ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Optimization of Performance and Security by Division and Replication of Data in Cloud

Gandepalli Tanuja
M.Tech
Department of CSE
Lendi Institute of Engineering and Technology
Jonnada, Vizianagaram,
AP, India.

1. Abstract

Cloud computing is a third party administrative control; here our data are outsourced so it gives rise to security concerns. Data compromise occurs due to attacks or within the nodes itself. High security measures needed to protect the data. In this paper, we propose Optimization of Performance and security by Division and Replication of Data in Cloud for excellent performance and security that collectively approaches the security and performance issues. In this methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes.

Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker, In Optimization of Performance and Security by Division and Replication of data in cloud methodology, it acquires more memory space and the data's won't be transact in a secure way & not in sequential order .To overcome these problem We choose the Algorithm of FS-Drops (Fragment and Snuffle -Drops) and Third Party Audit Cloud Server (TP-ACS).

Index Terms: ***Centrality, cloud security, fragmentation, replication, performance.***

1.1 Introduction

In this Internet era storing of data in manual scripts is not a wise thing we all know the importance of data storage and security. Dealing with data is became part of our day to day life. Storing of data is being done by Internet although some other transactions also being done by internet most of it roams around data so when come to security of data it will not providing sufficient Security .We need to opt another sophisticated way to store data, one among is cloud computing. Cloud computing is a third party administrative control; here our data is outsourced so it gives rise to security concerns. Data compromise occurs due to attacks or within the nodes itself. High security measures needed to protect the data. In this project, we propose Optimization of Performance and Security by Division and Replication of data in Cloud for excellent performance and security that collectively approaches the security and performance issues. In this methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes.

Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. In optimization of performance and security by division and replication of data in cloud methodology, it acquires more memory space and the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

data's won't be transact in a secure way & not in sequential order .To overcome these problem We choose the Algorithm of FS-Drops (Fragment and Snuffle -Drops) and Third Part Audit Cloud Server (TP-ACS).

2. Literature Survey

Providers such as Google and Amazon have the existing infrastructure to deflect and survive a cyber attack, but not every cloud has such capability. If a cybercriminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target.

Mazhar Al et al. [1] presented a technique to ensure the integrity, freshness, and availability of data in a cloud.

The public cloud outsourced data need to be secured. Unauthorized data access by other users and Processes (whether unintentionally or intentionally) must be prevented. A cloud must ensure throughput, reliability, and security. The third party requires more memory space and the data can't be transmitting in a secure way & not in sequential order. Unauthorized data access by other users and processes (whether accidental or deliberate) which must be prevented. The security mechanism must substantially increase an attacker's effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud.

So we can deduce that both security and performance for the next generation large-scale systems becomes critical, such as clouds. Therefore, we proposed, we collectively approach the issue of security and performance as a secure data replication problem. In our proposed system to overcome these problems we implemented division and replication of data in the cloud for excellent performance and security, we correlated the particular data replication between division of a file into fragments .third party and the end user any other person can't interfere due to security reasons .we implemented data replications by two algorithms are used first one is FS-Drops (fragment and snuffle -drops) which will fragment a file into 4 pieces and shuffled (like 1-2, 2-3, 3-4, 4-1). And store in different server so in future some server is not available are hacked we can get back our original data from remaining server. The second algorithm is third party audit cloud server, time to time will audit our storage sever for data integrity, also for every data modification it will do audit so that the storage server performance will not be affected and data will be very safe, data's sequential order will find easily, it provide better communication between the user and cloud, saves the file is an easy task.

An analysis of cloud computing security issues, Akhil Behl and Kanika Behl [2] investigating the vivid security issues and presents a cloud security solution.

Standards and regulations stated by the providers for the customers to ensure sufficient security. Virtualization security, identity and access management, threat management, content security, and data privacy need to be given priority and require more focus. Data encryption all through the lifecycle can be one method of data protection. In cloud we are not known where our data resides, what we know is these are shared servers.

D.Boru, et al. Energy-efficient data replication in cloud computing datacenters, [3] this project reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications.

Bharti Dhote, A.M. Kanthe, Secure Approach for Data in Cloud Computing,[4] described the method for data security, which is the major parameter of the quality of service. Paper includes data division, server misbehavior, checking integrity of data with the help of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

token pre-computation. The previous work does not support for dynamic insertion but here supports. This also ensures the data availability in case of communication link failure.

W. A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, [5] presented the data replication in cloud computing data centers with energy-efficiency and bandwidth consumption of the system. The results obtained guide the design of future data replication solutions.

Jules and opera [6] presented a technique to ensure the integrity, freshness, and availability of data in a cloud. The data migration 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 freshness of the data using a Markel tree. The file blocks, MAC codes, and version numbers are stored at various levels of the tree. The proposed technique in [6] heavily depends on the user's employed scheme for data confidentiality. Moreover, the probable amount of loss in case of data tempering as a result of intrusion or access by other VMs cannot be decreased. Our proposed strategy does not depend on the traditional cryptographic techniques for data security. Moreover, the OPSDR methodology does not store the whole file on a single node to avoid compromise of all of the data in case of successful attack on the node.

Our information is shared among cloud nodes. So the chances are that the data might be leaked. It is important to have a strong security strategy for giving relief. This can curb data leakage and protect your valuable data [7], Fragmentation and Data Allocation in the Distributed Environments‖, this paper focuses on fragmentation and data allocation. The fragmentation in a distributed database management system improves the level of concurrency and so automatically increases the system throughput for query processing. [8] In the existing system the data compromise may occur due to attacks by other users and nodes within the cloud and the employed security strategy must also take into account the optimization of the data retrieval time.

Cloud Security:

With the increasing popularity of cloud computing, technology experts along with security specialists are always trying different standards to secure their infrastructure in cloud locking them from outside networks. As of today there is no universal perfect solution for cloud security. Cloud devices are likely to attacks from cyber criminals.

Data privacy and data protection are major concerns for any security expert in an organization regarding their infrastructure in the cloud. Data may not get stored in the same system within a public or community cloud, resulting in multiple concerns legally. As of today, there are no safety standards and regulations stated by the providers for the customers to ensure sufficient security. Virtualization security, identity and access management, threat management, content security, and data privacy need to be given priority and require more focus.

Data encryption all through the lifecycle can be one method of data protection. In cloud we are not known where our data resides, what we know is these are shared servers. Our information is shared among cloud nodes. So the chances are that the data might be leaked. It is important to have a strong security strategy for giving relief. This can curb data leakage and protect your valuable data [9].

Data fragmentation

In large scale system the security depends upon the whole system as well as the single node of a system. If the file is attacked by an attacker then there will be single point failure. So to avoid this data division or fragmentation technology is used. Fragmentation can increase an attacker's effort. In a fragmentation schema file f is split into n fragments, all fragments are signed and distributed to n remote servers, one fragment per

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

server. The user can reconstruct file f by accessing m fragments arbitrarily chosen. [10].

Replication

The tremendous growth of cloud computing enabled the deployment of immense IT services that are built on top of geographically distributed platforms and offered globally. For better reliability and performance, resources are replicated at the redundant locations and using redundant infrastructures. Number of data replication methods has been proposed to address an exponential increase in Internet data traffic and optimize energy and bandwidth in datacenter systems [11]. Availability is assured by replication, without encryption, with the idea that files can be encrypted by the client before storing when confidentiality is an issue [12]. Data replication means maintaining multiple copies of same data on same server or on different servers. If data is present at one site only, then it will be single point failure. Server will face a heavy load balancing condition and system performance. Also if that site fails, all that data will be lost, this is also a serious concern. Replication is necessary for maintaining the availability, performance level, backing up the data and also for balancing load [13].

2.1 Related Work

The utilized security technique use should likewise consider the advancement of the information recovery time. Optimization Performance and Security by Division and Replication of Data in Cloud (OPSDR).In this methodologies, the security and execution issues. We divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker, In optimization of performance and security by division and replication of data methodology, it acquires more memory space and the data's won't be transact in a secure way & not in sequential order .To overcome these problem We choose the Algorithm of FS-Drops (Fragment and Snuffle -Drops) and Third Party Audit Cloud Server (TP-ACS).

Manzano et.al. [14] proposed a frame work, a collectively approach the Optimization performance security by Division and Replication of Data in Cloud. In our proposed system to overcome these problems we implemented division and replication of data in the cloud for excellent performance and security, we correlated the particular data replication between division of a file into fragments .third party and the end user any other person can't interfere due to security reasons .we implemented data replications by two algorithms are used first one is FS-drops (fragment and snuffle -drops) which will fragment a file into 4 pieces and shuffled (like 1-2, 2-3, 3-4, 4-1). And store in different server so in future some server is not available are hacked we can get back our original data from remaining server. The second algorithm is third party audit cloud server, time to time will audit our storage sever for data integrity, also for every data modification it will do audit so that the storage server performance will not be affected and data will be very safe, data's sequential order will find easily, it provide better communication between the user and cloud, saves the file is an easy task.

Deswarte et.al [15**]** Cloud computing is an emerging paradigm that provides computing resources as a service over a network. Communication resources often become a bottleneck in service provisioning for many cloud applications. Therefore, data replication, which brings data closer to data consumers, is seen as a promising solution. It allows minimizing network delays and bandwidth usage. In this paper we study data replication in cloud computing data centers. Unlike other approaches available in the literature, we consider both energy efficiency and bandwidth consumption of the system, in addition to the improved Quality of Service as a result of the reduced communication delays. The evaluation results obtained during extensive simulations help to unveil Performance and energy

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

efficiency tradeoffs and guide the design of future data replication solutions.

Carlson [8] have proposed an analysis over cloud computing for the issues of security and have proposed solution within that. The proposed solution over security concerned with cloud computing data. Neela [9] have concerned the same security issues within quality of service parameter for data security. They had discussed over the misbehavior of server division of data for checking the data integrity for helping the pre-computation token. These previous work is not supporting the dynamic insertion supports. The process is ensuring the case of data availability for failure of link communication.

A. R. Khan et.al in their paper **[16]** said Cloud computing is emerging as a powerful architecture to perform large-scale and complex computing. It extends the information technology (IT) capability by providing on demand access to computer resources for dedicated use. The information security and privacy are the major concerns over the cloud from user perspective. This paper surveys and evaluates the architecture, data security and privacy issues in cloud computing like data confidentiality, integrity, authentication, trust, service level agreements and regulatory issues. The objective of this paper is to review comprehensively the current challenges of data security and privacy being faced by cloud computing and critically analyses these issues.

In this paper, to improve the resource limitation of mobile devices, mobile users may utilize cloud-computational and storage services. Although the utilization of the cloud services improves the processing and storage capacity of mobile devices, the migration of confidential information on untreated cloud raises security and privacy issues. Considering the security of mobile-cloud-computing subscribers' information, a mechanism to authenticate legitimate mobile users in the cloud environment is sought. Usually, the mobile users are authenticated in the cloud environment through digital credential methods, such as password. Once the users' credential information theft occurs, the adversary can use the hacked information for impersonating the mobile user later on. The alarming situation is that the mobile user is unaware about adversary's malicious activities. In this paper, a light-weight security scheme is proposed for mobile user in cloud environment to protect the mobile user's identity with dynamic credentials. The proposed scheme offloads the frequently occurring dynamic credential generation operations on a trusted entity to keep minimum processing burden on the mobile device. To enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange.

2.2 Proposed Solution

Our main aim is to build a system where Optimization of Performance and Security of data in the cloud is enhanced. We implemented division and replication of data in the cloud for excellent performance and security; we correlated the particular data replication between division of a file into fragments. Third party and the end user, any other person can't interfere due to security reasons. We implemented data replications by two algorithms are used first one is FS-Drops (Fragment and Snuffle -Drops) Which will fragment a file into 4 pieces and shuffled (like 1-2, 2-3, 3-4, 4-1) And store in different server So in future some Server is not available are Hacked we can get back our original data from remaining Server.

The second algorithm is Third Party Audit Cloud Server (TP-ACS), Time to time will audit our Storage Sever for Data Integrity, also for every data modification it will do audit So that the Storage Server Performance will not be affected and Data will be very Safe. Data's sequential order will find easily, a fast and efficient data retrieval to cloud storage, it provide better Communication between the user and cloud, saves the file is an easy task. The proposed system based on the following model:

The OPSDR (Optimal Performance and Security by Division and Replication of Data in Cloud) techniques

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

solve the performance and security problem. The nodes in the cloud separated with definite distance by using Third Party Audit Cloud Server (TP-ACS) and FS-Drops (Fragment and Snuffle -Drops).The fragment of the single file store in different node. To avoid replication problem. We proposed OPSDR technique which fragments files and replicates the strategic locations in cloud. The OPSDR prevent the attacks even if attack is severe no meaningful data revealed to attacker.

Non-cryptographic scheme is proposed to make retrieval and placement on data. Using these techniques we control the file fragments replication.

1. Splitting and Merging Module
2. Decryption,
3. Fragment Allocation,
4. Third Party Auditor and
5. Cloud server

3. System Architecture

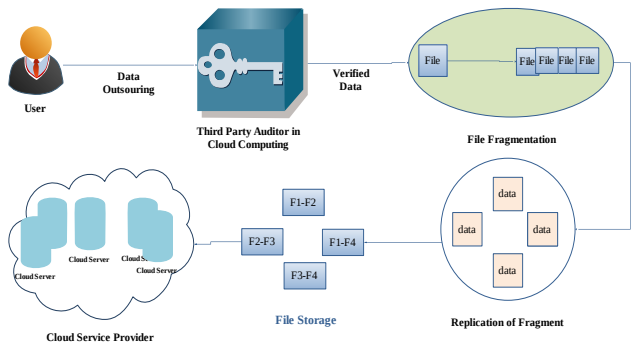


Fig: 3a System Architecture

Algorithm:

- FS-Drops (Fragment and Snuffle -Drops)
- Third Party Audit Cloud Server(TP-ACS)

Fs-drops

This FS-Algorithm for file allocation that guarantees high assurance, availability, and scalability in a large distributed file system. The algorithm can use replication and fragmentation schemes to allocate the files over multiple servers. The file confidentiality and integrity are preserved, even in the presence of a successful attack that compromises a subset of the file servers. The algorithm is adaptive in the sense that it changes the file allocation as the read-write patterns and the location of the clients in the network change. In this FS-DROPS (Fragment and shuffle) algorithm will fragment a file into 4 pieces and shuffled (like 1-4, 2-3, 3-2, 4-1) And stored in different server. In future when the server is low or hacked by attackers, we can retrieve our original data by the rest of the server.

Third Party Audit Cloud Server (TP-ACS)

This algorithm will audit our Storage Sever for Data Integrity, and also audit if any modification will be done in data with the regular intervals of time. , So that the Storage Server Performance will not be affected and Data stored in the server also be very secured. Here a third party can be used as an auditor.

In cloud environment the computing resources are under control of service provider and the third-party auditor ensures the data integrity over out sourced data. TPA used to protect the privacy and integrity of outsourced data. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud. the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. It supports scalable and efficient public auditing in the Cloud Computing. In particular, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data.

Platform Overview

Introduction to Cloud Computing

Cloud computing is Internet based development and use of computer technology. In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

The term cloud is used as a metaphor for the Internet, based on how the Internet is depicted in computer network diagrams and is an abstraction of the underlying infrastructure it conceals. Typical cloud computing services provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers.

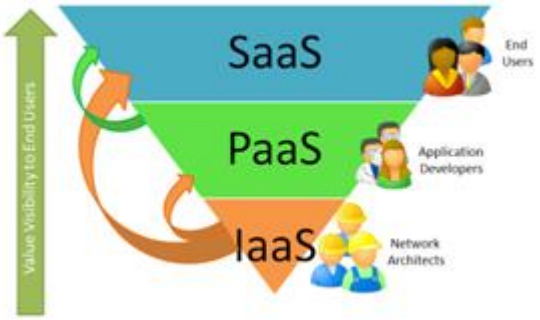


Fig: 3b Cloud Services

Types of Services

Cloud computing can describe services being provided at any of the traditional layers from hardware to applications. In practice, cloud service providers tend to offer services that can be grouped into three categories: software as a service, platform as a service, and infrastructure as a service.

Software as a service (SaaS)

Software as a service features a complete application offered as a service on demand. A single instance of the software runs on the cloud and services multiple end users or client organizations. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service.

Platform as a service (PaaS)

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. There are at least two perspectives on PaaS depending on the perspective of the producer or consumer of the services:

- Someone *producing* PaaS might produce a platform by integrating an OS, middleware, application software, and even a development environment that is then provided to a customer as a service.
- Someone *using* PaaS would see an encapsulated service that is presented to them through an API. The customer interacts with the platform through the API, and the platform does what is necessary to manage and scale itself to provide a given level of service. Virtual appliances can be classified as instances of PaaS. A content switch appliance, for example, would have all of its component software hidden from the customer, and only an API or GUI for configuring and deploying the service provided to them.

PaaS offerings can provide for every phase of software development and testing, or they can be specialized around a particular area such as content management. Commercial examples of PaaS include the Google Apps Engine, which serves applications on Google's infrastructure. PaaS services such as these can provide a

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

powerful basis on which to deploy applications, however they may be constrained by the capabilities that the cloud provider chooses to deliver.

Infrastructure as a service (IaaS)

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications. Commercial examples of IaaS include Joyent, whose main product is a line of virtualized servers that provide a highly available on-demand infrastructure.

Algorithm Specification

Algorithm 1 Algorithm for fragment placement
Inputs and initializations:
O = {O1;O2; :::;ON}
o = {sizeof (O1); sizeof (O2); :::::; sizeof (ON)}
col = {open color; close color}
cen = {cen1; cen2; :::; cenM}
col _ open color¦ i
cen _ ceni¦ i
Compute:
for each Ok > O **do**
select Si S Si _ indexof(max(ceni))
if colSi = open color and si >= ok then
Si _ Ok
si _ si – ok
colSi _ close color
Si'_ distance (Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si'*/
colSi. _ close color
end if
end for

Algorithm 2 Algorithm for fragments replication
for each Ok in O **do**
select Si that has max(Rik+Wik)
if colSi = open color and si >= ok then
Si _ Ok
si _ si – ok
colSi _ close color
Si'_ distance(Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si'*/
colSi. _ close color
end if
end for

Symbols	Meanings
M	Total number of nodes in the cloud
N	Total number of file fragments to be placed
O_k	k-th fragment of
O_k	file Size of O_k
S^i	i-th node
S_i	SizeofS^i
Cen_i	Centrality measure for S^i
ColSi	Color assigned to S^i
T	A set containing distances by which assignment of fragments must be separated
r^i_k	Number of reads for O_k from S^i
R^i_K	Aggregate read cost of r^i
NNi K	Nearest neighbor of S^iholding O_k
$c(i,j)$	Communication cost between $S^i$and S^j
P_k	Primary node for O_k
R_k	Replication schema of O_k
RT	Replication time
w^i_k	Number of writes for O_k from S^i

TABLE: Notations and their meanings

3.1 Data Fragmentation

The security of a large-scale system, such as cloud depends on the security of the system as a whole and the security of individual nodes. A successful intrusion into a single node may have severe consequences, not only for data and applications on the victim node, but also for the other nodes. The data on the victim node may be revealed fully because of the presence of the whole file [17]. A successful intrusion may be a result of some software or administrative vulnerability [17]. In case of homogenous systems, the same flaw can be utilized to target other nodes within the system. The success of an attack on the subsequent nodes will require less effort as compared to the effort on the first node. Comparatively, more effort is required for heterogeneous systems. However, compromising a

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

single file will require the effort to penetrate only a single node. The amount of compromised data can be reduced by making fragments of a data file and storing them on separate nodes. If M = 30, s = 10, and z = 7, then P (10; 7) = 0:0046. However, if we choose M = 50, s = 20, and z = 15, then P (20; 15) = 0:000046. With the increase in M, the probability of a state reduces further. Therefore, we can say that the greater the value of M, the less probable that an attacker will obtain the data file. In cloud systems with thousands of nodes, the probability for an attacker to obtain a considerable amount of data reduces significantly. However, placing each fragment once in the system will increase the data retrieval time. To improve the data retrieval time, fragments can be replicated in a manner that reduces retrieval time to an extent that does not increase the aforesaid probability.

4. OPSDR

4.1 System Model

Consider a cloud that consists of M nodes, each with its own storage capacity. Let S^i represents the name of i-th node and s_i denotes total storage capacity of S^i. The communication time between S^i and S^j is the total time of all of the links within a selected path

From S^i to S^j represented by c(i, j). We consider N number of file fragments such that O_k denotes k-th fragment of a file while o_k represents the size of k-th fragment. Let the total read and write requests from S^i for O_k be represented by r_k^i and w_k^i, respectively. Let P_k denote the primary node. that stores the primary copy of O_k. The replication scheme for O_k denoted by R_k is also stored at P_k. Moreover, every S^i contains a two-field record, storing P_k for O_k and NN^i_k that represents the nearest node storing O_k. Whenever there is an update in O_k, the updated version is sent to P_k that broadcasts the updated version to all of the nodes in R_k. Let b(i,j) and t(i,j) be the total bandwidth of the link and traffic between sites S^i and S^j, respectively . The centrality measure for S^i is represented by cen_i. Let $col_S i$ store the value of assigned color to S^i. The $col_S i$ can have one out of two values, namely: open color and close color. The value open color represents that the node is available for storing the file fragment. The value close color shows that the node cannot store the file fragment. Let T be a set of integers starting from zero and ending on a pre-specified number. If the selected number is three, then T = {0; 1; 2; 3}. The set T is used to restrict the node selection to those nodes that are at hop-distances not belonging to T. For the ease of reading, the most commonly used notations are listed in Table 1.

Algorithm 1 Algorithm for fragment placement
O = {O1;O2; :::;ON}
o = {sizeof (O1); sizeof (O2); :::::; sizeof (ON)}
col = {open color; close color}
cen = {cen1; cen2; :::; cenM}
col _ open color¦ i
cen _ ceni¦ i
Compute:
for each Ok > O **do**
select Si S Si _ indexof(max(ceni))
if colSi = open color and si >= ok then
Si _ Ok
si _ si – ok
colSi _ close color
Si'_ distance (Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si'*/
colSi. _ close color
end if
end for

Algorithm 2 Algorithm for fragments replication
for each Ok in O **do**
select Si that has max(Rik+Wik)
if colSi = open color and si >= ok then
Si _ Ok
si _ si – ok
colSi _ close color
Si'_ distance(Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si'*/
colSi. _ close color
end if
end for
end for

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Once the file is split into fragments, the OPSDR methodology selects the cloud nodes for fragment placement. The selection is made by keeping an equal focus on both security and performance in terms of the access time. We choose the nodes that are most central to the cloud network to provide better access time. For the aforesaid purpose, the OPSDR methodology uses the concept of centrality to reduce access time. The centralities determine how central a node is based on different measures as discussed in Section 3.2. We implement OPSDR with three centrality measures, namely: **(a)** betweenness, **(b)** closeness, and **(c)** eccentricity centrality. However, if all of the fragments are placed on the nodes based on the descending order of centrality, then there is a possibility that adjacent nodes are selected for fragment placement. Such a placement can provide clues to an attacker as to where other fragments might be present, reducing the security level of the data. To deal with the security aspects of placing fragments, we assign colors to the nodes, such that, initially, all of the nodes are given the open color. Once a fragment is placed on the node, all of the nodes within the neighborhood at a distance belonging to T are assigned close color. In the aforesaid process, we lose some of the central nodes that may increase the retrieval time but we achieve a higher security level. If somehow the intruder compromises a node and obtains a fragment, then the location of the other fragments cannot be determined. The attacker can only keep on guessing the location of the other fragments. However, as stated previously in Section 3.1, the probability of a successful coordinated attack is extremely minute. The process is repeated until all of the fragments are placed at the nodes. Algorithm 1 represents the fragment placement methodology.

In addition to placing the fragments on the central nodes, we also perform a controlled replication to increase the data availability, reliability, and improve data retrieval time. We place the fragment on the node that provides the decreased access cost with an objective to improve retrieval time for accessing the fragments for reconstruction of original file.

To handle the download request from user, the cloud manager collects all the fragments from the nodes and reassembles them into a single file. After-wards, the file is sent to the user.

3 Discussions

A node is compromised with a certain amount of an attacker's effort. If the compromised node stores the data file in totality, then a successful attack on a cloud node will result in compromise of an entire data file. However, if the node stores only a fragment of a file, then a successful attack reveals only a fragment of a data file. Because the OPSDR methodology stores fragments of data files over distinct nodes, an attacker has to compromise a large number of nodes to obtain meaningful information.

Attack	Description
Data Recovery	Rollback of VM to some previous state. May expose previously stored data.
Cross VM attack	Malicious VM attacking co-resident VM that may lead to data breach.
Improper media sanitization	Data exposure due to improper sanitization of storage devices.
E-discovery	Data exposure of one user due to seized hardware for investigations related to some other users.
VM escape	A malicious user or VM escapes from the control of VMM. Provides access to storage and compute devices.
VM rollback	Rollback of VM to some previous state. May expose previously stored data.

TABLE 2: Various attacks handled by OPSDR methodology

Nodes must be greater than n because each of the compromised nodes may not give fragment in the OPSDR methodology as the nodes are separated based on the fragments and snuffling algorithm. Alternatively, an attacker has to compromise the authentication system of cloud. The effort required by an attacker to compromise a node

$$E_{Conf} = \min(E_{Auth}; n \times E_{BreakIn}); \quad (8)$$

where E_{Conf} is the effort required to compromise the confidentiality, E_{Auth} is the effort required to compromise authentication, and $E_{BreakIn}$ is the effort required to compromise a single node. Our focus in this paper is on the security of the data in the cloud and we do not take into account the security of the authentication system. Therefore, we can say that to obtain n fragments, the effort of an attacker increases by a factor of n.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Moreover, in case of the OPSDR methodology, the attacker must correctly guess the nodes storing fragments of file. Therefore, in the worst case scenario, the set of nodes compromised by the attacker will contain all of the nodes storing the file fragments. From Equation (1), we observe that the probability of the worst case to be successful is very low. The probability that some of the machines (average case) storing the file fragments will be selected is high in comparison to the worst case probability. However, the compromised fragments will not be enough to reconstruct the whole data. In terms of the probability, the worst, average, and best cases are dependent on the number of nodes storing fragments that are selected for an attack. Therefore, all of the three cases are captured by Equation (1).

Besides the general attack of a compromised node, the OPSDR methodology can handle the attacks in which attacker gets hold of user data by avoiding or disrupting security defenses. Table 2 presents some of the attacks that are handled by the OPSDR methodology. The presented attacks are cloud specific that stem from clouds core technologies.

Table 2 also provides a brief description of the attacks. It is noteworthy that even in case of successful attacks (that are mentioned), the OPSDR methodology ensures that the attacker gets only a fragment of file as OPSDR methodology stores only a single fragment on the node. Moreover, the successful attack has to be on the node that stores the fragment.

5. User Interface Design

Adaptive Team Collaborative Process ATCP recognizes user interface analysis and design as separate discipline as per the ATCP the user interface design has the following advantages like follow very similar process pattern as in object-oriented analysis and design .However, do not focus on what happens "inside" system – just at the system boundary build the content model and navigation map using UML

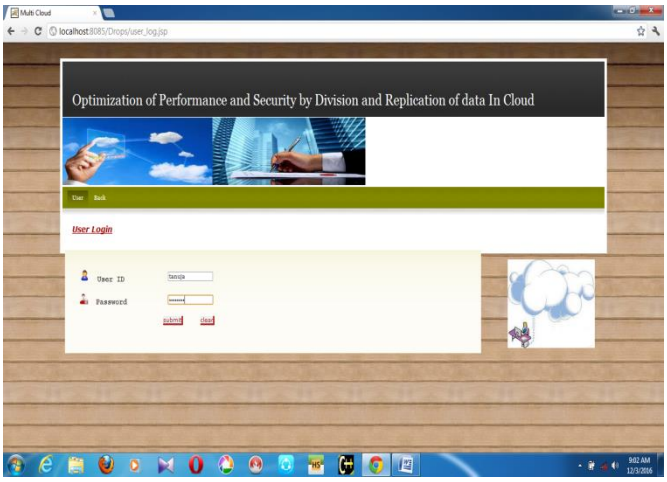


Fig:5a Optimization Performances by Division and Replication of Data in Cloud User login page

5.1 Data Replication

Data replication which brings data (e.g., databases) closer to data consumers (e.g., cloud applications) is seen as a promising solution. It allows minimizing network delays and bandwidth usage. In this project we study data replication in cloud computing data centers. Unlike other approaches available in the literature, we consider both energy efficiency and bandwidth consumption of the system.

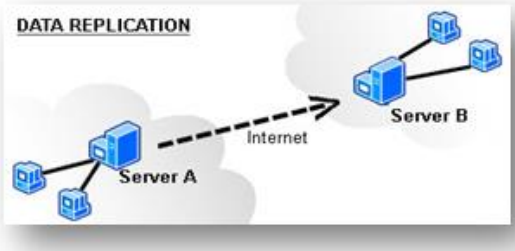


Fig: 5b Display list of Data Replication

Multi cloud storage

Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks. The cloud users upload the data into multi cloud. Cloud computing environment is constructed

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud .A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

Third Party Auditor

Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data blocks and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data blocks. If any modification tried by cloud owner a alert is send to the Trusted Third Party.

Cloud User

The Cloud User who has a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. The User's Data is converted into data blocks. The data block is uploaded to the cloud. The TPA views the data blocks and Uploaded in multi cloud. The user can update the uploaded data. If the user wants to download their files, the data's in multi cloud is integrated and downloaded.

5.2 Flowchart Diagram

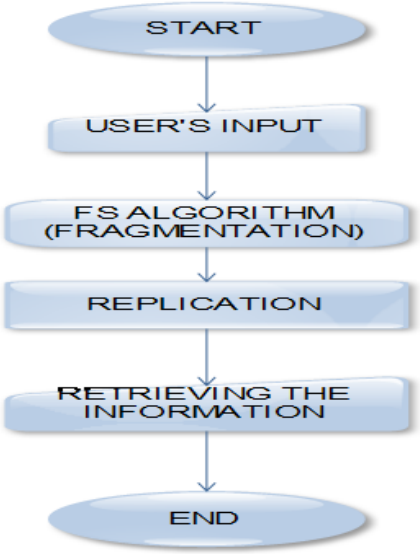


Fig: 5c Flow Chart Diagram

5.3 Dataflow Diagram:

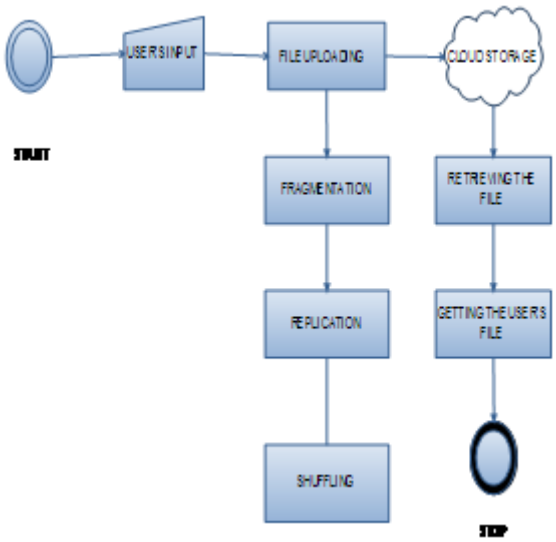
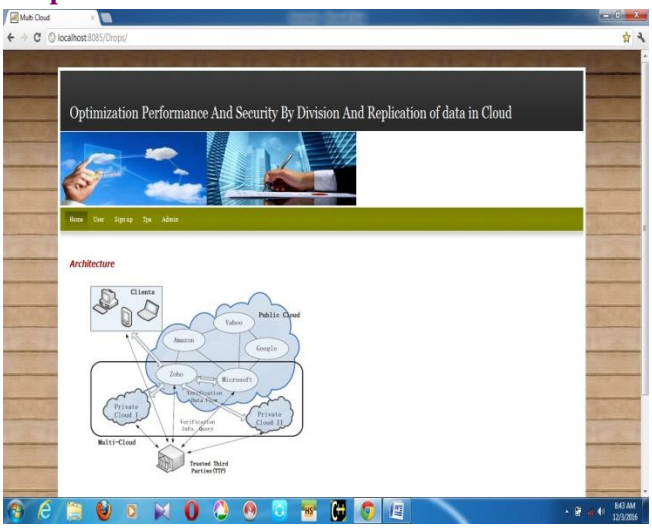


Fig:5d Dataflow Diagram

Sample Screen



CONCLUSIONS

- The data file was fragmented and the fragments are dispersed over multiple nodes.
- The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack.
- No node in the cloud, stored more than a single fragment of the same file. Our proposed methodology resulted in increased security level of data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- Currently with the drops methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The aforesaid future work will save the time and resources to download, update and upload the file again.

REFERENCES

[1] Mazhar Al, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, Albert Y.Zomaya "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security"DOI 10.1109/TCC.2015.2400460, IEEE Transactions on Cloud Computing.

[2] Akhil Behl and Kanika Behl, ‖An analysis of cloud computing security issues, IEEE 2012.

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

[4] Bharti Dhote, A.M. Kanthe, Secure Approach for Data in Cloud Computing, International Journal of Computer Applications (0975 – 8887) Volume 64– No.22, February 2013.

[5] W. A. Jansen, ―Cloud hooks: Security and privacy issues in cloud computing, In 44th Hawaii IEEE International Conference on System Sciences (HICSS), 2011, pp. 1-10.

[6]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.

[7] 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.

[8] Frederick R. Carlson Saint Petersburg College Saint Petersburg, Florida 352-586-2621 "Security Analysis of Cloud Computing"fcarlson@ieee.org

[9] K.L.NEELA et al. "A Survey on Security Issues and Vulnerabilities on Cloud Computing "International Journal of Computer Science & Engineering Technology (IJCSET)

[10] MukeshSinghal and Santosh Chandrasekhar, TingjianGe, Ravi Sandhu and Ram Krishnan, Gail-JoonAhn, Elisa Bertino," Collaboration in Multicloud Computing Environments: Framework and Security Issues IEEE Transactions on Cloud Computing VOL:46 NO:2 YEAR 2013

[11] Nicoleta - Magdalena Iacob (Ciobanu), Fragmentation and Data Allocation in the Distributed Environments, Annals of the University of Craiova, Mathematics and Computer Science Series Volume 38(3), 2011.

[12] DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE

[13] DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE

[14] 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, A Hybrid Cloud Approach for Secure Authorized Replication" IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013.

[15] Y. Deswarte, L.Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, 110-121, 1991.

[16] A. R. Khan, M. Othman, S. A. Madani, S. U. Khan, "A survey of mobile cloud computing application models," IEEE Communications Surveys and Tutorials, DOI: 10.1109/SURV.2013.06261

Author Details

Gandepalli Tanuja is currently pursuing her 2 years M.Tech in Department of Computer Science and Engineering at Lendi Institute of Engineering and Technology, Jonnada, Vizianagaram, AP, India. Her area of interest includes Cloud Computing.