A Study On Virtualization Techniques And Challenges In Cloud Computing

Durairaj. M, Kannan.P

Abstract: Cloud computing is a modern technology that increase application potentialities in terms of functioning, elastic resource management and collaborative execution approach. The central part of cloud computing is virtualization which enables industry or academic IT resources through on-demand allocation dynamically. The resources have different forms such as network, server, storage, application and client. This paper focus as on how virtualization helps to improve elasticity of the resources in cloud computing environment. In addition to, this paper gives a detailed review on open source virtualization techniques, challenges and future research direction.

Index Terms: challenges, cloud computing, elasticity, hypervisor, virtualization.

1 Introduction

Cloud computing refers to a collaborative IT (Information Technology) environment, which is planned with the intention of measurable and remotely purveying scalable IT resources for effective and efficient utilization. National Institute of Standards and Technology (NIST) has given a definition [1] for Cloud computing which says that “Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Five essential characteristics of cloud computing listed by NIST are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Mobile cloud computing is the computing which refers to anytime, anywhere accessibility to applications and data through internet using mobile devices. Traditional computing resources are stored in an individual device and accessed by an authenticated user. In Cloud computing, resource are stored in centralized manner and accessed on demand basis. In recent days, mobile devices and subsequent mobile computing become an imperative component in cloud computing. Internet made the possibilities of accessing applications and data from anywhere at any time. According to Juniper research [2], the mobile users and enterprise market for mobile cloud based applications worth are expected to increase to $9.5 billion by 2014. Aepona [3] describes that MCC (Mobile Cloud Computing) as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile devices to powerful and centralized computing platforms located in clouds. These centralized applications are then accessed over the wireless connection based on a thin native client or web browser on the mobile devices.

Virtualization [4] [5] [6] [7] is a technique which allows to creates abstract layer of system resources and hides the complexity of hardware and software working environment. The virtualization provides hardware independence, isolation of guest operating system and encapsulation of entire virtual machine grouped in a single file. Virtualization commonly implemented with hypervisor [8] [9] technology, which is a software or firmware elements that can virtualizes system resources. The remaining part of this paper is formed as follows: Section II gives an introduction to the cloud computing technology. Section III presents various virtualization techniques in cloud computing environment. Section IV describes the types of virtualization. Challenges and analysis of open source based hypervisor models for cloud are explained in section V. Section V concludes the paper.

2 Virtualization for Cloud

Virtualization [10] [11] technology diverts the human’s perspective for utilizing IT resources from physical to logical. The goal of virtualization is to collaboratively utilize the IT resources such as storage, processor and network to maximum level and to reduce the cost of IT resources which can be achieved by combining multiple idle resources into shared pools and creating different virtual machines to perform various tasks simultaneously. The resources can be allocated or altered dynamically. User should be conscious of basic techniques such as emulation, hypervisor, full, para and hardware assisted virtualization while using virtualization in cloud computing environment.

Emulation: It is a virtualization technique which converts the behavior of the computer hardware to a software program and lies in the operating system layer which lies on the hardware. Emulation provides enormous flexibility to guest operating system but the speed of translation process is low compared to hypervisor and requires a high configuration of hardware resources to run the software [12].

Virtual Machine Monitor or Hypervisor: A software layer that can monitor and virtualize the resources of a host machine conferring to the user requirements [13]. It is an intermediate layer between operating system and hardware. Basically, hypervisor is classified as native and hosted [14]. The native based hypervisor runs directly on the hardware whereas host based hypervisor runs on the host operating

- *Assistant Professor, School of Computer Science, Engineering and Applications, Bharathidasan University, India. Email: durairaj.bdu@gmail.com*
- *Research Scholar, School of Computer Science, Engineering and Applications, Bharathidasan University, India. Email: kannancsbdu@gmail.com*

system. The software layer creates virtual resources such as CPU, memory, storage and drivers.

Para Virtualization: This technique provides special hypercalls that substitutes the instruction set architecture of host machine. It relates communication between hypervisor and guest operating system to improve efficiency and performance. Accessing resources in para virtualization [15] is better than the full virtualization model since all resources must be emulated in full virtualization model. The drawback of this technique is to modify the kernel of guest operating system using hypercalls. This model is only suitable with open source operating systems.

Full Virtualization: Hypervisor creates isolated environment between the guest or virtual server and the host or server hardware. Operating systems directly access the hardware controllers and its peripheral devices without cognizant of virtualized environment and requirement modifications [16].

3 VIRTUALIZATION TYPES

There are 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 1.

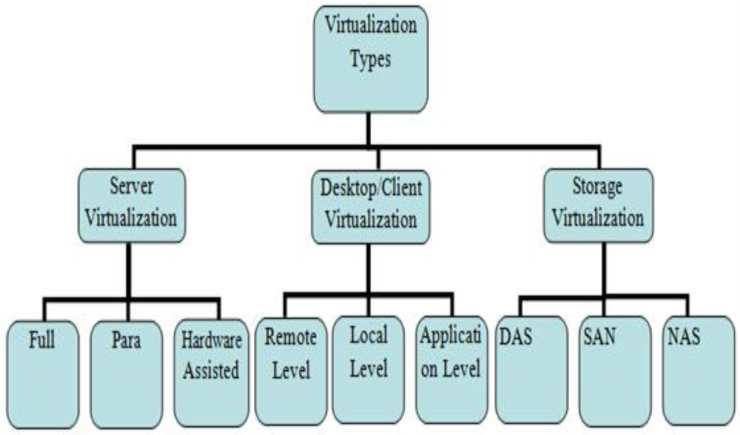

Fig 1 Virtualization types

Server Virtualization: In server virtualization, single server performs the task of multiple servers by portioning out the resources of an individual server across multi-environment. The hypervisor layer allows for hosting multiple applications and operating systems locally or remotely. The advantages of virtualization include cost savings, lower capital expenses, high availability and efficient use of resources.

Client Virtualization: This client virtualization technology makes the system administrator to virtually monitor and update the client machines like workstation desktop, laptop and mobile devices. It improves the client machines management and enhances the security to defend from hackers and cybercriminals. There are three types of client virtualization [17]. First, remote or server hosted virtualization which is hosted on a server machine and operated by the client across a network. Second, local or client hosted virtualization in which the secured and virtualized operating environment runs on local machine. Third, application virtualization [18] that provides multiple ways to run an application which is not in traditional manner. In this technique an isolated virtualized environment or partitioning technique is used to run an application.

Storage Virtualization: It creates the abstraction of logical storage from physical storage. Three kinds of data storage are used in virtualization, they are DAS (Direct Attached Storage), NAS (Network Attached Storage) and SAN (Storage Area Network). DAS is the conventional method of data storage where storage drives are directly attached to server machine. NAS is the shared storage mechanism which connects through network. The NAS is used for file sharing, device sharing and backup storing among machines. SAN is a storage device that are shared with different server over a high accelerate network. Hypervisor is the software package that controls working access to the physical hardware of host machine. There are two kinds of hypervisor models as hosted and bare metal / native. Hosted hypervisor instance operates on top of the host operating system whereas bare metal based hypervisor operates directly on the hardware of host machine. Fig 2 shows the comparison between traditional, bare metal and hosted models.

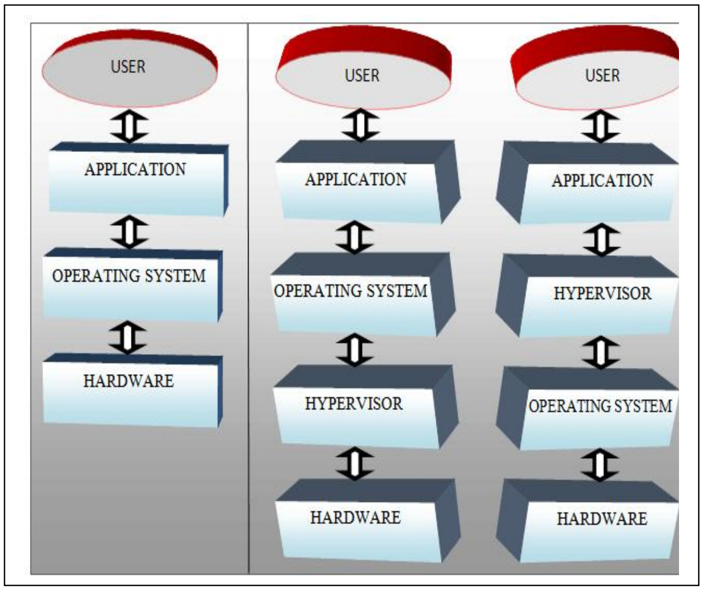

Fig 2 Traditional Model Vs Bare Model Vs Hosted Model

Majority of obstacles arises in the acceptance and development of virtualization and cloud computing are concerned to the basic management aspects such as data leakage, virtualization security threats, data remanense issue, privacy and elastic resource management.

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 [19] are happens through hacking data location, securing remote access, third party storage and unsecure multitenant environment in hypervisor level. 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 leakage.

Virtualization Security Threats: Security threats [20] 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. Hypervisor threat rivets Virtual-Machine-Based Rootkit (VMBR) attack and Blue Pill Attack [21] 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.

Data Remanence issue [22]: 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.

Privacy: Privacy [23] 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.

Elastic Resource Management: Cloud computing system produce new disputes because of system clusters and high volume data generated by these systems. In order to work effective elastic resource management, we need to look at the issues such as resource allocation, resource provisioning, resource mapping and resource adaptation [24][25][26][27]. Cloud services encounter issues on the requirements of service level elasticity and availability. The high performance of cloud can be achieved through implementing effective elastic resource management techniques as a result user could get efficient services from service providers. Table 1 represents the virtualization techniques from open source providers like Redhat, Citrix systems, Oracle, OpenVZ, Linux-vserver and Proxmox. In the table, we compare different hypervisor models with different virtualization techniques. As we discussed in earlier sections, virtualization is the concept of creating virtual resources from physical resources such as operating systems, network and storage components.

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

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. In future, we aim to develop new policies, framework and techniques to maintain elastic resources and data availability, as a result, the performances of cloud services could steps into next higher level. This study paper discussed various issues pertaining to cloud services which can be used to design strong framework for effective elastic resource management in cloud.

References

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Version 15, 2009.

[2] S. Perez, "Mobile cloud computing: $9.5 billion by 2014", http://exoplanet.eu/catalog.php, 2010.

[3] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.

[4] B. Loganayagi, S. Sujatha, "Creating virtual platform for cloud computing", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC 2010), 28-29 Dec. 2010, pp.1-4.

[5] Dawei Sun, Guiran Chang, Qiang Guo, Chuan Wang, Xingwei Wang., "A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques", First International Conference on Pervasive Computing, Signal Processing and Applications (PCSPA); 2010, pp.305-310.

[6] Karen Scarfone, Murugiah Souppaya, and Paul Hoffman, "Guide to Security for Full Virtualization Technologies", Special Publication 800-125, National Institute of Standards and Technology (NIST), 2011.

[7] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield, "Xen and the art of virtualization", in: Proc. 19th ACM Symposium on Operating Systems Principles, SOSP 2003, Bolton Landing, USA, Oct. 2003.

[8] Joanna Rutkowska and Alexander Tereshkin, "Bluepilling the Xen Hypervisor", Xen 0wning Trilogy part III, Black Hat USA, aug 2008.

[9] Samuel T. King, Peter M. Chen, Yi min Wang, Chad Verbowski, Helen J. Wang, and Jacob R. Lorch, "Subvirt: Implementing Malware with Virtual Machines", In IEEE Symposium on Security and Privacy, 2006.

[10] Z. Pan, Q. He, W. Jiang, Y. Chen, and Y. Dong, "Nestcloud: Towards practical nested virtualization," in Proc. Int Cloud and Service Computing (CSC) Conf, 2011, pp. 321–329.

[11] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions", in Proc. Informatics and Systems (INFOS), 2010 The 7th International Conference on, 2010, pp. 1 –8.

[12] Calheiros RN, Buyya R, De Rose CAF, "Building an automated and self-configurable emulation testbed for grid applications", Software: Practice and Experience, April 2010; Vol. 40(5), Pp. 405–429.

[13] A. Whitaker, M. Shaw, S. D. Gribble, "Denali: Lightweight virtual machines for distributed and networked applications", Tech. rep. (Feb. 08 2002).

[14] IBM, "IBM systems virtualization", version 2 release 1, http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/eicay/eicay.pdf (2005).

[15] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization", In SOSP '03: Proceedings of the nineteenth ACM symposium on operating systems principles (New York, NY, USA, 2003), ACM Press, pp. 164–177.

[16] Asma ben letaifa, Amed haji, Maha Jebalia, Sami Tabbane, "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), December 2010, 69-88.

[17] IBM Virtual Infrastructure Access Service Product. https://www-935.ibm.com/services/au/gts/pdf/end03005usen.pdf.

[18] B. Siddhisena, Lakmal Wruasawithana, Mithila Mendis, "Next generation muti tenant virtualization cloud computing platform", In: Proceedings of 13th International conference on advanced communication technology(ICACT), vol. 12, no.3; 2011. p.405–10.

[19] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009.

[20] Timur Mirzoev, Baijian Yang, "Securing Virtualized Datacenters", International Journal of Engineering Research & Innovation, vol. 2, no. 1, spring 2010.

[21] J. Rutkowska, "Subverting Vista Kernel For Fun and Profit", Aug 2006, Black Hat conference. http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf.

[22] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)", O'Reilly Media, Sep.2009; ISBN: 9780596802769.http://oreilly.com/catalog/9780596802776

[23] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[24] Sunilkumar S.Manvi, Gopal Krishna Shyam, "Resource anagement for Infrastructure as a Service(IaaS) in cloud computing: A survey", Journal of Network and Computer Applications 41, (2014) 424–440.

[25] Chase JS, Darrell C Anderson, Prachi N Thakar, Amin M Vahdat, "Managing energy and server resources in hosting centers", In: Proceedings of 11th IEEE/ACM international conference on grid computing (GRID), vol.12, no.4; 2010. p.50–2.

[26] B. Urgaonkar, P. Shenoy, A. Chandra, P. Goyal, T. Wood, "Agile dynamic provisioning of multi-tier Internet applications", ACM Trans Auton Adaptive Syst 2010; 5 (5):139–48.

[27] Vaquero LM, Luis Rodero-Merino, Rajkumar Buyya, "Dynamically scaling applications in the cloud", In: Proceedings of the ACM SIGCOMM computer communication review, vol.41, no.1; 2011. p.45–52.