ISSN No:-2456-2165

A Secure Reliable Erasure Code-Based Cloud Storage System with Data Forwarding

Nupur[1], B.Kalyan[2], O.Mrudula[3], Gunda Sai Harish[4], J.Maniksharan[5]
[1,2,4,5]B.Tech (IV) Year Student , Department of Computer Science and Engineering
SRM Institute of Science and Technology, Chennai, India
[3,]Assistant Professor, Department of Computer Science and Technology
SRM Institute of Science and Technology, Chennai, India

Abstract:- **The project entitled as "A Secure Reliable Erasure Code-Based Cloud Storage System with Data Forwarding" is a secure cloud storage system that supports the function of secure data forwarding by using a threshold proxy re-encryption scheme. This system is highly distributed and secured where storage servers independently encode and forward messages and key servers independently perform partial decryption. High-speed networks and ubiquitous Internet access become available to users for access anywhere at any time. This technology of computing is a notion which provides possessions on the Internet by way of an combined component, a cloud. It stores an archetypal of schmoozed accessible storage where facts is kept in virtualized tarns of storage which are commonly hosted by third parties. Holding companies operate enormous data centers, and people who require their data to be presented buy or tenancy storage aptitude from them. The records epicenter operatives, in the appropriate, virtualized the belongings according to the wishes of the customer and interpretation them as stowage slicks, which the customers can themselves use to hoard files. Substantially, the source may extent diagonally various servers.**

Keywords:- *Distributed File System; Erasure Code; Load Balancing; Cloud.*

I. INTRODUCTION

According to today's world of technology, an incredible volume of informations is being boomed over the Internet. This technology offers stowage to this data to the cloud on the Internet and at the same time act as a warehouse in which the files is to be maintained and therefore made available to the consumers for the entire world. These building of technologies for cloud comprises distributed file systems, erasure code, Advance Encryption Standard and so onwards. Organization of various facts in cloud needs an unusual sort of system which can be identified as distributed file system, that has high performance and security feature of conventional file systems and also they provide degrees of transparency to the users, heterogeneity, and imitation transparency as well. This file system provides the effective concept to every client such that all the data are located closer to each other. Usually, it comprises of architecture in which the server which preserves over the worldwide reference book and all the data and metadata statistics of all the base servers whereas, it represents a server that preserves the record which is connected to boss server and other storage servers as well. This type of storage server knobs the thousands of consumer desires in DFS. The distribution of requests are based on these storage servers is rutted which then leads to overall degradation. These are not exploited, as some of the servers acquires a lot many requests and endure idle. In this system, load can be in positions of demands handled by a server or stowage size of that server equally. In this paper, we have intended a methodology for load balancing of the request of clients to be handled by a server. Thus, we have planned a policy to balance the load of requests for overloaded servers and sites in a distributed file system. During load balancing parameters like CPU utilization, storage utilization, buffer space, and network bandwidth plays a key role. Load balancing using these parameters might be difficult so an intelligent way is required to handle each server efficiently.

II. OBJECTIVE

The importance of this process is to construct a secure cloud storage system that enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Threshold proxy re-encryption scheme which supports decentralized erasure codes is used to construct highly distributed storage system. The major objectives of this project are:

- To provide free online storage system
- Ensuring secure data forwarding
- Reducing the computational overhead and minimizing the storage size of the storage servers
- Using eraser codes for recovering the failure servers and providing high secure storage system by enabling threshold proxy re-encryption scheme.

III. SYSTEM ARCHITECTURE

The system consider the 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 distributed systems require independent servers to perform all operations and for that a novel beginning proxy re-encryption arrangement was anticipated and assimilated with a sheltered regionalized code to form a secure dispersed storage system.

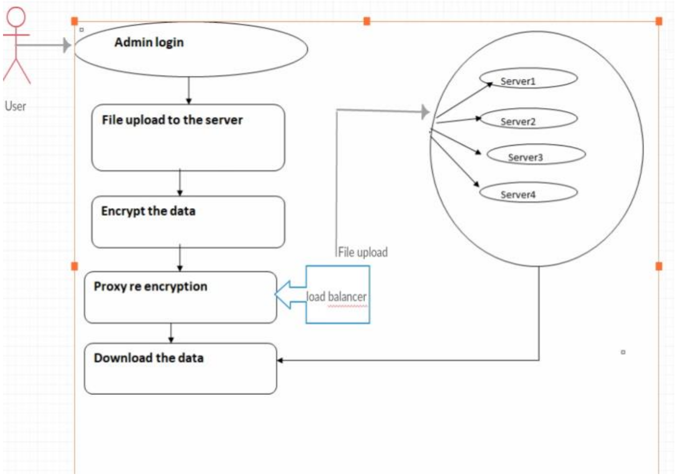

Fig 1:- System Overview

These key servers are exceedingly endangered by sanctuary contrivances. The encryption scheme supports encoding tasks over encrypted memos and accelerating procedures over encrypted and encoded messages.

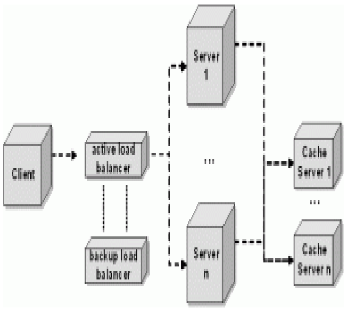

Fig 2:- Overall Architecture

A. Advantages

- Snug assimilation of programming, encryption, and forwarding makes the storage system proficiently come across the necessities of data sturdiness, data confidentiality, and data forwarding.
- The loading servers independently accomplish translating and re-encryption procedure and the key servers autonomously perform the process of decryption.
- Flexible adjustment between the number of storage servers and robustness will increase.

B. System Specification

Hardware Requirements

PROCESSOR	:	Pentium III & above
RAM	:	256MB
HARD DISK	:	40GB

Software Requirements

OPERATING SYSTEM	:	Windows XP
FRONT END	:	Java
BACK END	:	MY SQL

C. Drawbacks of Existing System

- Computation and communication traffic between the user and storage servers is huge.
- The user has to manage his symmetric and asymmetric keys otherwise the security has to be broken.
- The data storing and retrieving, it is hard for storage servers to directly support other functions.

IV. PROJECT DESCRIPTION

Cloud computing has turn out to be a social portent used by utmost people every day. Fundamentally, cloud stowage permits users to upload specific data from their private drives to an Internet server. Through this in case any lost of original files can be obtained easily. It provides access to the files stored in the cloud for other devices, and sometimes also enable access to the documents for other people to. As with every important social singularity there are matters that limit its prevalent assumption.

- The robustness of data is a major requirement for storage systems. In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the perfection and accessibility of the data files being stockpiled on the dispersed cloud servers must be assured. One of the key subjects is to meritoriously detect any unapproved data modification and dishonesty, perhaps due to server concession and disasters.
- Storing data in a third party's cloud system causes serious confidentiality for messages in storage servers, straightforward integration of encryption and encoding was used. There are some problems in the above straightforward integration of encryption and encoding.
- The user has to do utmost calculation and the communication traffic among the handler and storage servers is high.
- The handler has to accomplish his cryptographic keys. If the user's device of loading the keys is mislaid or conceded, the haven is smashed.
- Further data loading and regaining, it is stiff for stowage servers to openly support other roles such as data progressing.
- It is difficult for forwarding data to another user by storage servers directly under the command of the data owner. Stowage servers cannot openly headlong a user's posts to another one. The owner of messages has to retrieve, decode, decrypt and then forward them to another user.

A. Overview of the Project

The purpose of this process is to construct a cloud storage system that enables users to remotely store their data with confidentiality and functionality.

Data robustness is provided by replicate a message such that each stowage server provisions a replica of the memo. It is very vigorous as the memo can be recovered as long as one storage server subsists.

A reorganized erasure code is a code that freely figures each code term symbol for a missive. The various letdown servers is under the lenience dawn of the erasure code, the note can be mended from the code word ciphers stored in the offered storage servers by the decrypting method. This delivers an interchange between the stowage size and the lenience onset of letdown servers.

A storage server disappointment is demonstrated as an erasure slip of the stored code term icon.

Secure cloud stowage system provisions the purpose of vulnerable data dispatching by using a threshold alternative re-encryption scheme which is combined with a secure decentralized code to form a secure dispersed storage system. The encryption structure cares reorganized erasure codes over encrypted messages and progressing tasks over encrypted and encoded messages.

System considers the model that consists of distributed storage servers and key servers. Since loading cryptographic keys in a sole device is unsafe, a worker allots his cryptographic key to key servers that shall achieve cryptographic functions on behalf of the operator. These key servers are highly protected by security mechanisms.

B. Database Design

A database is a systematized apparatus that has the proficiency of durable evidence through which a user can recover stored information in an active and effective manner. The process of creating a thorough data in a prototypical manner is named as Database Design.

It is a two level process. In the first step, user necessities are noted and a database is planned which will meet the needs of the user as clearly as possible .this step is called information level design.

In the second step, these information level designs are transferred into a project for the precise DBMS that will be used to implement the system in question. This process is called as physical level design. It is aimed to achieve the following two major objectives.

- Data integrity
- Data independence

The database design can also be used to spread over the whole process of scheming, not just the base data edifices, but also the methods are used as a portion of the overall database solicitation within the database managing system.

C. Input Design

It is a part of inclusive system policy. The key detached during this is as given below-

- To produce a cost effective method of input
- To achieve the highest possible level of accuracy
- To ensure that the input is acceptable and understood by the user.

In information systems the input data are entered according to the format, which is already defined in accurate input data are the most common case of error in data entry, these can be controlled by proper input design.

Input design is a process of converting user organized input to a computer based format. Input data are precise and organized into clutch of similar data. The objective of scheming input facts is to style data entry as easy, logical and free from errors as possible.

The user has to register by giving user name, password, E-Mail ID, mobile number and user product key. After that random image registration page will appear, and user has to browse the images randomly.

D. System Implementation

It is the phase of the assignment when the conjectural strategy is turned out into a waged system. Thus it can be stately to be the most hazardous stage in following a fruitful innovative system and in giving the user, self-reliance that the new system will graft and be effective.

This stage includes watchful forecasting, exploration of the prevailing system and its constrictions on enactment, designing of methods to achieve switch assessment of swop systems.

The proposed system was developed using Net beans IDE. The existing system caused several integrity and security problems but the proposed system has a very good user friendly online storage system with secured data forwarding.

V. CONCLUSION

Fabricating a protected storage system that wires numerous tasks is stimulating when the storage system is scattered and has no essential expert. To decrypt a message of k blocks that are encrypted and encoded to n code word symbols, each key server only has to partially decrypt two code word symbols in our system. By using the verge proxy re-encryption pattern, we extant a safe cloud stowage system that provides secure data storage and secure data progressing functionality in a dispersed construction. Additionally, each storage server individually performs re-encryption and each key server execute to a limited decryption.

REFERENCES

[1]. S. Sree Vivek, S. Sharmila Deva Selvi, V. Radhakishan, C. Pandu Rangan, “efficient conditional proxy re encryption with chosen cipher text security”, International Journal of Network

[2]. R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker, “Total Recall: System Support for Automated Availability Management,” Proc. First Symp. Networked Systems Design and Implementation (NSDI), pp. 337-350, 2004.

[3]. K.D. Bowers, A. Juels, and A. Oprea, “HAIL: A High-Availability and Integrity Layer for Cloud Storage,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS), pp. 187-198, 2009.

[4]. http://www.ijarcsse.com