independently perform encoding and re-encryption process and the key servers independently perform partial decryption process.

### 3.5 SYSTEM REQUIREMENTS

**Hardware:**

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

**Software:**

- Language : Java
- Software :JDK,Net NetBeans IDE 8.0.2,SQLyog
- Web Server : Glassfish
- Operating System : Windows 7 32 Bit

## CHAPTER - 4 SYSTEM DESIGN

### 4.1 SYSTEM ARCHITECTURE

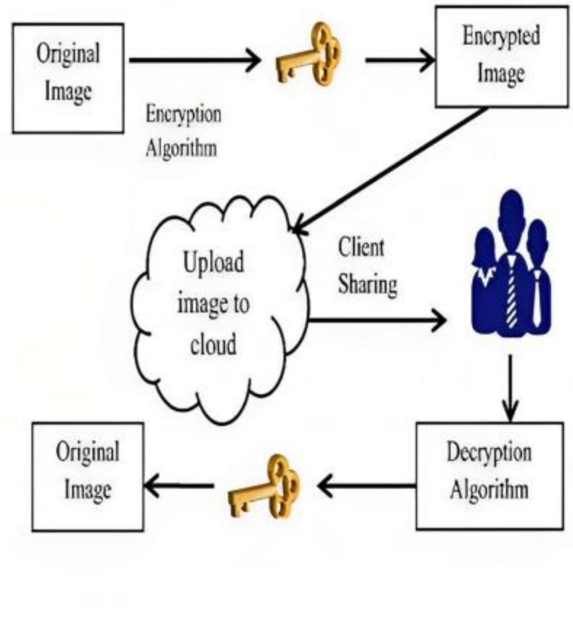
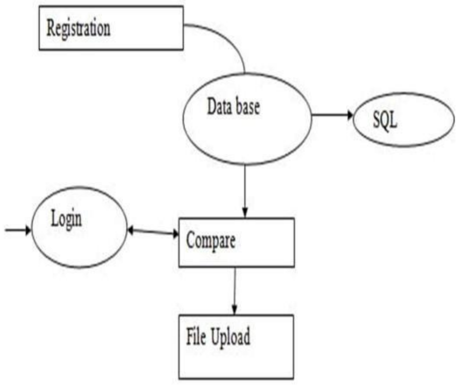


Fig4.1.1.secure file storage on cloud using hybrid cryptography

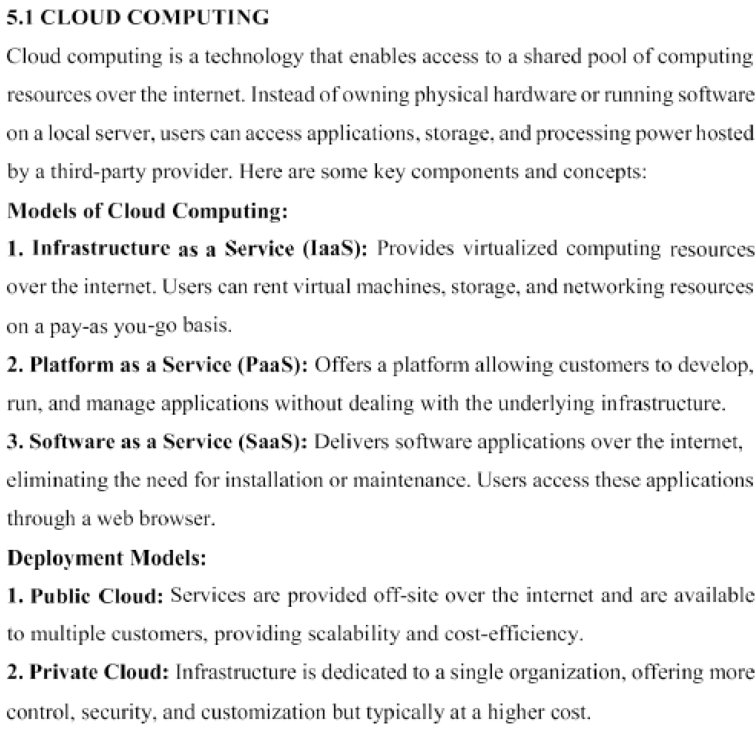
4.3 UML DIAGRAMS DATA FLOW DIAGRAM:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system.

Level 0:



## CHAPTER - 5 SYSTEM IMPLEMENTATION



### 5.1 CLOUD COMPUTING

Cloud computing is a technology that enables access to a shared pool of computing resources over the internet. Instead of owning physical hardware or running software on a local server, users can access applications, storage, and processing power hosted by a third-party provider. Here are some key components and concepts:

**Models of Cloud Computing:**

**1. Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet. Users can rent virtual machines, storage, and networking resources on a pay-as you-go basis.

**2. Platform as a Service (PaaS):** Offers a platform allowing customers to develop, run, and manage applications without dealing with the underlying infrastructure.

**3. Software as a Service (SaaS):** Delivers software applications over the internet, eliminating the need for installation or maintenance. Users access these applications through a web browser.

**Deployment Models:**

**1. Public Cloud:** Services are provided off-site over the internet and are available to multiple customers, providing scalability and cost-efficiency.

**2. Private Cloud:** Infrastructure is dedicated to a single organization, offering more control, security, and customization but typically at a higher cost.

## CHAPTER - 6 TESTING

### 6.1 TESTING

**The various levels of testing are**

1. White Box Testing
2. Black Box Testing
3. Unit Testing
4. Functional Testing

**1. White Box Testing**

White-box testing (also known as

clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing).

### 2. Black Box Testing

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings (see white-box testing).

### 3. Unit Testing

In computer programming, unit testing is a method by which individual units of source code, sets of one or more computer program modules together with associated control data, usage procedures, and operating procedures are tested to determine if they are fit for use.

### 4. Functional Testing

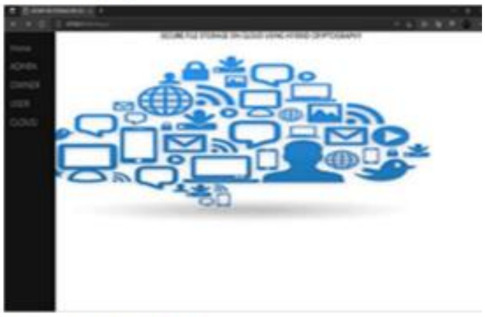
Functional testing is a quality assurance (QA) process and a type of black box testing that bases its test cases on the specifications of the software component under test.

## CHAPTER - 7

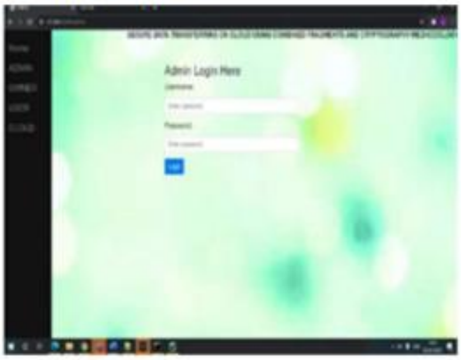
## RESULTS

### 7.1 SCREEN SHORTS

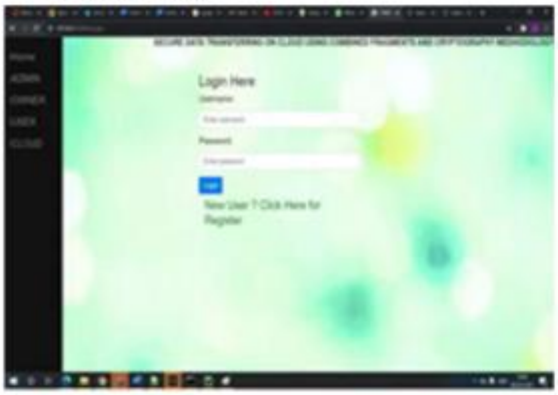
i. Homepage



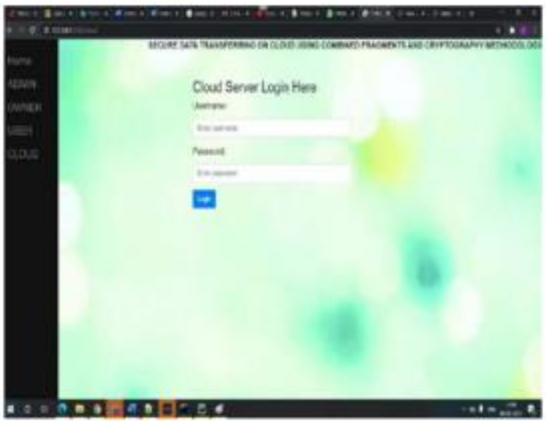
ii. Admin Login Page



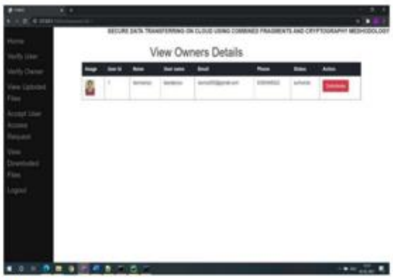
i. User Login Page


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY METHODOLOGY
Home
ADMIN
OWNER
USER
CLOUD
Login Here
Username
Password
Login
New User ? Click Here for Register

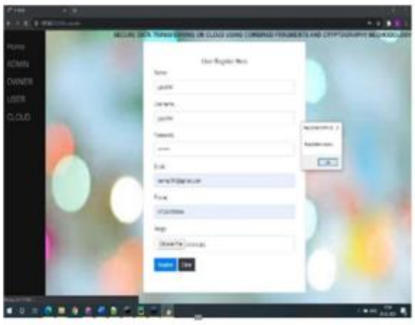
ii. Cloud Login Page


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY METHODOLOGY
Home
ADMIN
OWNER
USER
CLOUD
Cloud Server Login Here
Username
Password
Login

ii. Admin Verifying Owner


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY METHODOLOGY
View Owners Details
Home
Logout

iii. User Registration Form


SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY METHODOLOGY
Home
ADMIN
OWNER
USER
CLOUD

## CHAPTER - 8 CONCLUSION

### 8.1 CONCLUSION

Erasure codes are promising for improving the reliability of the storage system due to its space efficiency compared to the replication methods. Traditional erasure codes split data into equal sized data blocks and encode strips in different data blocks.

## CHAPTER - 9 FUTURE ENHANCEMEN T

### 9.1 FUTURE ENHANCEMENT

As a response, erasure coding as an alternative to backup has emerged as a method of protecting against drive failure. Raid just does not cut it in the age of high-capacity HDDs. The larger a disk's capacity, the greater the chance of bit error. And when a disk fails, the Raid rebuild process begins, during which there is no protection against a second (or third) mechanism failure.

## REFERENCES

1. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” J. Soc. Ind. Appl. Math., vol. 8, no. 2, pp. 300–304, 1960.
2. J. S. Plank and L. Xu, “Optimizing Cauchy Reed-Solomon codes for faulttolerant network storage applications,” in Proc. IEEE Int. Symp. Netw. Comp. Appl., 2006, pp. 173–180.
3. M. Blaum, J. Brady, J. Bruck, and J. Menon, “EVENODD: An efficient scheme for tolerating double disk failures in RAID architectures,” IEEE Trans. Comput., vol. 44, no. 2, pp. 192– 202, Feb. 1995.
4. P. Corbett, et al., “Row-diagonal parity for double disk failure correction,” in Proc. 3rd USENIX Conf. File Storage Technol., 2004, pp. 1–14.