

The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing

Ahmad Mateen
University of Agriculture
Faisalabad, 38000 Pakistan

Amir Waheed
University of Agriculture
Faisalabad, 38000 Pakistan

ABSTRACT

Cloud computing is a new trend which increase application ability in terms of functionality, resource management and collaborative aspect in term of distributed as well as centralized computing environment. Cloud computing system produce new disputes because of system clusters and high volume data generated by these systems. Storage virtualization makes stockpiling a ware. This makes for some intriguing courses for organizations to lessen their expenses. The central part of cloud computing is virtualization which enables industry or academic IT resources through on-demand allocation dynamically. The main importance in cloud computing is virtualization, which perform user requests on different logical machines in term of their execution in a predefined manner. Cloud computing is unquestionably conceivable without virtualization, however requires more work and time to really pull it off; by utilizing virtualization, it would be fundamentally getting a great deal of the work accomplished for nothing. The resources can be multiple networks in a client server environment having storage as well as applications. The main purpose of this research is how to increase resource management with virtualization which will improve the performance of cloud computing resource allocation its challenges and proposed new approach which will helpful to optimize the performance in sharing network infrastructure.

Keywords

Challenges, cloud computing, elasticity, hypervisor, virtualization

1. INTRODUCTION

Cloud computing alludes to a collective IT (Information Technology) environment, which is arranged with the aim of quantifiable and remotely providing versatile IT assets for powerful and productive usage. National Institute of Standards and Technology (NIST) has given a definition for Cloud figuring which says that —Cloud Computing is a model for empowering helpful, on-interest system access to a common pool of configurable registering assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with insignificant administration exertion or administration supplier interaction[1]. Five key qualities of distributed computing recorded by NIST are on-interest self-administration, wide system access, asset pooling, fast flexibility and measured administration. Portable distributed computing is the registering which alludes to at whatever time, anyplace openness to applications and information through web utilizing cell phones. Customary processing assets are put away in an individual gadget and got to by a verified client [2].In Cloud registering, asset are put away in brought together way and got toon interest premise [3]. As of late, cell phones and resulting versatile registering turn into a basic

segment in cloud registering [4]. Web made the potential outcomes of getting to applications and information from anyplace whenever [5]. As per Juniper research, the versatile clients and endeavor market for portable cloud based applications worth are relied upon to increment to \$9.5 billion by 2014[6]. Aepona portrays that MCC (Mobile Cloud Computing) as another worldview for versatile applications whereby the information preparing and capacity are moved from the cell phones to capable and brought together processing stages situated in mists. These concentrated applications are then gotten to over the remote association in view of a flimsy local customer or web program on the cell phones [7].

Virtualization is a procedure which permits to makes extract layer of framework assets and conceals the intricacy of equipment and programming working environment [8]. The virtualization gives equipment autonomy, separation of visitor working framework and embodiment of whole virtual machine gathered in a solitary document. Virtualization normally actualized with hypervisor innovation, which is a product or firmware components that can virtualizes framework assets [9]. The remaining a portion of this paper is framed as takes after: Section II gives a prologue to the distributed computing innovation. Area III presents different virtualization strategies in distributed computing environment. Segment IV depicts the sorts of virtualization. Difficulties and examination of open source based hypervisor models for cloud are clarified in area V. Segment V finishes up the paper [10].

1.1 Virtualization for Cloud

Virtualization innovation redirects the human's viewpoint for using IT assets from physical to sensible [11]. The objective of virtualization is to cooperatively use the IT assets, for example, stockpiling, processor and system to most extreme level and to lessen the expense of IT assets which can be accomplished by joining numerous unmoving assets into shared pools and making diverse virtual machines to perform different undertakings all the while[12]. The assets can be dispensed or adjusted powerfully. Client ought to be aware of fundamental strategies, for example, copying, hypervisor, full, para and equipment helped virtualization while utilizing virtualization as a part of distributed computing environment.

2. RELATED WORK

2.1 Virtual Machine Monitor or Hypervisor

A product layer that can screen and virtualize the assets of a host machine giving to the client prerequisites [13]. It is a middle of the road layer between working framework and equipment. Essentially, hypervisor is delegated local and facilitated [14]. The local construct hypervisor runs specifically with respect to the equipment though have construct hypervisor keeps running in light of the host

working framework. The product layer makes virtual assets, for example, CPU, memory, stockpiling and drivers.

2.2 Emulation

It is a virtualization procedure which changes over the conduct of the PC equipment to a product program and lies in the working framework layer which lies on the equipment. Imitating gives tremendous adaptability to visitor working framework yet the rate of interpretation procedure is low contrasted with hypervisor and requires a high design of equipment assets to run the product [15].

2.3 Full Virtualization

Hypervisor makes confined environment between the visitor or virtual server and the host or server equipment. Working frameworks specifically get to the equipment controllers and its fringe gadgets without perceptive of virtualized environment and prerequisite alterations [16].

2.4 Para Virtualization

This strategy gives unique hypercalls that substitutes the direction set design of host machine. It relates correspondence in the middle of hypervisor and visitor working framework to enhance effectiveness and execution. Getting to assets in para virtualization is superior to the full virtualization model since all assets must be copied in full virtualization model [17]. The downside of this procedure is to adjust the piece of visitor working framework utilizing hypercalls. This model is just suitable with open source working frameworks.

2.5 Data Leakage

Organizations are in high risk of data leakage when an employee secures the access to its data stored in cloud system. Data leakages are happens through hacking data location, securing remote access, third party storage and unsecure multitenant environment in hypervisor level [18]. Cloud provider or broker can enhance the prevention and detection mechanism and implement the collaborative security policy in hypervisor level to protect data from data

3. PROPOSED WORK

3.1 Client Virtualization

This customer virtualization innovation makes the framework overseer to for all intents and purposes screen and redesign the customer machines like workstation desktop, portable PC and cell phones. It enhances the customer machines administration and upgrades the security to guard from programmers and cybercriminals. There are three sorts of customer virtualization [19]. In the first place, remote or server facilitated virtualization which is facilitated on a server machine and worked by the customer over a system. Second, nearby or customer facilitated virtualization in which the secured and virtualized working environment keeps running on neighborhood machine. Third, application virtualization that gives different approaches to run an application which is not in customary way [20]. In this procedure a disconnected virtualized environment or apportioning method is utilized to run an application.

3.2 Server Virtualization

Single server performs the undertaking of numerous servers by assigning out the assets of an individual server crosswise over multi-environment. The hypervisor layer takes into account facilitating numerous applications and working frameworks locally or remotely. The upsides of virtualization incorporate cost reserve funds, lower capital costs, high accessibility and productive utilization of assets.

3.3 Storage Virtualization

It makes the reflection of coherent stockpiling from physical stockpiling. Three sorts of information stockpiling are utilized as a part of virtualization, they are DAS (Direct Attached Storage), NAS (Network Attached Storage) and SAN (Storage Area Network).

DAS is the customary technique for information stockpiling where capacity drives are specifically joined to server machine. NAS is the common stockpiling system which interfaces through system. The NAS is utilized for document

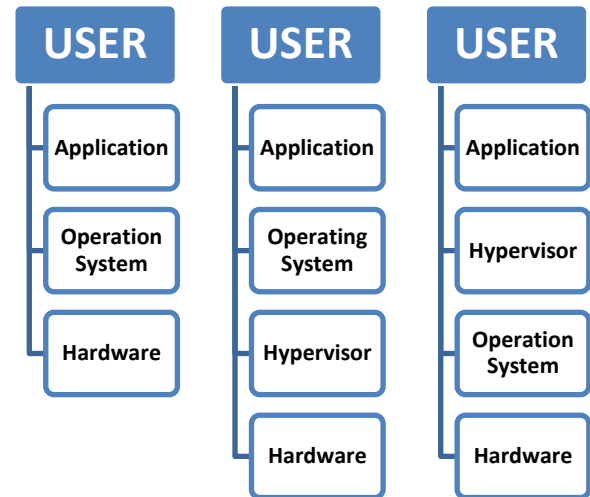


Fig 1 Traditional Model Vs Bare Model Vs Hosted Model

Sharing, gadget sharing and reinforcement putting away among machines. SAN is a capacity gadget that are imparted to various server over a high quicken system. Hypervisor is the product bundle that controls working access to the physical equipment of host machine. There are two sorts of hypervisor models as facilitated and uncovered metal/local. Facilitated hypervisor example works on top of the host working framework though uncovered metal construct hypervisor works specifically in light of the equipment of host machine. Fig 1 demonstrates the examination between customary, exposed metal and facilitated models.

3.4 Virtualization Security Threats

Security threats in virtualization are classified into virtual machine threat, hypervisor threat, virtual infrastructure and virtual network threat. The virtual machine threat surfaces while processing status of virtual machine, software updates, resource contention, patching and virtual machine conurbation [21]. Hypervisor threat rivets Virtual-Machine-Based Rootkit (VMBR) attack and Blue Pill Attack where hypervisor plays the vital role of Virtualization. Virtual infrastructure threats are concerted on physical access threat and single point of control threat. Virtual network threats can be effectively addressed by the security tools of intrusion detection, prevention mechanism, virtual switches and networks conferring to the requirements.

3.5 Data Remanence issue

Once the life time of data is used, then it will be deleted in secure manner and cannot be recovered by malicious users. In traditional manner, company has all control of their servers which can be overwrite the used data. But in cloud, the end user/cloud users are not given secure delete access to the cloud provider physical device. Cloud provider should focus to ensure no data will be recovered by any malicious users.

3.6 Virtualization Structure

Three major types of virtualization such as Server virtualization, Client virtualization and Storage virtualization. The architecture and categorization of virtualization techniques are illustrated in Fig 2.

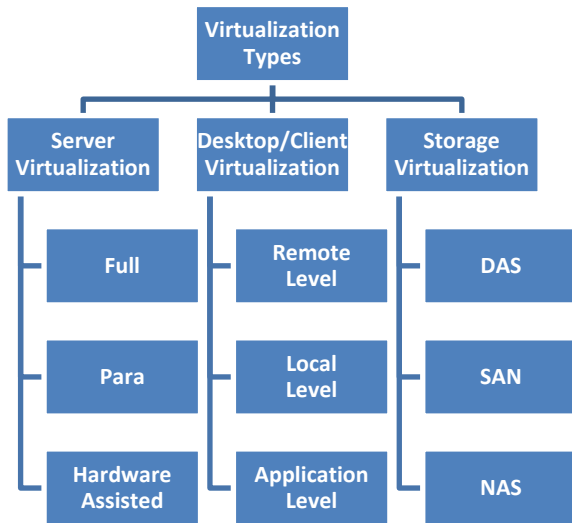


Fig 2 Virtualization Types

3.7 Privacy

Privacy becomes a major concern among cloud users' data which is stored in the data center of cloud service providers physically located in different places. In cloud, there are some circumstances which lead to the privacy threats. First, the storage issues that surface when user store data in multiple storage locations which are hidden from the user and have the possibilities of transferring data without owner's permission. Second major concern is to ensure the destruction time policy among cloud provider, broker and user once the data reach their expiration period. Third concern is data breaches which studies on how data breaches occur and who are going to take responsibility if data breach occurs in cloud. When a user opt for using cloud services, the user should read the terms and conditions thoroughly before prompt to cloud. The fourth concern is on regular auditing and monitoring policies. Cloud clients should constantly monitor / audit the activities of cloud service provider to ensure their stakeholder personal information will not be leaked while cloud resources are sharing with others.

3.8 Elastic Resource Management

Distributed computing framework create new question in view of framework bunches and high volume information produced by these frameworks [22]. With a specific end goal to work powerful versatile asset administration, there have to take a gander at the issues, for example, asset designation, asset provisioning, asset mapping and asset adjustment Cloud administrations experience issues on the prerequisites of administration level flexibility and accessibility. The elite of cloud can be accomplished through executing viable versatile asset administration systems therefore client could get effective administrations from administration suppliers.

3.9 SIGAR

When SIGAR object class is added in hypervisor environment which is very effective in processor load balancing, effectively maintain the platform specific state as well as caching level of different machines. The API also helpful for

route selection of networks, file system information and established protocol connection between network devices.

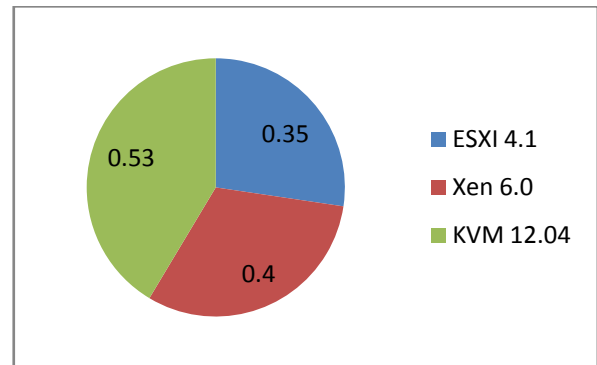


Fig 3. Utilization of CPU by using SIGAR

When CPU utilization is checked in different hypervisor as shown in figure 3 CPU utilization of ESXI4.1, Xen6.0 and KVM-Ubuntu 12.04 by using SIGAR method and the utilization of ESXI 4.1 is better then other because in this method lower value is better as mention above.

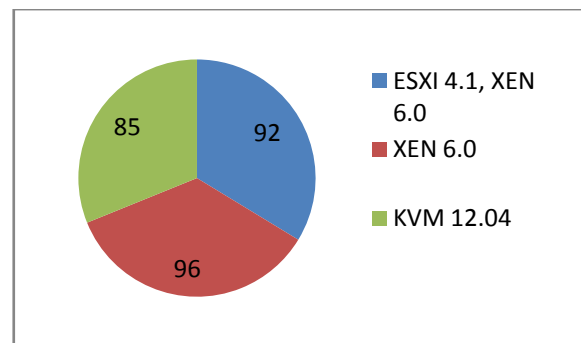


Fig. 3. Available Memory captured using SIGAR

In Fig.3 memory availability of ESXI4.1, Xen6.0 and KVM-Ubuntu 12.04 by using SIGAR method and the memory availability of Xen 6.0 is better then other because in this method higher value is better as mention above.

3.10 PASSMARK

In figure 4 the results of benchmark are shown for the Disk I/o read pass mark creates tests. In the private cloud environment two tests that are Progressive Read and Sequential Write are used that are coordinate on the three hypervisor. Both Xen Server and ES Xi perform skirting on identical to neighborhood execution. In Sequential Read and Sequential Write Xen Server barely shows favored execution over that of VM Ware ES Xi Server. When all is said in done circle mark execution Xen Server exhibits 2.7% overhead versus Neighborhood while ES Xi shows 3.4% overhead versus nearby. KVM inside and out falls behind other two hypervisors and nearby too.

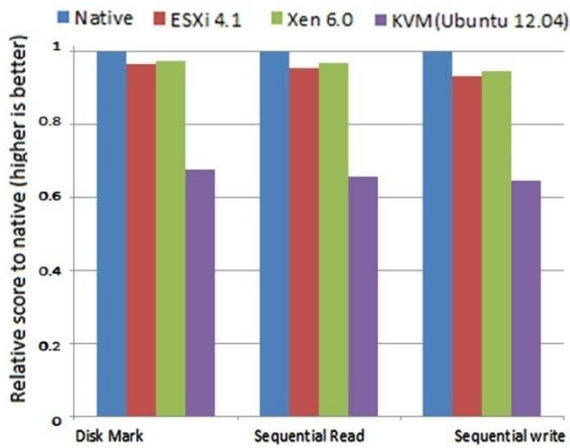


Fig. 4. Pass mark result of Disk Read Write vs native

The ESXi server shows not better yet performance as compared to Xen server. In this sequential read and sequential write mechanism, ESXi interposes 3% transparency vs native whereas Xen-server interposes 2.5% transparency vs native in this overall disk mark performance.

3.11 NETPERF

In this research, we measure the performance of different types of network by using netperf benchmark. In netperf, TCP_stream test is the default test. The quality data is transferred from system running netperf to system running server. Netperf TCP stream test is basically used for all results. Fig. 5 shows the Netperf results for send and get tests. Xen Server and ESXi displayed close nearby execution in Netperf test, while KVM lags.

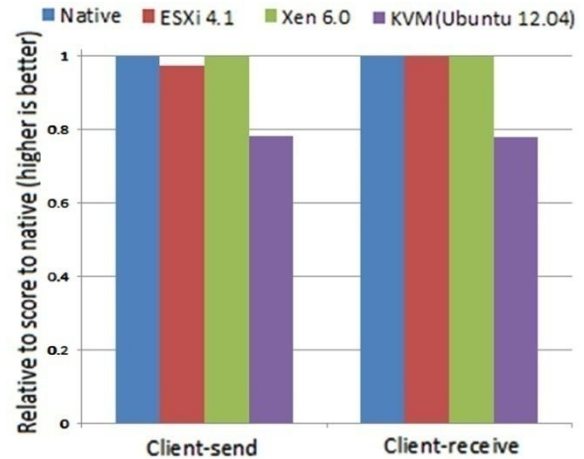


Fig 5 show the compared results of Netperf to native

The results of Netperf for send and receive tests are shown in figure 5. Xen Server and ESXi demonstrate in close proximity to indigenous performance in netperf tests, while KVM lags and other hypervisors are behind indigenous. Table 1 explains the virtualization strategies from open source suppliers like Redhat, Citrix frameworks, Oracle, OpenVZ, Linux-vserver and Proxmox. Below tabular information explains diverse hypervisor models and distinctive virtualization systems. As it would be talked about in before areas, virtualization is the idea of making virtual assets from physical assets, for example, working frameworks, system and capacity parts.

Table 1. Comparison of open source based hypervisor virtualization types

S. No	Hypervisor Name	Company	Hypervisor Model	Virtualization Types			
				Full	Para	Hardware assisted	Operating system
1	KVM	Red Hat	Hosted	Yes	No	No	No
2	XEN	Citrix systems, inc.	Bare Metal	No	Yes	Yes	No
3	VirtualBox	Oracle	Hosted	No	Yes	Yes	No
4	OpenVZ Linux	OpenVZ	Hosted	No	No	No	Yes
5	Linux-Vserver	Linux-Vserver	Hosted	No	No	No	Yes
6	Proxmox VE	Proxmox	Bare Metal	Yes	No	No	Yes

4. RESULTS

Consequences of Execution Demonstrate that the convincingly of Xen Server and ESXi Server perform equivalently well in all examinations close adjacent execution without suggesting at the any virtualization overhead next to KVM. Overdues other two hypervisors and Neighborhood in addition. In the test of CPU ESXi CPU use is 0.07% not as much as that of Xen Server and 0.25% not as much as that of KVM along these lines demonstrating better execution in CPU use. In the tested memory of Xen Server open memory is one percent higher than that of ESXi Server and six percent greater than in KVM so this way demonstrating better memory execution among different hypervisors.

5. CONCLUSION AND FUTURE WORK

This paper discussed various virtualization techniques, virtualization types, hypervisor techniques and challenges in cloud computing system to reduce IT costs and effective utilization of cloud resources such as rapid elastic provisioning of virtual machines, elastic application programming model. In addition, the virtualization techniques

get universal support when users consider elastic resource management issues and security issues before moving into cloud. This study discussed various issues pertaining to cloud services which can be used to design strong framework for effective elastic resource management in cloud. In future, the aim of this research is to develop new policies, framework and techniques to maintain elastic resources and data availability as a result the performances of cloud services could step into next higher level.

6. REFERENCES

- [1] Bhuvnesh P., T.Sharma, S.Jarged, 2016. "Virtualization Techniques In Cloud Computing", *Imperial Journal of Interdisciplinary Research* 5(2): 2454-136.
- [2] Almond C, 2013. "A Practical Guide to Cloud Computing Security", Black Hat conference, 15(6): 213-765.
- [3] Asma, L., A. Haji, M. Jebalia, S. Tabbane, 2010. State of the Art and Research Challenges of new services architecture technologies: Virtualization, SOA and Cloud

- Computing]. *International Journal of Grid and Distributed Computing* 3(4): 69-88.
- [4] Barham, P., B. Dragovic, K Fraser, S Hand, T Harris, 2012. Xen and the art of virtualization in operating systems principles, ", *International Journal of Engineering Research & Innovation*, 10(3):164–177
- [5] Dragovic, B., P. Barham, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, 2012. Xen and the art of virtualization]. In *SOSP '03: Proceedings of the nineteenth ACM symposium on operating systems principles*, 8(2) :164–177.
- [6] Dawoud, W., I. Takouna, and C. Meinel, 2010. Infrastructure as a service security: Challenges and solutions]. in *Proc. Informatics and Systems (INFOS), The 7th International Conference*, 16(5): 1–8.
- [7] Dell, "Overcoming 7 Key Challenges to Virtualization", <http://www.dell.com/downloads/global/power/pslq09-50o9o198-F5.pdf>, 2013.
- [8] Feldhaus, F., S. Freitag and C. El Amrani, 2011. "Large-Scale Computing Techniques for Complex System Simulations", *Wiley-IEEE Computer Society*, 23(8): 21-56.
- [9] IBM Virtual Infrastructure Access Service Product. <https://www-935.ibm.com/services/au/gts/pdf/endo3oo5usen.pdf>.
- [10] Jorjien, X., Z. Xiao and Y. Xiao, 2013. Security and Privacy in Cloud Computing]. *IEEE Communications Surveys & Tutorials*, 15(2): 843–859.
- [11] Kim, S., F. Machida, and K. S. Trivedi, 2012. "Availability Modeling and Analysis of a Virtualized System," in *Proceedings of the 15th IEEE Pacific Rim International Symposium on Dependable Computing*, 15(2): 365–371.
- [12] Mell, P., T. Grance, 2011. The NIST Definition of Cloud Computing]. National Institute of Standards and Technology, Information Technology Laboratory, 12(4): 324-456.
- [13] Qian, H., D. Medhi, and K. Trivedi, 2011. "A Hierarchical Model to Evaluate Quality of Experience of Online Services hosted by Cloud Computing," 5(3): 1–8
- [14] Rutkowska, J., 2010. "Subverting Vista Kernel for Fun and Profit", *Black Hat conference*, 16(5): 76-234.
- [15] Perez, S., 2014. Mobile cloud computing: \$9.5 billion by 2014]. <http://exoplanet.eu/catalog.php>.
- [16] Scarfone, K., M. Souppaya, and P. Hoffman, 2011. Guide to Security for Full Virtualization Technologies]. *National Institute of Standards and Technology*, 18(8): 800-125.
- [17] Siddhisena, B., L. Wruasawithana, M. Mendis, 2011. Next generation multitenant virtualization cloud computing platform]. In: *Proceedings of 13th International conference on advanced communication technology*, 12(3): 405–10.
- [18] Sun, Y., H. Yan, C. Lu, R. Bie, Z. Zhou, 2014. Constructing the web of events from raw data in the web of things. *Mobile InfSyst* 10(1): 105–125.
- [19] Tim, M., S. Kumaraswamy, S. Latif, 2011. Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance]. *International Journal of Engineering Research & Innovation*, 10(3): 164–177.
- [20] Timur, M., B. Yang, 2010. "Securing Virtualized Datacenters", *International Journal of Engineering Research & Innovation*, 2(1): 43-76.
- [21] Urgaonkar, B., P. Shenoy, A. Chandra, P. Goyal, T. Wood, 2010. Agile dynamic provisioning of multi-tier Internet applications, *ACM Trans Auton Adaptive Syst* 5(5): 139–48.
- [22] Ashwini, K., V.R. Wadhankar, 2011 "Security Enhancement for Privacy Preservation in Cloud Computing by Anonymous Request Access" *International Journal of Engineering Research & Innovation*, 4(1): 139-142.