IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENHANCING SECURED CLOUD SERVICES BY LOAD BALANCING & ENERGY EFFICIENCY TECHNIQUES

Rohit V. Ujawane*, Prof. Kanchan Dhote

* Dept. of Wireless Communication & Computing Tulsiramji Gaikwad-Patil College of Engg.& Tech.Nagpur.

Head,Dept. of Electronics Engineering Tulsiramji Gaikwad-Patil College of Engg. & Tech.Nagpur.

ABSTRACT

Cloud computing is at its boon. Cloud computing is provide to manage a large amount of database in the networking, for that purpose large power is required which is provided by the power plant. Carbon emission controlling is responsible to reduce the energy required for cloud and it is easy to controlling the traffic of router. In this paper the attacks such as Malicious Server attack, Finger printing server attack etc. can be controlled and what are its impact on the clouds is reduced.

KEYWORDS: cloud computing , Load balancing for carbon emissions control, security attacks in cloud.

INTRODUCTION

To provide confidentiality and privacy is very important today to enterprises and other users to use cloud services. Cloud computing is a buzz word which means that accessing and storing of data and programs over the Internet instead of your computer's hard drive. Security and privacy represent major concerns in the adoption of cloud technologies for data storage. Security and confidentiality of records in cloud server can be performed with the help of encryption. The Traditional Encryption Approach is not sufficient for assure the confidentiality of records from the cloud server.Proposed research will help to provide a self-routing solution to long messages in data-centre applications of various fields. Increase the level of performance or efficiency even in a more number of cloud networks.

LITERATURE REVIEW

1) Singh proposed a novel load balancing algorithm called Vector Dot. It handles the hierarchical complexity of the data center and multidimensionality of resource loads across servers, network switches, and storage in an agile data center that has integrated server and storage virtualization technologies. Vector Dot uses dot product to distinguish nodes based on the item requirements and helps in removing overloads on servers, switches and storage nodes.

2) R.Stanojevic proposed a mechanism CARTON for cloud control that unifies the use of LB and DRL. LB (Load Balancing) is used to equally distribute the jobs to different servers so that the associated costs can be minimized and DRL (Distributed Rate Limiting) is used to make sure that the resources are distributed in a way to keep a fair resource allocation. DRL also adapts to server capacities for the dynamic workloads so that performance levels at all servers are equal. With very low computation and communication overhead, this algorithm is simple and easy to implement.

3) Y. Zhao addressed the problem of intra cloud load balancing amongst physical hosts by adaptive live migration of virtual machines. A load balancing model is designed and implemented to reduce virtual machines' migration time by shared storage, to balance load amongst servers according to their processor or IO usage, etc. And to keep virtual machines' zero downtime in the process. A distributed load balancing algorithm COMPARE AND BALANCE is also proposed that is based on sampling and reaches equilibrium very fast. This algorithm assures that the migration of VMs is always from high cost physical hosts to low cost host but assumes that each physical host has enough memory which is a weak assumption.

4) V. Nae presented an event driven load balancing algorithm for real time Massively Multiplayer Online Games (MMOG). This algorithm after receiving capacity events as input, analyzes its components in context of the resources

and the global state of the game session, thereby generating the game session load balancing actions. It is capable of scaling up and down a game session on multiple resources according to the variable user load but has occasional QoS breaches.

5) J. Hu Proposed a scheduling strategy on load balancing of VM resources that uses historical data and current state of the system. This strategy achieves the best load balancing and reduced dynamic migration by using a genetic algorithm. It helps in resolving the issue of load imbalance and high cost of migration thus achieving better resource utilization.

PROPOSED SYSTEM

1. By the help of Server Controller module, in this system we properly balance the load and in an appropriate manner.
2. The objective of the system is to perform load balancing on server side like the client side.
3. Another feature of the system is we provide the strong security and authentication.
4. For Securing Access Of user Data there is use of AES Encryption algorithm, The data of User is stored in a data centre Using AES Encryption Algorithm.

For Accessing Secure data there is a use of Identity Token assigned for every User.

PROPOSED METHODOLOGY

1) By doing Literature Survey the problem in existing system is the load balancing is not on server-to-server side, it was present on only server-to-client side. In this system we will overcome this problem.
2) We will proposed a control server that balance the load of the cloud, so that it reduces carbon emissions and control server which is used for balancing the load and controlling the carbon emissions in the cloud is also responsible to remove the attacks.

DATA FLOW DIAGRAME

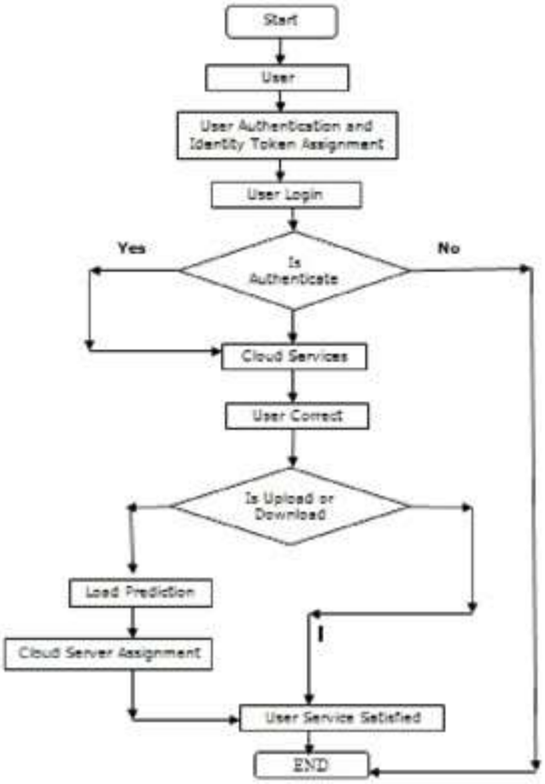


Fig 1data flow diagram

LOAD BALANCING CONCEPTS

Load Balancing:

Weighted Least Load (Successive Transactions)	Like the Least Connections methods, these load balancing methods select pool members or nodes based on the number of Successive Transactions. However, the Weighted Least Successive Transactions methods also base their selections on server capacity.	Weighted Least Connections methods work best in environments where the servers have differing capacities. For example, if two servers have the same number of Successive Transactions then We Use FIFO Mechanism in a System.

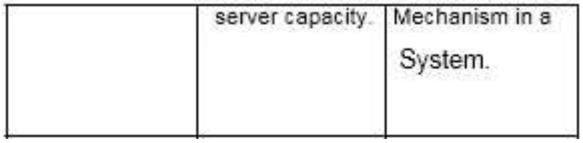


Table 1: Load balancing concept

MODULE DESCRIPTION

MODULE 1: (USER CREATION, SERVICE PROVIDER, AUTHENTICATION AND ISSUING IDENTITY TOKEN TO USER ACCESSING CLOUD)

In this system, we create the number of clouds in the environment,each clouds has its own server. There is a one authority Body known as Server Controller who Put eye on a server Load and Also on User Sessions. Creation of User Panel and Issuing of Personal Private Identity token known as OTP key for each n every user in a cloud Network. Authentication Assignment by Server Controller. After Successesive User Authentication Assigned User Services To them As Upload file on cloud using (AES Encryption) and download files using the same algorithm with users Identity token.

MODULE 2: (ATTACKER PREVENTION AND DETECTION ON A CLOUD NETWORK)

Here We Ensure That our system is preventing Any Data Fording and unauthorized Access to cloud Network. We introduce some Attacks and their Preventions Rather, The Server controller put eye on user session by monitoring their sessions and at a record of any frauding transactions is there.

MODULE3: (PERFORMANCE ANALYSIS AND IMPLEMENTATION OF LOAD BALANCING PROBLEM)

Create a Sever of nodes and implement load balancing problem in existing Severs and transfer the packets from Source to Destination. Load balancing outputs are shown using graphs. Compare Load balancing problem with using the measured parameters shown using graphs.

ALGORITHM

AES - Advanced Encryption Standard Algorithm like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively.

A number of AES parameters depend on the key length. e.g., if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

Rijndael was designed to have the following characteristics

Resistance against all known attacks.

Speed and code compactness on a wide range of platforms.

Design Simplicity

VARIOUS TYPES OF CLOUDS

Public Clouds

When the services and infrastructure are provided off-site over the Internet the cloud is said to be public cloud. Greatest level of efficiency in shared resources is offered by this type of cloud.

Private Clouds

When the services and infrastructure are maintained on a private network the cloud is said to be private cloud. High level security and control are the services offered by this cloud, but the company still has to maintain and purchase the software and the infrastructure, reducing the cost.

Hybrid clouds

A combination of a variety of public and private options in cloud with many providers is hybrid cloud. The cloud providers and attackers can easily disclose the real identity of the user, as there is no assurance of privacy identity, so users may not be willing to join in Cloud Computing Systems.

ATTACKS IN CLOUD

Malicious server attack, Finger-printing server attack, Distributed Denial of Service is the attacks described in this paper.

Malicious Server Attack

Services that are accessible to clients are exposed by server. Server also exposes vulnerabilities that can be attacked.

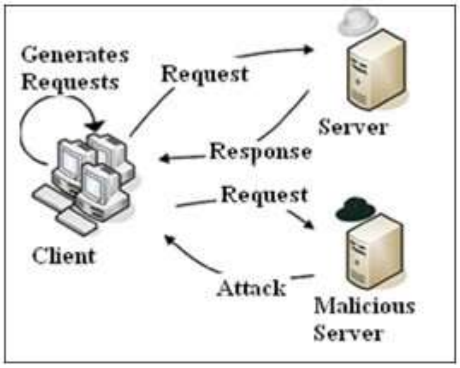


Fig 2: Malicious Server attack

Finger –Printing server Attack:-
When a client makes a login to access a service in a cloud his logs are maintained on the server and are deleted once the user logs out. But if the server is a malicious one this logs from the log file is not deleted. Such an attack is referred to as Fingerprinting attack.

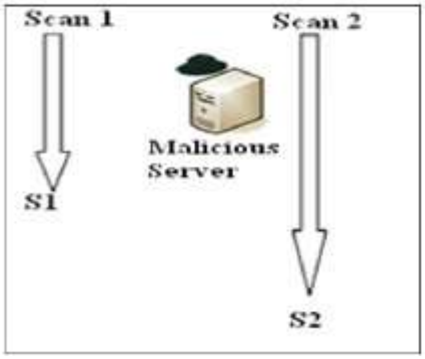


Fig 3: Finger-printing attack

Distributed Denial of service attack:-
Sometimes a cracker uses a network of zombie computers (A computer under the control of Intruders) to attack a specific server. A cracker tells all the computers on his bonnet (group of zombie computers) to contact a specific server continuously. The sudden increase in traffic can cause the server to load very slowly for authorized users. This heavy traffic is enough to stop the working of the site. This attack is known as Distributed Denial of Service attack. In other words it is an effort to make a network resource unavailable to its intentional users.

Malicious Server attack can be tracked and removed by dummy client method. Fig 3.Gives the Malicious server in the network. Fig 3tracks the malicious server in the network by dummy client method.

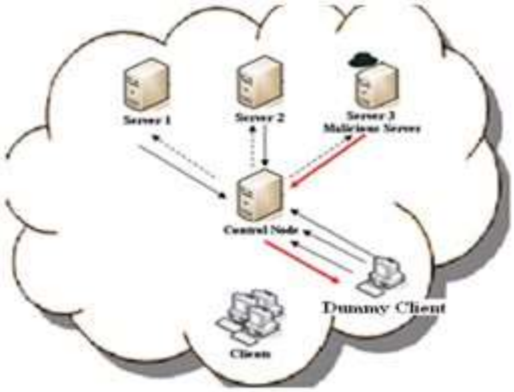


Fig 3.Track the Malicious server using Dummy Client

The dummy client generates 'n' number of requests and sends it to the control node. The control node then directs these requests to the appropriate servers depending upon their load. If the server to which the request is forwarded is a malicious one it will send back the same response every time. The dummy client on receiving these same responses from a server can determine that server to be a malicious server.

Finger-printing Attack can be tracked and removed by double file check method. Fig2. Denotes the Finger-printing attack. Fig 4 tracks the finger-printing attack by double file check method. In double file check, we scan the server and calculate the size of various logging files in the system once a user gets logged in. After the logout request we scan the system again and calculate the size of various logging files. If the size of a file in second scan is greater than the first one, it means that the user is not completely logged out and his logs are still not deleted. Double file check method deletes the log and prevents finger-printing attack.

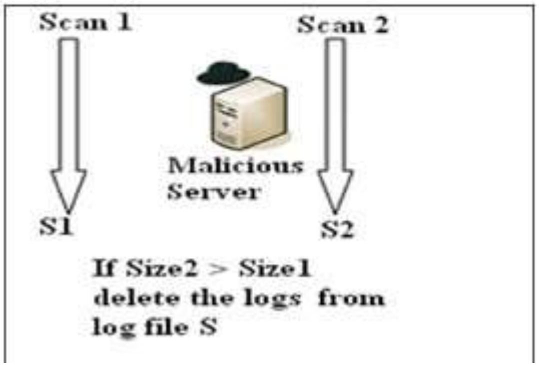


Fig 4: Track Finger-printing attack by double file check method

Distributed Denial of Service can be tracked and removed by considering various parameters on which the traffic depends. If a particular IP is monitored for over n consecutive packets, with packet size of more than m within path time period, then it is considered as malicious and packets from this source are dropped thereafter.

LOAD BALANCING

Load Balancing are applied to computing resources (network, servers, hard drives) to solve a certain problem in a specific area. Different algorithm has been proposed by many researchers and has been discussed in many literatures [4]. From the literature dynamic load balancing algorithm is applied either as distributed or non-distributed. The task of the load balancing is shared among the node in the distributed system.

Load balancing can take two forms: cooperative and non-cooperative. In the cooperative the nodes are working side-by-side to achieve a common objective was to improve the overall response time. In the non-cooperative node works independently toward a goal like to improve the response time of a local task.

RESULT ANALYSIS

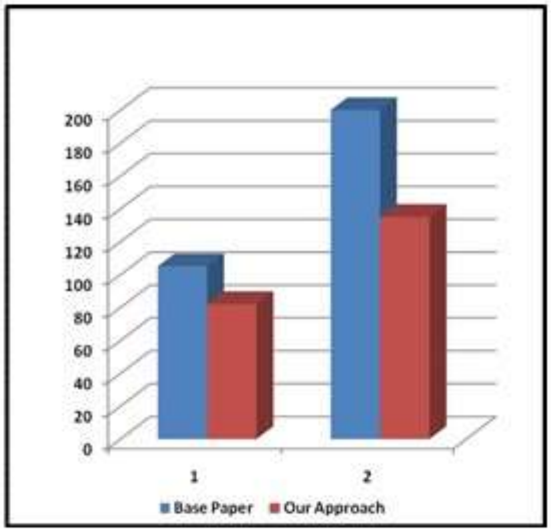
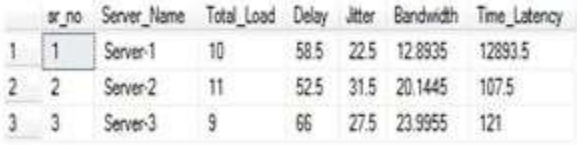
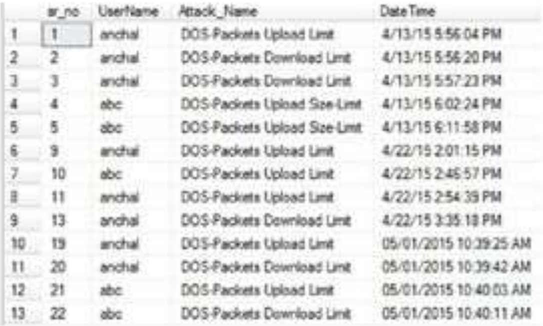


Fig. 7.1 Comparison with Existing System



	sr_no	Server_Name	Total_Load	Delay	Jitter	Bandwidth	Time_Latency
1	1	Server-1	10	58.5	22.5	12.8935	12893.5
2	2	Server-2	11	52.5	31.5	20.1445	107.5
3	3	Server-3	9	66	27.5	23.9955	121

Fig.7.2: Load Balancing Result



	ar_no	UserName	Attack_Name	DateTime
1	1	anchal	DOS-Packets Upload Limit	4/13/15 5:56:04 PM
2	2	anchal	DOS-Packets Download Limit	4/13/15 5:56:20 PM
3	3	anchal	DOS-Packets Download Limit	4/13/15 5:57:23 PM
4	4	abc	DOS-Packets Upload Size-Limit	4/13/15 6:02:24 PM
5	5	abc	DOS-Packets Upload Size-Limit	4/13/15 6:11:58 PM
6	9	anchal	DOS-Packets Upload Limit	4/22/15 2:01:15 PM
7	10	abc	DOS-Packets Upload Limit	4/22/15 2:46:57 PM
8	11	anchal	DOS-Packets Upload Limit	4/22/15 2:54:39 PM
9	13	anchal	DOS-Packets Download Limit	4/22/15 3:35:18 PM
10	19	anchal	DOS-Packets Upload Limit	05/01/2015 10:39:25 AM
11	20	anchal	DOS-Packets Download Limit	05/01/2015 10:39:42 AM
12	21	abc	DOS-Packets Upload Limit	05/01/2015 10:40:03 AM
13	22	abc	DOS-Packets Download Limit	05/01/2015 10:40:11 AM

Fig.7.2: Attack Result

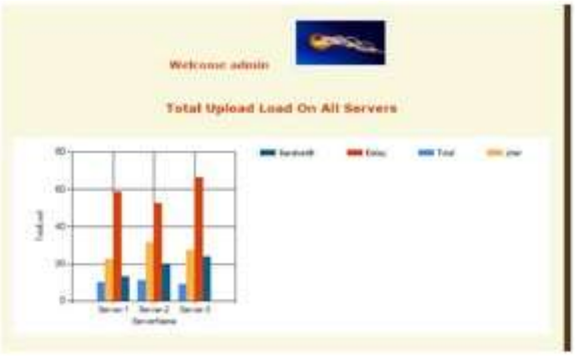


Fig 7.4: Result Analysis

Thus we have studied various cloud balancing techniques and algorithms, cloud security attacks, and the cloud security issue We have also discussed the techniques used to track and remove these attacks. Therefore the proposed project is an intelligent software system that balances the load on server side and also reduces the carbon emissions in the cloud and also tracks the server attacks and helps remove it.

REFERENCES

[1] Joseph Doyle, Robert Shorten, and Donal O'Mahony, Stratus: Load Balancing the Cloud, IEEETRANSACTIONS ON CLOUD COMPUTING, VOL. 1, NO. 1, JANUARY-JUNE 2013.

[2] Doddini Probhuling L. Dept. of computer science, Shivaji Polytechnic, Karad, India, LOAD BALANCING ALGORITHMS IN CLOUD COMPUTING, International Journal of Advanced Computer and Mathematical Sciences ISSN 2230-9624. Vol4, Issue3, 2013, pp229-233.

[3] Divya Thazhathethil*, Nishat Katre, Jyoti Mane-Deshmukh, Mahesh Kshirsagar, A Model for load balancing by Partitioning the Public Cloud, International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3, March 2014

[4] N.S.Raghava*,and Deepti Singh, Comparative Study on Load Load Balancing Techniques in Cloud Computing, Open Journal of Mobile Computing And Cloud Computing Volume1,Number 1,August.

[5] Soumya Ray and Ajanta De Sarkar, Execution Analysis of Load Balancing Algorithms in Cloud Computing Environment, International Journal on Cloud Computing Services and Architecture(IJCCSA),Vol.2,No.5,October 2012.

[6] Suriya Begum*, Dr. Prashanth C.S.R, Review of Load Balancing in Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 2, January 2013

[7] SATYENDRA SINGH RAWAT & UMESH BINDAL EFFECTIVE LOAD BALANCING IN CLOUD COMPUTING USING GENETIC ALGORITHM, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 4, Oct 2013, 91-98

[8] Steve Gibbs, Cloud Computing, International journal of Innovative Research in Engineering & Science, issue 1, Volume 1, July, 2012.

[9] Calheiros Rodrigo N., Rajiv Ranjan, César A. F. De Rose, Rajkumar Buyya (2009): Cloud Sim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services CoRR abs/0903.2525: (2009)

[10] Vikas Kumar and Shiva Prakash, A Load Balancing Based Cloud Computing Techniques and Challenges, International Journal of scientific research and management (IJSRM) ||Volume||2||Issue||5 ||Pages|| 815-824 ||2014.

[11] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.

[12] Zaigham Mahmood , " Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web Technologies, 2011.

[13] Ashish Kumar Singh, Sandeep Sahu, Kamalendra Kumar Gautam, Mangal Nath Tiwari, Private Cloud Scheduling with SJF, Bound Waiting, Priority and Load Balancing, IJARCSSE, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.

[14] Nils Gruschka and Meiko Jensen, “Attack Surfaces: Taxonomy for Attacks on Cloud Services”. IEEE rd International Conference on Cloud Computing, 2010.