RESEARCH ARTICLE OPEN ACCESS

Virtualization for Cloud Computing: A Perspective View

Suman Pandey
Alambagh, Lucknow
India

ABSTRACT

Cloud computing is hottest area of research in these days which goes in parallel with one more important concept of virtualization technology in distributed operating environment. Cloud computing has increased application potential by enlarged set of its functionality, efficient resource management and collaborative execution approach and virtualization helps to improve elasticity of the resources in distributed and cloud computing environment. Thus virtualization is enabling technology of cloud computing which facilitates clients to access to IT resources such as server, network, storage, application as per demand of user.

Cloud computing and virtualization both together have carefully carved a niche in the world of business and IT. With better service provisioning prospects of these two technologies it is easy to predict that these two will continue to revolutionize and transform in future.

This paper presents a comprehensive study of virtualization, techniques of creating virtualization and also discusses issues, challenges and privacy concerns raised due to virtualization for cloud computing. This work also identifies virtualization vulnerabilities known as security threats and attacks. The aim of this work is to review the work to identify future research directions that certainly help science and engineering community.

Keywords:- challenges, cloud computing, elasticity, hypervisor, virtualization.

I. INTRODUCTION

Cloud computing is a technology which allows users to access large reserve of dataset, information and several other resources as per their needs and pays for it according. Virtualization is main building block or enabling technology of distributed and cloud computing. A virtual machine facilitates to improve the efficiency of service provisioning of cloud computing. Based on virtualization, the cloud computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines.

A cloud computing platform provides a programming model for supporting self-recovery, redundancy, highly scalability and allows data to recover from failures of hardware and software as clients pay only for their usage such as storage or communication infrastructure. A virtual operating environment also relieves some significant issues of management as most of the software updates, maintenance, configuration and other management tasks are operated by centralized data centre in and cloud provider owns this responsibility. Virtualization for cloud computing, being a new technology lacks efficient security and privacy.

Virtualization is top strategic technology that is responsible to transform the landscape of IT industry and the way users compute. Virtualization multiplexes various virtual machines in the same hardware machine. This enhances sharing of resources and improves performance of machine in terms of resource utilization and application flexibility. Hardware resources such as memory CPU, CPU, I/O devices, etc. or software resources such as operating system and software libraries can be virtualized in various functional layers. With the help of virtualization, it is possible to work on multiple operating systems and applications simultaneously over the same physical server. Thus it increases the utility and flexibility of computing resources of a network.

This paper is organized in following way. The section II describes virtualization with its architecture and implementation techniques in detail. The section III introduces possibility of threats and attacks in virtualization. The section IV discusses some of important issues and challenges of distributed computing environment. The section V has discussed some of important virtualization tools used to create different type of virtualization and finally, section VI concludes the work mentioning future research direction.

II. VIRTUALIZATION: A COMPUTER ARCHITECTURE TECHNOLOGY

A technology [1,2] of utilizing the IT resources such as processor, storage and network to optimized level. This reduces the usage cost by combining various idle resources into shared pools and by creating different virtual machines to process multiple tasks simultaneously. Allocation of the resources can be changed dynamically as per demand of client.

A. Virtualization: Basic Types

There are certain basic techniques for creating virtualization in cloud computing environment.

1. Emulation

This technique of virtualization converts the behaviour of the computer hardware to a software program and it is placed in the operating system layer and that resides over the hardware. Emulation facilitates guest operating system with enormous flexibility but the speed of translation process is low compared to hypervisor and needs highly configured hardware resources to implement the software [3].

2. Hypervisor

A hypervisor runs on a computer known as a host machine, and each configured virtual machine over the host is known as a guest machine. The hypervisor provides a virtual platform to manage and execute the guest operating systems. It is defined as a layer of software, hardware or firmware which monitors and virtualizes the computing resources of a host machine to serve the user requirements [4].

This layer is placed in between hardware and operating system. Hypervisor connects the guest (virtual machine) to host machine in native or hosted [5] model. In host based hypervisor operates from operating system of host whereas the native hypervisor runs directly over the hardware. This software module virtualizes the resources such as CPU, memory, storage and drivers. Many operating systems may share the virtualized hardware resources for example macOS, windows and linux instances can all run on a single physical x86 machine.

3. Para Virtualization

In this technology special hyper calls are used in place of the instruction set architecture of host machine. It connects hypervisor and guest operating system to improve efficiency and performance. Accessing resources in para virtualization [6] 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 only suits with open source operating systems. On contrary to full virtualization guest servers are known to each other. Hypervisor does not need much processing power to manage guest operating system and the entire system performs as a single consolidated unit. In this guest operating system directly communicate with hypervisor interface and as an efficient virtualization this allows clients to use modified device drivers.

In para virtualization the guest operating system needs to be modified to interact with para virtualization interfaces and requires significant support and management issues in production environment.

4. Full Virtualization

Hypervisor creates isolated environment between the virtual guest machine and the host server hardware. Operating systems of hypervisor directly access the hardware controllers and its peripheral devices without cognizant of virtualized environment and requirement modifications [7].

This type of virtualization offers true isolation and security for virtual machine. In this isolated multiple guest machine run concurrently on same hardware. It is only choice requiring no hardware or operating system assistance to virtualize sensitive and privileged instructions. But full virtualization is usually slower in comparison to as all emulations and hypervisor has the device driver and it might be very difficult to install new device drivers by the clients.

B. Virtualization: Types of Resources

Depending upon type of resource server, client and storage there are three distinguished types of virtualization as explained below.

1. Server Virtualization

In server virtualization the single server platform behaves as multiple servers by partitioning resources of physical machine in distributed and computing environment. The hypervisor layer allows for hosting multiple applications and operating systems locally or remotely. The virtualization is beneficial in saving the cost, capital expenses, high availability and efficient utilization of resources.

2. Desktop/ Client Virtualization

This type of virtualization technique makes the administrator of system enable to monitor and update the client machines such as laptop, desktop and mobile devices virtually. By improving management of the client machines it enhances the security against hackers and cyber criminals. There are three variation of this virtualization at [8].

1. Remote or server hosted virtualization in which server machine is monitored and operated by the client across a network.
2. Local or client virtualization in which virtualized operating system which is secured against risk runs on local machine.
3. At application level, the virtualization [9] provides multiple ways to run an application not possible in traditional manner. A partitioning or isolated virtualized environment is used to run an application in many ways.

3. Storage Virtualization

It creates the abstraction of logical storage from physical storage. Three kinds of data storage are used in virtualization, which are as follows.

1. DAS (Direct Attached Storage)- this is the traditional technique of storing data where storage drives are directly attached to server machine.
2. NAS (Network Attached Storage)- This is the storage mechanism based on sharing which connects through network and is used for device sharing, file sharing and backup storage among machines.
3. SAN (Storage Area Network). This is a storage device being shared with different server over a high accelerate network.

C. Virtualization: Level of Implementation

1. Instruction Set Architecture Level

At this level of virtualization is implemented by translating the ISA of guest machine by the instruction set architecture of the host machine. In this approach, a large amount of legacy binary code developed for various processors is run on any other hardware host machine and this way it creates virtual ISAs for any hardware machine. It works through code interpretation and that interprets the source instructions to target instructions one by one. One source (guest machine) instruction may require hundreds of target (host) instructions to perform its function. This process is relatively slow so it requires dynamic binary translation to improve performance.

2. Hardware Abstraction Level

This virtualization is implemented just over the bare hardware. At one side this approach creates a virtual hardware environment for guest (VM) machine while at the other side, underlying hardware is managed through virtualization. This technique virtualizes resources of computer such as storage, processors and I/O devices. The approach optimizes hardware utilization by serving multiple users in parallel. The idea was implemented in the IBM VM/370 in the 1960s and most recently, the Xen hypervisor is used to virtualize x86-based machines to run Linux or other guest operating systems.

3. Operating System Level

This provides abstraction between user applications and traditional operating systems. At this level, virtualization creates isolated chambers on a single physical server and the OS instances to utilize the hardware and software in data centre. These chambers behave as real servers. The operating system virtualization mainly creates virtual hosting environments to assign hardware resources among multiple users. This enhances utilization of server hardware by dividing the services and directing each into created chambers or VMs on one server host.

4. Library Support Level

Mostly applications use APIs to provide libraries rather than using system calls by the operating system. Since most systems provide APIs so it is also virtualized. Virtualization of library interfaces is made possible by controlling the connection between applications and the rest of a system via API hooks. A software tool WINE has implemented it to support Windows applications on top of UNIX hosts. The vCUDA another tool that allows applications be executed within VMs to leverage server hardware acceleration.

5. User Application Level

At the application level this virtualizes an application as a virtual machine (VM). On a traditional operating system, an application runs as a process. So application level virtualization is termed as process level virtualization. In this approach high level language (HLL) VMs is deployed. In this case, the virtualization layer acts as an application program on top of the operating system and this layer provides an abstraction of a VM that can run software module written and compiled in a particular specific machine definition. The Microsoft .NET CLR and Java Virtual Machine (JVM) are two most popular examples of this class of virtual machine. The other types of application level virtualization are known as application isolation, application sandboxing, or application streaming. This process involves encapsulating the application in a layer isolated from the host operating system and other applications and thus an application that is much easier to distribute and remove from user workstations. The LANDesk provides application virtualization platform and deploys applications as self-contained, executable files in an isolated environment without needing system modifications, installation, or enhanced security privileges.

III. THREATS AND ATTACKS IN VIRTUALIZATION

A. Threats

Clients view their systems as a highly configured machine isolated from other users, even though every user share the same machine. In this context, a virtual machine is an operating system that is managed by an underlying control program and that must be secured. In virtualization there are certain vulnerable points that

must be secured. Here, some levels of software program and hardware with certain possibility of attacks are described as follows.

1. **Virtual Machine Level Attacks**

Cloud vendors continue to be potential problem in multi-tenant architecture [10] of cloud computing. These technologies use virtual machines the remote versions of traditional on site machine comprising of hardware and operating system. These virtual machines can be added or deleted to meet users' demand satisfactorily. An intruder may attack on virtual machine by blocking it.

2. **Cloud Provider Vulnerabilities**

These are at platform level such as attacking SQL statement or cross-site scripting that resides in service layer of cloud hampers the security of distributed execution environment.

3. **Expanded Network Attack Surface**

The client of cloud must protect the infrastructure which he uses to communicate with the cloud as the cloud in many cases is kept outside the firewall [10].

4. **Authentication and Authorization**

The authentication and authorization framework of enterprise is generally not extended into the cloud if not demanded as it is paid service. So enterprises must include security policies of cloud with their own security policies.

5. **Lock-in**

There is a lot against lock-in in cloud computing. The cloud provider can encrypt user data in particular format and if user decides to migrate to another vendor or something like [11].

6. **Data Control in Cloud**

In case of having full control over entire IT portfolio if inserting some program modules into the cloud infrastructure it continues the operation with little advance warning as of degraded or interrupted service [12] then it is very vulnerable point of attack and must be secured.

7. **Communication in Virtualization Level**

By it virtue, virtual machines communicate and share data with each other and If these communications do not meet security parameters significantly then they have potential of becoming target of attack.

B. Attacks

These days, many cyber-attacks are in the IT world. As cloud provides services to legal client it may serve to malicious users. For example a hacker of any cyber site uses a cloud to host a malicious application and collects his targeted. Scenarios of attacks are described below.

1. **DDoS attacks**

Distributed Denial of Service (DDoS) attacks generally target IP packets of high quantity at specific entry point in network. This is defined usually as form of hardware that performs on prohibited pattern and is quickly overrun. In cloud computing scenario as same infrastructure executes several virtual machines as clients, DDoS attacks have much potential than against single tenant architectures. In case cloud lacks sufficient resources to serve its clients then may cause undesirable DDoS attacks. For this situation a traditional solution is increase critical resources in cache. But in maliciously created situation, the DDoS may harm the IT industry. In current scenarios protection from DDoS must be reside in the network layer of virtualization rather than server virtualization. Cloud computing virtualizes machines and may overcome this problem by ARP spoofing technique at the network layer. This is basically about how to provide layer security across multiple networks.

2. **Client to Client Attacks**

One malicious virtual machine may corrupt all other virtual machines running in a physical server (host). In distributed and virtual environment, attacking a client virtual machine may fly to other virtual machines hosted in the same physical machine and this leading to the biggest security risk. When attacker focuses on virtual machines it is very easy to attack and in time during the attacker attacks one virtual machine it can lead to infect other virtual machines and thereby bypassing the hypervisor and accessing the operating environment level that was prohibited from access at virtual machine level. Thus, this is biggest security risk for virtualized and distributed environments and is termed as client-to-client attacks. In this serious attack, the malicious user acquires the administrator power over the infrastructure level of virtualized operating environment and finally it has access over all virtual machines. Anyhow, If attacker could get control over hypervisor then he will be having control over all data being transmitted between the virtual machines and hypervisor. Such attacks must be avoided by introducing controls or checks over network layer program.

IV. ISSUES OF VIRTUALIZATION

A. Data Leakage

In cloud environment, client's data is stored away from its native machine and data will move to multi-tenant

from a single-tenant environment. These changes are responsible for data leakage. For organization it has become one of the major security risk [13]. Virtually every government worldwide has rules and regulations mandate to protect from [13] such security issue. The provider of the services of cloud should have the ability to map its policy to the security mandate that user must comply with.

1. **DLP**

To protect data software developer are interested in using data leakage prevention (DLP) applications. These products maintain data confidentiality and help identifying the unauthorized access of data but unable to ensure the integrity or availability of data [14]. Currently, it is not expected of DLP products to ensure the data in integrity in any cloud environment. All encryption techniques are based on secure and impressive key management architectures. One of critical issue lies in encryption key management. In cloud computing environments, several users use their own encryption methodology and the managing these keys become another issue to be addressed in the context of encrypted data.

Organizations have high risk of leaking data when client probably be employee of that organization accesses to its data storage in a cloud environment.

Data leakage [15] takes place at hacked data location, securing remote access, third party storage and unsecure multi-tenant environment in hypervisor level. Provider of cloud service or attacker can enhance the prevention and detection mechanism and implement the collaborative security policy in hypervisor level to protect data from data leakage.

B. Security Threats

Security threats [16] in virtualization are classified into hypervisor threat, virtual machine threat, virtual infrastructure and virtual network threat. The virtual machine threat comes while it is processing resource contention, software updates or doing patching and virtual machine **conurbation.** Hypervisor threat rivets Virtual-Machine-Based Rootkit (VMBR) attack and Blue Pill Attack [17] where hypervisor plays the vital role of Virtualization. Virtual infrastructure threats occur on physical access. Virtual network threats can be effectively solved by the security tools doing intrusion detection, prevention mechanism, virtual switches and networks serving to the requirements.

C. Data Reminisce Issue

Data reminisce is physical representation of residual data that has been in some way erased. When storage media is erased there are some physical characteristics allows data to be recovered [18]. Thus any critical data must not only be secured against unauthorized access, but also be securely erased. Basically, IT organizations having their own servers and certainly keep control on their servers and for privacy they use various tools enabling them to destroy unwanted and important data safely. In case they migrate to cloud environment and have virtual servers controlled by third-party.

D. Privacy

Privacy [19] is an issue of major concern of users' data stored in the data centre of cloud service providers which is physically located in different places. In cloud, there are many privacy threats as follows.

1. The storage issue occurs when user data is stored in multiple storage location and hidden from the user and there is possibility of transferring data without permission of owner.
2. This occurs once data reaches its expiry time so ensure to implement destruction time policy among service provider of cloud.
3. This concern arises when data breaches and studies why data breach and who are responsible for this data breaches in cloud. So, to opt for using cloud services, the user should understand the terms and conditions.
4. This concern occurs during cloud clients 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.

E. 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 [20][21][22][23]. 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

V. VIRTUALIZATION TOOLS

Some of the popular virtualization tools used in various computing fields is as follows:

1. **Virtual Network User Mode Linux (VNUML)**

VNUML [24] is basically an open source tool used for creating multiple virtual machines of Linux operating system. These virtual machine acts as guests which run their application programs along with Linux OS of its original system as host.

2. Virtual Box

Virtual Box is used to implement virtual machines on the physical computers and servers. It performs full virtualization in the host computer machine. This states that without modifying the operating system of host the guest operating system is executed over the host machine [25].

3. VMware Server

This is also a virtualization tool for Windows operating system and Linux [26]. VMware Server does full virtualization.

4. QEMU

QEMU is also used for virtualizing operating systems like Linux and Windows both. It is a popular and open source [27] emulator providing fast emulation by using dynamic translation. It is provided with useful commands to manage of virtual machines.

5. Xen

Xen is also an open source tool used for virtualization preferably used for creating para virtualization in the host machine and guest machine [28].

6. VMware

A virtual machine platform helps executing unmodified operating system on the host or user level application hardware. Operating system being executed with VMware may be reinstalled, crashed, rebooted without affecting the application running on the host computer. VMware separates the guest operating system from host operating system so that failing guest operating system do not affect host machine [29]. VMware creates an illusion of standard PC inside the virtual machine. Therefore the VMware creates and execute several guest instances of guest operating systems concurrently over the single hardware machine of specific operating system.

7. EMF Tool

EMF virtualization is plug tool having an eclipse based on EMF basis to hold virtual models all based on EMF. To create virtual model by EMF tool, the users should provide contributing models along with meta models for the virtualization.

There are three main elements any virtual model formed by EMF tool.

1. Composition Meta model- It specifies virtual model concepts and that may be defined by the user or it may amalgamation of various distinguished composition processes.

2. Correspondence Model-It comes along with the AMW2 tool. This model includes all virtual links related with the contributing elements defines manner they are to be composed.

3. Virtual Model- it in form of a file specifies the physical location of all hardware resources which are to be used in the virtual composition process.

8. Virtual EMF

This is a virtualization model composition tool and its specification allows overcoming the limitations of virtual models such as not supporting concrete data although easily accessed. This help manipulates the original data contained in other models of EMF and is also built on Eclipse or EMF1.

VI. CONCLUSION AND FUTURE WORK

This paper has discussed various virtualization types and techniques. Various issues and challenges in virtualization for cloud computing system were discussed to take action to against them and to make system reliable. The virtualization techniques get universal support when users consider elastic resource management issues and security issues before moving into cloud. In future, this is aim to develop new framework, policies and techniques to manage elastic resources and data availability. This paper has discussed various issues regarding to virtualization to achieve cloud services. This study can be utilized to design more suitable framework to continue service of cloud by the future researchers.

VII. REFERENCES

[1] 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, pp. 321–329, 2011.

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

[3] R.N. Calheiros, R. Buyya and D. R. CAF, "Building an Automated and Self-Configurable Emulation Testbed for Grid Applications', Software: Practice and Experience, Vol. 40(5), pp. 405–429, April 2010.

[4] A. Whitaker, M. Shaw and S. D. Gribble, "Denali: Lightweight Virtual Machines for Distributed and Networked Applications", Tech. rep. Feb. 08 2002.

[5] IBM, ―IBM Systems Virtualization‖, version 2 release 1, http://publib.boulder.ibm.com/infocenter/eserver/v1r2/ topic / eicay / eicay.pdf. 2005.

[6] 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 ACM Press, pp. 164–177, New York, NY, USA, 2003.

[7] A. letaifa, A. haji, M. Jebalia, and S. 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), 69-88, December 2010.

[8] IBM Virtual Infrastructure Access Service Product. https://www-935.ibm.com/services /au/gts/pdf /end03005 usen .pdf

[9] B. Siddhisena, L. Wruasawithana, and M. Mendis, "Next Generation Muti Tenant Virtualization Cloud Computing Platform', In: Proceedings of 13th International Conference on Advanced Communication Technology(ICACT), vol. 12, no.3; pp.405–10, 2011.

[10] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masouka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the ACM Cloud Computing Security Workshop, Chicago, Illinois, USA., 2009.

[11] P. Sefton, "Privacy and Data Control in the Era of Cloud Computing".

[12] D. Rowe, "The Impact of Cloud on Mid-size Businesses," 2011.

[13] C. Almond, "A Practical Guide to Cloud Computing Security," 2009.

[14] F. Sabahi, "Security of Virtualization Level in Cloud Computing," in Proc. 4th Intl. Conf. on Computer Science and Information Technology, Chengdu, China, pp. 197-201 2011,

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

[26] T. Mirzoev, B. Yang, "Securing Virtualized Datacenters", International Journal of Engineering Research & Innovation, vol. 2, no. 1, Spring 2010.

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

[18] P. R. Gallagher, A Guide to Understanding Data Reminisce in Automated Information Systems: The Rainbow Books, ch.3 & ch.4,1991.

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

[20] S. Kumar, S.Manvi, G. K. Shyam, "Resource Management for Infrastructure as a Service (IaaS) in Cloud Computing: A Survey", Journal of Network and Computer Applications 41, 424–440, 2014.

[21] J.S. Chase, D. C Anderson, P. N. Thakar, and A.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; p.50–2, 2010.

[22] B. Urgaonkar, P. Shenoy, A. Chandra, P. Goyal, and T. Wood, "Agile Dynamic Provisioning of Multi-tier Internet Applications", ACM Trans Auton Adaptive Syst, 5 (5):139–48, 2010.

[23]L.M. Vaquero, L. Rodero-Merino, R. Buyya, "Dynamically Scaling Applications in the Cloud", In: Proceedings of the ACM SIGCOMM Computer Communication Review, vol.41, no.1,pp.45–52. 2011.

[24] 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". ACM SIGOPS Operating Systems Review 37: 164-177, 2003.

[25] G. Geiselhart, L. Dupin, D. George, R. Heij, J. Langer, G. Norris, D. Robbins, B. Robinson, G. Sansoni and S. Thoss," Linux on IBM Eserver" zSeries and S/390, 2003.

[26] Cox, T. E. N. A. L. 2007, "Towards an Operating Platform for Network Control Management. In Workshop on Programmable Routers for the Extensive Services of Tomorrow (PRESTO), Princeton University, Princeton, NJ pp.

[27] R., P. and C. M. 2007. "Case Study: Nationwide Uses Linux and High-Power Virtualization for Web Presence', Gartner RAS Core Research, Note G-00148213.

[28] A. Bavier, N. Feamster, M. Huang, L. Peterson and J. Rexford, "In VINI Veritas: Realistic and Controlled Network Experimentation," in ACM SIGCOMM Computer Communication Review, pp. 3-14, 2006.

[29]W.M. Fuertes, and J. E. L. de Vergara, "A Quantitative Comparison of Virtual Network Environments Based on Performance Measurements", in Proceedings of the 14th HP Software University Association Workshop, Garching, Munich, Germany, pp. 8-11.