MAPLE TREE PUBLISHING HOUSE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION (IRJMT)

http://www.mapletreejournals.com/index.php/IRJMT
Received 20 March 2019 ISSN 2582-1040
Accepted 23 March 2019 2019; 1(2); 66-72
Published online 25 March 2019

Detaching and Reproducting of Data in a Cloud for Excellent Performance and Security

D. Ravi[1], T. Ravina[2*], P. Buvanasundhari[2], G.K. Vikram[2]

[1] Assistant Professor, Dept of Computer Science & Engineering,Kathir College of Engineering,Coimbatore,TN, India
[2]UG Scholar,Dept of Computer Science & Engineering,Kathir College of Engineering,Coimbatore,TN, India

**Corresponding author E-Mail ID: t.ravinacbe@gmail.com, Mobile: +91 9444626495*

DOI: https://doi.org/10.34256/irjmt1929

ABSTRACT

Cloud computing is third party administrative control so our data is outsourced it gives rise to security concerns.security is one of the important aspect of any technology. Therefore high security measures are required to protect our data. In this paper, we propose Detaching and Reproducting of Data in a cloud for excellent performance and security that collectively approaches security issues and data sharing protectively. In this methodology, we divide the file into fragments and replicated over cloud nodes. Files are fragmented and shuffled like (1-2,2-3,3-4.4-1)in sequential order and stored in multiple servers. Moreover nodes sharing fragments are separated with certain distance by using T-colouring graph to prohibit an attacker by guessing the location of fragments. This methodology does not rely on traditional cryptography techniques.

Keywords: cloud security, fragmentation, replication, T-colouring graph, data splitting

1. INTRODUCTION

Cloud computing is one the top most technology in our world. Cloud computing is innovative technology that uses advanced computational power and enhancing storage capabilities. Cloud computing is mainly used for storage and management of information technology framework. Cloud computing are characterized by

- On-demand self-services
- Ubiquitous network accesses
- Resource pooling
- Elasticity
- Measured services.

Cloud security issues may stem due to the core technologies implementation (virtual machine (VM) escape, session riding, etc.), cloud service presenting (structured query language injection, weak authentication schemes, etc.), and arising from cloud computing characteristics (data recovery vulnerabilities, Internet protocol vulnerabilities, etc.). Some benefits of cloud are

- Minimum cost
- Negligible management
- Greater elasticity

- Cost savings

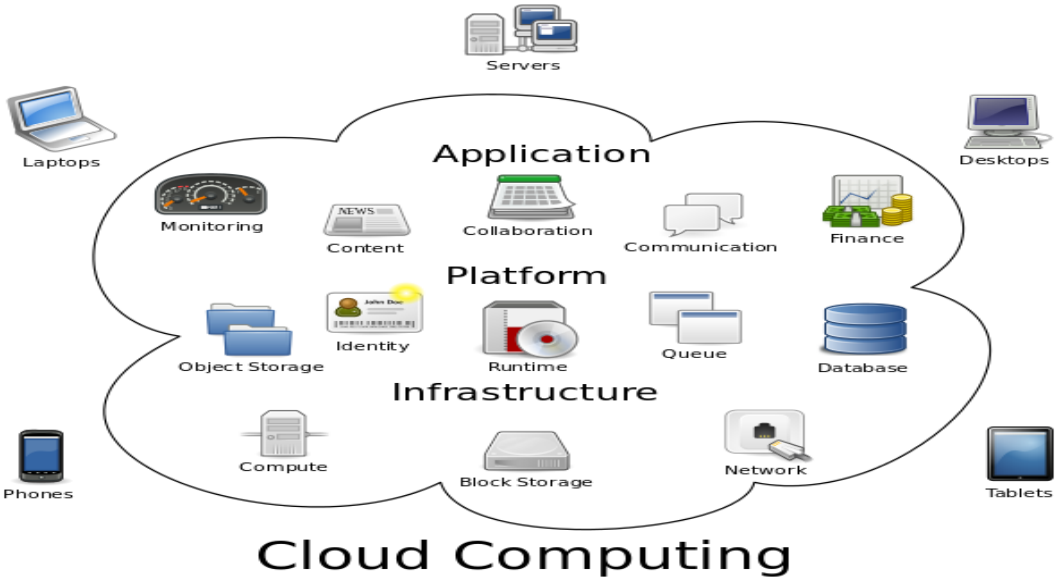

Fig 1.Cloud Infrastructures

2.LITERATURE SURVEY

Juels et al., [2] presented a technique to make sure the integrity, novelty, and availability of data in a cloud. The data is moving to the cloud is performed by the Iris file system. A gateway application is designed and employed in the organization that ensures the integrity and novelty of the data using a Merkle tree. The file blocks, MAC codes, and version numbers are at various levels of the tree. Moreover, the amount of loss in case of data tempering as a result of damage or access by other VMs cannot be decreased. G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, [3] presented the virtualized and multi-tenancy related issues in the cloud computing storage by utilizing the combinedstorage and local access control. The Dike authorization architecture is proposed that combines the local access control and the tenant name space isolation.

3. SYSTEM ANALYSIS

3.1 Existing System

Our data is outsourced in public cloud must be secured.Data is accessed by unauthorized users where accidently or deliberately.In this Methodology,we divide the file into fragments and replicated fragments over the cloud nodes.And shuffling will be done by Graph T-colouring.Here the fragments are scattered through user cannot find sequential order in this method but retrieval time is very high.Moreover chance of data loss and data are not arranged in sequential order**.**

3.2 Disadvantages

- The data compromise occurred by attacking from other users and nodes within the cloud.
- The employed security strategy must also take the optimization of the data retrieval time.

3.3 Proposed System

We presented the Detaching and reproducting of data in cloud for excellent performance and security for protecting the data by splitting the file into fragments. This Methodology judicially fragments user files into pieces and replicates them at strategic locations within the

cloud.The division of file into fragments are performed based on user criteria such that individual fragments do not reveal the meaningful information.we use FS-DROPS (Fragment and snuffle drops)ALGORITHM which will fragmenting the user files into four pieces and shuffled like(1-2.2-3,3-4,4-1) and stored in multiple servers. So in future some Server is not available are Hacked we can get back our original data from remaining Server.

3.4 Advantages

- Cost Efficient & data Protection in cloud is good.
- The nodes are selected based on the centrality measures that ensure an improved access time and improve the retrieval time.

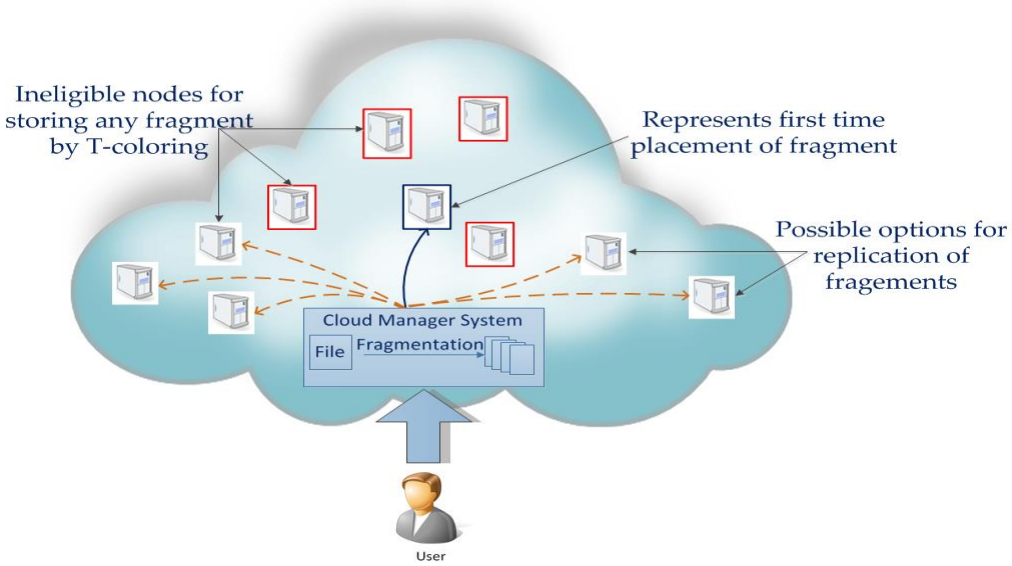

Fig 2.Fragmentation

3.5 System Study

3.5.1 Feasibility Study

The feasibility study of project are analyzed in phase and business proposal is put with general plan for project and cost estimation. For feasibility analysis we need to understanding the major requirements of the system is essential. The feasibility study investigates the problem and stakeholders needs of information. The analyst conducting the study gathers information using a variety of methods, the most popular of which are:

- Interviewing users, employees, managers, and customers.
- Developing and administering questionnaires to the stakeholders, such as users of the information system.
- Observing users of the current system to determine their needs as well as their satisfaction and dissatisfaction with the current system. These components are:

1. Economic Feasibility
2. Technical Feasibility
3. Social Feasibility
4. Operational Feasibility

3.5.2 Economic Feasibility

This economical feasibility study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the system research and system development is limited. The expenditures must be justified.

3.5.3 Technical Feasibility

This technical feasibility study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed that must not have a high demand on the technical resources availability. This will lead to the high demands on the technical resources.

3.5.4 Social Feasibility

This social feasibility study is to check the level of acceptance of the system by the user. The process to use the system efficiently by training the user. The user must not felt threatened by the system, instead must accept it as required.

3.5.5 Operational Feasibility

The ability, desire, and willingness of the interested stakeholders to use, support, and operate the proposed computer information system efficiently. The stakeholders include management, employees or partners, customers, and suppliers, vendors.

3.6 System Design

3.6.1 Input Design

Input design is the process of converting that user gives originated inputs to a computer-based format. Input design is one of the most expensive phases of the operation of computerized system and is often it is the major problem of a system.

In this paper, the input design is made in various web forms with various methods. For example, in the user creation form, the empty username and password is not allowed. The username is already exist in the database, the input is considered to be invalid and that input not accepted. Likewise, during the login process, the username is a must and must be available in the user list in the database. Then only login is allowed. The input design contains the file to upload, the file sharing request with secret key and the file fragments are the inputs.

3.6.2 Output Design

Output design refers to the results and information that are generated for many end-users by the system. Output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application.

In the project, the fragmentation details, the file encryption details and file RDVM results for the cloud server availability and anomaly users are the output.

3.6.3 Database Design

The database design is necessary for developing any application especially more for the data store projects. Since the chatting method involves storing the message in the table and produced to the sender and receiver, proper handling of the database table is a must. In the paper, login table is specially designed to be unique in accepting the username and the length of the username and password should be greater than zero. The different users view the data in different format according to the different privileges given.

3.6.4 System Architecture

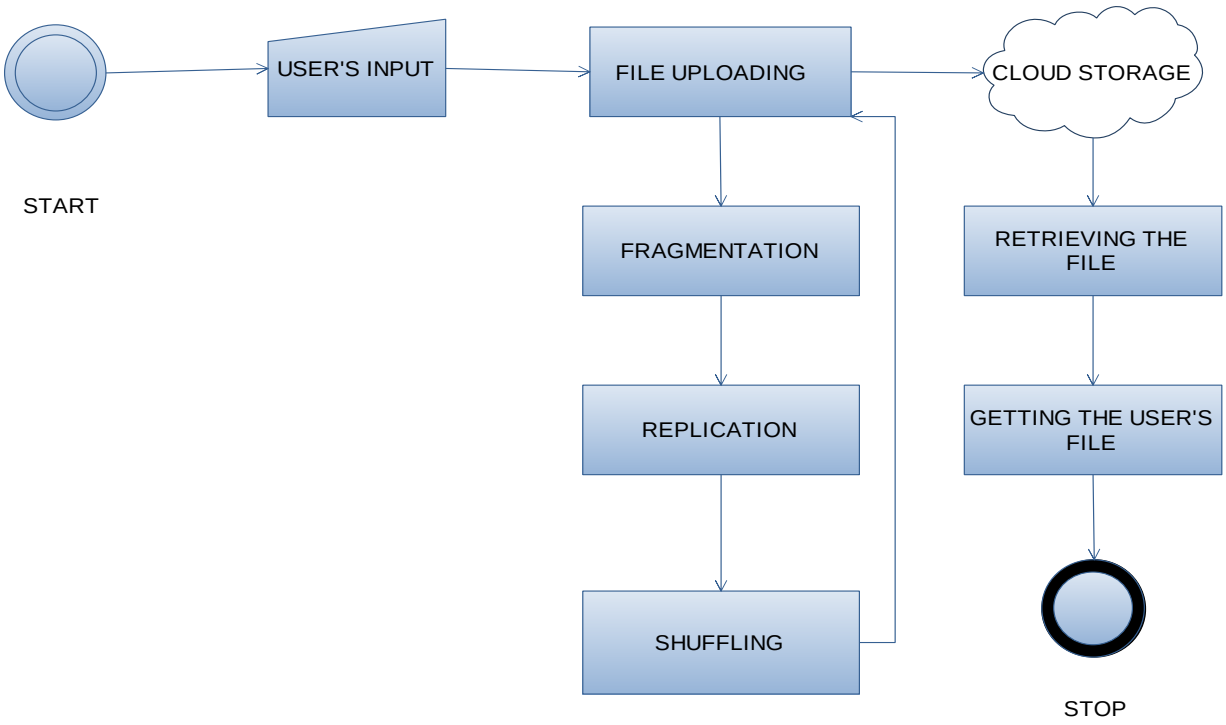

Fig 3. System Architecture

3.6.5 Flow Chart Diagram

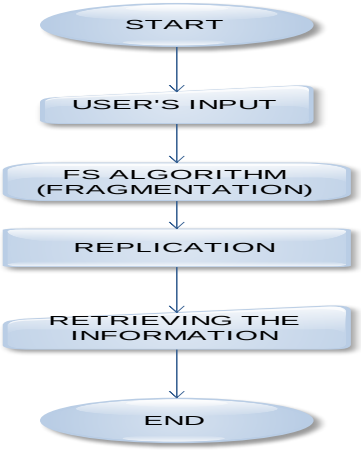

Fig 4. Flow chart

4. MODULE DESCRIPTION

The following are the modules involved in the project.

- ✓ User Authentication
- ✓ Fragmentation
- ✓ Data Replication & Data Encryption
- ✓ Server Analysis

- ✓ Data Retrieval & Decryption

4.1. User Authentication

User Authentication is the process of identity verification you are trying to prove a user is who they say they are. For a user to prove their identity, a user needs to provide some sort of proof of identity that your system understands and trust. The authentication process starts with creating an Login Context.For example uses the Login Context variety. The first parameter is the name and the second parameter is a callback handler used for passing that information in login to the Log server. Callback Handler has a handle method which transfers to the Log server by required information.

4.2. Fragmentation

We are splitting the file in to small fragments. Once the file is split into fragments, this concept selects the cloud nodes for fragment placement. The selection is made by keeping both security and performance in terms of the access time. The process is repeated until all of that splitting files into fragments are placed at the data nodes. Partial Replication represents the fragment placement methodology.

4.3. Data Replication & Data Encryption

This component supports the replication mechanisms by invoking replicas and managing their execution based on client's requirements. We denote that set of VM instances that are controlled by a single implementation of a replication mechanism as a replica group. Each replica within a cloud can be uniquely identified, and a set of rules *R* that must be satisfied by a replica group are specified.

4.4. Server Analysis

The task is offered fault analysis as a service that needs the service provider to realize fault analysis mechanisms such that the client's applications in virtual machine(VM) instances. That VM instances transparently obtain server status properties. we define *ft−unit* as the fundamental module that applies a coherent server analysis mechanism to a recurrent system failure at the granularity of a VM instance.

4.5. Data Retrieval & Decryption

The data retrieval module describe the retrieve data from different virtual server only authenticate user. Data are encrypted in different virtual server with fragments. Data are retrieved from different virtual server and combine the data and convert to decrypted format

5. RESULT & PERFORMANCE

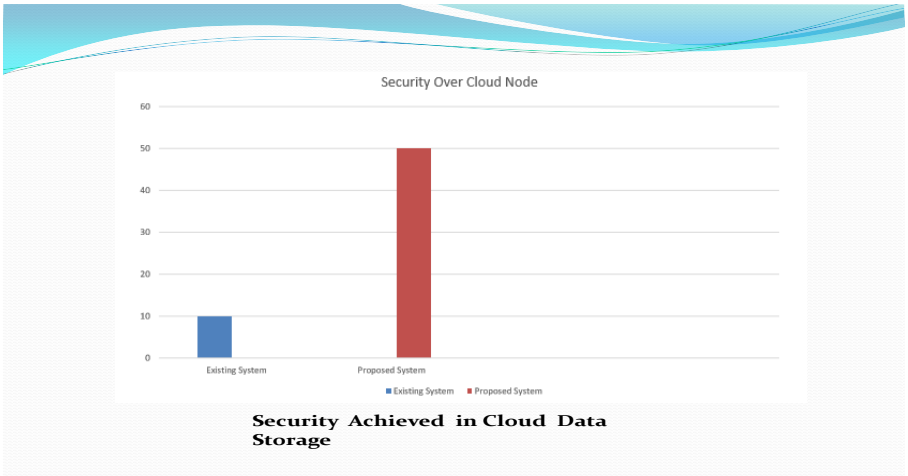

Fig 5. Result

6. CONCLUSION

We proposed the detaching and reproducting of data in a cloud for excellent performance and security methodology, a cloud storage security scheme that collectively deals with the security and performance in retrieval time. The user file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. The fragmentation and dispersal ensured that no significant information was obtained by an adversary in case of a successful attack. No node in cloud, stored more than a single fragment of the same file. The performance of this methodology was compared with full-scale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance, resulted in increased security level of data accompanied by a slight performance drop.

REFERENCES

[1] K. V. Vishwanath and N. Nagappan, Characterizing the cloud computing hardware reliability, in Proc. 1st ACM Symp. Cloud Comput., 2010.

[2] R. Jhawar, V. Piuri, and M. D. Santambrogio, A comprehensive conceptual system-level approach to fault tolerance in cloud computing technology, in Proc. IEEE Int. Syst. Conf., Mar. 2012.

[3] B. Grobauer, T.Walloschek, and E. Stocker, Understanding the cloud computing technology vulnerabilities, IEEE Security and Privacy, 2011, Vol.9, No. 2, pp. 50-57.

[4] W. K. Hale, Frequency assignment: Theory and applications,Proceedings of IEEE, 1980, Vol. 68, No. 12, pp. 1497-1514.

[5] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, An analysis of the security issues for cloud computing, Journal of Internet Services and Applications, 2013, Vol.4, No. 1, pp. 1-13.

Conflict of Interest

None of the authors have any conflicts of interest to declare.