A study of virtualization technology and its applications in cloud computing

Dr. Amit Chaturvedi[*1] **and Pankaj Nandan**[#2]

Engineering College, Ajmer[*1]*, Govt. Degree College, Basohli, J&K*[#2]

Abstract: *Virtualization in Cloud Computing is making a virtual platform of server operating system and storage devices. This will help the user by providing multiple machines at the same time. It also allows sharing a single physical instance of resource or an application to multiple users. Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient. Cloud Computing is growing and every solution provider wants to be part of the hype. This new trend promises to abstract IT professionals from the underlying nuts and bolts of server virtualization, storage allocation, scalability, availability, and operational overhead. One of the important features of virtualization is that it allows sharing of applications to multiple customers and companies. Virtualization provides numerous benefits to cloud computing like security, more economical solutions, greater flexibility in transfer of data, etc. Secure and more economical solution in turn provides flexible operation of the cloud services and expands the scope of cloud application services, and with greater flexible & secure transfer of data eliminates the risk of system failure.*

Keywords: **virtualization, cloud computing, hypervisor, VMM, virtual machine, applications.**

1. Introduction

As virtualization hides the complexity of the underlying hardware and its functionality. It provides a virtual platform, from where users may ask for the resources and for the application services. In cloud computing environment resources like hardware, operating systems, applications, user's data, etc are managed in a layered architecture. Cloud computing has a layered architecture and the layers with their objectives are marked separately as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a service).

Infrastructure as a Service (IaaS) layer provides infrastructure capabilities like processing, storage, networking, security, and other resources that allows consumers to deploy their applications and data. This is the lowest layer in the cloud computing architecture. Some of the major infrastructure providers are Amazon S3/EC2, Microsoft Windows Azure, and VMWare vCloud, etc. Platform as a service (PaaS) provides application infrastructure such as programming languages, database management systems, web servers, applications servers, etc that allow applications to run. The virtualization technology makes user free from managing the underlying platform complexities including networking, operating systems, etc. Some of the popular examples of platform as a service providers are Google App Engine, Microsoft Azure Services Platform, ORACLE/AWS, etc. Software as a Service (SaaS) is the most sophisticated model hiding the underlying details of networking, storage, operating system, database management systems, application servers, etc from the consumers. It provides the end-user software application services most commonly through a web browser. Some examples of the SaaS providers are Salesforce CRM, Oracle CRM on Demand, Microsoft Online Services, and Google Apps.

The virtualization technology is mainly service oriented and focuses on cost reduction, hardware reduction and pay just for service concept. Virtualization in cloud computing is making a virtual image of the storage devices servers or network resources so that they can be used on multiple machines at the same time. The major characteristics of the cloud computing are on-demand self service, broadband network access, rapid elasticity, resource pooled, and measured services.

According to the NIST, National Institute of Standards and Technology, cloud computing is:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

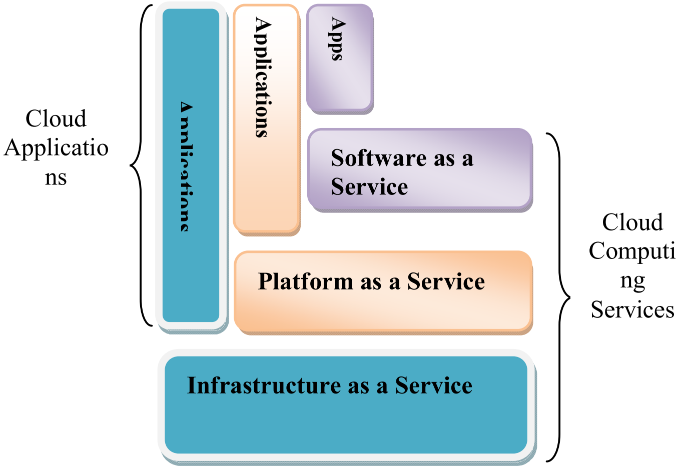

Figure 1 : Basic Architecture of Cloud Computing

2. Virtualization Architecture

Virtual machine is computer software that runs operating system and applications. It creates the image of the required APIs of OS and application software that the customer or end-user actually requires. This image is virtual that hides the complexity of working between applications, operating system, and hardware. This image is called as Virtual Machines. The physical server on which one or more virtual machines are running is defined as host. The virtual machines are called guests. Multiple virtual systems (VMs) can run on a single physical system.

Full virtualization is a technique in which a complete installation of one machine is run on another. Full virtualization runs any non-modified operating system which supports the platform being emulated. The main disadvantages of emulations are low performance and low density. Examples are Microsoft Hyper-V, VMware Workstation. Other forms of virtualization are Hardware Assisted Virtualization, Partial Virtualization, Para virtualization, OS level Virtualization, Multi-server cluster virtualization, hypervisor-based virtualization, the application level virtualization, and network virtualization.

Virtualization technology permits a single machine to run several platforms concurrently, for example different versions of windows running at the same time on a single machine. Sometimes referred to as machine or processor virtualization, it allows a single physical machine to emulate the behavior of various machines, with the ability to host multiple/heterogeneous operating system on the same hardware. The hosted operating systems are called guest operating systems.

Virtualization allows for server consolidation in data centre’s, where multiple operating systems that would have been underutilized on their host to be moved to the same physical resources. This enables a reduction in the number of physical machines and their improved exploitation at higher saturation levels thus saving cost and energy. Virtualization can be seen as using computer resources to imitate other computer resources or whole computer. It separates resources and services from the underlining physical delivery environment.

Benefits of Virtualization

Virtualization technology offers applications an abstract view through interfaces of the underlying hardware platform and resources with the following benefits.

1) Functional Execution Isolation: The hyper visor handles the protection among virtual machines (VMs) and therefore among the applications on different VMs. Users can be granted privileges within their VM without compromising the isolation or host integrity.

2) Customized Environment: Virtualization enables the provisioning of a highly customized and specialized environment that may contain specific purpose operating systems, libraries, and run time environments. Virtualization offers multiple views over the same physical hardware through functional isolation.

3) Easier Management: Customized run-time environment can be started-up, migrated, shutdown in a very flexible way depending on the need of who provides the underlying hardware.

4) Coexistence with Legacy Application: Legacy applications can coexist with brand new ones. VMs help to preserve binary compatibility in the run-time environment for legacy applications.

5) Testing and Debugging Parallel Apps: Testing parallel applications can leverage virtualized environments, as a full distribute system may be emulated within a single physical host.

6) Enhance Reliability: Hypervisors and their live migration capabilities allow for enhanced reliability of hosted virtualized applications. This makes them independent of the reliability of the underlying hardware in a seamless and transparent manner for applications.

7) VM Migration: VM migration is an interesting feature of cloud computing which is aimed to respond to dynamic requests of VMs in order to guarantee the promised SLA to the cloud consumer. Thus when VM request for some resources which cannot be provided in the hosted physical machine, the VM is migrated to another physical machine to satisfy the VMs requested resource. Also VMs may be migrated to provide better management of the physical machines and data centre's. One of the most important operations which are conducted as part of the VM migration is the VM placement in which a proper physical machine is selected to host the VM.

3. REVIEW OF LITERATURE

Cloud computing is an archetype that enables access to a shared pool of computing resources for cloud users in an on-demand or pay-per-use, fashion. Cloud computing offers several benefits to users and organizations, in terms of capital expenditure and savings in operational expenditure. Despite the existence of such benefits, there are some obstacles that place restrictions on the usage of cloud computing. Security is a major issue that is always considered. The lack of this vital feature results in the negative impact of the computing archetype thus resulting in personal, ethical, and financial harm. This paper will focus and explore the security challenges that are faced by cloud entities. These entities include Cloud Service Provider, the Data Owner and Cloud User. Focusing on the crypto-cloud that constitutes of different Communication, Computation, and Service Level Agreement. Studying the causes and effects of various cyber-attacks it will provide the necessary upgrades [1].

The paper discusses the constructive framework for writing hypervisor on the top of the VM. Hypervisor plays a vital role in monitoring VM in cloud. Hypervisors are system programs that virtualizes the running of the architecture. These are critical, safe, small and hard program to write and debug or evaluate. Hypervisors are system software programs that virtualize the architecture they run on. They are typically small, safety-critical, and hard to debug, which makes them a feasible and interesting target for formal verification. Previous functional verifications of system software were all based on interactive theorem proving, requiring substantial human effort complemented by expert proven knowledge. In this paper we present the frame work of a hypervisor and basic implementation module of hypervisor and simulator module of hypervisor. The virtual environment is controlled and managed by software known as the hypervisor. The hypervisor executes at a higher privilege level than the “guest” operating systems; the hypervisor can access any memory assigned to any guest operating system. Furthermore, a guest operating system cannot access resources in the system unless permitted to do so by the hypervisor [2].

Despite the many researches that have been conducted in the field of Cloud computing, it is still facing some issues and challenges, such as load balancing which still needs more optimizing methodologies and models to improve performance and achieve high user satisfaction. In this paper, Machine Learning Technique, which is classification, is used to make groups of VMs based on their CPU and RAM utilization, as well as to classify user jobs/tasks into different groups based on their sizes and based on information from log files. The approach arranges virtual machines in groups, and several tasks share the same VM resources. The goal of our proposal is to allow more dynamic resources and to improve the QoS requirements by maximizing the usage of the resources and user satisfaction, such as increasing resource utilization and reducing the number of job rejections [3].

Prior to 2017, the data center at Sichuan Top IT Vocational Institute adopted a centralized and traditional mode of "foundation based support" with a high degree of coupling between network applications and physical servers. With the type of network services and business volume continuing to increase, the centralized and highly coupled architecture model cannot meet the growing demand for huge amounts of data and services, which exposed more and more disadvantages in resource integration, energy consumption, QoS, utilization, reliability, economy, manageability, security, etc. After full technical demonstration it is decided to adopt the H3C CAS virtualization cloud computing platform to transform and upgrade the data center1. The project has been completed its implementation in January 2017. After nearly three months of routine operating conditions and statistics analysis, in terms of energy consumption, QoS, resource utilization, failure rate and so on it has achieved the intended expectations. Meanwhile a typical test program has been designed to simulate the mass visit, which verified that the system fully capable of peak concurrent access [4].

Virtual machine migration is an important method for achieving scalability through optimized resource utilization in the modern data centers. Most of the previous works concentrated on how to migrate the virtual machinewith huge traffic demands in the cloud environment. It mainly focused on energy consumed by the virtual machines and the network traffic between them. None of the earlier algorithms focused from the client’s perspective, like the delay faced by them to get their services processed. In this paper a new paradigm for virtual machine migration, based on the demands of the clients is considered. One of the clients demand is faster service time. To achieve this an algorithm called Virtual Machine Migration Approach Based on Distance and Traffic is developed. The methodology is based on the traffic and the geographical locations of the data centers. The algorithm is executed at regular intervals to check for the traffic in the network. It also checks for the distance of the data centers where the client request has to be placed. The request is placed to the nearest data center with less traffic. This improves the performance by reducing the round trip time. As the traffic is less so there is an optimized utilization of the resources. The reduction in round trip time and maintaining the round trip time without much fluctuation even in the case of a failure of one of the physical machine helps to improve the performance by providing faster services to the clients [5].

In the cloud infrastructure, the co-resident attack is a critical security threat. Through virtualization technology provided by Cloud Service Provider, tenants' virtual machines (VMs) are possible to be allocated on the same host. Multi-tenant environment provides malicious tenants an opportunity to launch the co-resident attack and steal other tenants' information by side channels. To prevent this type of attack, previous works mostly pay attention to eliminating side channels and few of them study VM deployment strategy. Hence, we focus on deploying VMs with a secure and effective allocation strategy to reduce the probability of VM coresidence. A novel VM allocation strategy is proposed with three optimization objectives including security, load balancing and energy consumption. Finally, we implement our VM allocation strategy and prove its effectiveness on the simulation platform CloudSim [6].

The existence of a virtualization layer within the cloud affects the resources optimization and the reduction of requirements of its implementation. In this publication the focus will be the use of jail environments, provided by the FreeBSD Operating System, which present a relevant set of features that can enhance the increase of performance. A set of data collection tests that allows measuring the degree of optimization obtainable in current models of cloud computing, based on the use of hypervisors tests, are presented. These tests proved that the increase in performance and optimization of resources is possible, bringing up the need to adapt the current models of cloud computing for the use of such solutions. However, this increase in performance, leads to a loss of flexibility of the usage of independent operating systems, which is not relevant to the model of cloud computing business [7].

As an emerging technology and business paradigm, Cloud Computing has taken commercial computing by storm. Cloud computing platforms provide easy access to a company's high-performance computing and storage infrastructure through web services. With cloud computing, the aim is to hide the complexity of IT infrastructure management from its users. At the same time, cloud computing platforms provide massive scalability, 99.999% reliability, high performance, and specifiable configurability. These capabilities are provided at relatively low costs compared to dedicated infrastructures. This article gives a quick introduction to cloud storage. It covers the key technologies in Cloud Computing and Cloud Storage, several different types of clouds services, and describes the advantages and challenges of Cloud Storage after the introduction of the Cloud Storage reference model [8].

Cloud computing is basically to perform computation on a centralized facility provided by third party. It also provides storage facilities operated by the third party. Cloud computing allows us to hire entire platform for software

development, hardware resources or setup a platform in house. Cloud computing offers everything as-a-service. It provides infrastructure as-a-service, platform as-a-service, software as-a-service and human as-a-service. This paper gives an introduction to what the cloud computing is, services it provide, how it is deployed, with its features and challenges. This paper focus on database management in cloud computing. It also analyses cloud DBMS characteristics, challenges and also compare various types of cloud databases [9].

Cloud Computing constitutes an alternative for organizations who do not intend to invest in in-house IT resources. It offers a service model on the premise that the consumer has at its disposal the means for manipulating information, over the internet, according to its current needs. However, outsourcing IT poses various challenges, such as the effective control of IT, attention to an increasing number of threats posed by the Internet ecosystem and concerns regarding the efficient use of resources. Hence, the uncertainties about the migration to Cloud Computing can have a negative impact on the adoption of this technology. In order to better inform the decision process launched by organizations considering the alternative of Cloud Computing, this study presents a list of key issues compiled from literature that could assist IT managers steering the organization towards the path of adopting Cloud Computing solutions efficiently and securely. In addition, to better understand those issues and rank them in terms of importance, interviews were conducted with IT directors of enterprises that use and provide Cloud services, endowing the list of issues with the views of practitioners that successfully experienced the migration to the Cloud environment [10].

The evolution of cloud computing has revolutionized how the computing is abstracted and utilized on remote third party infrastructure. It is now feasible to try out novel ideas over the cloud with no or very low initial cost. Cloud computing is attractive to companies and organizations as it eliminates the requirement for them to plan ahead for provisioning, and allows them to start with small resources and increase gradually as the service demand rises. There are challenges in adopting cloud computing; but with obstacles, we have opportunities for research in several aspects of cloud computing. One of the main issue is the data security and privacy of information stored and processed at the cloud service provider’s systems. In this work, We surveyed several research work on cloud computing related to security challenges and privacy issues. The primary goal of this paper is to provide a better understanding of the security challenges of cloud computing and identify approaches and solutions which have been proposed and adopted by the cloud service industry [11].

According to a Forbes’ report published in 2015, cloud-based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This paper summarizes a number of peer-reviewed articles on security threats in cloud computing and the preventive methods. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combating threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting [12].

4. OUTCOME OF THE STUDY

Let us understand the role of virtualization layer in cloud architecture from the below given figure 2. As shown in the figure 2, the lowest layer or layer 0 shows the underlying hardware or physical resources available with the server(s), if we use bottom up approach. On the top of it, the Host OS or Layer 1 works with its required API and provides the services of accessing or allocation of the hardware resources. On top of it, the virtualization layer or Layer 2 exist, this layer may contain multiple Hypervisor(s) or Virtual Machine Monitor(s) (VMMs). This virtualization layer provides variety of services, most importantly the efficient resource allocation with full of elasticity like storage, network, availability, security, scalability, hosting etc. For example, Microsoft Windows Azure is the Microsoft product to provide the service of this virtualization layer. Above this layer, the Management Layer or Layer 3 exists. This layer is basically responsible for providing the required management services like Hypervisor Interface, Load Distribution, Security, Validation Engine, Virtual Jobs, Scheduler, Internal and External Cloud API. Above this layer, the Guest OS exists with its all required binaries/ libraries to support the developers or its end users for the development of applications or execution or running the applications. The Guest OS with the binaries/ libraries and applications forms Virtual Machine (VM). A virtual machine (VM) is an isolated runtime environment. Multiple virtual systems (VMs) can run on a single physical system.

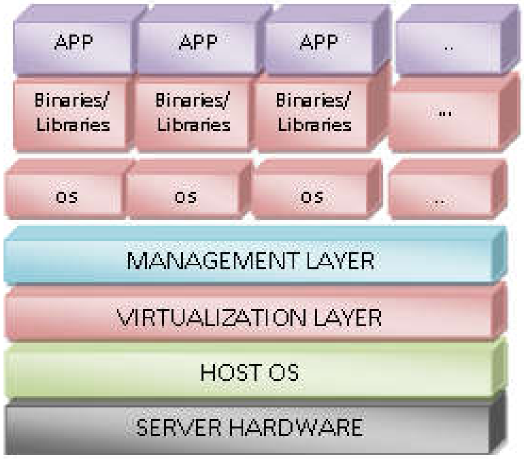

Figure 2: Layered Architecture of Virtualization in Cloud Computing

Service Level Agreement (SLA) is another very important document for providing a shared virtual platform to the multiple clients through virtualization. Because clients and providers of the cloud service both are bounded with this SLA. This SLA covers all the service level agreements, metering related agreements and protocols decided by the various regulating bodies of the internet and other internet based services. SLA violations may result into declination in return on investment or contract termination sometimes. The implementation of the SLA is one of the major objectives of the management layer, it covers the proper functioning of the virtual jobs, security, and load distribution.

5. PROPOSED MODEL AND METHODOLOGY

Following is the Model and Methodology of Virtual Machine Monitors for handling virtual jobs.

Step 1 - Generation of Cloudlets: In present Scenario, with an environment of cloud the job is divided and disseminated into same size of small jobs i.e. Cloudlets. These Cloudlets as well as Virtual Machines are scheduled according to the different scheduling policy for e.g. FCFS, Round Robin etc. Generally in Cloud Computing scenario user suggest the task to be performed / executed. Cloud Coordinator (CC) divides the task into identical sized cloudlets and passes it to Datacenter (DC). Normally it takes a lot of time because the cloudlets are processed one at a time in FCFS manner as and when they reach to VM. VM executes the cloudlets here in the queue as they reach the VM's. Basically this default job scheduled policy is enormously Time-Consuming, Cost insensitive and inefficient.

Step 2 - Selection of Scheduling Algorithm: In this step user has to choose the one algorithm out of three that are Shortest Job First (SJF), Earliest Deadline First (EDF), and Credit-Based Scheduling (CBS) Algorithm

- In Shortest Job First Algorithm the length of the job is considered. The job having minimum length will execute first. The job having largest length will be executed at the last part.
- In Earliest Deadline First Algorithm the deadline of job is considered. The job having uppermost priority is considered first.
- In Credit-Based Scheduling Algorithm length as well as the priority of job is considered.

Step 3 - Submission of Cloudlets (jobs) Length: Next step is entering the length of jobs as necessary. The deadline of algorithm will enter only in earliest deadline first and credit based scheduling algorithm.

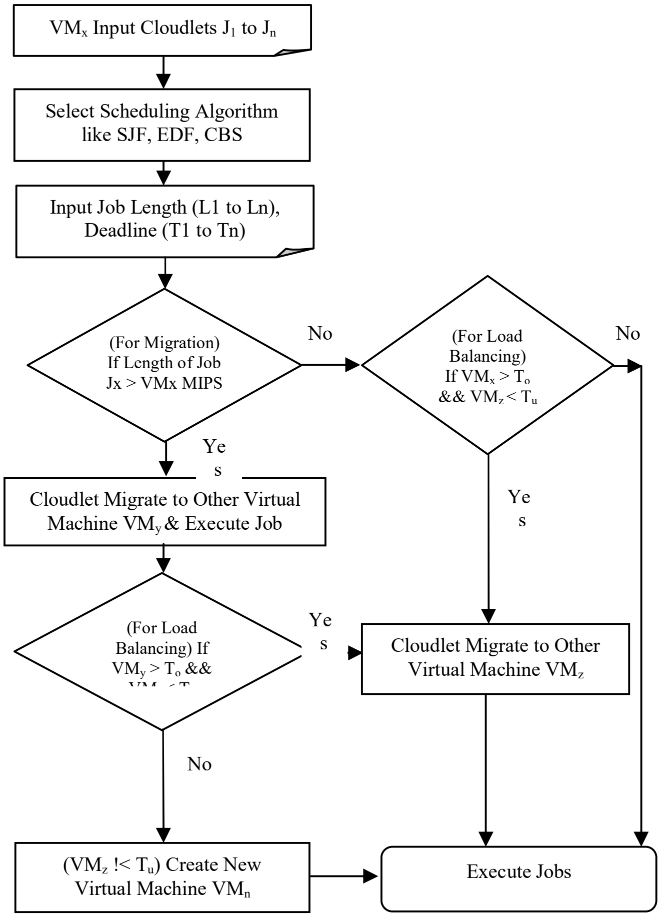
VM_x Input Cloudlets J_1 to J_n
Select Scheduling Algorithm like SJF, EDF, CBS
Input Job Length (L1 to Ln), Deadline (T1 to Tn)
(For Migration) If Length of Job Jx > VMx MIPS
No
(For Load Balancing) If $VM_x > T_o$ && $VM_z < T_u$
No
Ye s
Cloudlet Migrate to Other Virtual Machine VM_y & Execute Job
Ye s
(For Load Balancing) If $VM_y > T_o$ &&
Ye s
Cloudlet Migrate to Other Virtual Machine VM_z
No
(VM_z !< T_u) Create New Virtual Machine VM_n
Execute Jobs

Figure 3: Functionality of Virtual Machine Monitors

Step 4 - (For Migration) Check Length of Job Jx > VMx MIPS: The system offers three virtual machines by default of mips 200, 500, 1000. If the job demand of greater than 1000 comes then first it will show out of bound message then cloudlet migrates to other virtual machine VMy which can execute the given job.

In our propose method for proficient live migration getting inspired by optimized pre-copy approach we will alter optimized pre-copy approach by setting one parameter D (i.e. dirty page rate) value of D is derived by dirty pages divided by total number of pages. After getting value of D we will set one threshold value T.

D = Dirty pages / Total number of pages

After deciding both parameter value we will compare both D and T if value of dirty page rate (D) is larger than threshold value (T) (i.e. high dirty page rate) we will apply our optimized pre-copy approach and if D is less than T (i.e. low dirty page rate) we will apply basic pre-copy approach. So our new propose approach will work better for both high dirty page rate and low dirty page rate environment and then we will compress that entire data with RLC (Run Length Compression) algorithm so that overall migration time and downtime will get reduced to produce optimal results.

Step 5: (For Load Balancing) Check VMx > To && VMz < Tu, Also Check VMy > To && VMz < Tu

A load balancing method based on migration of preferred tasks among virtual machines in a cloud computing environment is presented here. The suggested dynamic load balancing algorithm avoid the under loaded virtual machines from quick overburdening instantaneous load balancing orders by centralized server to same under loaded virtual machines should not result into abrupt overburdening of such under loaded virtual machines.

Let TO be the threshold workload which helps in identifying whether a designated virtual machine is overloaded or not. Let TU be the threshold workload value which helps in identifying whether a designated virtual machine is under loaded or not.

VMx ≥ TO: Virtual machine VM deserves load balancing; but not available for load balancing requests. VMz ≤ TU: Virtual machine VM is available for load balancing requests.

```
Module loadBalanceCloud()
{
struct VM_Status VMO;
struct VM_Status VMU;
while(true)
{
VMO = null;
VMU = null;
identifyUnderLoadedVM(VMU);
if (not found VMU) then
continue;
identifyOverLoadedVM(VMO);
if (not found VMO) then
continue;
setVirtualMachineStatusPassive(VMU);
…
performLoadBalancing(VMO, VMU);
…
thread_ManageVirtualMachineStatus();
}
}
```

Definition of the data structure VM_Status is as follows:

```
struct VM_Status
{
int VM_ID;
char VM_IP[16];
int VM_STATUS;
float VM_LOAD[4];
…
}
```

Step 6- Creation of New Virtual Machine: If the job request is not balanced on any VMz due to absence of any under loaded virtual machine, then first it will show unavailability of virtual machine message then create new virtual machine VMn which can execute the given job.

Step 7- Execution of Cloudlets: After completing the above steps the cloudlets (job request) will be executed. In this way the system works.

6. CONCLUSION

Virtualization in cloud computing is provided in the form of a layered architecture. The goals and objectives of each layer are different. The virtualization layer and management layers are the two very important layers of the cloud computing architecture. In this study, we have observed that management layers have more scopes for future research. As this layer is concerned with the hypervisor interface, load distribution, security, validation engine, virtual jobs Scheduler, Internal and External Cloud API. Among these major objectives of the management layer, Load Distribution and Security are the two upcoming areas for the researchers. The proposed model illustrated the internal handling of the virtual jobs and load balancing on the virtual servers.

Appendix

Abbreviations	Full Form
CC	Cloud Computing
IT	Information Technology
VM	Virtual Machines
IDC	International Data Corporation
DoS	Denial of Service
API	Application Programming Interface
SLA	Service Level Agreement
OS	Operating System
CPU	Central Processing Unit
MDD	Migration with Data Duplication
RLE	Run Length Encoding

Acknowledgments

The authors are highly thankful for the people who are directly or indirectly supports for the preparation of this paper.

REFERENCES

[1] *Nalini Subramanian, Andrews Jeyaraj, "Recent security challenges in cloud computing", Journal of Computers and Electrical Engineering, vol. 71 (2018), pp. 28-42*

[2] *M. Ambika, Dr. Kolasani Ramchand H Rao, "A NOVEL FRAMEWORK FOR HYPERVISOR DESIGN", 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science, vol. 79 (2016), pp. 190 - 198*

[3] *Mousa Elrotub, Abdelouahed Gherbi, "Virtual Machine Classification-based Approach to Enhanced Workload Balancing for Cloud Computing Applications", The 9th International Conference on Ambient Systems, Networks and Technologies (ANT 2018), Procedia Computer Science, vol. 130 (2018), pp. 683-688*

[4] *Liang Wang, Hong Xia Zhang, "Performance Analysis and Massive Concurrent Access Response Test of Sichuan Top IT Vocational Institute Data Center Based on Virtualized Cloud Computing", 8th International Congress of Information and Communication Technology (ICICT-2018), Procedia Computer Science 131 (2018) 102-107*

[5] *Nagamani H Shahapure, P Jayarekha, "Distance and Traffic Based Virtual Machine Migration for Scalability in Cloud Computing", International Conference on Computational Intelligence and Data Science (ICCIDS 2018), Procedia Computer Science, vol. 132 (2018), pp. 728-737*

[6] *Hefei Jiaa, Xu Liua, Xiaoqiang Dia, Hui Qia, Ligang Conga, Jinqing Lia, Huamin Yanga, "Security Strategy for Virtual Machine Allocation in Cloud Computing", 2018 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2018, Procedia Computer Science, vol. 147 (2019), pp. 140-144*

[7] *Carlos Antunes, Ricardo Vardasca, "Performance of Jails versus Virtualization for Cloud Computing Solutions", CENTERIS 2014, Procedia Technology, vol. 16 (2014), pp. 649 - 658*

[8] *Jiyi WU, Lingdi PING, Xiaoping GE, Ya Wang, Jianqing FU, "Cloud Storage as the Infrastructure of Cloud Computing", 2010 International Conference on Intelligent Computing and Cognitive Informatics, IEEE Computer Society, ISBN : 978-0-7695-4014-6, pp. 380-383*

[9] *Manjeet Singh, "STUDY ON CLOUD COMPUTING AND CLOUD DATABASE", International Conference on Computing, Communication and Automation (ICCCA2015), ISBN:978-1-4799-8890-7, pp. 708-713*

[10] *Teófilo Branco Jr., Filipe de Sá-Soares, Alfonso Lopez Rivero, "Key Issues for the Successful Adoption of Cloud Computing", CENTERIS- 2017, Procedia Computer Science, vol. 121 (2017), pp. 115-122*

[11] *Farrukh Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", The 6th International Symposium on Applications of Ad hoc and Sensor Networks (AASNET'14), Procedia Computer Science, vol. 37 (2014), pp. 357 - 362*

[12] *Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017), Procedia Computer Science, vol. 110 (2017), pp. 465-472.*