OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

# ENSURING DATA SECURITY IN CLOUD

**Balkrishna Patil[1], Ashwini Rajguru[2]**
*HOD, Computer Science, EES College of Engineering, Aurangabad, India[1]*
*Student ME , Computer Science, EES College of Engineering, Aurangabad, India[2]*
*cseroyal7@gmail.com [1], ashwinirajguru22@gmail.com[2]*

***Abstract:*** **In Cloud System considering Security issue We propose a Data Division and Replication method in cloud i.e DRDC which handles the security issues and maintain the performance. In this system, file uploaded by the client is first encrypted then divided into fragments. Then these fragments are replicated means another copy of that fragment is created over the cloud nodes. Each node contains only a single fragment during the fragmentation and replication process. Thus if any one or another of the node is added by hacker, no significant information is obtained, and thus security of System is maintained. To further increase the security, nodes are separated by using T-coloring graph method. In T Coloring Method no two adjacent nodes at same place Due to the T-coloring, the effort needed by an attacker to break the security is increased multiple times or it is difficult for hacker.**

***Keywords:*** *T-Coloring, Cloud Storage, AES Algorithm, Division & Replication of data in cloud(DRDC).*

## I INTRODUCTION

Cloud computing can refer to provides Software as a Service (SaaS),Platform as a Service(PaaS), Application as a Service(AaaS), Storage as a Service(SaaS),Web-oriented architecture (WOA),this paper focus on storage as a service where Current cloud computing systems has serious limitation of protecting user's data confidentiality. Since user's data is presented in unencrypted forms to re-mote machines owned and operated by unauthorized disclosure of third party service providers, the risks of of the user's sensitive data by service providers may be quite high. There are many techniques for protecting user's data from outside attackers.An approach is used to protecting the confidentiality of user's data from service providers in our paper, and ensures that service providers cannot collect user's confidential data while the data is stored and processed by cloud computing systems. Cloud computing systems provide various internet based data storage and services [1].

Users of the cloud aren't aware about the location of the data and ultimately have to rely on the cloud service provider for exercising appropriate security measures. Therefore cloud security issue is the most important and highlighted topic among the IT professionals. Security in cloud computing is of two types first is Data security it mainly focuses on software and hardware associated with the cloud and protect it. It deals with choosing an apt location for data centers so as to protect it from internal threats, different types of weather conditions, even physical attacks that might destroy the center physically and external threats avoiding unauthorized access and break ins and Second is Network security which protecting the network from where cloud is running from various attacks. Attack on data acts a single user whereas a successful attack on Network has the potential to act as multiple users. Therefore network security has more importance.

## II LITERATURE SURVEY

In Literature Survey we have studied about Cloud and cloud Security. To make application to be secure on cloud different techniques can be used such as encryption, T-Coloring, hash code calculator and many more. using this technique we can upload file on cloud and access it from anywhere without any changes. thus we get original document and Security of document can be achieved.

There is much more research done on this concept, but existing systems have some drawbacks related to either security or performance or both. In previous systems challenge of data privacy was there because user's data is sensitive and this data is outsourced by user to cloud[2]. So privacy must be kept of user's data. In proposed system using T-coloring fragments are stored in such a way that even in case of successful intrusion of node; attacker will not get any significant information [3]. Encryption is used to protect the confidentiality before outsourcing the data into cloud.

Number of requests and the response time are considered as key points for which site within the region the file has to be placed. Therefore, their strategy increases the data availability and also reduces the number of unnecessary replications [4].M. Tu et al. presented a secure and optimal placement of data objects in a distribution system. The encryption key is divided and division is done through threshold secret sharing scheme [5]. This scheme pays attention to the replication problem with security and access time improvement [6]. In this scheme data files are not fragmented and are handled as a single file. This scheme mainly focuses on encryption key security unlike our methodology [7]. Any weak entity may lead to put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase an attacker's effort to retrieve a measureable amount of data even after a successful intrusion in the cloud is happen. Moreover, the probable amount of loss (as a result of data leakage) must also be minimized [8].

## III PROPOSED SYSTEM

The Previous Problems related to cloud security is overcome in proposed system i.e If in a cloud, file is stored on a single node, there is significant risk for data security. In this kind of system the retrieval time can be decreased by replicating the files at multiple nodes. To balance the security and performance DRDC methodology helps, as it does not store entire file on a single node. This system fragments the file and then replication of fragmented file is done. Thus even in a case of security breach, no significant information is revealed to an attacker. Replication is also in a controlled manner so that each fragmented file has only one replica, thus data security is not compromised in spite of maintaining performance.

There's a cloud manager in the DRDC system which is a secured entity. The cloud manager performs following functions –

- Receiving the file
- Encryption of file by AES algorithm
- Fragmentation of file
- Nodal selection and each fragment assigned a single node with the help of T-coloring.

The user can divide the file efficiently so that no significant information is there in a single fragment The cloud manager has to pay attention to the communication channel between cloud manager and client, and make sure that the channel is secure.

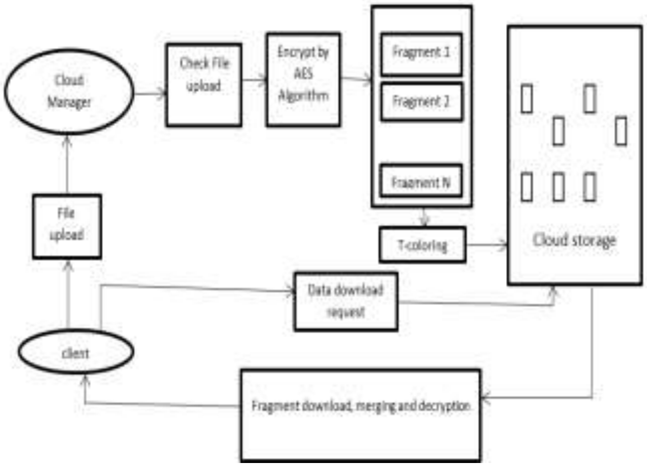

*Figure 1 DRDC Framework*

As soon as file is divided into fragments, this system assigns the cloud nodes for each fragment. This is where the concept of T-coloring is justified. In this concept a set T is built starting from zero to random positive number. To make this system work, colors are given to the nodes. Let's consider there's an open_color before placing the fragment, as soon as fragment is placed on one of the node, then close_color is given to nodes surrounding the assigned node up to the T distance. This system makes cloud more secure, although somewhat performance is decreased due to less availability of central nodes.

Components:

i)AES Algorithm

1. Key Expansions—round keys are derived from the cipher key using Rijndael key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

i) Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

i) Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

ii) Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

iii) Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

iv) Add Round Key

4. Final Round (no Mix Columns)

i) Sub Bytes

ii) Shift Rows

iii) Fragmentation

. In this system attack on one node results in compromised security of information available only on that node, because in this system data file is fragmented and stored on different nodes. In addition to this, the possibility of finding fragments on all of the nodes is very less, if an attacker is not sure about fragment's location.

If number of nodes increases the probability of an intruder to obtain the data file decreases. If there are thousands of nodes in a cloud system, then that cloud system is relatively more secure.

iv) T-coloring

In T-coloring graph the vertices are colored to distinguish the node. While coloring the vertices one thing is kept in mind that two adjacent vertices does not appear in one T field. For example, suppose 'p' and 'q' are two adjacent vertices, then coloring is done in such a way that 'p' and 'q' does not appear in $T_{pq}$, where $T_{pq}$ is a set of nonnegative integers associated to the edge [p, q]. This is called vertex coloring.

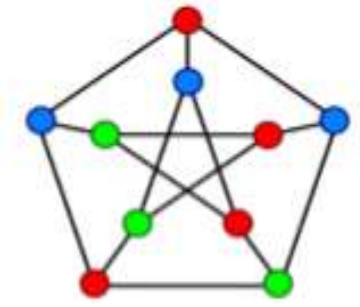

***Figure 2 T-coloring node presentations.***

Similarly, there's an edge coloring in which no two adjacent edges are of same color.

ALGORITHM 2: Fragment placement by T coloring [8].

```
Inputs and initialization:
$F= \{ F_1, F_{2,\ldots\ldots,} F_N \}$
$F = \{sizeof( F_1 ), sizeof( F_2 ), \ldots.. sizeof( F_N ) \}$
$Col = \{open\_color,close\_color\}$
$Cen = \{cen_{1,} cen_{2\ldots\ldots,} cen_{N,}\}$
$Col \leftarrow open\_color \ \forall p$
$Cen \leftarrow cen_q \ \forall p$
Compute:
$for\ each\ O_r \in O\ do$
    $Select\ S^i|S^i \leftarrow indexof\ (\ max\ (\ cen_q)\ )$
    $If\ col_S^i = open\_color\ and\ s_i >= o_r\ then$
        $S^i \leftarrow O_r$
        $s_q \leftarrow s_q - o_r$
        $col_S^i \leftarrow close\_color$
        $S^{i\prime} \leftarrow distance(S^i,T)$
        $Col_S^{q\prime} \leftarrow close\_color$
    $end\ if$
$end\ for$
```

v)Replication

Replication is in a controlled manner. So that only one replica of each fragment is made i.e in limited way. Due to replication the access time is reduced hence performance is increased. Again nodal placement of replicated fragments is done with the help of T-coloring.

ALGORITHM 3: For fragment's replication [8]

```
For each $O_r$ in O do
select $S^i$ that has max $(P_i^k + Q_k^i)$
if $col_S^i$ = open_color and $s_q >= o_r$ then
$S^i \leftarrow O_r$
$s_q \leftarrow s_q - o_r$
$col_S^i \leftarrow$ close_color
$S^{i'} \leftarrow$ mdistance($S^i$,T)
$Col_S^{i'} \leftarrow$ close_color
End  if
end for
```

## IV RESULTS AND ANALYSIS

In our methodology, person has to intrude large number of nodes to obtain significant data. This is because in our methodology fragments are stored on distinct nodes with the help of T-coloring. For an attack to be successful the number of nodes which are intruded must be greater than n.

There's an equation which determine an effort done by a person to attack a node.

$$E_{Total} = \min(E_{Auth}, n \times E_{Node}) \quad (1)$$

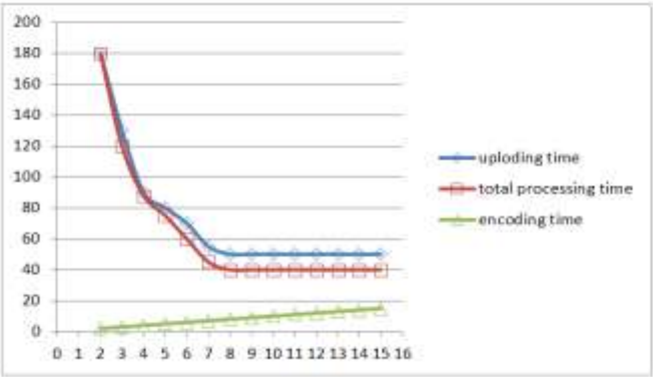

*Figure 3 Encoding and uploading time verses number of fragments*

Where $E_{Total}$ is effort necessary to breach the data; $E_{Auth}$ is an effort needed to break in authentication and $E_{Node}$ is effort needed to breach a single node.For experimental analysis, we selected text file of size not more than 1 MB. In figure 3 shows the relation of encoding and uploading time with the number fragments. Thus when we increase the number of fragments, the uploading time falls sharply with slight increase in encoding time. We also compared the increase in number of fragments with decoding and downloading time, in figure 4 shows the comparison between the same.

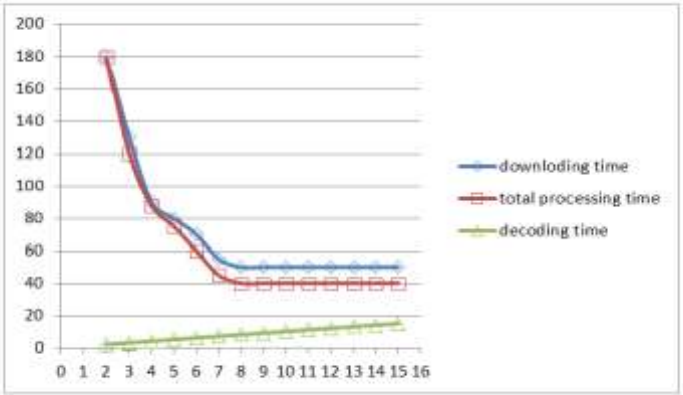

*Figure 4 Downloading and decoding time verses number of fragments*

From the above results we can say that increase in number of fragments will result in decrease in the downloading time along with the decrease in total processing time.

Thus moderate increase in number of fragments will result in decrease in processing time and increase in performance during both uploading and downloading the data.

## V CONCLUSION

In this dissertation we proposed a secured system for storage of data in cloud that is also very good in performance. The file which is uploaded on the server first encrypted, and then fragmentation and replication of fragments takes place. Nodes are assigned to the fragments and replicas with the help of T-coloring. Fragments are placed over the nodes in such a way that no node contains more than one fragment. This system of fragmentation and T-coloring increases the effort of an attacker to intrude the system. Even in case of successful attack on a fragment, no significant information is revealed to an attacker. In addition to a high level of security, performance of this system is also very good. In this replication is also in a controlled manner, so that performance is increased without compromising security.

## ACKNOWLEDGMENT

It is my great pleasure in expressing sincere and deep gratitude towards my guide Prof. B.K.Patil for providing me various sources, valuable and firm suggestion, guidance and constant support throughout this work.

## 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] T. Loukopoulos and I. Ahmad, “Static and adaptive distributed data replication using genetic algorithms,” Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp. 1270-1285.

[4] 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.

[5] L. M. Kaufman, “Data security in the world of cloud computing,” IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[6] S. U. Khan, and I. Ahmad, “Comparison and analysis of ten static heuristics-based Internet data replication techniques,” Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008, pp. 113-136.

[7] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, “Towards Secure Mobile Cloud Computing: A Survey,” Future Generation Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.

[8] A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, “Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, The Journal of Supercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706 .