ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

An Novel Distributed Load Balancing Technique with Multiple Cloud Architecture to Avoid Congestion and Hotspot

K.Kiruthika[1], G.Gayathri[2], M.Evangelin, Tribursiya[3], Harini Sri[4]

Associate Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India[1]

U.G. Student, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India[2]

U.G. Student, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India[3]

U.G. Student, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India[4]

ABSTRACT: In current Technology world, the possibility of accounting overall resource usage in all applications become very difficult and providing security for the data stored in cloud becoming very tough .Nevertheless, in the domains where small number of shared services serve to a plethora of different entities requests, auditing resource which come to be significantly challenging. In the beginning, the global resource utilization at the shared service is the accumulate of the resource utilization for number foreign entities whose identities are not exposed to the shared service. Second, even though such information available, normal monitoring tools (e.g., top) are not able to hand over correct break-down of resource utilization after all sharing occurs at sub instance level (i.e. service instances are not exclusive) and not able to provide security for the resources. We review inherent challenges of carrying out resource utilization of shared resource and provide security to the resource stored in cloud by using encryption. To provide data secure repository or data recovery in cloud storage we proposed muti-cloud architecture, where the user data is split into 2 parts and one half is encrypted using AES encryption algorithm and other half is encrypted using attribute based encryption algorithm and stored in Cloud 1, Cloud 2. During the request our technique will merge the 2 parts and provide the response to the requested user. We measure two non-interfering approaches having distinct balance among local monitoring and collective inference – (1)Linear regression that makes uses of easily-available tools which gives total measurement and executing well-known linear regression as inference, and (2) Rameter that inserts huge intensity on acquisition of fine-grained per-thread information from within the hypervisor and applying light inference on the data

KEYWORDS: Cloud computing, Load balancing, Energy efficiency.

I. INTRODUCTION

Cloud server act as a container which contains data or information. Multi-cloud in the combination of public, private or managed clouds including managed services or service providers. Multi-Cloud data systems have the capacity to enhance data sharing and this aspect will be significantly of great help to data users. Most business organizations share most of their data with either their clients or suppliers and consider data sharing as a priority. In generally we are sent the file to cloud in this project the proposed system we send the file with authentication by encrypt and it can retrieve the data from multiple cloud before retrieve the file its enhancing whole file then decrypt method were use to retrieve the file to view and ID-DPDP protocol can realize private verification, delegated verification and public verification We propose a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects. Also we propose the splitting and merging concepts during storage in cloud environment. For experimental results, we are implementing ***Apache server*** as the accounting load balancer to keep track of the virtual machine status. ***Tomcat server*** is installed in virtual machine to obtain the job status. For data secure repository or data recovery in cloud storage we proposed **muti-cloud architecture**, where the user data is split into 2 parts and one half is encrypted using ***AES encryption algorithm*** stored in Cloud 1 , Cloud 2 and , cloud 3. During the request our technique will merge the 2 parts and provide the response to the requested user. In this project, we are developing a load balancer for effective user request monitoring and file access. In existing research articles, no papers focus on experimental results and it deals only with types of algorithms used for load balancing. In our proposed system, apache server is used as a server for processing the user request and tomcat is used as virtual machines. The status (idle, busy), session time, packet size, virtual machine name, type, hostname, port address and bytes read in each virtual machines are been monitored in apache server and based on the status the job is allocated to the virtual machines. Thus our proposed project provides an efficient load balancer to avoid congestion and overloading of server in the data centre. For dynamic load balancing, we used **ANT colony algorithm.** The motivation of the survey of existing load balancing techniques in cloud computing is to encourage the amateur researcher to contribute in developing more efficient load balancing algorithms. This will benefit interested researchers to carry out further work in this research area. This paper is organized as follows: Section II discusses Green computing in clouds, Section III presents the needof load balancing in clouds, Section IV shows the study and analysis of the existing load balancing techniques icloud computing, Section V identifies the metricsconsidered in the existing load balancing techniques andcarries out the comparison between them based on those identified metrics and Section VI concludes the paper. To the best of our knowledge, none of the techniques hasfocused on energy consumption and carbon emission factors that are a dire need of cloud computing.enabled by high-speed computer networks that allow applications to run more efficiently on these remote, broadband computer networks, compared to local personal computers. These data-centres cost less for application hosting and operation than individual application software licenses running on clusters of on-site computer clusters[11]. However, the explosion of cloud computing networks and the growing demand drastically increases the energy consumption of data-centers, which has become a critical issue and a major concern for both industry and society [8]. This increase in energy consumption not only increases energy cost but also increases carbon-emission. High energy cost results in reducing cloud providers' profit margin and high carbon emission is not good for the environment [7]. Hence, energy-efficient solutions that can address the high energy consumption, both from the perspective of the cloud provider and the environment are required. This is a dire need of cloud computing to achieve Green computing. This whole scenario is depicted in. Load balancing can be one such energy-saving solution in cloud computing environment.

2. Load Balancing in Cloud Computing.

Load balancing in clouds is a mechanism that distributed the excess dynamic local workload evenly across all the nodes. It is used to achieve a high user satisfaction and resource utilization ratio making sure that no single node is overwhelmed, hence improving the overall performance of the system. Proper load balancing can helping utilizing the available resources optimally, thereby minimizing the resource consumption. It also helps in implementing fail-over, enabling scalability, avoiding bottlenecks and over-provisioning, reducing response time etc. Apart from the above-mentioned factors, load balancing is also required to achieve Green computing in clouds which can be done with the help of the following two factors:

- Reducing Energy Consumption - Load balancing helps in avoiding overheating by balancing the workload across all the nodes of a cloud, hence reducing the amount of energy consumed.
- Reducing Carbon Emission - Energy consumption and carbon emission go hand in hand. The more the energy Consumed, higher is the carbon footprint. As the energy consumption is reduced with the help of Load balancing so is the carbon emission helping in achieving Green computing.

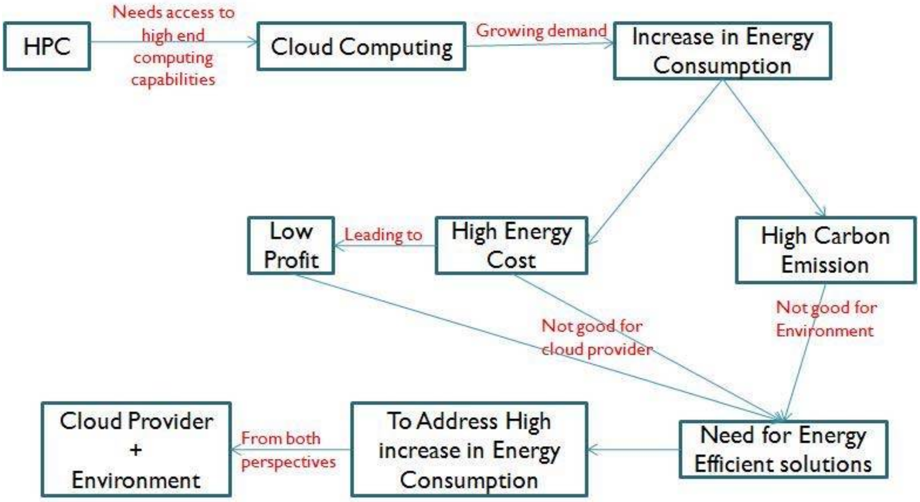
HPC
Needs access to high end computing capabilities
Cloud Computing
Growing demand
Increase in Energy Consumption
Low Profit
Leading to
High Energy Cost
High Carbon Emission
Not good for cloud provider
Not good for Environment
Cloud Provider + Environment
From both perspectives
To Address High increase in Energy Consumption
Need for Energy Efficient solutions

Fig.1. Load Balancing.

3. Existing Load Balancing Techniques in Cloud Computing:
Following load balancing techniques are currently prevalent in clouds:-
• Decentralized content aware load balancing - H. Mehta et al. [13] proposed a new contentaware load balancing policy named as workload and client aware policy (WCAP). It uses a unique and special property (USP) to specify the unique and special property of the requests as well as computing nodes. USP helps the scheduler to decide the best suitable node for the processing the requests. This strategy is implemented in a decentralized manner with low overhead. By using the content information to narrow down the search, thistechnique improves the searching performance and hence overall performance of the system. It also helps in reducing the idle time of the computing nodes hence
• Scheduling strategy on load balancing of virtual machine resources - J. Hu et al. [11]proposed a scheduling strategy on load balancing of VM resources that uses historicaldata and current state of the system. This strategy achieves the best load balancing andreduced dynamic migration by using agenetic algorithm.
It helps in resolving the issue of load-imbalance and high cost of migration thus achieving. Better resource utilization.
• Central load balancing policy for virtual machines - A. improving thei utilization.
• Server-based load balancing for Internet distributed services proposed a new serverbased load balancing policy for web servers which are It helps in reducing the service response times by using a protocol that limits the redirection of requests to the closest remote serverswithout overloading them. A middleware is described to implement this protocol. It also usesa heuristic to help web servers to endure overloads.

II.RELATED WORK

Most customers are aware of the danger of letting data control out of their hands and storing data with an outside Cloud Computing provider. There is a lack of transparency for customers on how, when, why and where their data is processed. This is in opposition to the data protection requirement that customers know what happens with their data.

Many Cloud Computing providers are technically able to perform data mining techniques to analyses user data. This is a very sensitive function and even more so, as users are often storing and processing sensitive data when using Cloud Computing services.

Security risks that threaten the transfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks.

The paradigm shifts in Cloud computing makes the use of traditional risk management approaches hard or even impossible Irrespective of the fact that control over data is transferred to the Cloud Computing provider, risk management and compliance issues are split between the Cloud Computing provider, Internet provider and customer.Cloud computing depends on a reliable and secure telecommunications network that assures and guarantees the operations of the terminal users of the services provided in the cloud by the cloud computing provider. Telecommunications networks are often provided separately from the Cloud computing services.

III.IMPLIMENTATION

Risk management and (legal) compliance issues must be well defined in the contract between multi- Cloud Computing provider and customer and should enable transparency with regard to the processing and storage of data.

The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation.

An open and clear specification of the measurements taken to ensure the security the phase Extract, PKG creates the private key for the client.The client creates the block-tag pair and uploads it to combine. The combiner distributes the block-tag pairs to the different cloud servers according to the storage metadata.

The verifier sends the challenge to combiner and the combiner distributes the challenge query to the corresponding cloud servers according to the storage metadata.The cloud servers respond the challenge and the combiner aggregates these responses from the cloud servers. The combiner sends the aggregated response to the verifier.

The telecommunications network that supports the cloud computing services should be secured and protected against malware and DOS attacks.Secure storage using splitting and merging concepts in cloud storage environment.

We proposed dynamic algorithm for resource planning. We proposed Ant Colony Optimization Based Load Balancing Algorithm.

Our proposed resource planning load balancer involves both request monitoring and file access. Also the load balancer will keep track of the virtual machine status i.e, Busy or Ideal, session time, packet size, virtual machine name, type, hostname, port address and bytes read in each virtual machines are been monitored in apache server and based on the status the job is allocated to the virtual machines.

Our proposed system will help to analyse the HEAP memory space of the server (maximum request load).

Our proposed system uses hierarchical load balancing technique. These can be modeled using tree data structure wherein every node in the tree is balanced under the supervision of its parent node. Master or manager can use light weight agent process to get statistics of slave nodes or child nodes.

Hence in this project, we have designed and implemented the resource accounting technique, called **Rameter**. Rameter consists of 2 parts : 1. Keeps track of the distributed requests. 2. Keeps an account of the resource usage. Also integrated **Linear Regression** (LR) to monitor the accountability of the CPU usage. For experimental results, we are implementing ***Apache server*** as the accounting load balancer to keep track of the virtual machine status. ***Tomcat server*** is installed in virtual machine to obtain the job status.

For data secure repository or data recovery in cloud storage we proposed **muti-cloud architecture**, where the user data is split into 2 parts and one half is encrypted using ***AES encryption algorithm*** and other half is encrypted using ***attribute based encryption algorithm*** and stored in Cloud 1 and Cloud 2. During the request our technique will merge the 2 parts and provide the response to the requested user

ADVANTAGES

The use of multiple cloud providers leads to a perceived advantage in terms of security, based on the perception of shared and thus mitigated risks.The use of more than two different cloud providers (n clouds approach) improves on integrity and availability.In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible based on the client’s authorization.

The proposed ID-DPDP protocol can realize private verification delegated verification and public verification

The cloud computing services should be secured and protected against malware and DOS attacks.

Secure architecture for storage of files in the cloud environment.

DISADVANTAGES

Security risks that threaten the transfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks.

It creates a number of issues, among which security aspects are regarded as the most critical factors when considering cloud computing adoption. The risk for data and applications in a public cloud is the simultaneous usage of multiple clouds.

IV. MODULES DESCRIPTION

1. User Authentication
2. AES based Encryption
3. Ant Colony
4. Load Balancing
5. Multiple Cloud

6.File merging and Information retrieval

1. User Authentication

In this module, the new user has registered their details in given field. After registration the user will be posted to authenticated user. The same registered details but different username means the details must be hacked by third party. The authenticated user only able to login their details and move on to forward process in our application. The third party will able to login his details the browser does not enter our application the login failed message shown in that type of users. Finally the authenticated user only allowed.

2. AES based Encryption

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number
of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

3. Ant Colony

The ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. The first algorithm was aiming to search for an optimal path in a graph, based on the behaviour of ants seeking a pathbetween their colony and a source of food. The original idea has since diversified to solve a wider class of numerical problems, and as a result, several problems have emerged, drawing on various aspects of the behaviour of ants. From a broader perspective, ACO performs a model-based search and share some similarities with Estimation of Distribution.

Ant colony optimization algorithms have been applied to many combinatorial optimization problems, ranging from quadratic assignment to protein folding or routing vehicles and a lot of derived methods have been adapted to dynamic problems in real variables, stochastic problems, multi-targets and parallel implementations. It has also been used to produce near-optimal solutions to the travelling salesman problem. They have an advantage over simulated annealing and genetic algorithm approaches of similar problems when the graph may change dynamically; the ant colony algorithm can be run continuously and adapt to changes in real time. This is of interest in network routing and urban transportation systems.

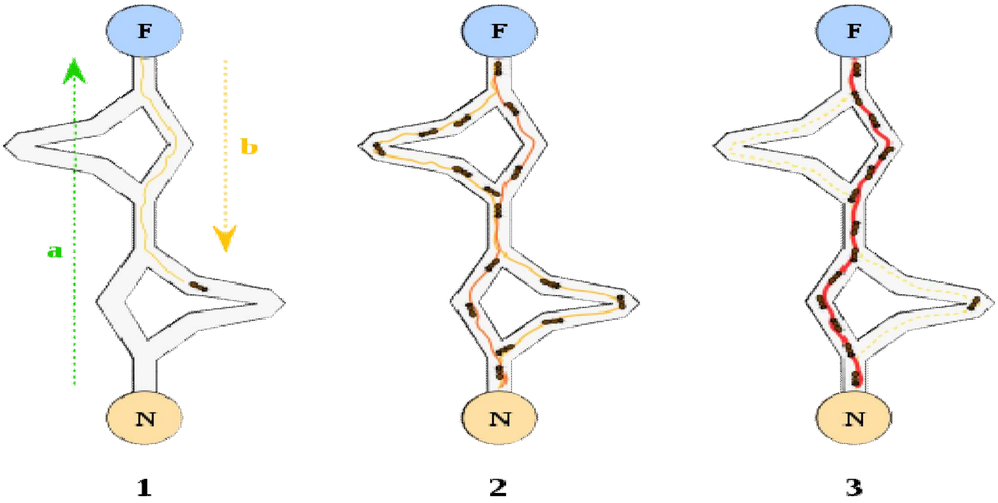

Fig.2. Ant colony

4. Load Balancing

This algorithm is designed to seek out the optimal path among the food and colony of ant, based on its actions. The main aim of this approach is to distribute the work load among the nodes in an efficient manner. The regional load balancing node is preferred as head node in Cloud Computing Service Provider. As the request is being sent, the ant starts is first movement from the head node. The ants collect the information from the cloud node and assign the tasks to the particular node. Once the task is assigned to the head node, the ant moves in a forward direction with the overloaded node to the next node checking whether the node is overloaded or not. During the movement, if it finds any loaded node again it moves in a forward direction, else it finds the overloaded node, it moves in backward direction and replaces were the node found before.Once the job gets successful it is updated, then the result is reported based on the individual result of the ant. After receiving the individual result they are combined together to build the complete report. The solution set is updated automatically, when the ant updates the result for every movement. To prevent backward movement, the ant commits suicide when it reaches the target node.

5. Multiple Cloud

The user wants to store their file on cloud server in distributed manner. For this purpose, input files are subdivided into several fragments. These fragments are store on multiple servers on cloud storage, which are accomplished by single main cloud. In this module, user can upload the file on cloud. For this, file is fragmented and store on multiple servers in distributed manner. This process maintains the security and privacy of data stored on multiple servers and reduces the chances of data corruption.

6. File merging and response retrieval

File saved in multi-cloud which were in cloud me after client send her request to owner to download the file from multi-cloud then owner will check out which client send the request from registration want to download the file then owner send its response with key generation after client received its response from owner now client will download hole file with the help of merging algorithm response retrieval to download and view the file the process based of encryption and decryption algorithm.

In proposed system, we use AES for encryption and then the files are split into equal fragments while uploading. We split the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file. The basic plan is to use many clouds at constant time to mitigate the risks of malicious knowledge manipulation, disclosure, and method meddling. This design changed targets the confidentiality of knowledge and process logic. It provides a solution to the subsequent question: however will a cloud user avoid absolutely revealing the information or process logic to the cloud provider. The information shouldn't solely be protected whereas within the persistent storage, however particularly once it's processed. The idea of this design is that the applying logic must be divided into fine-grained components and these components area unit distributed to distinct cloud. In coding technique, the user encrypts the information together with his key and uploads the cipher texts to the Cloud. Thus different fragments for a single file would be saved in 3 different clouds.

V. CONCLUSION

In multi-cloud storage, this paper formalizes the ID-DPDP system model and security model. At the same time, we propose the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.Cloud Computing has widely been adopted by theindustry, though there are many existing issues like LoadBalancing, Virtual Machine Migration, Server Consolidation, Energy Management, etc. which have notbeen fully addressed. Central to these issues is the issueof load balancing, that is required to distribute the excessdynamic local workload evenly to all the nodes in the whole Cloud to achieve a high user satisfaction andresource utilization ratio. It also ensures that everycomputing resource is distributed efficiently and fairly.Existing Load Balancing techniques that have beenstudied, mainly focus on reducing overhead, serviceresponse time and improving performance etc...

VI. FORTHCOMING ENHANCEMENT

More performance metric such as latency etc. can be considered. These performance metrics can be used to improve the performance of applications running in the cloud. These performance metric tests can be run on large EC2 instancesMore performance metric such as latency etc. can be considered.
During uploading and download user has to answer the security question and security
are provided by user during the registration phase .
So uploading/downloading operation if user is normal then he can answer that security question if he/she cannot answer that question thus using this we can provide more security We can provide the security to upload data and the digest by using the encryption algorithm

REFERENCES

[1] Alibaba. Alibaba cloud computing [Online]. Available: http://www.aliyun.com/, Apr. 2015.
[2] Amazon. Amazon elastic compute cloud (amazon ec2) [Online]. Available: http://aws.amazon.com/cn/ec2/, Apr. 2015.
[3] L. Andrew, A. Wierman, and A. Tang, "Optimal speed scaling under arbitrary power functions," ACM SIGMETRICS Perform. Eval.Rev., vol. 37, no. 2, pp. 39–41, 2009.
[4] A. Antoniadis and C.-C.Huang, "Non-preemptive speed scaling," J. Scheduling, vol. 16, no. 4, pp. 385–394, 2013.
[5] Apache. Apache hadoop [Online]. Available: http://hadoop. apache.org/, Apr. 2015.
[6] Maria Spinola, ―An Essential Guide to Possibilities and Risks of Cloud Computing: a Pragmatic Effective and Hype Free Approach for Strategic Enterprise Decision Making‖. (white paper) 2009
[7] Ratan Mishra and AnantJaiswal, ―Ant Colony Optimization: A solution of Load Balancing in Cloud‖, International Journal of Web & Semantic Technology (IJWesT), April 2012
[8] VenubabuKunamneni, "Dynamic Load Balancing for the cloud", International Journal of Computer Science and Electrical Engineering, 2012.
[9] PoojaSamal, Pranati Mishra, ‖Analysis of variants in Round Robin Algorithms for load balancing in Cloud Computing‖ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 416-419.
[10] Che-Lun Hung1, Hsiao-hsi Wang2 and Yu-Chen Hu2, ―Efficient Load Balancing Algorithm for Cloud Computing Network‖. IEEE Vol. 9, pp: 70-78, 2012
[11] T. Kokilavani, Dr. D. I. George Amalarethinam ―Load Balanced Min-Min Algorithm for Static Meta Task Scheduling in Grid computing‖ International Journal of Computer Applications Vol20 No.2, 2011.
[12] UpendraBhoi, Purvi N. Ramanuj, ―Enhanced Max-min Task Scheduling Algorithm in Cloud Computing‖ International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue
[13] K. M. Nagothu, B. Kelley, J. Prevost, and M. Jamshidi,"Ultra low energy cloud computing using adaptive loadprediction", Proceedings of IEEE World AutomationCongress(WAC) , Kobe, September 2010, pages 1-7.