FACTORS THAT INFLUENCE THE CHOICE OF VIRTUALIZED ENVIRONMENTS IN SMALL MEDIUM ENTERPRISES.

Vincent Motochi, Dr. Samuel Mbugua, Dr. Shem AngoloMbandu,

ABSTRACT

Virtualization is an emerging technology in the recent computing worlds and has become a platform for the implementation of utility computing (e.g. cloud computing) and the rising Virtual Private Networks. It helps to centralize and integrate IT resources there by reducing costs and energy usage. Organizations are implementing this technology, however, what factors determine the choice of virtual environments to be implemented? Moreover, to what extend therefore can an organization virtualize? This research proposes a paper that will investigate the above stated factors so that they can be able to breakeven and survive the ever changing economic times. The research shall achieve this by identifying and investigating factors that determine the choice of virtualized environments in these organizations. This will be accomplished by a qualitative design through a desktop research. This research is important for small and medium organizations who would need to evaluate the factors that they would consider before they choose to go virtualization. Some of the benefits that come with this technology include to reduce operating costs based on virtualization platforms, promote efficiency on clouds and enable organizations to shift the emphasis on the management, rather than ownership of ICT resources.

Index terms: virtualization, security, hypervisor, SME

I. INTRODUCTION

SMEs play a significant role in economic, social and political growth and development of a nation. They also serve as seedbeds for medium and large scale entrepreneurs, contribute to more balanced socio-economic development and facilitate the process of adjustment in large enterprises; emerging as competent suppliers of products and services previously not available in the market place [5]. According to the definition by the European Union SMEs there is no special definition for them however,

they are organizations that may have a maximum of 250 employees, an annual turnover of about 40 Euro Million and allow not more than 25% of capital ownership or voting rights held by one or more enterprises who are not themselves SMEs. Therefore, SMEs make indispensable contributions to the economy. They act as major job providers, produce a significant part of the total value added, feed the larger industries with their needed inputs, as well as acting as distributors/buyers of their products. Small firms provide a large segment of the lower and middle-income population with low priced consumption goods and services. Small firms also represent a channel through which small savings are being translated into investments. Small enterprises could become major sources of constant innovation and experimentation and could thereby in some cases change the market structure. SMEs have been viewed as a source of technological progress, especially in new industries. The continuous influx of small firms in all sectors of the economy by all segments of the society is considered a healthy phenomenon and a crucial barometer for social and economic well-being [6]. ICT enhances SME efficiency, reduces costs, and broadens market reach, locally and globally; resulting in job creation, revenue generation and overall country competitiveness. Small enterprises are generally seen as being at a disadvantage to larger businesses. They are characterized by limited availability of resources in terms of time, money and expertise (Wymer& Regan, 2005). Their inferior technology and managerial capabilities have often shown to be a constraint on their effective use of new technologies (Caldeira and Ward, 2002). Whereas ICT is not a panacea for all development problems, it offers enormous opportunities to small enterprises. It will increasingly empower SMEs to participate in the knowledge economy by facilitating connectivity; helping to create and deliver products and services on a global scale, and providing access to new markets and new sources of competitive advantage to boost income growth.

Today, organization's data center, have attracted a lot of interest in the enterprise networks and virtualization. Data centers for organizations are used to provide data storage and files transfer where end stations and branches are interconnected systems over the Internet. A data center represents the heart of any

organization's network infrastructure. SMEs and Companies rely on the data stored in the data centers to interact with its employees and customers.

Virtualization has become popular in organizations since it provides an easy mechanism to cleanly partition physical resources, allowing multiple applications to run in isolation on a single server [11]. Virtualization helps with consolidation of hardware, software, network infrastructures and information systems that provides flexible resource management and administration mechanisms to an organization. Virtualization is not a new technology, but it has regained popularity in recent years because of the promise of improved resource utilization through server consolidation. In [3], the authors enlist the data center hardware and software components.

This paper discusses factors affecting the choice of virtualization, and its importance. It also discusses the main security threats and attacks. Then, it shows two main security frameworks, and discusses the advantages and disadvantages of each one and how they are different. The paper concludes by suggesting a framework to cloud vendors; its implementation depends on the environment. A critique of both frameworks is also presented.

The paper is structured as follows: Section 2 reviews the basic concepts of virtualization. Section 3 exposes some related work in this context. Section 4 presents the findings under study. Section 5 analyzes and discusses the factors that determine the choice of virtualization environments choice. Finally, Section 7 concludes the paper and sheds light on future work.

1.2 Statement of the Problem

A Data Center is the consolidation point for provisioning multiple services that drive an enterprise business process [7]. It is also known as the server farm or the computer room. The data center is where the majority of enterprise servers and storage systems are located, operated and managed like the ERPs, application servers, and security systems. Ethernet switching technology is the foundation, upon which many of these services are built [8]. Organizations are today embracing emerging technologies and virtualization in data center and networks are common.

Data center networks are still largely relying on traditional TCP/IP protocol stack, resulting in a number of limitations:

- *No performance isolation*:

Many of todays cloud applications, like search engines and web services have strict requirements on network performance in terms of latency and throughput. However, traditional networking technologies only provide best-effort delivery service with no performance isolation. Thus, it is difficult to provide predictable quality of service (QoS) for these applications.

- *Increased security risks*: Traditional data center networks do not restrict the communication pattern and bandwidth usage of each application. As a result, the network is vulnerable to insider attacks such as performance interference and Denial of Service (DoS) attacks [1].
- *Poor application deployability*: Today many enterprise applications use application-specific protocols and address spaces [2]. Migrating these applications to data center environments is a major hurdle because it often requires cumbersome modifications to these protocols and the application source code.
- *Limited management flexibility*: In a data center environment where both servers and networks are shared among multiple applications, application owners often wish to control and manage the network fabric for a variety of purposes such as load balancing, fault diagnosis, and security protection. However, traditional data center network architectures do not provide the flexibility for tenants to manage their communication fabric in a data center.
- *No support for network innovation*: Inflexibility of the traditional data center architecture prohibits network innovation. As a result, it is difficult to introduce changes in traditional data center networks such as upgrading network protocols or introducing new network services. In the long run, it will reduce the effectiveness of the initial capital investment in data center networks.

Motivated by these limitations, there is an emerging trend towards virtualizing

data center networks in addition to server virtualization.

There is need to investigate factors that influence the choice of virtualized environments used in SMEs.

1.3 AIM

The main objective of this paper is to investigate factors that influence the choice of virtualized environments used in SMEs.

II. REVIEW OF LITERATURE

Virtualization is a technology that has been there for some time. This concept was firstly introduced by IBM in the 1960s to provide concurrent, interactive access to a mainframe computer—IBM 360, which supports many instances of OSs running on the same hardware platform [9].

2.3.1 Virtualization in System Platforms

Virtualization technology supports multiple OSs running on a single hardware platform, and provides a convenient means to manage the OSs. The OS and applications running on the virtualization management platform are considered as VMs [10]. Virtualization provides a new approach to solve the traditional security problems, and it also brings new security issues to computer systems (Rosenblum &Garfinkel, 2010). The security of virtualization-based cloud computing comes down to that of virtualization itself. Virtualization is also an emerging concept in telecommunication and computer networks. This is what has given rise to technologies such as VPNs and VLANs, which have become key integral part in our organizations.

The concept of virtualization originated in the 1960s when the costs of mainframes were very expensive. IBM divided a large UNIX main-frame into multiple logic instance to enable users to fully utilize a mainframe's calculation resources (Singh, 2004). Each logic instance is essentially a virtual machine (VM) or a guest operating system (OS). As the OS or the hardware of the mainframe computer may have different compatibilities with VMs, a virtual machine monitor, called hypervisor, may be needed to serve as the interface between VMs and the physical hardware [13]. As shown in figure 3, each virtual machine has its own virtualized resources including I/O ports and DMA channels, and these VMs are capable of running on any OS through the hypervisor, as long as the

hardware is supported by the OS [13]. In other words, the hypervisor is the key. In the example of VMware's solution, the hypervisor of VMware, called VMware Virtualization Layer, is capable of hosting multiple virtual machines with a shared CPU, memory, network driver and hard disk space. On the other hand, the hypervisor is inevitably having security vulnerability and is susceptible to hacker attacks, requiring a higher level of information security management [4].

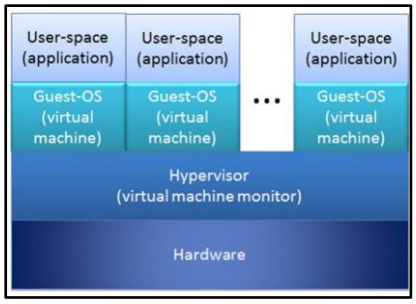

Figure 1: Overview of virtualization environments
(Adopted from source: T. Jones 2007)

2.3.2 Virtualization in Networks

Network virtualization enables multiple logical networks to share the physical resources of the underlying network infrastructure. Virtual Networks (VN): deploy customizable network protocols by leasing the required infrastructure resources from multiple NIs. Each virtual network is a combination of multiple virtual routers and links. When initiating a service, the VN confines to the Service Level Agreements (SLA) with set of NIs and receives the requested resources. Each VN then instantiates the service (e.g., novel network protocol) on the allocated resources to form a virtual network topology by connecting end users to the network. End Users are similar to the current Internet architecture but have the opportunity to choose from multiple virtual network services.

For any virtual network, the above architectural separation reduces the cost involved in setting up the physical resources and maintaining them. This three-tier architecture promises to introduce flexibility through programmability, improved scalability and reduction in maintenance costs. Figure 2 shows two virtual networks sharing the network infrastructure resources. Both VNs deploy their customized network services on the shared infrastructure components and establish end-to-end connectivity between end users.

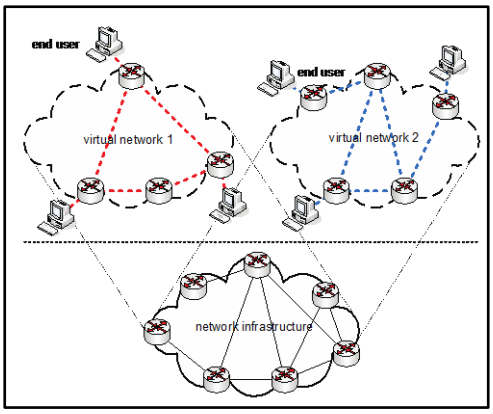

Figure 2.2: Virtualized network infrastructure, Adopted from (Source: Natarajan and Tilman, 2013)

III. METHODOLOGY

The research study proposed will use qualitative approach to conduct this research. This will include reviewing a published paper based on an empirical finding from an experiment and other papers relating on virtualization in relation to energy usage and green computing. The research study used qualitative approach to conduct this research. This included reviewing a published paper based on an empirical finding from an experiment and other papers relating on virtualization in relation to energy usage and green computing.

IV. FINDINGS

This section presents findings on the objective as per reviewed desktop research, which further generalize a few fundamental insights.

The researcher evaluated various published documents to determine the factors that determine the choice of virtual environments for SMEs. The findings were recorded as follows:

Finding (a):virtualization is implemented in various thematic areas. Some virtualizations are implemented in operating systems platforms or hardware systems while others are implemented in networks.

Finding (b): there are two main levels of virtualization, para virtualization and full virtualization. However, we also have a special one implemented at the application level called *Execution Environments for Virtual Machines Over the Host OS. This has been implemented by Java programming and software developments.*

Finding (c): there are various factors, which determine the choice of virtual environments that an organization chooses from which suit his business. Some of the factors are chosen with an aim to reduce costs and maximize returns. The following factors are key:

System Platforms

a) Capability of a computer hosting two or more operating systems
b) Software testing and runtime debugging:

c) Consolidation of hardware resources
d) Transparent storage
e) Inter-process communication
f) On demand research
g) Fault tolerant
h) Easier to implement specialized applications
i) Managed general and customized licenses

Network virtualization

a. Establishment of virtual networks on physical networks
b. Security
c. Test bed for next generation research:
d. Network testing and troubleshooting
e. Fault tolerant
f. Easier to implement specialized networks
g. Managed general and customized licenses
h. Transparent storage
i. Consolidation of network resources

All these factors are also directly connected to the type of business an organization is performing and therefore they vary from one organization to another. For example organizations that manage content will go for virtual storage while those that are charged with software development will go for virtual environments that for purposes of separation of code license agreements.

All these factors have been discussed in detail in the next section of this paper.

V. DISCUSSION

In this section, the researcher discusses the findings as recorded in section iv in detail in line with the research main objective as stated below:

Objective: The main objective of this paper was to investigate factors that influence the choice of virtualized environments used in SMEs. Based on the objective under study the researcher describes the following factors which have been characterized into two main domains:

1. Platform Virtualization

The historical main advantage of virtualization is the implementation of time-sharing mechanisms, which at their turn lead to increased efficiency in using the available physical resources. Furthermore, the concept of isolation is also inherent in the deployment of virtualization, perceived either from the point of view of easy deployment of bundle applications, or as run-time isolation of parallel

incompatible applications running on the same physical infrastructure. Virtualization rendered for the first time the operating system independent of the underlying hardware. This feature opened the way for software portability from one hardware entity to another. The resulting isolation, if properly exploited, can reduce system downtime significantly. Malicious or poorly written programs are isolated in such a way that they cannot influence the rest of the system functionality, hence increasing the robustness and protection of the overall system.

These concepts spawn a number of benefits exploited so far by service providers and everyday users:

i. Capability of a computer hosting two or more operating systems**:** A virtual machine installed on a single host machine allows the installing and parallel functioning of two or more separate OSs. In turn, this allows the user of this machine to run different OS specific applications, without requiring yet another dedicated hardware for each OS.

ii. Inter-process communication**:** Virtualization limits the communication between processes running on different virtual machines, hence isolating processes from each other. For example, the effect of malware can be limited, without affecting the hardware or other applications running outside the specific virtual environment.

iii. On demand research**:** Virtualization allows for the developing and debugging of a new instance of an OS on the same hardware. This allows for new research ideas to be implemented and tested.

iv. Software testing and runtime debugging**:** Virtualization offers a stable and convenient way to create a reproducible environment for software testing. This provides an easy way to test and debug new software before and during deployment into production environments.

v. Consolidation of hardware resources**:** Virtualizing hardware equipment makes it possible to accommodate multiple processing/computation environments, hence it is

possible to aggregate multiple servers on the same machine, up to capacity, and reduce the hardware number and costs (e.g. cloud computing).

vi. Fault tolerant**:** Executing processes can be moved transparently from one hardware system to another. In case of system failure, machine virtualization enables the transparent migration of running processes to a different machine, which insures service availability. Job migration can also be used for load balancing and energy saving by moving jobs from a lightly loaded machine and subsequently powering down the hardware.

vii. Transparent storage**:** Storage becomes independent of the services it is used for, and the management functionality becomes easier. Addressing of individual storage devices, e.g. hard-drives, becomes transparent to the service, its administrator, as well as the user.

viii. Easier to implement specialized applications**:** Deployment of specialized applications is not straightforward, as they require specific versions of operating system libraries and thus may not coexist well on the same machine. Virtual machines can alleviate this problem because incompatible applications can be put into separate virtual machines. Full ISO images containing the correct OS version together with the necessary applications can easily be deployed in one virtual machine, without changing the current configuration of the machine (and e.g. avoiding the ‘’DLL Hell’’ problem).

ix. Managed general and customized licenses**:** The isolation offered by a virtual machine enables proprietary code to be cleanly separated from GPL code and its viral license requirements. This facilitates the production of fully GPL-compliant products.

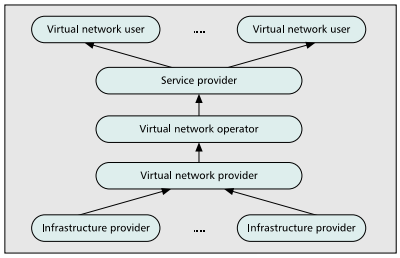

Figure 3: Adopted from IEEE Communication magazine 2012

2. Network virtualization

The researcher assumes a general architecture for network virtualizationas shown in the figure 5.1 below, where the network infrastructure resources are gathered under the virtualization layer, and become transparent to the virtual network operators. Network virtualization is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. The idea is that virtualization disguises the true complexity of the network by separating it into manageable parts. We consider access to the network via service access points, the exact location of which is irrelevant for this discussion, be it in the core network or a socket-like interface on a host.

Starting from the benefits and concepts for virtualization as presented earlier, then define use cases for network virtualization. The following factors are key towards shelving machine virtualization into network virtualization with use cases below:

i. Establishment of virtual networks on physical networks**:** Virtualization technologies, when applied to networking, can create multiple virtual/logical networks on the same physical substrate network. It is also possible to maintain isolation in between these networks. This isolation would facilitate the deployment of multiple, sometimes conflicting networking techniques in the same physical network, e.g. different, incompatible routing protocols. It could also enable accommodating multiple generations of cellular networks, e.g. 4G and 5G on the same physical network.

ii. Security**:** Isolation is a great weapon for protecting an entity from its surroundings. Different

virtual networks may have different protection features, such as access control or mandatory traffic encryption. One such isolated, encrypted, access controlled network can be used, for example, for banking applications. Adding access control also on the servers joining such a network can be used to create a safer Internet for children.

At present, the most prominent way of realizing secured and thus protected sessions is by means of virtual private networks (VPN). Regardless to whether PPTP, L2TP or IPSec is used, the basic principle is tunneling. User data, including or excluding the IP header, is encrypted, and additional headers, e.g. PPP, GRE, IP etc., are appended with the encrypted user packets for authentication and routing purpose. The content of the user packet, including source and destination IP, remain transparent to the core transport network. Although VPN protects the secrecy of user data, it is a point-to-point protection rather than a multipoint-to-multipoint protection, i.e. network-wide isolation that is envisioned in network virtualization.

iii. Test bed for next generation research**:** The concept of network virtualization emerges from the need for a large-scale general purpose testbed for next generation network research. The isolation guarantees that the malfunctioning of one experiment cannot take the whole physical testbed down and thus, other experiments running in parallel stay unharmed. NSF GENI is pursuing such a testbed.

iv. Network testing and troubleshooting**:** Operators, owning networks with a nation-wide reach, lack large-scale testing facilities where they can sufficiently test their new services before commercially deploying them on their servicing network. By using virtualization technologies, it is possible to create slices in operators' servicing nodes and create a testing facility as large as the commercial network. In such a testing environment,

commercial operators can test their under-development services and have a better opportunity to make the service robust enough before commercial deployment. Isolating this virtual network for testing from the commercial networks guarantees resiliency to the commercial slices in case of malfunctions in the test slices, thus ensuring service availability to the users. If the network nodes can be virtualized such that the complete network can be simulated on a smaller amount of hardware than the number of network nodes would stipulate, significant cost savings could be realized for testbeds. The same technology can be used to experiment with deployed applications in order to pinpoint hard-to-trace runtime problems.

v. Consolidation of network resources**:** By dynamically allocating virtual network nodes to the physical substrate, the existing hardware can be utilized for multiple virtual networks up to capacity and thus minimize cost for the infrastructure provider. The reason network virtualization might be needed on network nodes is if different administrative domains want to administer their own policies on these nodes. The problem of resource mapping between the physical substrate and the virtual networks is currently one of the most actively pursued problems in academic research.

vi. Fault tolerant**:** In the case of network virtualization, slices take the role of jobs. A slice is a virtual machine inside a network node. Slices can migrate from one network node to another. This migration provides an easy way of re-configuring the network topology without deploying much re-wiring. Slice migration can create a completely different network topology on the fly, which can see its use in topology optimization in commercial networks or for creating topology for experimentation in academia. Such migration techniques can also be used to reduce downtime during

network upgrade.

vii. Transparent storage**:** Current network abstractions do not include storage of permanent state as a main feature of the network. However, if we change the boundary of the abstraction to include content delivery as a part of the core network service, e.g. CDNs and P2P networks, virtualization can help retrieve content from the same logical address, regardless of its physical location. In fact, virtualization can help adapt the physical location of content according to its access pattern, e.g. flash crowds and local news.

viii. Easier to implement specialized networks**:** The equivalent of an application in networks is a service. Many network services require a specific network architecture (e.g. WLAN, sensor networks, corporate intranet). If many of such services are deployed simultaneously in a network, the resulting network architecture supporting all deployed services can become overly complex. This problem could be alleviated by deploying services that don't rely on each other in separate virtual networks.

ix. Managed general and customized licenses**:** Network virtualization not only facilitates separation of different classes of quality of service agreements, but would also allow different traffic routes due to differing peering agreements. For example, one could ensure that certain traffic does not get routed through networks the data shouldn't stray into. The traffic in question could be data sensitive for national security, or media streams for which the distributor has rights only in certain countries. In this regard, some authors have shown service-based network virtualization by using multi-layer traffic engineering in GMPLS.

The expected improvements brought by network virtualization lie in the domain of increased flexibility and level of service, increased separation between network and service providers, or reduced management cost and

energy consumption.

On the other hand, potential disadvantages of network virtualization technologies include the potential reduction of the statistical multiplexing advantage, the extra complexity of the inter-slice management operations, and the cumbersome interaction between control and management entities functioning inside a network slice with those functioning at the hypervisor level.

FORMS OF VIRTUALIZATION

The hypervisor exposes an interface that represents hardware and can be used to host full-fledged operating systems. On the other hand, there are virtual machines that run on top of operating systems, and are execution environments for individual programs written in bytecode (e.g. Java virtual machines).

The hypervisor may either run stand-alone like a micro-kernel or supported by a host operating system. However, most commercially available hypervisors make use of a host operating system that allows easy management and installation of guest operating systems.

To each guest OS, hypervisors will assign their own resources, thus isolating them from each other. Therefore, processes running in different guest OSs cannot communicate with each other using the usual OS primitives of semaphores, signals, pipes, or shared memory. In general, these processes will have to rely on network services to communicate with each other.

Programs running in virtual machines representing a byte-code execution environment have a wider variety of communication mechanisms to choose from, as such features are usually an integral part of the execution environment (e.g. .NET remoting)

Server Virtualization

Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments.There exist several forms of virtualization that are deployed in information technology environments. There are other many forms of virtualization as discussed below and each and every business

organization would choose a particular form based on its nature of business activities that they engage in and one that fits them well.

A. Full Virtualization

Full virtualization is a virtualization technique used to provide a certain kind of virtual machine environment, namely, one that is a complete simulation of the underlying hardware. This type of server virtualization abstracts both the hardware resources on the server and the guest OS.

This form provides the virtualization environment the ability to entirely simulate the underlying hardware. The resultant is a system where any software that is capable of execution on the physical host is able to run in the VM, and any OS that is supported by the underlying physical host can run in each individual VM. Different operating systems can run concurrently in a full virtualization setup. In addition, the Input/Output (I/O) devices are allocated to the guest OSs by emulating the physical devices in the VMM, interacting with these devices in the virtual environment are then directed to the real physical devices either by the host OS driver or by the VM driver.

The advantages of this approach are that it provides complete isolation between each VM and the any other VM residing on the same physical host and between the VMs and the VMM. Moreover, it is easy to use, in the sense any user can install a software product such as VMware Workstation on the preferred choice of OS and once they switch it on the VMware workstation; a guest OS can be installed and used. In addition, it provides near-native CPU and memory performance.

The disadvantages of this technique are that it requires the exact appropriate blend of hardware and software components and poor performance of the emulated VM due to the impact by trap and emulate techniques of x86 privileged instructions. Advantages of full virtualization:

- This approach to virtualization means that applications run in a truly isolated guest OS, with one or more of these guest OSs running simultaneously on the same hardware. Not only does this method support multiple OSes, it can support dissimilar OSes, differing in minor ways (for example, version and patch level) or in major ways (for example, completely different OSes like Windows and Linux);

- The guest OS is not aware it is being virtualized and requires no modification. Full virtualization is the only option that requires no hardware assist or operating system assist to virtualize sensitive and privileged instructions. The hypervisor translates all operating system instructions on the fly and caches the results for future use, while user level instructions run unmodified at native speed;
- The VMM provides a standardized hardware environment that the guest OS resides on and interacts with. Because the guest OS and the VMM form a consistent package, that package can be migrated from one machine to another, even though the physical machines the packages run upon may differ;
- Full virtualization offers the best isolation and security for virtual machines, and simplifies migration and portability as the same guest OS instance can run virtualized or on native hardware.

B. Para-virtualization

Para virtualization is an enhancement of virtualization technology in which a guest OS is recompiled prior to installation inside a virtual machine. Para virtualization allows for an interface to the virtual machine that can differ somewhat from that of the underlying hardware. Para virtualization provides partial simulation of the underlying hardware. Wherein, most but not necessarily all hardware components are simulated. There exists a thin software interface between the host hardware and the modified guest operating system. A fascinating point in this technique is that the guest machines are aware of the fact that they are running in a virtualized environment.

The main limitation of para virtualization is the fact that the guest OS must be tailored specifically to run on top of the virtual machine monitor (VMM), the host program that allows a single computer to support multiple, identical execution environments. However, para virtualization eliminates the need for the virtual machine to trap privileged instructions. Trapping, a means of handling unexpected or unallowable conditions, can be time-consuming and can adversely impact performance in systems that employ full virtualization.

Resource Virtualization

Resource virtualization characterizes the following types of virtualizations:

A. Operating System Virtualization

Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power.

B. Application Virtualization

This is abstracting the application layer away from the operating system. This way the application can run in an encapsulated form without being depended upon on the operating system underneath. This can allow a Windows application to run on Linux and vice versa, in addition to adding a level of isolation.

Virtualization can be viewed as part of an overall trend in enterprise IT that includes automatic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The usual goal of virtualization is to centralize administrative tasks while improving scalability and workloads.

Data virtualization is abstracting the traditional technical details of data and data management, such as location, performance or format, in favor of broader access and more resiliency tied to business nee

Desktop virtualization is virtualizing a workstation load rather than a server. This allows the user to access the desktop remotely, typically using a thin client at the desk. Since the workstation is essentially running in a data center server, access to it can be both more secure and portable. The operating system license does still need to be accounted for as well as the infrastructure.

C. Storage Virtualization

Storage virtualization is the pooling of physical storage from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Storage virtualization is commonly used in storage area networks.

D. Network Virtualization

Network virtualization is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others and can be assigned -- or reassigned -- to a particular server or device in real time. The idea is that

virtualization disguises the true complexity of the network by separating it into manageable parts, much like your partitioned hard drive makes it easier to manage your files.

Full Virtualization in Networks – Network virtualization (NV) is defined by the ability to create logical, virtual networks that are decoupled from the underlying network hardware to ensure the network can better integrate with and support increasingly virtual environments. Over the past decade, organizations have been adopting virtualization technologies at an accelerated rate. Network virtualization abstracts networking connectivity and services that have traditionally been delivered via hardware into a logical virtual network that is decoupled from and runs independently on top of a physical network in a hypervisor. Beyond L2-3 services like switching and routing, NV typically incorporates virtualized L4-7 services including fireballing and server load-balancing. NV solves a lot of the networking challenges in today's data centers, helping organizations centrally program and provision the network, on-demand, without having to physically touch the underlying infrastructure. With NV, organizations can simplify how they roll out, scale and adjust workloads and resources to meet evolving computing needs.

With virtualization, companies can take advantage of the efficiencies and agility of software-based compute and storage resources. While networks have been moving towards greater virtualization, it is only recently, with the true decoupling of the control and forwarding planes, as advocated by software defined networking and network functions virtualization, that network virtualization has become more of a focus.

Para-virtualization in Networks- This solution requires the guest OS to be modified for the hypervisor. The L3-VPN customer edge (CE) solutions in this category, as the customer system has to establish, maintain, and isolate its session. Hence, the user must adapt the VPN tunnels to the underlying provider network in between two CE routers. L2-VPN is also similar, as the L2-switch at the session generating host side has to modify the session, i.e. tagging to receive the VPN service from the L2 network. The application layer (layer 7) needs special addressing and flow control to receive desired services from the transport network, e.g. transparency, overlay maintenance, and other services the

transport doesn't provide in general. The Open Signaling Approach falls in this category as well, as the user has to adapt its applications to the API provided by the underlying abstraction layer.

Execution Environments for Virtual Machines Over the Host OS - Java Virtual Machine and Microsoft Common Language Runtime are two examples of such virtualization techniques. The virtual machine execution environment offers a hardware independent instruction set that is responsible for translating Java byte code or Intermediate Language Code to machine language.

A network, historically and inherently, is a virtualized environment of this category. All the application sessions are in general isolated, and receive different treatment according to the QoS requirements (best effort excluded) mentioned by the originator of the session, i.e. end system. Avoiding here the philosophical argument of "the waist of the hour-glass in the network protocol stack is not IP but HTTP," the Virtual Machine Execution Environment in this scenario is analogous to the waist of the hour-glass in machine virtualization. It adapts the application to the hardware in a machine, whereas any application session in a network can use IP and needs not be aware of the underlying transport technology. The network has always been a virtualized multi-user use space. Cellular networks even isolate sessions on a per user basis.

VI. CONCLUSION

Data centers have become a cost-effective infrastructure for data storage and hosting large-scale network applications. However, traditional data center network architectures are ill-suited for future multi-tenant data center environments. Virtualization is a promising technology for designing scalable and easily deployable data centers that flexibly meet the needs of tenant applications while reducing infrastructure cost, improving management flexibility, and decreasing energy consumption.

In this paper, the researcheranalysed the factors that determine the choice of virtual environments to be implemented in organizations. The researcher went on to detail the types of virtualizations available, the levels of virtualizations and the thematic areas where virtualization is implemented.

VII. RECOMMENDATIONS AND WAY FORWARD

Although current virtualization proposals improve scalability, provide mechanisms for load balancing, ensure bandwidth guarantees, reduce operating costs, there are challenging and important issues that are yet to be explored. Designing smart-edge networks, providing strict performance guarantees, devising effective business and pricing models, ensuring security and programmability, supporting multi-tiered and multi-sited data center infrastructures, implementing flexible provisioning and management interfaces between tenants and providers, and developing efficient tools for managing virtualized data centers are important directions for future research.

REFERENCES

[1] Shieh A., S. Kandulaz, A. Greenberg, C. Kim, and B. Saha, "Sharing the Data Center Network," in *Proc. USENIX NSDI*, March 2011.

[2]Benson T., A. Akella, A. Shaikh, and S. Sahu, "CloudNaaS: A Cloud Networking Platform for Enterprise Applications," in *Proc. ACM SOCC*, June 2011.

[3] Jalal Frihati, FloricaMoldoveanu, AlinMoldoveanu, General guidelines for the security of a large scale data centre design, U.P.B. Sci. Bull., Series C, Vol. 71, Issue 3, 2009.

[4] Higgins K.J., VMs create potential risks. Available at http://www.darkreading.com/ security/security-management/208804369/index.html 2007.

[5] Republic of Kenya (2002). National Development Plan 2002-2008: Effective Management for Sustainable Economic Growth and Poverty Reduction. Nairobi: Government Printer

[6] Irgens, M. Abdelghany, and S. El-Araby, "Towards SMEs Sustainability through TQM Adoption in Developing Countries – A Case Study", Stimulating Manufacturing Excellence in Small and Medium Enterprises, SMESME 2005, Strathclyde, Scotland, UK, (2005).

[7] Emerson, Network Power white paper, Balancing Scalability and

Reliability in the Critical Power System: When does ‗N+1' Become Too Many +1'? http://www.EmersonNetworkPower.com, 2004.

[8] Emerson, Network Power white paper, Power Management Strategies for High-Density IT Facilities and Systems, http://www.EmersonNetworkPower.com, 2007.

[9] Rosenblum, M. &Garfinkel, T. (2010). When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. Stanford University.

[10] Feng, Z., Hai J., Xiang G., Deqing, Z., Song, W., Min, L., &Weide Z. (2011). A VMM-based intrusion prevention system in cloud computing environment. Springer Science Business Media.

[11] Timothy Wood, "Improving data center resource Management, deployment, and availability with virtualization", PHD thesis June, 2009,(Unpublished)

[12] Jalal Frihati, FloricaMoldoveanu, AlinMoldoveanu, General guidelines for the security of a large scale data centre design, U.P.B. Sci. Bull., Series C, Vol. 71, Issue 3, 2009.

[13] Hoesing M. T., Virtualization security assessment, Inf.Secur.J.:Glob.Perspect.18(3) (2009) 124–130.

[14] Jones T., Discover the Linux Kernel Virtual Machine. Available at: http://www-128. ibm.com/developerworks/linux/library/l-linux-kvm/ 2007.

Authors' Profiles

Vincent Motochi is a PhD student in Information Technology at Kibabii University, which is in Bungoma County (Kenya). He holds a Master of Science in Information Technology and Bachelor of Science in Computer Science both from MasindeMuliro University of Science and Technology (Kenya). Currently he is the Head of ICT for the County Government of Kakamega. Before that he was the ICT Manager of the County Government of Vihiga on Interim terms for one year. Before that he was the Computer Programmer for the former County Council of

Kakamega. He has special interests in information security and has published papers on the same topics and he is also a member of the Association of Computing Machinery (ACM).

Dr. Samuel Mbuguais a senior lecturer of Kibabiiuniversity. He is also the ICT director for the university. Dr. Mbugua holds a Doctor of Philosophy degree in Information Technology fromMasindeMuliro University of Science and Technology; and a Master of Science degree in Computer Based Information Systems from Sunderland University. Before that, he also attained his first degree in Science Electronics. He is a member of the Association of Computing Machinery.

Dr. Shem MbanduAngolo holds a PhD Computer Science degree from the University of Electronic Science and Technology of China (UESTC), ChengDu, PRC, an MSc. Information Systems degree from University of Nairobi and a Bachelors of Education degree from Moi University. His research interests are in Applied Cryptography, Information Security and Machine Learning. He is also the dean, school of information communication and technology with vibrant programs which are reviewed time to time to reflect the current trends and needs of the dynamic field of computing.