DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5675

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY PAPER ON IMPROVING PERFORMANCE AND ENHANCING SECURITY BY USING DIVISION AND REPLICATION OF DATA IN CLOUD

Osama Razi
Department of Computer Engineering,
Dr. D. Y. Patil Institute of Technology,
Pimpri, Pune, MS India

Sumit Sanyal*
Department of Computer Engineering,
Dr. D. Y. Patil Institute of Technology, Pimpri, Pune,
MS, India,

Mohsin Raza
Department of Computer Engineering,
Dr. D. Y. Patil Institute of Technology,
Pimpri, Pune, MS, India

Shashi Sourav
Department of Computer Engineering
Dr. D. Y. Patil Institute of Technology,
Pimpri, Pune, MS, India

Prof. Rachna Somkunwar
Assistant Professor,
,Department of Computer Engineering,
Dr. D. Y. Patil Institute of Technology,
Pimpri, Pune, MS, India

Abstract: Cloud computing is an information technology paradigm model which offers clients access to shared pool of resources. Replication and division of data takes into consideration the performance and security issues. A given file is divided into fragments and then replicated. They are placed over the nodes (servers) and every node stores a single fragment of data in order to improve security. The nodes that store the replicas and fragments are not adjacent to each other by applying T-coloring method hence preventing the attacker from gaining access to useful information. The user can download the file from anywhere but has to specify the exact location as well as the time and date in order to get maximum security as compared to other systems. The likelihood of finding andcompromising the nodes that store the fragments of a file is very low.

Keywords: Cloud Computing, Centrality, Fragmentation, Cloud Security, Replication, T-Coloring

1. INTRODUCTION

Cloud Computing is a prototype that offers Clients access to a huge shared pool of computing resources. The main reason to migrate to Cloud is its ability to use and make payment for resources on-demand and fast elasticity according to user’s perspective.

The cloud computing paradigm has completely transformed the management and usage of the information technology infrastructure. It is a paradigm that reduces cost through optimization and increased operating and economic efficiencies. Cloud computing is a technology that offers low cost, scalable computation capacity, services to organizations and enterprises on-demand for expand their organization.

Security is of the highest priority amongst the most vital and critical perspectives among the individuals who forbid the adoption of Cloud computing. Cloud security issues happen because of the core technology execution, like, virtual machine (VM) escape, session riding, Structured Query Language injection, frail authentication schemes, and so on., and emerging from cloud characteristics (data recover vulnerability, Internet Protocol defenselessness, and so on.). For a given framework with various units, the largest amount of the frameworks security is equivalent to the security level of the weakest substance. In this way, the security of the benefits is not exclusively dependent on an individual's security effort in Cloud. The neighboring flaws gives a chance to attacker to overcome the client's defenses.

2. BASIC DEFINITIONS

i. Fragmentation:-

It is the process of creating fragments of files at the server side for improved security. The Fragmentation algorithm is used for this process. In this process a file is considered as input and the fragments are the desired outputs.

ii. Replication:-

Replication is the process of creating duplicate fragments of original fragmented file.It is useful in case the fragments gets damaged in an attack. Hence, in order to deliver the fragments to the user, admin replaces the damaged fragment by its replica and combines all fragments together so that the files are received by authorized data owner.

iii. Allocation:-

After the files are fragmented and the replicated, eachfragment is assigned on the cloud server for storing data

and it also considers security issues while placing fragment. The
T-Coloring graph concept is utilized to place the fragments on the nodes in cloud.

iv. Data Owner:-
Data owner can view all the files uploaded by any user in cloud. The data owner knows all the information related to fragments and its replicas.

v. User:-
Data user may also work as data owner. Data user can download or view files that is uploaded by other user. Data user must be an authenticated user.

vi. Admin:-Admin has the authorization power to validate all data users and data owners.Admin can remove any false data user.

3. LITERATURE REVIEW

Before starting the project implementation, there is a need to gain some data about it. Apart from the domain information, there is requirement to study techniques and applications that already exist. This process was done with a view of understanding the scope of the project. Thus it helped in unveiling different methods by which we could bring our project statement into existence.

In paper [1], authorhas exhibited a strategy to fulfill the trustworthiness to provide accessibility of useful information from the cloud. In this information movement takes place which is achieved with the help of file system known as Iris. It is an authenticated file system that migrates an enterprise file cloud system operations.

In this paper[2] author has worked on issues related to virtualization and various independent organization in cloud storage by using method joined stockpiling and nearby obtain control. Architecture proposed is actually to merge the local and independent organization space separation.

In this work [3] author has focused on the utilization of a trustworthy user for providing full benefits of security and availability of data in cloud. A public key infrastructure is used to improve user's trust in various fields such as authentic validity, honesty and data privatization. These keys are created and supervised by certified third party authority.

In this research [4], authors have proposed a central database, placed in network of wide area. It provides various important data essential for the cloud based applications. For maximizing the speed of accessibility and reducing unwanted delays, these database center host or organize a local database.

In this paper [5], author has designed Encryption technique process like fragmentation for keeping the data private in cloud storage. Fragmentation is a process of breaking or splitting the features of available data and generating various fragments in such a manner that fragments placed at external providers do not ignore necessities.

In a distributed environment the main aim of author is to develop a specific solution for providing assurance and nonlinear optimization problem of data objects. The splitting of an encryption key is done into n shares and spread on several sites inside the system [6].

In this paper [7], author has proposed a Scheme which is Cost-efficient having much accessibility of integrating two key functions. The first is picking a few reasonable mists and a precise excess methodology used to accumulate information and to guarantee accessibility with reducing financial expense. Secondly accelerating a move procedure through which data is distribute again and again in compliance with the rules of different access patterns and cost of cloud.

In this research [8], author has evaluated an improved solution with different approaches for File division and integration. File is split into multiple fragments and then these fragments are merge together by using File Splitter program.

In the existing system data is stored over the cloud which are maintained by the third party and user have to rely on it for the security. The third party manages user’s access request and time required to reply and also creates replicas of file which can be used as replaceable for the corrupted file. Take example, for a node containing documents and creating replicas of file into m pieces rather than a single will increases the chances of attack, from 1/n to m/n in which n is the aggregate of nodes.

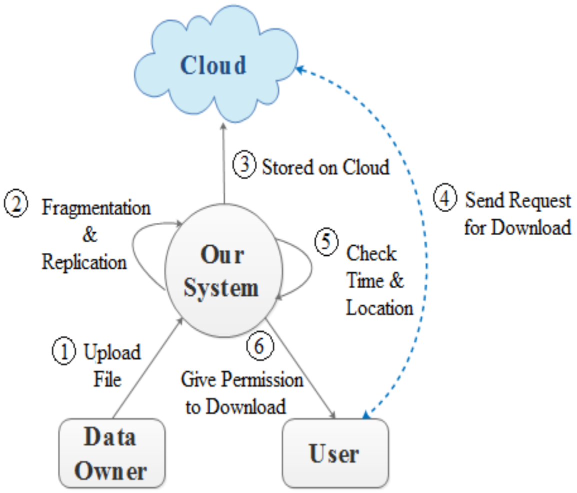
Existing framework was not accomplishing legitimate security. Even though it provides security managed by third party, it is unable to give full security. In our new system these problems will be solved by applying various strategies like geographical Location, one time password generation and date and time constraint. Using the above techniques we can achieve security of files very efficiently.

4. PROPOSED SYSTEM

The proposed architecture is a new idea of Secure Dynamic Fragmentation and Allocation of replica with optimal security and performance in cloud that jointly approaches the performance and security issues with respect to time retrieval. The proposed architecture guarantees that even if there is a successful attack no important information is revealed to the attacker. The conventional cryptographic techniques are used for security. The non-cryptographic type of the proposed architecture makes it efficient to execute thedesired functions (arrangement and recovery) for the information. We ensure that there is a proper replication process of the parts of the document wherein each of the pieces is duplicated only once with the goal of proper and better security. A cloud storage security conspire mutually manages the security and execution regarding recovery time. The advantage is improved security, performance, no load in single node of cloud, number of fragment are decided according to owner’s choice.

The advantage of this approach is that there is no load on single node of cloud, no useful information is revealed to the attacker and number of fragments are decided according to the owner's choice.

5. PROPOSED ARCHITECTURE


Cloud
③ Stored on Cloud
④ Send Request for Download
② Fragmentation & Replication
Our System
⑤ Check Time & Location
① Upload File
⑥ Give Permission to Download
Data Owner
User

i. FRAGMENTATION

In this procedure the uses first register and then login into the system. The user transfer file on cloud. When the user is transferring the document into the cloud this module comes into the picture in which the input document is divided. To divide the file user need to enter the number of fragments of a file. Using the size, the documents gets its original fragments.

ii. REPLICATION

After fragmentation, the replica of each of the fragment is created. It provides security to the files and also protect it if original fragment is destroyed.

iii. FRAGMENT AND ITS REPLICA PLACEMENT

It selects the cloud nodes for fragment placement using t-coloring algorithm. The selection is achieved by considering security and performance in terms of access time.it uses the concept of centrality in which only those nodes are selected which are closer to Cloud network.

iv. INTEGRITY CHECKING

For auditing the integrity of files, PA (Third Party Auditor) is responsible. Hash value is generated of each fragment and is the basis for checking integrity of files. Any tampered file is replaced by its original fragment present on any node

6. CONCLUSION

We have proposed a design technique which uses replication and fragmentation methods to provide security of file and also time required for retrieving file from the System is optimized. To maximize security we also introduced concept of one time password generation, date and time constraints and geographical location. With the help of these techniques, problem related to replication and fragmentation methods in security is solved and possibility of attack has dropped largely.

A user can download and upload files having text format only. The design technique has some limitations such as audio, video, image files cannot be uploaded. In future work such problems will get resolved and user will be able to upload and download audio, video, image files.

7. REFERENCES

[1] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.

[2] A. Juels and A. Opera, "New approaches to security and availability for cloud data," Communications of the ACM, Vol.56, No. 2, 2013, pp. 64-73.

[3] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant FileSystems,"University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[4] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Quantitative comparisons of the state of the art data center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3,2012, pp. 583-592.

[6] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters,"In IEEE Globecom Workshops, 2013, pp. 446-451.

[7] Sabrina De Capitani di Vimercati1, Robert F. Erbacher2, "Encryption and fragmentation for data confidentiality in the cloud".\

[8] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, Nov. 2012, pp. 903-916.