IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Security in Cloud Computing and Different Algorithms for Load Balancing

Anitha R[1], Dr C Vidyaraj[2]

Associate Professor, Dept of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India[1]

Professor, Dept of Computer Science and Engg, The National Institute of Engineering, Mysuru, Karnataka, India[2]

Abstract: Cloud computing opens up a new era in Information Technology, in order to reduce the enormous investments of the customers in their own infrastructure, it provides various IT services such as pay-as you-go flexibly and and is also scalable where the customers can use the same. In this philosophy, cloud storage service users do not need to physically and directly control the data. Data security relates to an important use of the cloud. Existing research work has shown enabling data integrity to be checked without the actual data file. When the scan is from a trusted third party, this verification process is also known as the data auditing, and the third part which does this is known as auditor. Our work gives a brief description over how cloud works, how the data in the cloud is accessed, and the process of load balancing in cloud computing. Load balancing is an important aspect of cloud computing environment. Efficient charge balancing scheme ensures the efficient use of resources and the supply of cloud resources to the users on-demand based on the payment. Load balancing can even support the prioritization of the user through the proper implementation of the scheduling criteria.

Keywords: IP networks, Hop by hop, optimal routing, adaptive routing, link state.

1. INTRODUCTION

Cloud Computing is intense to the most influential innovations in information technology referred to it in recent years. With virtualization of resources cloud computing can provide services based on pay as-you-go mode, which is set to the favorable day-Life be similar to utilities such as electricity, gas, water and telephone in a future to operate next.

These cloud computing service also provide many services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-service (PaaS) and Software-as-a-service (SaaS). Many international IT companies now offer efficient public cloud services to users on an individual scale for companies around the world; Examples include Amazon AWS, Microsoft Azure and IBM Smart.

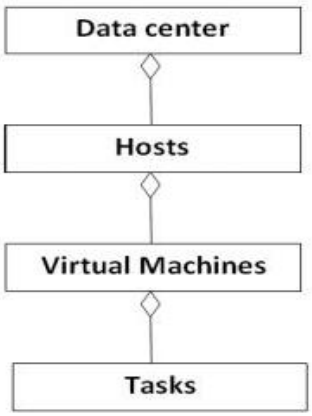

Fig.1: Class diagram of cloud.

Although the current development and dissemination of cloud computing is fast, debates and concerns about the cloud shutdown use there. Privacy / Online privacy is a major concern in the adoption of cloud computing. Compared to conventional systems, users will lose their direct control over their data. In this post we will examine the problem of integrity control for large data storage in the cloud. This problem can be therefore called audit data, if the test is carried out by a trusted third party. From the cloud user auditing as-a-service point of view, therefore, can be called. A research to solve the problems in the auditing is being done. In a remote system for review, the server cloud storage, enter a valid proof of integrity in an amount of data to a tester unless all these data are intact. In order to ensure stored the integrity of users to cloud service providers of data, not least than any Data Protection Mechanism by cloud service -provider (CSP) develops this support, no matter how safe you seem, in fact, that will provide the tester of a piece of direct intelligence, reliable, real-time exceeded the integrity of user data in the cloud through a request for challenge.

2. LOAD BALANCING

Load balancing in cloud computing provides an efficient solution to various issues residing in cloud computing environment set-up and usage. Load balancing must take into account two major tasks, one is the resource provisioning or resource allocation and other is task scheduling in distributed environment. Efficient

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

provisioning of resources and scheduling of resources as well as tasks will ensure:

a. Resources are easily available on demand.
b. Resources are efficiently utilized under condition of high/low load.
c. Energy is saved in case of low load (i.e. when usage of cloud resources is below certain threshold).
d. Cost of using resources is reduced.

For measuring the efficiency and effectiveness of Load Balancing algorithms simulation environment are required. CloudSim is the most efficient tool that can be used for modeling of Cloud. During the lifecycle of a Cloud, CloudSim allows VMs to be managed by hosts which in turn are managed by datacenters. Cloudsim provides architecture with four basic entities. These entities allow user to set-up a basic cloud computing environment and measure the effectiveness of Load Balancing algorithms. A typical Cloud modeled using CloudSim consists of following four entities:

- Datacenters,
- Hosts,
- Virtual Machines and
- Application as well as System Software.

Datacenters entity has the responsibility of providing Infrastructure level Services to the Cloud Users. They act as a home to several Host Entities or several instances hosts' entities aggregate to form a single Datacenter entity. Hosts in Cloud are Physical Servers that have pre-configured processing capabilities. Host is responsible for providing Software level service to the Cloud Users. Hosts have their own storage and memory. Processing capabilities of hosts is expressed in MIPS (million instructions per second). They act as a home to Virtual Machines or several instances of Virtual machine entity aggregate to form a Host entity. Virtual Machine allows development as well as deployment of custom application service models. They are mapped to a host that matches their critical characteristics like storage, processing, memory, software and availability requirements.

CloudSim:
CloudSim is a toolkit (library) for simulation of Cloud computing scenarios. It provides basic classes for describing data centers, virtual machines, applications, users, computational resources, and policies for management of diverse parts of the system (e.g., scheduling and provisioning). These components can be put together for users to evaluate new strategies in utilization of Clouds (policies, scheduling algorithms, mapping and load balancing policies, etc). It can also be used to evaluate efficiency of strategies from different perspectives, from cost/profit to speed up of application execution time. It also supports evaluation of Green IT policies.

The above are some common scenarios we envisioned and that users have been explored. Nevertheless, there is no limit on the utilization you can make from it: classes can be extended or replaced, new policies can be added and new scenarios for utilization can be coded. Think of it as the building blocks for your own simulated Cloud environment.
Therefore, CloudSim is not a ready-to-use solution were you set parameters and collect results for use in your project. Being a library, CloudSim requires that you write a Java program using its components to compose the desired scenario. Nevertheless, CloudSim can be used to build such a ready-to-use solution.

3. SECURITY IN CLOUD

Security in cloud is an important aspect in cloud computing which is to be taken care of. Although strong security is important in many services, such as e-commerce and telemedicine, many other services, such as the provision of public information, can function with much less security. Even users of the same service can have different security needs because their data might not have the same assets. For example, a user needs a high security level for a voice service that concerns a business discussion, but only a low level for the same service when calling a friend to meet for lunch. Similarly, an e-mail service user needs content encryption when the message contains sensitive information, but only plaintext for general e-mail.
The stronger the security, the greater the consumption of computing, memory, and bandwidth resources and the more difficult the service is to use, requiring manual configuration of security mechanism parameters. Thus, protecting services and data at a higher level than they need erodes the advantages of a cloud-computing platform.

Security Domains:
Network:
The main threats while data is in transmission are fabricated identity, man-in-the-middle, and denial-of-service attacks. To protect against these threats, the network security domain includes mechanisms such as the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols, IPSec, network-based intrusion detection, and traffic cleaning.

The security gateway, which mediates all communications to and from the system, is an important entity in this domain because it enables more fine-grained access control. If a malicious act occurs, such as a distributed denial-of-service attack, the gateway can immediately limit or even turn off malicious communication, thus thwarting the attacker. For legitimate connections, the network security domain specifies using a security protocol such as SSL or IPSec to protect against possible man-in-the-middle attacks and information leaks.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

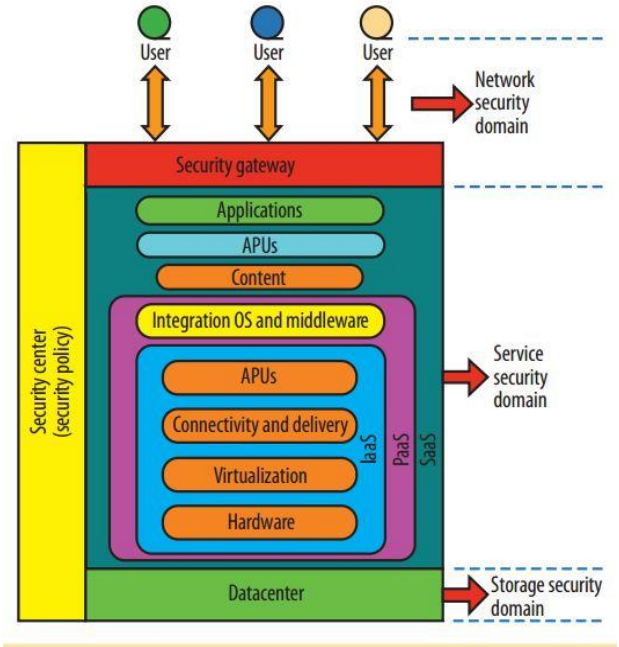

Fig.2: Security Domains in Cloud.

Service:
The main threats to data in the cloud services (IaaS, PaaS, and SaaS) are a fabricated service process, an illegally controlled service, and malicious service interruption. To address these threats, the service security domain includes mechanisms such as authentication, authorization, vulnerability scanning, data isolation, and virus detection. To protect legitimate services from illegal control and process interruption, an intrusion detection and prevention system monitors all user actions. The system can also use honeypot technology—a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use—to capture malicious actions at intervals. To avoid viral infection and service hijacking, SaaS, PaaS, and IaaS for each user can run in logical isolation.

Storage:
The main threats while data is in storage are unauthorized access and data alteration and theft. Protection mechanisms include encryption, marking data with different access levels to enable access control, and integrity verification. Backup techniques, such as a redundant array of independent disks and data recovery, insure against data loss.

4. RELATED WORK TO LOAD BALANCING ALGORITHMS

Cloud is made up of massive resources. Management of these resources requires efficient planning and proper layout. While designing an algorithm for resource provisioning on cloud the developer must take into consideration different cloud scenarios and must be aware of the issues that are to be resolved by the proposed algorithm. Therefore, resource provisioning algorithm can be categorized into different classes based upon the environment, purpose and technique of proposed solution.

4.1. Load Balancing on the basis of cloud Environment
Cloud computing environment can be static or dynamic as cloud developers require by the cloud provider.

4.1.1. Static Environment
Static environment in the cloud provider installed homogeneous resources. The resources in the cloud are not flexible when around made static. In this scenario, the cloud knowledge node capacity, processing power, memory and performance statistics of user requests must. These user requirements are not subjected to a change in the term. Proposed algorithms to achieve load balancing in static environment, not adapt to the runtime load changes. Although static environment easier to simulate, but not well suited for heterogeneous cloud environment.

4.1.2 Dynamic Environment
In dynamic cloud provider environment installed heterogeneous resources. The funds are flexible in a dynamic environment. In this scenario, the cloud cannot rely on prior knowledge while they considered the runtime statistics. The flexibility of the user requirements (ie they may change during the term).

Algorithm proposed in order to achieve load balancing in a dynamic environment can easily adapt to changes in run-time load. It's hard to simulate dynamic environment, but is very adaptable with cloud computing in WLC environment. Based (weighted least connection) algorithm, Ren propose a load balancing technique called dynamic environment ESWLC. He attributes the appeal of a minimum weight to a task and takes into account node capabilities. Based on the weight and capacity of the node the task is assigned to a node. LBMM (Load Balancing Min-Min) algorithm uses three levels of allocation for resource frames in the dynamic environment. It uses the BPC (opportunistic load balancing algorithm) as a base. Since cloud is highly scalable and autonomous, dynamic programming is a better choice compared to the static schedule

4.2. Load Balancing based on Spatial Distribution of nodes
Node in the cloud are highly distributed. Therefore, the node that regulates causes providing decision algorithm to use as the category. There are three types of algorithms that determine which node is responsible for load balancing cloud computing environment.

4.2.1. Centralized Load Balancing
The centralized load balancing technique any decision allocation and programming are made by a single node. This node is responsible for storing Knowledge Base of the entire cloud network and can apply static or dynamic approach to load balancing. This technique reduces the time required to analyze the different cloud resources , but

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

creates a great burden on the central node. Therefore, the network is no longer fault-tolerant in this scenario as a failure intensity overwhelmed centralized node is high and the recovery may not be easy in case of node failure .

4.2.2. Distributed Load Balancing

In distributed load balancing technique in single node responsible for resource allocation and task scheduling decision. It is the only domain Responsible for monitoring the network cloud rather than multiple domains monitor the network in order to make precise load balancing decision . Each node in the network path Maintains knowledge base to an efficient distribution of tasks in static environment Verify and re- distribution in the dynamic environment . In distributed scenario failure intensity of a node is not neglected . Therefore, the system is fault tolerant and balanced , and is overloaded in each node to meet the load balancing decision .

4.2.3. Hierarchical Load Balancing

Hierarchical load balancing involves different levels of the cloud in load balancing decision. Such load balancing techniques mostly operate in master slave mode. 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. Based upon the information gathered by the parent node provisioning or scheduling decision is made. Three-phase hierarchical scheduling has multiple phases of scheduling. Request monitor acts as a head of the network and is responsible for monitoring service manager which in turn monitor service nodes. First phase uses BTO (Best Task Order) scheduling, second phase uses EOLB (Enhanced Opportunistic Load Balancing) scheduling and third phase uses EMM (Enhanced Min-Min) scheduling.

4.3. Load Balancing Based on Task dependencies

Dependent tasks are those whose execution is dependent on one or more sub-tasks. They can be executed only after completion of the sub-tasks on which it is dependent. Therefore, scheduling of such task prior to execution of sub-tasks is in-efficient. Task dependency is modeled using workflow based algorithms. Workflow basically uses DAG as knowledge base to represent task dependency. Different workflow based solution consider different parameters. Algorithm are designed keeping in mind whether single or multiple workflows are to be modeled or single or multiple QoS are to be maintained in the system. Different workflows with or without completely different structure are termed as multiple workflows. Workflows can also be classified as Transaction Incentive (multiple instances of one workflow that have same structure) and Data Incentive workflows (size and quantity of data is large).Cost based scheduling algorithm is designed for single workflows. It partitions the workflows and assigns each partition a deadline. Zhifeng Yu and Weisong Shi designed an algorithm for multiple workflows which focus only on execution time.

5. CONCLUSION

With the proposed proactive workload management technology, the hybrid cloud computing model allows users to develop a new architecture where a dedicated resource platform runs for hosting base service workload, and a separate and shared resource platform serves flash crowd peak load. Load balancing is clearly explained with different scenarios in the paper. Load Balancing is an essential task in Cloud Computing environment to achieve maximum utilization of resources. In this paper, we discussed various load balancing schemes, each having some pros and cons. On one hand static load balancing scheme provide easiest simulation and monitoring of environment but fail to model heterogeneous nature of cloud. On the other hand, dynamic load balancing algorithm are difficult to simulate but are best suited in heterogeneous environment of cloud computing. Dynamic load balancing techniques in distributed or hierarchical environment provide better performance. However, performance of the cloud computing environment can be further maximized if dependencies between tasks are modeled using workflows.

REFERENCES

[1] 'Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates' Chang Liu, Jinjun Chen,Senior Member, IEEE, Laurence T. Yang, Member, IEEE, Xuyun Zhang, Chi Yang, Rajiv Ranjan, and Ramamohanarao Kotagiri

[2] 'Proactive Workload Management in Hybrid Cloud Computing' Hui Zhang, Guofei Jiang, Kenji Yoshihira, and Haifeng Chen

[3] 'A Comparative Study of Load Balancing Algorithms in Cloud Computing Environment' Mayanka Katyal, Atul Mishra

[4] Foster, I., Zhao, Y., Raicu, I. & Lu, S. (2008). Cloud computing and grid computing 360-degree compared. IEEE Grid Computing Environment Workshops.

[5] Luo, S., Lin, Z. & Chenm, X. (2011). 'Virtualization security for cloud computing service. 2011 International Conference on Cloud and Service Computing' ©2011 IEEE. Shenzhen, China: ZTE Corporation.

[6] D. Zissis and D. Lekkas, 'Addressing Cloud Computing Security Issues,' Future Gen. Comput. Syst., vol. 28, no. 3, pp. 583-592, Mar. 2011.

[7] S.Nepal, S.Chen, J.Yao, and D.Thilakanathan, ''DIaaS:Data Integrity as a Service in the Cloud,'' in Proc. 4th Int'l Conf. on Cloud Computing (IEEE CLOUD), 2011, pp. 308-315

[8] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, 'A View of Cloud Computing,' Commun. ACM, vol. 53, no. 4, pp. 50 58,Apr. 2010