Review on Resource Virtualization for Increasing Users Computing Power

[1] Radhika R. Nawabasi, [2] Dr. V. M. Thakre, [3] Dr. U. S. Junghare

[1] S. M. D. Bharti college, Arni, MS. India.

[2] SGB Amravati University, Amravati. MS. India.

[3] Brijlal Biyani Science College, Amravati. MS. India.

Abstract - The cloud computing is emerging need for the user's computing and storage. As the users uses different computing devices(mobile or fixed),they requires reliable, secure and fast computing technologies. This paper illustrates the use of the virtualized cloud resources for both the mobile and fixed user computing. The virtualization technique is used for providing the reliable and secure computing power of the different resources as network, desktop, processing, server etc.

Keywords - *Cloud computing, virtualization, mobile computing.*

1. Introduction

Cloud computing is a model which provides virtualized resources through the network to the user as per the user need. The client is charged as per the quality and quantity of use. The user can demand the resources from any location. Some of the computing resources are networks, sever, storage, applications and services.

The cloud computing provides the infrastructure, platform, and software as a service to the user. Cloud is classified as private, public, community and hybrid. A private cloud is owned by the single organization. A public cloud provides services to all the general people. Community cloud are organized by group of several organization of similar need and the hybrid cloud is the combination any of three clouds.[4]

Now days the use of mobile devices is increasing but their computing power are limited because of battery capacity, processing power. By providing the cloud services to the mobile users the computing power of the mobile devices can be extended. This is known as the mobile cloud computing (MCC). The virtualization technique is use to increase the resource availability and the flexibility to the mobile cloud.

In virtualization, the physical machine is partitioned into number of logical machines. The virtual machine monitor (VMM) manages all the VMs and allows them to share cloud resources[3].

Virtualization of different resources like display, desktop, network, platform, and server are done to increase processing time, resource utilization, battery capacity of thin clients and to reduce interaction delay and power consumption of the user devices.[1][5][6][7][8]

However, the virtualization leads to the poor network performance because of the burden on the virtualization layer. In MCC, some networking challenges are occurred like network reliability, low bandwidth, and high access latency. To overcome this problem a flexible architecture is proposed to improve the networking performance. [3]
There are some disadvantages of cloud structure as the maintaining confidential data, integrity, and availability of sensitive data. The security policies are not controlled at the cloud. Because the business information is exposed to the third parties, there is more risk to confidential data. The service providers must provide privileges to the access sensitive business data[9].

The cloud protection system (cps) is an architecture which provides the security to the cloud resources and the hypeSec is an architecture which controls the inter-communication between the virtual machines (VMs). The hypeSec is integrated in the hypervisor Qemu. Eucalyptus is the cloud system environment which can be protected by the cps system by using full virtualization[2].

2. Various Resource Virtualizations in Cloud

2.1. Display Virtualization

In mobile computing, the thin client devices provide only the GUI to the end-users, and the processing is done at the server. It uses remote display protocol to communicate client and server. The rendering of the screen is done at the server in the cloud and the image of display is send to the client, this is known as a virtualization of the display.[1]

2.2. Desktop Virtualization

In desktop virtualization system, the execution of OS and the application are done at the remote data centers instead of user's local system. The user only handles the attached hardware. Because of this the user system becomes a lightweight system device. In desktop virtualization system only the application window are send to the client not the whole desktop.[6]

2.3. Optical Network Virtualization

The cloud computing provides the Infrastructure as a service (IaaS) ,in which infrastructure of a cloud is provided to the users for user computing based on the pay as use. This required a very capacity network to connect to the user and the data centers to provide the flexibility, security, high capacity.

Our proposed architecture provides the high capacity connection between the end users (mobile users and fixed user) and the data centers by using heterogeneous network i.e. optical metro network and wireless network. The optical network technology provides the sub-wavelength switching granularity. And the wireless technology provide Long Term Evaluation (LTE) access network which supports end users mobility. The virtualization of technology domain is proposed in our architecture to provide quality of service. [8]

2.4. Platform Virtualization for Device Cloud

A device cloud or resource pool is created by decoupling of the hardware devices like display, input devices, disk or processor from their physical platform on which they resides. The stratus framework constructs the virtual platform by using device clouds and the network devices. The advantage of creating device cloud or VP is that all the devices in the cloud compose of different operating environment and application in terms of power consumption, processing speed, display size and presence of some accelerator. Then the particular device is chosen according to the user policies and the computation can be migrated to that device, so that the performance can be increased. The hypervisor controls all the devices and communication between those devices. This hypervisor is found on all the machines in the virtual platform. [5]

2.5. Multi-Tenant Virtualization

In The multi-tenant virtualization, the virtualization is software based. The unmodified Lamp applications can run flexibly and securely at the multi-tenant platform. The tremendous concurrent visualization environment is occurred in the multi-tenant virtualization. This can be done by sharing software or hardware platform. It can benefit in the isolation between instants. Multi-tenant platform is also referred as "Uranus". [7]

3. Techniques Used for Resource Virtualization

3.1. Advadams Architecture for Display Virtualization

Shridhar S. at.el. proposed The ADVADAMS architecture to minimize the delay in the interaction. In this architecture the display updates are calculated in advance. This model use push and pull methodology. In pull methodology, the client requests the server for the next display update. And in push methodology, server compute display updates in advance and sends to the client. At the server side, the server calculates all the possible states of the display based on the applications metadata. Then server computes the display updates and sent all the frames to the client. This frames or states are given priorities and numbers by predicating the next key press. The higher priority frames are buffered first at the client side.

In the non-prefetching scheme the interaction latency remain constant with respect to the increasing in interaction rate. Whereas in the prefetching scheme, the interaction latency increases as the interaction rate increases as shown in figure 1. If the bandwidth increases, the more number of frames can be pushed to the client. As well as if the buffer size is increased with the increased in the bandwidth, the rate of the frames pushed to the buffer also increases as shown in figure 2.

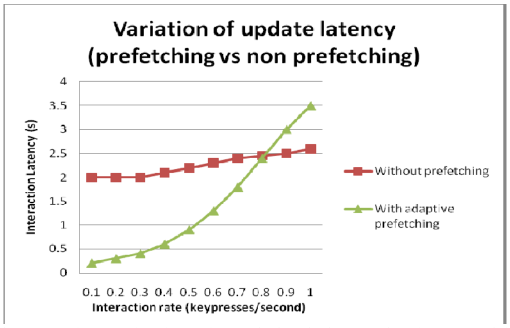

Figure1. The graphs show the variation in interaction latency with respect to the interaction rate.

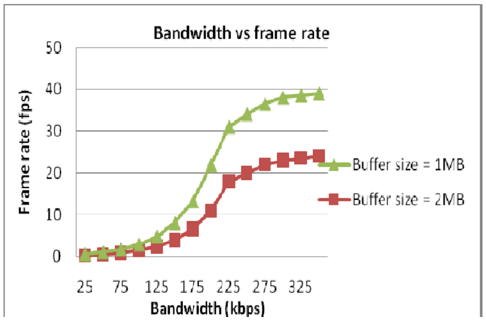

Figure2. Variation of frame rate in the client's display vs bandwidth for given buffer

3.2. Architecture for Desktop Virtualization

The architecture of desktop virtualization system consists of two layers. The first layer is application streaming layer which provides remote application to the client. And second is a resource management layer who manages the high computing capability servers at the remote. The remote order transmission (ROT) protocol is responsible for the interaction between these two layers.

The desktop transparentization technique is used to capture only the window information to the client. The Linux API at the server side removes the background information of the desktop and sends the requested application window to the client. The desktop transparentization method transfer the window information in the bitmap format (pixel data).hence the window cannot be resizing at the client desktop. To remove this drawback, a window monitor is used at both the server and client side. The window monitor detects the mouse event at the client, and sends to the server. Server does the same modification to the window and sends a new image to the client. The numbers of virtual machines are establishes on the physical server. And each virtual machine is assigned the application computing according to their availability.

3.2.1. Resource Management Modules

1. Daemon: It processes the client request. Following are the different type of the request.

Authorization: the access authorization is given to the user by identifying the user authorization.

Connect information: The connection information is stored for reconnecting the same data in future.

Application list: user can request list of application list that are that are accessible to that user.

Launching application: User requests the authorization for the application launching. Daemon sends the request to the VM manager.

Connection cancelation: user request for the connection termination.

2. VMmanager: it is responsible for managing the request from daemon and assign appropriate virtual machine to the application.

3. Scheduler: it schedules the VM to remove the burden on the VM.

4. DVMM: it manages the mapping between the virtual machines and the physical server.[6]

3.3 Architecture of Heterogeneous Network

3.3.1. Wireless Access and Backhauling Solution

The wireless domain is established by using heterogeneous topology comprises of LTE system. And the wireless microwave links are used to connect LTE-enabled base stations and the node edges on optical metro network. LTE's high data rate facilitates low packet transmission delay.

3.3.2. Optical Metro Network Solution

The optical metro network technology is a wave-length division multiplexed. It is also known as time shared optical network (TSON).

The TSON is implemented as frame-based, time multiplexing metro network solution. it provided the dynamic connectivity with high bandwidth granularity. The sub-wavelength bandwidth granularity provides the facilities like Fast time to service, QOS, and low end to end delay.

This architecture is based on the cross domain virtualization. In which both the IT resources and the optical network topology are virtualized. The aim of cross domain virtualization is to offer solution on energy consumption and the resource requirement. [8]

3.4. Stratus Framework

The stratus framework introduced by Minsung Jang at. el. composed of stratus master, stratus node, features, communication channels and policies.

Stratus master: it manages the construction and rejection of the virtual platform based on the user policies. it also manages the information about all stratus node connected to it.

Stratus node: it gives features to the VP. When nodes are register in the VP, they give their features to the master. Each node has given a unique identification (ID).

Management channel: the management channel is used to connect stratus node to the stratus master.

Event forwarding: to combine the features of from the different node event are forwarded from one node to another. This can be fulfilled by using management channel.

User policies: user policies are the features required by the users. The policies are sent to the master .the master finds available resources and if they are available master creates the VP.

3.4.1. Establishing Virtual Platform

Joining device cloud: the device is registered as a stratus node at the master and finds the available features in the cloud.

Creation of virtual platform: the user sends the policy to the master and then master create the virtual platform according to the required policy.

Termination of virtual platform: if user done with its work, the master terminates the VP by releasing the features allocated to the Platform. Normal termination is done by user request while abnormal termination is done because of power failure.

Leaving device cloud: it can be done by sending quit notification.

Stratus provide the high performance platform by providing the device availability and migrating user computing and by selecting the high processing power devises power consumption can be reduced. It enhances battery life of the device achieved by offloading computing to the long lasting battery devices.

3.5. Uranus Architecture

This architecture is proposed byBuddhikasiddhisena at. el. consists of two layers.

1. Reverse proxy layer: this layer handles the user http request .this layer is made up of number of apache servers. The server sends the user's http request to the virtualization layer. The servers are configured by using reverse proxy configuration. It is implemented by using apache modules as proxy, proxy connect and proxy-http. The user's http requests are cached at this layer in cache and mem_cache module of the apache server to increase the performance.

2. Virtualization layer: this layer consists of LAMP components, each of which consists of apache and MYSQL servers. Separate LAMP applications are deployed to each LAMP components. In the virtualization layer each tenant has its own system components but has only one home directory.

   This directory can be shared by their own apache and MYSQL processes. Each process shares the physical binary application file. The advantage of sharing physical file is that any changes to the file only required to change only one instance rather than at each individual VM. The only processes of the tenants are maintained at the home directory. All the other data are maintained separately. Because of this the multi-tenant provides the high security level by isolating data and the process.

A DNA layer is situated outside the Uranus, whose task is to find the domain name of the site to be virtualized in the virtualization layer.

1. Apache virtualization: Each apache process of the tenant run on its own port as a tenant user. Because of this each process are isolated from each other and can be customized according to the required resources and can priorities its CPU allocation.

2. MYSQL virtualization:in MYSQL each instances are released on the mysqld_multi tool.

3.6. Cloudlet Architecture

Cloudlets are the collection of virtualized servers which are co-located with the base station or the access point. The mobile devises offloads the computing to the cloudlets instead of public cloud to reduce the interaction delay, because the cloudlets are connected to the mobile devices by a single hop.

The number of mobile devices forms a cloud infrastructure. The mobile devices offload the computing to the nearby mobile devices instead of offloading to the public cloud. This is because the processing powers of mobile devices are increasing.

A client first sends the request. The provider selects the feasible cloud in terms of bandwidth, delay, processing speed. And offload the computing to that cloud by creating VM to the cloud. The task can be moved from one to another cloud by moving VM.

The packet classification mechanism and the weighted scheduling are used to improve interaction delay. As it is noticed that the packets arrives at the network device, the driver domain establish packet classification mechanism. Each VM maintains a queue. Each queue is serviced by a weighted round robin scheduling. The target machine where the packets are waiting has received the notification through a single event channel. And each VM's queue size is decided according to the priorities of the queue. [3]

4. Security Issues

In cloud computing, the computing recourses are made available to the client on their demand. It also provides the services to the client like Saas, PaaS and IaaS. The client does not need servers, storage, processing power at their side. All the processing and can be done at the cloud. Different deployment model are available for the cloud such as public, private, community and hybrid [4].

However, there are some disadvantages of cloud structure as the maintaining confidential data, integrity, and availability of sensitive data. The security policies are not controlled at the cloud. Because the business informationis exposed to the third parties, there is more risk to confidential data. The service providers must provide privileges to the access sensitive business data. [9]

4.1. Various Attacks Lead to The Malicious Use of Cloud Resources

1. Host hopping attacks: These types of attacks are caused by recourse sharing, if cloud providers do not isolate the resources like memory, servers, from each other. These are dangerous for public cloud and PaaS service models, where multiple client shares the same physical machine.
2. Malicious insiders and abuse of privileges. : Because of sharing and multi-tenancy nature of the resources, the insiders of the cloud such as the system administrator are responsible for the privilege abuse.
3. Identity theft attack: the hacker can make their accounts and can use the cloud resources. By using this they can create the fraud cloud and create the services as emails, then provide that services to the user. When client uses those services, the client is under the attack of hackers.
4. Service engine attack: the service engine is responsible for monitoring all the resources and the cloud structure and Iaas structure. The hackers can rent for the recourses from inside and abuse the use of resources and attack the service engine. [9]

5. Security through Virtualization

To provide the security to the cloud components and the virtual machine, the virtualization technique is used. The cloud protection system (cps) is an architecture which provides the security to the cloud resources. And the hypeSec is an architecture which controls the inter-communication between the virtual machines (VMs). The hypeSec is integrated in the hypervisor Qemu. Eucalyptus is the cloud system environment which can be protected by the cps system by using full virtualization.

5.1. Cloud Protection System (Cps)

In cps system, we provide the security to the cloud components by longing in and verifying checksum of cloud libraries and executable files periodically. The VMS are monitors by the host machine. We monitor the kernel of the virtual machine and the cloud components so that the any changes made to the kernel code and the data are detected. The green continues line represents the monitoring dataflow and the dashed red line represents the dangerous data flows. All the cps modules (the interceptor, warning recorder, warning queue, and evaluator) are located on the base machine. The interpreter notices any suspicious guest activity then it is recorded by the warning recorder into the warning queue. And then the threats are evaluated by the evaluator. If any changes are detected in the VM, the cps shut down the VM.

If any VM is affected by malicious code, all the remaining VMs are affected because all the VMs are collocated. Hence the hypeSec architecture is proposed to increase the security protection. The ACM module of the hypeSec controls the VMs communication. It controls the resources and the isolation of the VMs.ACM provides the authorization to access the VMs to the particular resources based on certain policy rules. Depending upon the rules ACM decides to allow the communication between the VMs or not. [2]

5.2. Attack Implementation

The attack is implemented by inserting the rootkit in to guest VM’s kernel. It changes in the syscall table values and the execution flow to execute the malicious code. The changes in checksum are identified by the cps and then the infected VM is powered off.

The cps is implemented on the eucalyptus cloud system. The eucalyptus consists of different components.

1. Node controller: it controls the execution, inspection and the termination of the VM instance on the host.
2. Cluster controller: it controls scheduling of the execution of VM on the particular node controller by collecting the information about the VM.
3. Storage controller: it controls the storing and the accessing of the VM image and the data.
4. Cloud controller: it makes high level scheduling decision[2].

6. Analysis

6.1. Advantages of Virtualization

1. The aim of cross domain virtualization is to offer solution on energy consumption and the resource requirement.
2. Stratus provide the high performance platform by providing the device availability and migrating user computing.
3. Reducing power consumption in device cloud: by selecting the high processing power devises power consumption can be reduced.
4. Enhance battery life of the device: This can be achieved by offloading computing to the long lasting battery devices.
5. Enabling VP mobility: the computing can be migrated from one VM to another for different features.
6. The multi-tenant virtualization provides the high security level by isolating data and the process.

7. In cps system, we provide the security to the cloud components by longing in and verifying checksum of cloud libraries and executable files periodically.

6.2. Disadvantages

1. Because the business information is exposed to the third parties, there is more risk to confidential data, maintaining confidential data, integrity and availability of sensitive data.
2. If any VM is affected by malicious code, all the remaining VMs are affected because all the VMs are collocated
3. In MCC, some networking challenges are occurred like network reliability, low bandwidth, and high access latency.

7. Conclusion

In this paper we see that the virtualization of different resources like display, desktop, network, platform and server are done to increase processing time, resource utilization, battery capacity of thin clients and to reduce interaction delay and power consumption of the user devices.

References

[1] ShridharS, SathishG, RajaG, SumalathaRamchadran, “Adaptive Display Virtualization And Dataflow Model Selection (ADVADAMS) for Reducing Interaction Latency in Thin Clients.”, 2012, IEEE.

[2] NiranjanaPadmanabhan, bijolin Edwin E, ”An Architecture for Providing Security to Cloud Resources”, In International conference on Emerging Technology Trends (ICETT),published by IJCA,2011.

[3] ManelBourguiba, KhaldounAl Agha, KamelHaddadou,”Improvingnetwork performance in virtual mobile clouds”.

[4] S. J. Mohana, M.Saroja,M.Venkatachalam,”Key infrastructure elements for cloud computing”,in International journal of computational engineering Research(ijceronline.com),volume2,issue 7,pageno:166-169,2012.

[5] Minsung Jang, Karsten Schwan,”STRATUS: Assembling virtual platforms from Device Clouds”, in IEEE 4thinternational conference on cloud computing, 2011, page no-476-483.

[6] Guangda Lai, HuaAong,Xiaola Lin, ”A Service Base lightweight Desktop Virtualization system” in International conference on service Science,2011.

[7] Buddhikasiddhisena,LakmalWarusawithana,Mithila Mendis.”Next Generation Multi-Tenant Virtualization Cloud Computing Platform”, in ICACT,13-16 feb,2011.page no.405-410.

[8] Anna Tazanakaki,MarkosP. Anastasopoulos, Georgios S. Zervas, BijanRahimzadehRofee, RezaNejabati, DimitraSimeonidou.”Virtualization of heterogeneouswireless-optical network and IT infrastructure in support of cloud and mobile cloud service. “, In IEEE communicating magazine, Aug 2013.

[9] Yasir Ahmed Hamaza, Marwan Dahar Omar, ”Cloud Computing Security: Abuse and Nefarious use of Cloud Computing.”, in International Journal of Computational engineering research,volume.03,Issue.6, June 2013.