Load Balancing Approach in Different Cloud Environment

Er. Ajit Kumar Singh[1], Dr.Archana[2], Mr. Kapil Saini[3]
Student Kurukshetra University, GEC, Panipat, Haryana
AssociateProfessor, CSE Department, Geeta University
Assistant Professor, CSE Department, Geeta University
ajitkrsingh@alchemysofttech.com,ksmeetsaini@gmail.com,
archanacse@geeta.edu.in

Abstract

Amidst the serious issue of cloud-computing, load adjusting is the basic issue. It tends to be finished through asset the executives, task booking, effective virtualization, and assignment asset planning [3]. In this head, the creators have demonstrated to better the cloud execution over load offsetting with shortcoming pattern. Wrong overseer, reiteration and check showing have been utilized to instrument adaptation to non-critical failure (receptive and proactive). This eliminates the flawed hub and doesn't make them accessible for task till its recuperation. Additionally, while portion load among handle, accomplishment proportion and past burden data is likewise contemplated. This has worked on the nature of administration as undertaking is getting planned with that hub whose achievement rate is more and present burden is less [1].

1. Introduction:

Cloud-computing has recently show up as another sort of the utility-based processing model for facilitating and conveying equipment and programming "as administrations". It furnishes its clients with the disarray of outright figuring and stockpiling assets which are perhaps accessible on-request from everyplace and whenever. Cloud-computing is wonderful since it drop the necessity for its client to prepare for material, by acknowledgment IT endeavors to begin from the little and to improvement assets just when there is an ascent in help application. All things considered, in sprit of this, the advancement of way to deal with make distributed computing strong is right now at its origin, with many issues still to be sent [1].

"The Cloud is a nature of equal and held onto framework rest of an assortment of snared and venerated PCs that are elements lead and introduced as at least one bound together figuring resource(s) in light of administration level arrangements laid out through understanding among the help laborer and customers" [2].

2. Proposed Methodology:

The essential thought behind this examination work is to improve the Performance, Scalability, Availability and Security in a cloud setting. To improve the presentation and accessibility in cloud, proposed philosophy is displayed in figure 1.3. FirstuploadtheHadoopDataFileSystem(HDFS)files.Theconsignmentmanagercompo nent fetches these HDFS files on the basis of First Come First Served. All the filesfetched by Load Balancer are divided into small and equal size of chunks. Load Balancermodule fetches the effective engine id having the powerful configuration and minimum loadassigned.Thevirtualmachineidhelpstoidentifythechunksstoredonaserver.Thisme chanism improves the performance and accessibility of information on cloud. Further toensure security of information in cloud environment, the secret message text policy basedattributebased encryption algorithm is used.

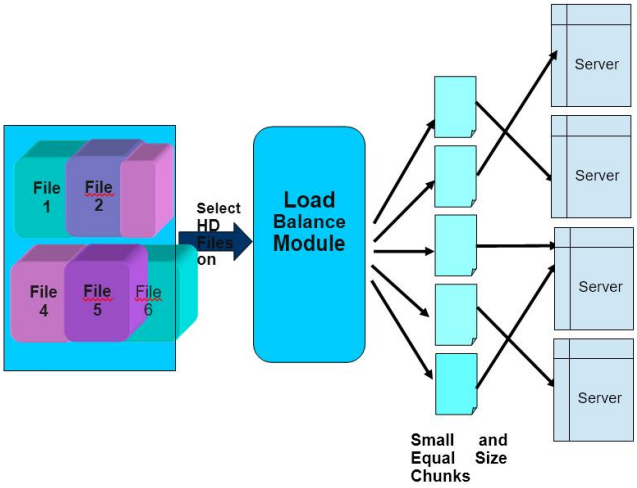

Fig. 1|Proposed Methodology

3. Objectives:

- To study the present security systems in Cloud Computing.
- To analyze and compare the present security techniques.
- Design an improved security system in Cloud Computing.
- Design effective Load Balancer Module with Scheduling algorithm in cloud computing.
- Apply data division into chunk for improving performance and availability in cloud computing.
- Implement/ stimulate the improved security system in Cloud Computing.
- Compare and analyze the performance of proposed security system with existing security system in Cloud Computing.

4. Existing Techniques:

Various algorithms enclose devising so far but the outcomes are not up to the satisfactory levels. Several of the real methods are listed and discussed below:

- **Scalability in computing of cloud**

An exhilarating & advantageous feature making cloud worthwhile to adopt [41]:Singular of the vital repayments of utilizing distributed computing worldview is its versatility. It is particularly adaptable offer the client's interest. Distributed computing permits clients or cloud sellers business to effortlessly increase or scale down their IT prerequisites as and when required [41].

Provisioning the capital precisely by carrying out Auto scaling system pursuing the cloud first decision for the different web based business associations dwelling on it [40].

- **Cloud Availability [12]**
  Cloud has the assets of individual effortlessly arrived at 24X7 hours. The openness trademark pursues cloud every association their most memorable decision to maintain their business. The online business associations like Amazon, Flipkart, and Snap bargain and so on are dependent on the openness of cloud.

- **Cloud Security [14]**
  This composition examines the information security in processing of cloud and furthermore centers on the investigation of data in the cloud and all viewpoints that are connected with concerning wellbeing. It additionally examines the plausible apprehension about information wellbeing during the cloud circumstance and their answers embrace by a grouping of specialist organizations to protect security of information. Examination paper will leave in to subtleties of guard for Data rules with approaches used to guarantee most extreme stronghold of information by diminishing dangers as well as dangers. Information accessibility in the cloud is profitable for various applications [4] [2.2].

- **Security intimidation in cloud**
  Processing of cloud is confronting a great deal of safety issues. Those issues are recorded beneath [4] [2.2]:

    - Information misfortune.
    - Noxious insiders.
    - Weakness of points of interaction and APIs.
    - Seizing of record and administration.
    - Spillage of information.
    - Forswearing of administration.
    - Innovation sharing gamble.
    - Coordination of information and assurance.

- **Load Balancing**

Now the most decisive tackle in computing of cloud is balancing of load. So, in order to manage this face up to there is a necessity of a divided solution. Cloud computing theatre an extremely significant role in assigning the accurate work to the servers. There are also chances of assorted kinds of safety issues, so following will be discussing some breed of security issues in this cloud computing technology. Some techniques have been taken into consideration in load balancing in large scale area. This has also come with the proper solutions and many divided rules and calculations have been examined to further develop the exhibitions boundaries. Cloud system associated with 3 most important workings issues such as [5] [3.3].

- Clients
- Data center
- Distributed servers

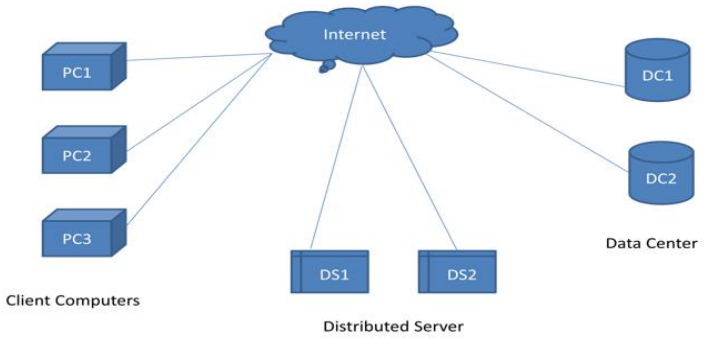

Figure 2 Appropriate cloud computing explanation

5. **Security Requirements In Cloud Computing:**
ISO (International standard association), Information Security ought to cover various suggested substance. Processing of cloud security ought to other than direct in such manner to turn into a great and secure innovation arrangement [4] [2.2]. Information Security prerequisites based on boundaries which are obligatory for public cloud, Private cloud and half breed cloud in distributed computing are displayed in figure 3.1.This figure additionally portrays the

administrations of cloud based on security necessities which are discretionary and important.

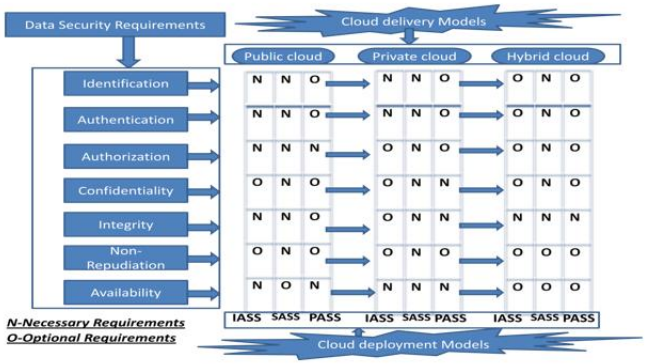

Figure 3 Security Requirements of Security in computing-cloud

Figure 3, addresses the security necessities in data firmly got together with the sending model of cloud and conveyance models [23]. In Figure 3.1, the different cloud conveyance models and sending models are matched facing the security prerequisite for data where "N" addresses important necessity sand "o" addresses the discretionary necessities. Anyway future assignment is required in exploring of the ideal equilibrium expected in getting Cloud registering. Figure 3 ought to be seen in setting as a rule in evaluating the security level. The cloud necessities of safety will be featured underneath in setting of Cloud registering.

6. **Parameters Of Security Algorithms:**
In cloud calculation, information security isn't just worried about encryption yet additionally numerous different cycles. Chance of information misfortune relies on the accompanying boundaries.

- Reset of information
- Transit of information
- **Reset of information:** At the point when cloud client gets to their information from the cloud with the assistance of web this is alluded as Reset of information. This cycle works with live information though reinforcements of information.
- **Transit of information:** Snapshot of information during the time spent done in the cloud is alluded as travel of information. At the point when client transfer their

data on the cloud around then it refereed as travel of information. So this is the ideal opportunity for the programmer to commandeering client's information, to forestall this Encryption and Decryption cycle ought to be embraced [16].

Encryption [4] [2.2] and unscrambling plays a significant part in cryptography methods. Presently day's two kinds of cryptography techniques utilized for encryption and decoding of information those are:

- Encryption with Symmetric key.
- Encryption with Asymmetric key.

Analyst reasons that Encryption with Asymmetric key is the most superb procedure for the Security of information. In this procedure two keys explicitly private and public will be utilized among source and collector to scramble and decode the information.

Presently a day's Different cryptography strategies are utilized for information encryption. Through the utilization of Cryptography level of safety will be further developed equivalent to a few significant boundaries likewise is expanded these are:

- Level of information insurance
- Integrity of items
- User confirmation
- Availability

Cryptography is the cycle for concealing unique substance at the hour of sending plain message. The Process of cryptography as follows:

- By use of encryption method cipher text will be encrypted.
- Assign encrypted key with this encrypted text at the sender end.
- Send this encrypted text with key to the other end.
- Decrypt this message at receiver end with the help of decryption key.

There are three basic algorithm and function used of cryptography [16].

- Ciphers Block
- Ciphers Stream
- Hash Functions
- Cipher Block

Cipher block: is an algorithm for encryption of data. This algorithm create block of data which are required for the user. So this algorithm applied on whole bock instead of every bit of data with the use of block mechanism this is called cipher block.

Cipher stream: Cipher stream technique [9] also known as state cipher because it is depending upon the cipher current state. This is not used block for encryption like cipher block. Basically this is the stream dependent method so here encryption will be applied on each data bit as well as encryption key also is applied on each data bit one at a time. Same procedure adopted at the time of decryption.

Hash function: Hash capability is the numerical capability .Hash capability replaces the info text worth to line of alphanumeric. This strategy likewise guarantees that no two strings can have same line of alphanumeric as a result. Hash capability is exceptionally straightforward numerical capability displayed as underneath [16].

F(x) = x mod 10. (1)

These previously mentioned strategies and procedures are broadly utilized for encoding the information in the cloud to guarantee security of information. These procedures might shift starting with one situation then onto the next. Anything that procedure is utilized these are enthusiastically prescribed strategies to guarantee the information security in both private and public mists.

Algorithm for (LB) Load Balancing

In today's state of affairs Computing in the cloud has became the most popular technique which is been adopted and used by several users all over the world. And this due it's flexible and easy to way nature. Several organizations and companies are using clouds in order to reach their customers in all parts of the area. This has also been used as it performance parameters are been enhancing day by day. In spite of the fact that mists are partitioned as open, private and mixture models however there wariness will be taken against the security of the information which has been saved in cloud. Presently just barely saving information yet it assumes a vital part in various regions like all person to person communication locales and numerous online applications to test the few distinct methods are additionally accessible in cloud to test the product. The most crucial role in cloud balancing is Load balancing in this surroundings which can help in up gradation of the optimum

use of the sources available by properly directing the task to each and every component and this also help in reduction of load on a single node and dividing the work among all the different nodes and this will help in increase the job efficiency as well as work can be done quickly. The algorithm which is been designed is not presented on the past states but are been designed by looking at the current scenario. There are some crucial points which kept in mind while designing this algorithm: assessment-load, link-load, strength of diverse system, act of system, communiqué flanked by the nodes, etc. [36].

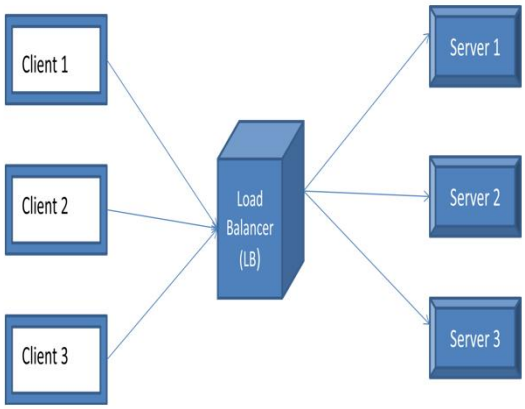

Fig. 3 (LB) Load Balancer

7. Parameters for Load Balancing Algorithm:

Here analysis is done in order to check whether there are proper and preventive actions are to be taken in order manage the traffic or the large amount of data .This predict whether the server is capable enough to manage the all other nodes as well as the information. So keeping all this in mind some important points are been discussed below:-[31]

Table 3.1: Load Balancing Parameters (LBP)

S.no	Parameters	Description
1	Throughput placed	It is determined as how much work finished against time consumed
2	Response	It is the old time between an enquiry on a framework and the reaction to that enquiry.
3	Flatulence Tolerance	It is the skill of the heap adjusting calculation that permits to keep working appropriately in Some disappointment state of the framework.
4	Scalable	It is the talent of the workstation relevance or a product to continue to function well When act upon changes in size or dimensions to convene user needs.
5	Achievements	It is the general check of the calculations working.
6	Resource	It is utilized to remain guarantee on the double-dealing of grouped assets.

8. **Architecture of Load Balancing:**

The heap adjusting structure, displayed in fig. comprises of four principal parts. These are the client, the work selector, the heap balancer and the calculation to be worn. Steps of this cycle as [24]:

- User command or request comes to the Data Centre Controller.
- Now here in Data Centre Controller forms the queue in order to properly allocate the request.
- Now after the queue is allocated in Central Load balancer now a proper database table is formed and then proper algorithm is been selected through virtual id and then goes back to the id.
- At last, Data Centre regulator or selector fulfil the request whose id they have

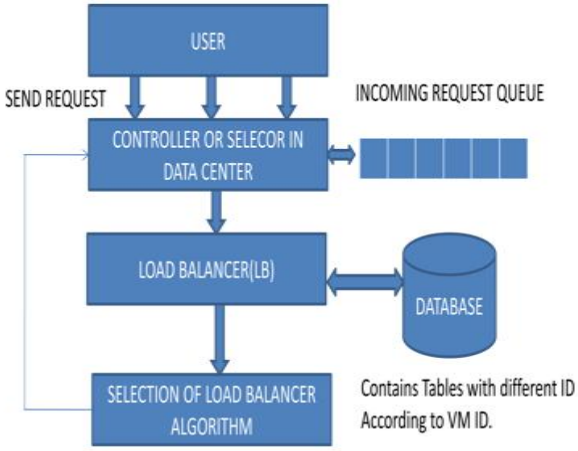

Fig. 3.2|Load balancer (LB) Architecture

9. **Algorithm for Static Load Balancing:**

Here in Static Load adjusting calculations allocation of the work is done only looking at the capability of the node and this depends on the new request. This whole procedure totally relies on the previous information and previous characteristics of the nodes.

1. Node's processing power
2. Memory
3. Storage capacity

Static load balancing algorithms are non-pre-emptive which means one node cannot be carried to another node. Subsequent is a portion of the static burden adjusting calculations:

A. RRA (Round-Robin-Algorithm).

B. MMLBA (Min-Min Algorithm of load balancing)

C. (TLBA) Throttled Algorithm of load balancing

A. RRA (Round Robin Algorithm) [16]

RRA load-balancing algorithm (RLBA) is the most popular and most commonly used algorithm for distributing the loads among the web servers this due to east to understand nature. Round Robin (RR) load balancing is today also used by many organizers. In this method request from the client is been divided among the servers' now further each server gets the clients' request and when it reaches to an end of the server list then it starts with its loop and allocate the server with the client request. The main benefit of RLBA is that it is very easy to execute. But in today's scenario where there is large amount of request are been waiting in queue it becomes a tough job to allocate servers with the all clients request. To resolve the above problem, weighted cooperative calculation was anticipated. In this move close, load will be allocated depending on the weights of all the nodes. This means each node should have equal amount of weight. When each node has equal weights, they will get same traffic. Still we can't assume the result before itself when it comes to load balancing.

B. MMLBA (Min-Min load balancing algorithm) [16]

The Min-Min algorithm is easy and most essential out of all present algorithms. Initially there are sets of unmapped assignments. Presently the assignment which will require some investment to finish will be found. Further, the undertaking with the least sum size is chosen and designated to the practically equivalent to asset (subsequently the Name Min is given).Finally the errand which is been thought about is been separated from the line and again a similar cycle is rehashed by Min until all undertakings are doled out (i.e., when the underlying set is unfilled).This algorithm complete single task at a time. One of major advantage all the task is been completed without any confusion and less chances of any error. But main Drawback is that so much of time is been utilize. Due to Time complexity of Min-Min algorithm sometimes it cannot make use of all its resources and cannot match with the load.

C. TLBA (Throttled load balancing algorithm) [15]

Here in this rule the task allocation but before there is a formation of table. A record table in this of Virtual machines with their states (2 states can be there: Available or occupied). Firstly, when clients makes request then request arrives to data center and here they check which type of virtual machine Should be allocating

the request so that it is suitable for the client's request or not. Now scanning is done to provide VM to the client to complete its job.

Dynamic load balancing algorithms [25]

Network bandwidth Many algorithm works on the group of knowledge where current as well as previous information are been merged and the proper nodes are been used from the clouds. And information of nodes during runtime are been checked and then selected nodes are then assigned the work. These algorithms allocate the tasks and may dynamically and then again join the nodes and make proper calculation. So these kind nodes must be managed correctly as one node fail it may stop working so in some cases they are harder to implement in Load-balancing.

Following are a portion of the unique calculations utilized in load adjusting:

A. ACO (Ant Colony Optimization)
B. GA (Genetic Algorithm).
C. HBF (Honey Bee Foraging)

A. ACO (Ant Colony Optimization) [6]

The inspiration of this algorithm is from ants. As the complex nature of ants and have the capacity to find the smallest way to accomplish their task. So that is why it is called ant colony optimization (ACO) which has immensely proved to be one of the most successful and widely recognized algorithmic method based on ant nature.[13] The insects leave a pheromone trail after moving starting with one Node then onto the next hub. By following the means trails, the insect consequently came to the food sources. The concentration of the pheromone may be different. As the ants make several trials to select their next node and like they have the ability to modify their paths as well so this how we can relate our Algorithm with these phenomena. [12].

B. GA (Genetic Algorithms) [21]

Genetic algorithms (GAs) the establishment of this algorithm is in order to solve the problems while dealing with the different programs and modify the evolutionary system. These are adaptive, (HS) heuristic-search-algorithms placed on the evolutionary opinion of usual assortment and analysis. All of these are the part of evolutionary computing, hurriedly mounting area of Artificial Intelligence

(AI) and are enthused by (DT) theory of Darwin's evolution-"Survival of the fittest". Genetic Algorithm (GA) is much popular for solving NP- Complete problems

C. HBF (Honey Bee Foraging) [5]

A group of (HB) honey bee can increase its way by its own over a large area in search of food and proper flower patches. The harvest the flowers and such honey through their nectar. A miniature tiny proportion of the colony finds the environment looking for new flower patches. When victuals spring is encountered the reconnoiter bees go in the meadow neighboring the hive and test out for quality favorable. Whilst they depart to the hive, the scouts collect the food harvested [36]. In the wake of finding the source it will return to its hive and follow up on shaking dance. By taking into account this dance different honey bees can easily detect the amount and detachedness of chow.

10. Algorithms Result & Comparison:

The table 3.2 gives the judgment between all calculations that are recently talked about from the reference segment. Based on these examination following boundaries is looked at for finding best appropriate Load adjusting calculation.

Abbreviations of Table 3.2 as follows:

L – Stands for LOW M - Medium
H - High
S - Slow
F - Fast
I - Improper
P - Proper

From the abovementioned, the correlations of the calculations depend on the accompanying component to figure out which burden adjusting Algorithm is best in giving compelling burden adjusting system in registering of cloud:

1. Throughput
2. Fault Tolerance
3. Response Time
4. Scalability
5. Performance

6. Resource utilization

So scientist finish up his exploration based on above boundaries That has been applied on RR, MMA, TA, ACO, GA, HBFA and find out the best load balancer algorithm on the basis of above parameter. Here as the outcome the use of ant colony algorithm is possible only in method is better as it can modify its path whenever it is required. As a result is they will can also work on the round robin approach so by adding some new methods on this algorithm can also enhance and improve the performance of this algorithm. Now if they add FCFS to the round robin so will improve the performance and many other approaches can be used to improve the algorithm according to the request by divagation of data in chunks of equal sizes this move toward will also be the amplify all the factor like Throughput, Fault Tolerance, Response Time, Scalability, Performance, Resource utilization.

Table 3.3: Algorithms of Load balancing (comparisons)

Algorithm	RRA (Round Robin Approac)	MMA (Min-Min Approach)	TA (Throttled Algorithm)	ACO (Ant Colony optimization)	GA (Genetic Approach)	HFA (Honey Bee Foraging Approach)
Throughput	L	L	M	H	H	H
Fault Tolerance	L	L	L	H	H	H
Response Time	S	F	F	F	F	F
Scalability	L	L	L	M	L	L
Performance	M	H	M	H	H	L
Resource Utilization	I	P	P	P	P	P

11. Proposed Algorithm:

In proposed work, we aim to ensure secure load balancing architecture by using a hybrid approach; the files are chosen on a FCFS basis and then passed onto the Load Balancer Module where the Load Balancer module brings the virtual machine id having the strong setup and least burden doled out. Further to guarantee security of information, we might utilize the code text strategy based characteristic based encryption calculation. Proposed calculation has been isolated into two modules for

These tasks that are given below

A. Load Balancer algorithm module for load balancing

B. Encryption module for improving security

A. Load Balancer algorithm module for load balancing

- Consider the clustered scenario, where there are different tasks
- Consider the scenario of multiple files (X1, X2, X3…XN).
- Select the file X1 based on its arrival time and partition file into smaller

chunks (x1,x2,x3…..xn).

- All the files are selected based on their arrival time and decomposed into chunks.
- Partitions are made of equal parts (let's consider threshold size of each partition as 500KB).
- The table 4.1 below shows the status of chunks made for each file
- Consider the scenario below with 3 servers:
- Chunk x1 of file X1 is allocated to server S1 and chunk x2 is allocated to server S2.
- Chunk x1 of file X2 is allocated to server S2.
- Chunk x1, x2, x3 and x4 of file X3 is allocated to S2, S3, S2, and S1 respectively.

Table 4.1 Status of chunks made for each file

File	File Size	No of Chunks (File Size/Threshold size)
X_1	1000 KB	2
X_2	500 KB	1
X_3	2000 KB	4
Total	3500 KB	7

The table 4.2 depicts the situation:

Table 4.2 Chunk Assignment to the respective servers

Server	No of Chunks
S1	2
S2	4
S3	1

The table clearly shows the misbalancing of load to the servers without security to resolve this problems the load balancing algorithms computes the number of chunks allocated to each server and performs attach function (AF) and detach functions (DF) in following manner.

Detach Function (DF): Detach function identifies the maximum no of chunks from the table 4.2 that is shown in table 4.3

Table 4.3 Identification of Maximum chunk

Server	No of Chunks
S2	4

Attach function (AF): Attach function assign this chunk Table 4.3 to the least load server S3 after the execution of chunk 1 that are already assigned to server S3 shown in table 4.

Table 4.4 Assignment of Maximum chunk to least load server

Server	No of Chunks
S3	1 (Executed)
S3	4

Encryption module for improving security: The documents are encoded through Cipher text strategy based and Attribute based encryption calculation to guarantee security of records.

Proposed Cipher text strategy based encryption conspire is a public key encryption plot where the public keys are created by taking verifiable boundaries while producing the confidential keys it thinks about the strategy. To scramble the information it predominantly requires the qualities of clients which were determined as access tree structure, we call it as strategy. Quality based encryption plot is likewise proposed which utilizations set of characteristics or accreditations of clients to scramble the information put away on cloud. Here proprietor will choose the beneficiaries to get to his information. Property Based Encryption is arranged into four standards:

1. Setup (S)
2. Encrypt (E)
3. Key Generation (KG)
4. Decrypt (D).

1) Setup (S): This step for setup.

Inputs: No, only implicit parameters will be considered

Outputs:

- Public-key(PK)
- Master-key (MK).

2) Encryption-(E): This is the step for encryption.

Inputs:

- It requires public key (PK) for the encryption (generated in step 1(a)).
- It requires Message (M).
- It requires collection of attributes(A)

Outputs:

Generates-Cipher-text (CT). Client whose ascribes coordinate with the arrangement just can get to the data.

3) Key Generation (KG): This step is for key generation.

Inputs:

- It requires Master key (MK) for key generation (generated in step 1(b)).
- Array of attributes (A []) with including the policy.

Outputs:

Generates private key (GPK).

4) Decryption (D):

Inputs:

- It requires public key(PK)
- It requires Cipher text(CT)
- It requires generated private key(GPK) Outputs:

On the off chance that the variety of qualities fulfills the approach no one but, he can decode and receive the message M.

12. Architecture of Proposed Method:

This architecture shows the working of proposed method .In this method having no of files as an input and apply defined modules sequentially to make it effective, reliable and secure in comparison of existing method.

The architecture of proposed method is divided into two categories shown in figure 4.1 and these are:

- **Module 1**: FCFS based Load Balancer Module.
- **Module2:** Cipher text attribute based Encryption and Decryption module

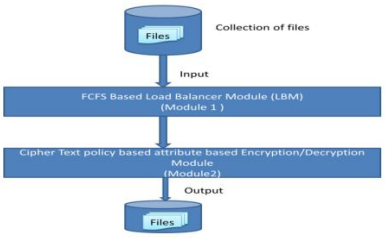

Fig. 5 Complete Architecture of proposed System

Now researcher elaborates the working of these modules with the help of figure these are given below.

Module 1: Load-Balancer-Module:

This is the principal module of proposed framework design in this module proposed framework perform load adjusting of various sort of documents in following advances.

- Take these files as an input.
- Select the files on the basis of their arrival time means at that time which file has Been selected that has minimum arrival time here FCFS based approach will also be Adopted.
- Apply Load balancer for this fetch VMID virtual machine id for each file and assigned minimum load.
- Now divide the file into equal size of chunks.
- Apply attach and detach function.
- Send these file to security module

Working procedure of module 1 is shown in figure 4.2 in this figure we are describing the whole process of Module 1 that is very easy to understand.

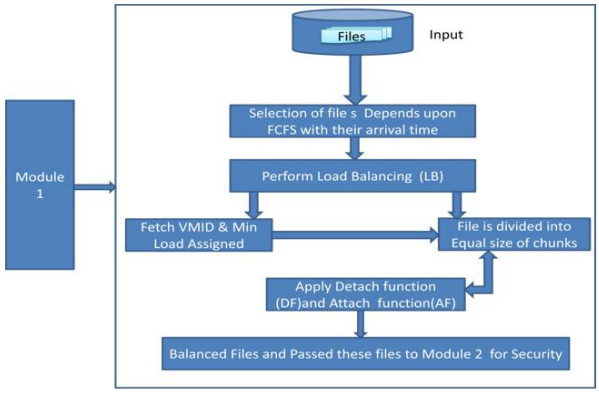

Fig 6 Load Balancer Module

Module 2: Security-module:

This is the 2nd module of the proposed framework uniquely intended to accomplish security. Working Security module is separated into following classes

- Take balanced file from module 1 as an input.
- Apply algorithm approach for encryption and decryption of file.
- Take encrypted file.
- Check the rules if rules are satisfied it will return decrypted file.

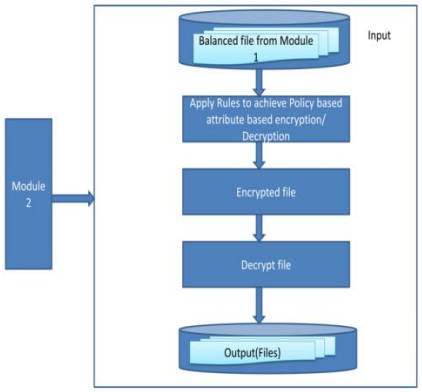

Fig 7 Security Module

13. Flow chart of Load balancer Module:

In this flow chart we are representing the whole working of load balancer module. How files have been selected on the FCFS basis and how selected file has divided into equal size of chunks? This flow chat also explain the working of attach function and detach functions.

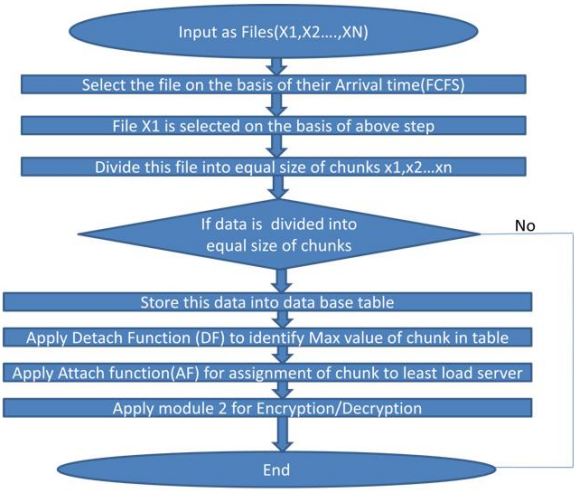

Fig. 8 Flow chart of Load balancer Module

Flow-chart of Security-Module

In figure text strategy characteristic based encryption. Client will at first solicitation for a document. Proprietor with records of (module 1) may acknowledge or dismiss the consent. Assume he acknowledges the solicitation then client will get the hint. Client attempts to download the document. Despite the fact that consent is allowed by proprietor, he/she can get to record just when their qualities fulfill the strategy. Assuming that ascribes are matched record can be unscrambled and downloaded. In the wake of downloading proprietor will get the implication about the client. Stream outline of proposed calculation (Security module) as displayed in figure 9.

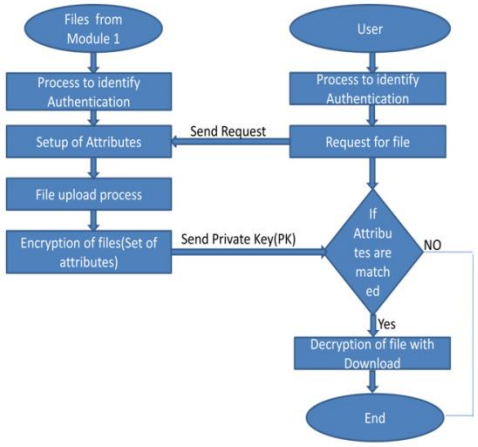

Figure 9 Flow-chart of Security-Module

While transferring document proprietor will enroll himself first. Proprietor will choose specific arrangement of traits connected with client that implies proprietor is confining the entrance of data to indicated client. Just those clients who fulfill the approach can get to the data. Confining access of data has fine grained admittance control. During transferring proprietor will choose the properties. Those trait sets are sent as boundary to scramble the record that is called as strategy. At the client end any client can send solicitation to get to the record. Proprietor might acknowledge or dismiss the solicitation. On the off chance that at all proprietor acknowledges the solicitation despite the fact that occasionally client can't download the record. Since his accreditations may not coordinate with the arrangement. So regardless of whether it is an untrusted network likewise proprietor can transfer the document with next to no strain.

14. Implementation Environment &Result Discussion:

The process of proposed system is divided into two categories

1. File-Uploading process on the server.
2. File-downloading process from the server

1. File-uploading process on the server

- File uploading process on the server is divided into following steps :
- Uploading file from client side (in our case its index.aspx provided by servlet server).
- File uploaded on servlet server for temporary purpose.
- Servlet server doing encryption on file and creating another encrypted file and delete original file.
- Private Key, Public Key and Master key store in servlet server.
- Encrypted file splitting into N no. of chunks according to N no. of servers and after delete the single encrypted file.
- Servlet server storing every unique chunk to particular load balancing server.
- Uploaded files details reflecting into UI also (Details like: Original File Name, file size, file uploaded time, execution process time).
- All uploaded file details store in details.json file on servlet server (Details like: No. of chunks, original file name, and unique id/directory).

2. File downloading process from the server

- If user/client wants that particular file than download request will send to servlet server (via index.jsp).
- Fetch requested file details form details.json.
- Copy N no. of chunks from N no. of load balancing servers to Servlet server.
- Merging all N no. of chunks and get an encrypted file and then delete all chunks from temp folder.
- Decrypting encrypted file and get original file using private key & public key and delete encrypted file.
- Original file send to particular user/client

15. Implementation Tools & Experiment Environment:

The execution instruments and examination climate were ready for a server and a client side. The Java language was utilized for the execution and depended on Eclipse IDE for the Java Developers. For the cut off side, a virtual server stage tomcat addressing a cloud server was introduced in a committed equipment server for this execution. The equipment server had the accompanying equipment and programming Specifications:

Model- (Motherboard): Hewlett-Packard HM65 CPU : i3- 2350 M CPU @2.30 GHz

Total memory : 6GB

Cache Memory : 3 MB

hard-disk storage: 320 GB (SATA HDD)

Software specification for the development as follows:

Operating System : Windows 10 Pro

Virtual Server : IIS

Front End : ASP.NET C#

Environment : Visual Studio 2022

16. Quantitative Evaluation:

Quantitative evaluation is based upon the comparative study of proposed method and existing method through table as well as graph. These results are generated via implemented software overall evaluation is divided in to two categories.

- Speed of file uploading/writing process in different-different files.
- Speed of file downloading/reading process in different-different files.
-

Speed of file uploading/writing process in different-different files

In this section researcher evaluates the speed of uploading of different-different files on the server. On the basis of literature survey existing System speed is Uploading/writing 5 MB/Sec. If researcher covert this result in KB then 1 MB = 1024 KB.

So 5 MB = 5120 KB

And 1 second = 1000 mili second.

Then uploading/ writing speed will be 5120 KB/1000 mili second. On the basis of this researcher Design new proposed system for enhance this speed and then implemented. These implemented Comparative results between proposed system and existing system are given table 10:

Fig. 10 Result Comparison of File uploading/writing process of different-different files

S.no	File name	File Size(KB)	Proposed System Uploading/writing Time(Milisec)	Existing System Uploading/writing Time(Milisec)
1.	Cloud Security.doc	1020	200	200
2.	Xlive.zip	5259	860	1028
3.	13 Hidden Google tricks.com	2753	620	538
4.	World Map.jpeg	1444	260	283
5.	Xlive.dll	10805	1740	2110
6.	Secure.zip	6295	1040	1230
7.	DAT-ABE Master.zip	4393	740	858

In Fig. 10 shows the seven files of different – different sizes and these files are uploaded on the Tomcat Apache server 7.0 at the time of uploading implement software is comparing the result on the basis of uploading time between existing system and proposed system. Uploading speed of existing system is constant for any size of file 5 MB/Sec [2]. But Speed of file uploading on the server in proposed system is not fixed it is varying according to the size of file due to effective design of proposed algorithm. Another important aspect of proposed system is when size of file is increased uploading speed is also be increased in comparison of existing system. So it has been proven that on the basis of table 5.1 proposed systems is more accurate and fast in comparison of existing system.

CONCLUSION

Presently toward the finish of this proposition, it is much clearer to us now that security and protection is significant Play a conclusive job for clients. Further this has also created awareness about among the people regarding privacy of their documents and also importance of their documents. Moreover, there are many advantages as well disadvantages of the cloud services all over the world there are many users which are still in confusion whether to trust on cloud or not. Furthermore, handling to cloud-computing frameworks. We have fundamentally depended how we might interpret various security and protection issues (weaknesses, dangers, and assaults), which we concentrated on in the wake of classifying them as security-just issues, security just issues, and entwined security

and security issues. We recognized and read up many new controls for these issues, similarly arranged as security-just controls, protection just controls, and interweaved security and security controls. In addition, proposed method is fast efficient and secure in comparison of existing method. Results of proposed method varying on the size of file it gives fast results for the large size of file whenever uploading and downloading process was fixed 5MB/Sec. Furthermore, proposed method is using latest CP-ABE algorithm for security and existing method used traditional RSA algorithm for preserving security so on the basis of these two algorithm proposed algorithm is more secure in comparison of existing method.

FUTURE WORK

The CIA group of three was referenced above as the exemplary meaning of safety, or, being more exact, the exemplary meaning of safety administrations. Notwithstanding, there are greater security benefits that are fundamental. Seven of them are given as the standard arrangement of safety administrations by International Standards Organization (ISO). Likewise, protection can be characterized by means of a bunch of security administrations. Later on, in the wake of distinguishing protection administrations (comparably to the ISO's seven security benefits), all security and protection issues (issues and arrangements) could be sorted by means of two-level characterization. At the high level we would in any case have the introduced order into three classes: security-just, protection just, and entwined. On the subsequent level, we would additionally sort each high level class into administration arranged subclasses.

As confirmed by researcher which have taken up the guarantee that cloud computing will one most leading technology in all over the world also one the most important that is to be highlighted that platform as a service will also show its improvement gradually and it has been used in most of the organization and MNCs too. Computing will more friendly for the user and convenient for many users with the help of cloud are computing and in terms of security reasons cloud computing will be improved more secure so that the user can rely on cloud. And also we can prevent our data from cyber-attacks by providing more security to the data. It cannot be hacked easily by unauthorized user or any cyber-atta.

References:

[1] Adhikari, M., Amgoth, T., 2018. Heuristic-based load-adjusting calculation for IaaS cloud. Futur. Gener. Comput. Syst. 81,156-165. https://doi.org/10.1016/j.future.2017.10.035.

[2] A. Jain and R. Kumar, "A Multi Stage Load Balancing Technique for Cloud Environment." International Conference on Information Communication and Embedded Systems (ICICES), Feb 2016, pp. 1-7.

[3] A. Shukla, S. Kumar, and H. Singh, "Fault resilience based load adjusting approach for web assets in cloud climate," Int. Middle Easterner J. Inf. Technol., vol. 17, no. 2, pp. 225-232, 2020.

[4] Amro Al-Said Ahmad, Peter Andras, "Estimating the Scalability of Cloud-based Software Services", IEEE World Congress on Services, 978-1-5386-7374-4/18/$31.00 ©2018 IEEE, pp. 5-6, 2018.

[5] Bhaskar. R, Deepu.S. R and Dr.B. S. Shylaja "Dynamic Allocation Method For Efficient Load Balancing In Virtual Machines For Cloud Computing Environment" September 2012.

[6] Bih-Hwang Lee, Ervin KusumaDewi, Muhammad FaridWajdi, "Information Security in Cloud Computing Using AES Under HEROKU Cloud", The 27th Wireless and Optical Communications Conference (WOCC2018),2018.

[7] EmanM.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, "Further developed Data Security Perfect for Cloud Computing", The eighth International Conference on Informatics and Systems (INFOS),pp. 12-17,2019.

[8] Ram PrassdPandhy (107CS046), P Goutam Prasad rao (107CS039). "Load-adjusting model in distributed computing framework" Department of software engineering and designing National Institute of Technology Rourkela, Rourkela-769008, Orissa, India May-2011.

[9] J. Sahoo, S. Mohapatra and R. strip "Virtualization: A review on ideas, scientific classification and related security issues" PC and organization innovation (ICCNT), IEEE, pp. 222-226. April 2010.

[10] R.Shimonski. Windows 2000 and Windows server 2003 grouping and burden adjusting. Emeryville. McGraw-Hill Professional distributing, CA, USA (2003), p 2, 2003.

[11] J. Kruskall and M. Liberman."The Symmetric Time Warping Problem: Persistent to Discrete. In Time Twists, String Edits and Macromolecules: The Theory and Practice of Sequence Correlation Comparison", pp. 125-161, Addison-Wesley Publishing Co., 1983.

[12] Mr. Nitin S. More, Mrs. Swapnaja R. Hiray and Mrs. Smita Shukla Patel," Load Balancing and Resource Observing in Cloud Monitoring in Cloud", International Journal of Advances in Computing and Information Researches ISSN: 22774068, Volume 1-No.2, April 2012.

[13] M Randles, D. Sheep, and A. Taleb-Bendiab, "A comparable report into spread load changing estimations for circulated registering," 2010 IEEE 24th global meeting on cutting edge data systems administration and application workshops,2010, pp. 551-556.

[14] Omar G. Abood, Shawkat K. Guirguis, "A Survey on Cryptography Algorithms", International Journal of Scientific and Research Publications, Volume 8, Issue 7, pp. 495-516, July 2018.

[15] R. X. T. also, X. F. Z,"A Load Balancing Strategy Based on the Combination of Static and Dynamic, in Database Technology and Applications (DBTA)",2nd International Workshop,2010.

[16] RavindraSandaruwanRanaweera†, Eiji Oki, and NattapongKitsuwan, "Non-neighborhood Data Fetch Scheme Based on Delay", fourth IEEE International Conference on Big Data Security on Cloud, 978-1-5386-4399-0/18/$31.00 ©2018 IEEE, pp.188-193, 2018.

[17] SeadMašović, MuzaferSaračević, HamzaKamberović, MensuraKudumović,"

Java innovation in the plan and execution of web applications", online diary https://www.researchgate.net/distribution/235788474,pp. 1-11, 2018.

[18] H. Jahanpour, H. Barati, and A. Mehranzadeh, "An energy productive adaptation to non-critical failure method in view of burden adjusting calculation for high performance figuring in distributed computing," J. Choose. Comput. Eng. Innov., vol. 8, no. 2, pp. 169-182, 2020.

[19] S. Setaouti, D. Djamel Amar Bensaber, R. Adjoudj, and M. Rebbah, "Fault resilience coordinated by administration level understanding in distributed computing conditions," Int. J. Comput. Digit. Syst., Aug. 2021.

[20] S. Akhbarifar, H. H. S. Javadi, A. M. Rahmani, and M. Hosseinzadeh, "A protected distant wellbeing checking model for early illness conclusion in cloud-based IoT climate," Pers. Pervasive Comput., pp. 1-17, Nov. 2020.

[21] V. Mohammadian, N. JafariNavimipour, M. Hosseinzadeh, and A. Darwesh, "Comprehensive and methodical concentrate on the adaptation to non-critical failure designs in distributed computing," J. Circuits, Syst. Comput., vol. 29, no. 15, 2020, Art. no. 2050240.

[22] V. Hayyolalam, B. Pourghebleh, and A. A. P. Kazem, "Trust the board of administrations (TMoS): Investigating the ongoing components," Trans. Emerg. Telecommun. Technol., vol. 31, no. 10, p. e4063, Oct. 2020.

[23] YashpalsinhJadeja and Kirit Modi, "Distributed computing - Concepts, Architecture and Challenges", International Conference onComputing, Electronics and Electrical Technologies [ICCEET], IEEE-2012.

[24] Yujiao Song, HaoWang, XiaochaoWei and LeiWu, "Productive Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud", International Conference on Hindawi Security and Communication Networks, Volume 2019, pp. 1-9, 2019.

[25] Z. Lv, D. Chen, R. Lou, and H. Tune, "Industrial security answer for

computer generated reality," IEEE Internet Things J., vol. 8, no. 8, pp. 6273-6281, Apr. 2021.