

# FTFT : Fault Tolerance with Fragmentation Technique for Cloud Storage Security

Babitha. R, Shilpa. V

School of Computing & Information Technology REVA University, Bangalore, Karnataka, India

## ABSTRACT

All the corporate people practicing to store the data in cloud storage. Most of the corporate build hybrid cloud structure in uploading data into cloud storage. In this system we propose a new novel idea FTFT Fault Tolerance Fragmentation technique for cloud storage security. When user uploads a file into the cloud storage the file is divided into N Blocks and for all the N blocks hash codes will be generated for integrity check. Then the blocks are stored in two cloud storage places to provide fault tolerance. When one cloud storage goes down the relevant blocks are retrieved from secondary cloud storage. By this we are providing high level of security and performance in cloud storage. Moreover, the FTFT technique does not rely upon the obsolete cryptographic strategies for information putting away and furthermore for the information security.

**Keywords :** Fragmentation Technique, Cloud Storage Security, Fault Tolerance

## I. INTRODUCTION

There are large benefits that exist by means of cloud computing to comfort association between users and establishments, and it also depends on safety and privacy of cloud services and the data of the user .it may be prevent by some users and group [1].cloud Users can manage their resources and particular service through a web interface that is provided by the cloud service Provider Ex.AWS. Resources sharing that exist in the cloud are in achieved in a large scale because it is cost effective and also it does not depend on location .since the cloud computing is a new technology and is in demand, many establishments are still depending on cloud to organize their industries in the cloud computing atmosphere due to the care in securing and sharing the resource . Cloud computing has 5 characteristic 1. on-demand self-services 2. ubiquitous network accesses, 3.resource pooling, 4. elasticity, and 5. measured services. The aforesaid characteristics of

cloud computing makes it has an outstanding entity establishments and organizations, and also for single operators for adoption. Nevertheless, the advantages of cloud technology deliver with low- cost, insignificant management and superior elasticity and comes with improved security anxieties. Security is a standout amongst the most significant angles those preventing the wide-spread selection of distributed computing. Cloud security complications may branch because of the Centre invention's usage (virtual machine (VM) escape, session riding, and so on.), cloud administration contributions (systematized question language infusion, powerless verification plans, and Hence forth.), and emerging from cloud qualities (data healing helplessness, Internet convention powerlessness, and Hence forth.).To talk about cloud it must be secure, the majority of the taking attention substances must be secured . In some random framework with numerous units, the most irregular amount of the framework's security is equivalent to the safety dimension of the weakest

unit. In this way, in a cloud computing, the advantages and safety of cloud does not exclusively rely upon a person's safety efforts. The neighbouring substances in could give a chance to a hacker to sidestep the user's guards. (since Pooling and elasticity are the feature of

a cloud, allows the physical resources to be shared among many users and Additionally, the shared resources may be redistributed to some other users at some occasion of time and that may result in data concession through data retrieval procedures .By outsourcing the information to private cloud,we have to make sure it is secure ,and data is not accessed by unauthorized process and users.

## II. RELATED WORK

When uploading the data in to cloud ,it is stored in a single node,By storing the data in single node it leads to access by unauthorized users ,since cloud computing pooling features enables the shared resource to be used by some other users and processes and it must be prevented AND also security is important when discussing about cloud. Cloud storage is a cloud computing model in which information is put away on remotely set servers and are accessed through the Internet. It is kept up, worked and achieved by a cloud storage specialist who is working on remote servers that are based on virtualization systems. This cloud is public, the user can store the file in the cloud storage and also provide the security to the file by encrypting the file. Disadvantages of existing system

- ✓ If the hacker gets the decrypted key, he can able to get the entire file content, this might be the privacy.
- ✓ File is not much secure in the public cloud storage.
- ✓ If the cloud server which is located remotely fails to connect due to internet connection and atmosphere, user will lose the files stored in the

cloud storage, because of there is no replication of the file.

The strategy proposed in our paper it does not work on cryptographic procedures for data protection. Digital data are very important now-a-days. The paper documentations are becoming are very less usage and all are moving to digital documentation. Industries, corporate, government are converting many processes into digitalization which lead to big data. There are many issues in digital documentation. The first issue is security, our sensitive data should not leak out, the second issue is recovery when our documents are digitized and we are not able to retrieve it. It leads to big problem. Our system considering these two issues and developed as a web-based Application so that it can be accessible in all the client system and is suitable for small, medium and large organization. A file in cloud environment is in its aggregate, kept as a node that leads to a sole fact of failure.

Specification, we must include only those requirements that are appropriate for our project.

## III. PROBLEM STATEMENT

The FTFT (fault tolerance with fragmentation technique for cloud storage security) that together approaches the safety and performance issue. Cloud security problems mainly rest on outstanding to the essential technology's operation of virtual machines such (Virtual Machine escape, Virtual Machine session riding, etc, cloud offers services such as (SQL injection, imperfect validation schemes, etc.), and developing from cloud features (recovery of data susceptibility, Internet protocol Susceptibility, etc.).

## IV. PROPOSED SYSTEM

We present Fault tolerance with fragmentation technique for cloud storage security that intelligently

fragments user files into pieces and duplicates them at desired locations within the cloud. The file is divided into smaller fragments and then the action is achieved based on a given user requirements and according to standards such that the distinct fragments do not contain any expressive information. An optimistic attack on a sole node must not reveal the places of other fragments that exist within the cloud. To keep a hacker ambiguous about the sites of the whereabouts of the fragments of file and to additional we have to take care to improve the safety and security, hence each node is selected in such way that two or three consecutive nodes of single file are not placed together and are at the convinced distance of point.

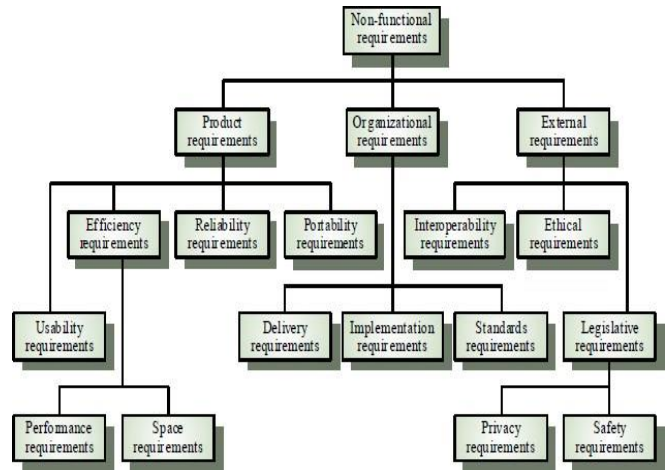
Advantages of proposed system

- ✓ We have developed a system for the data which is outsourced that make sure that it takes into explanation about both the security and operation. The proposed system fragments and duplicates the data file over cloud nodes.
- ✓ The planned FTFT scheme makes assures that even in the successful attack of single node does not reveal, no expressive information to the hacker.
- ✓ This Technique does not complete depend on outdated cryptographic procedures for security of the data. The non-cryptographical nature of the strategic system makes it to accomplish earlier the required actions such as location and recovery on the data.
- ✓ In this method, we have ensured that a skillful duplication of the file fragments, wherever each of the file fragments is duplicated individual once for the resolve data security.

2. Non-functional requirements

Non-efficient requirements define how a system must act and establish limits of its functionality. This type of requirements is also known as the system's quality attributes. Characteristics such as

performance, security, usability, compatibility are not the feature of the system, they are a required attribute. They are "developing" properties that emerge from the whole arrangement and hence we can't compose a particular line of code to execute them. Any attributes required by the customer are described by the



Some Non-Functional Requirements are as follows:

- ✓ Reliability
 

The structure must be reliable and strong in giving the functionalities. The movements must be made unmistakable by the structure when a customer has revealed a couple of enhancements. The progressions made by the Programmer must be Project developer and in addition the Testing person has to take care.
- ✓ Maintainability
 

The system inspecting and maintenance should be important and effort in its method. There should not be an additional of jobs running on various machines such that it gets solid to show whether the Processes are running without intervals.
- ✓ Performance
 

The framework will be operated by numerous representatives all the while. Since the structure will be encouraged on a single web server with single

database since the server is outside of anyone's capability to see, execution converts into an important concern. The structure should not yield when several customers would use the whole thing the while. It should allow brisk approachability to each and provide every piece to its customers. For instance, if two test experts are busy in attempting to report the locality of a bug, then there ought not to be any misdeed at the same time.

✓ Portability

The framework ought to be effectively versatile to a different framework. this is often obligated once the online server, that s facilitating the framework gets adhered as a result of a couple of problems, which needs the framework to be taken to a different framework.

✓ Scalability

The framework should be sufficiently adaptable to include new functionalities at a later stage. There should be a run of the mill channel, which can oblige the new functionalities.

✓ Flexibility

Flexibility is the capability of a framework to regulate to ever-changing things and circumstances, and to adapt to changes to business approaches and rules. Associate convertible framework is one that's something however troublesome to reconfigure or change due to numerous consumer framework stipulations. The deliberate division of considerations between trough and motor components helps ability as simply a touch little bit of the framework is influenced when strategies or principles modification.

**V. SYSTEM ARCHITECTURE AND DESIGN**

1. System design

System Planning design-identifies the multimedia system structure for the WebApp. Architecture strategy is tied to the goals to start for a WebApp. the content to be given ,the users who can visit and also the navigation philosophy that has been established .content coming up with ,focuses on the means during which content matters and arranged for presentation and navigation .Webapp design, addresses the way during which the appliance is structure to manage user interaction, handle internal process tasks, impact navigation and gift content. Webapp design is outlined at intervals the context of the event setting during which the appliance is to be enforced.

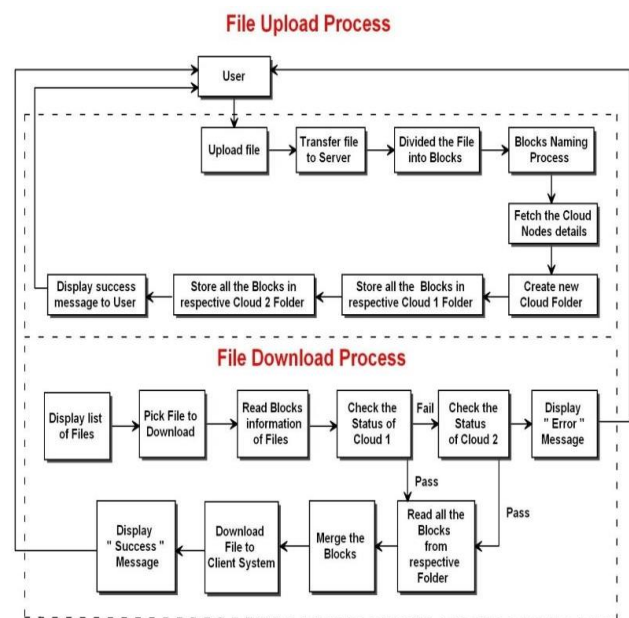


Fig 1. System Architecture

**VI. METHODOLOGY**

1. Block creation: When a user uploads a file into cloud storage, that file has to be divided into blocks, the blocks are divided based on fixed size. For each block the system has to create unique name based on some naming conventions. The Meta data of the uploaded file should be maintained in SQL table. And the blocks are uploaded into respective cloud storage.

2. Integrity Testing: For each block using hashing technique message digest is created and the message digest are stored in database. While user is downloading the file, the relevant file blocks downloaded from cloud for each block using hashing technique message digest will be created and generated message digest has to be compared with relevant block message digest in database, if there are any differences it has to display the notification to the user.
3. Fault tolerance: In this system files are divided into blocks and blocks are stored in two cloud storages to avoid retrieval failure. Consider a situation first cloud storage become deactivated, this system will retrieve all blocks from second cloud storage and form the file and give to user.
4. Model, View and Controller (MVC): This system is developed using MVC architecture on Java technology. Tomcat is used as a web server. Once this system is deployed on tomcat then all the client system connected with tomcat server can able to access this application. This application will work on both LAN and WAN.

## VII.RESULTS

### 1. Admin\_Login



Fig 2. Screenshot of Admin Login

### 2. User\_Login

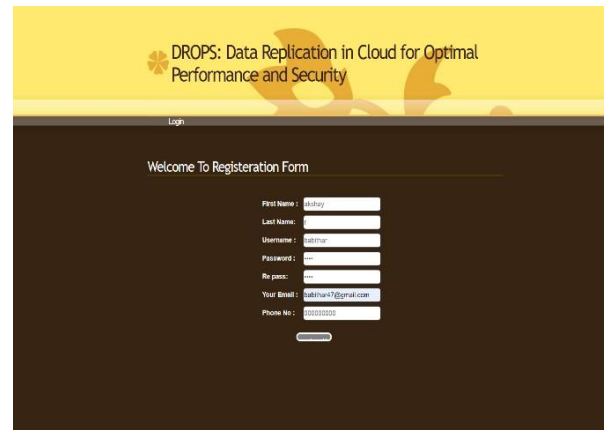


Fig 3. Screenshot of user Registering

## VIII. CONCLUSION

We provided methodology for Fault tolerance with Fragmentation technique for cloud storage security, a cloud storage security strategy that put together deals with the safety and performance of knowledge in terms of retrieval time. The data file which is received is fragmented and those fragments are dispersed over multiple nodes. Currently with the FTFT methodology, a user should transfer the file, update the contents, and transfer it once more. But this technique doesn't address automatic update mechanism in order that it will determine and update the specified fragments solely.

## IX. REFERENCES

- [1]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.
- [2]. A.-R. Sadeghi, T. Schneider, and M. Wynand, "Token- Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

- [3]. D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992
- [4]. C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., <http://www.crypto.stanford.edu/Craig>, 2009.
- [5]. J. Bettencourt, A. Sahai, and B. Waters, "Cipher-text-policy attribute-based encryption: An expressive, efficient, and provably secure realization" in Proceedings: Public Key Crypto Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

**Cite this article as :**

Babitha. R, Shilpa. V, "FTFT : Fault Tolerance with Fragmentation Technique for Cloud Storage Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 38-43, May-June 2019.  
Journal URL : <http://ijsrcseit.com/CSEIT195324>