SECURITY ISSUES IN VIRTUALIZED ENVIRONMENTS FOR SMALL AND 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 [1].

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 [2].

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 [3]. Their inferior technology and managerial capabilities have often shown to be a constraint on their effective use of new technologies [4]. 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 [5]. 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 [6], 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 [7]. 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 [8].
- *Poor application deployability*: Today many enterprise applications use application-specific protocols and address spaces [9]. 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 evaluate security threats and vulnerabilities present in the virtualized environments in SMEs.

1.3 AIM

The main objective of this paper is to evaluate security threats and vulnerabilities present in the virtualized environments 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 [10].

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 [11]. Virtualization provides a new approach to solve the traditional security problems, and it also brings new security issues to computer systems [10]. 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 [12]. 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 [14].

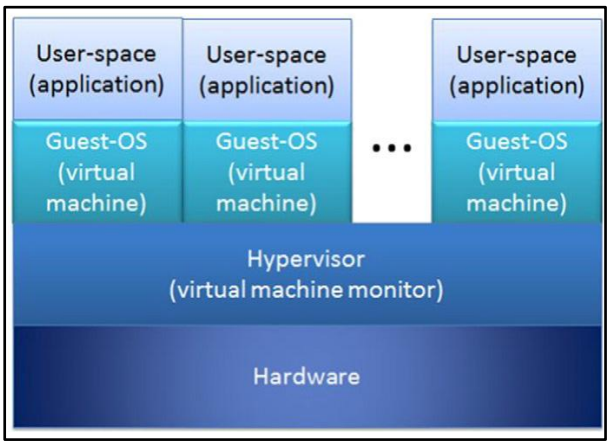

Figure 2.1: Overview of virtualization environments

(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 2.2 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.

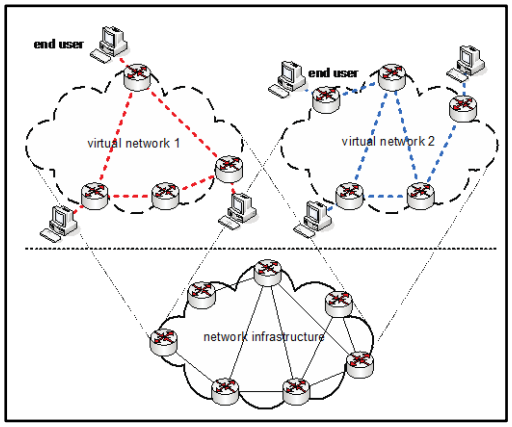

Figure 2.2: Virtualized network infrastructure, Adopted from (Source: Natarajan and Tilman, 2013)

III. METHODOLOGY

The research study proposed used a qualitative approach to conduct this research. This included reviewing published papers based on the virtualization and its associated security threats and vulnerabilities.

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 choice of security threats, attacks and vulnerabilities in virtual environments for SMEs. The findings were as follows:

Finding: there are various security threats and vulnerabilities in virtualized systems:

Security Issues in Virtualized Environments

In virtualization context, the virtual machines fundamentally pose a great threat in the first place. As the cloud provider increases the virtual machines, definitely some performance issues will begin crippling in immediately. For example as VMs continue to increase, factors such as CPU, Memory and I/O requests will automatically become bottlenecks. Therefore over-utilization of hardware resources in itself is a security threat of virtualization.

Virtualization sprawl or VM sprawl is another security concern in virtualization for SMEs. VM sprawl is defined as a large amount of virtual machines on your network without the proper IT management or control. For example, you may have cloud providers hosting multiple VMs from SMEsbut without proper procedures or control of the release of these virtual machines. Virtualization sprawl is a

phenomenon that occurs when the number of virtual machines (VMs) on a network reaches a point where the administrator can no longer manage them effectively. This can cause a serious security concern because unwarranted breaches will occur. Access control will definitely become unmanageable and in this scenario information will be compromised.

Another security threat in virtualization is data leakage. The unauthorized transfer of classified information from a computer or datacenter to the outside world. Data leakage can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding. In a virtualization scenario, data leakage means exposing customer's data or information to any other virtual machine on the multi-tenancy platform.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. In a virtualization scenario, this attack may affect the network facilitating the virtual servers. On the other hand virtual machines can attack one another or all VMs on the same physical server. This may bring the entire server down with all the hosted virtual machines for individual companies leading to unavailability of services.

In multi-tenancy, data remanence is another security threat which occurs when a VM is commissioned and later decommissioned for whatever reason. In this case while decommissioning, the owner of the VM may leave behind some traces or residual data and information which if accessed by unprecedented parties would cause a lot of harm especially to competing businesses. This can also expose the customer's data to unnecessary parties.

In virtualization, as customer's data keeps growing, it requires more storage to be allocated. Many cloud providers when faced with such challenges, they end up solving this by purchasing other storage facilities or servers in other cloud providers in the same location, different locations or even across the continent. This exposes

the customer's data or information to any security breaches that may arise depending on whoever accesses the data. This causes a serious privacy concern for users of virtual environments across world.

The host computer is today considered the most important asset in virtualization. This is because it is hosting many virtual machines and its monitors which may be as well be carrying many applications belonging to many businesses. It's important that the host computer is protected from security threats such as physical damage, denial of service attacks, access control and malicious infection. Different virtualization technologies have different implications for the host machine to influence the VMs up running in the system. Following are the possible ways for the host to influence the VMs:

- The host can start, shutdown, pause and restart the VMs.
- The host is able to monitor and modify the resources available for the virtual machines depending on the usage of host resources.
- The host may also monitor the applications running inside the VMs.
- The host can view, copy, and likely to modify the data stored in the virtual disks assigned to the VMs.
- The host can examine all the network traffic for all the attached VMs.

It is for this reason that the researcher discovered that the host can be the greatest security threat if it is not well protected. This would begin with the physical environment where the host is situated and the access control policies attached to it.

Other specific security concerns include:

- Hypervisor: multi tenancy can cause security breaches in virtualization. This is because competing corporates or businesses may load virtual machines with suspicious code with an intention of either sabotage or stealing secrets from the competitor company.
- SQL-injection and cross-site scripting security threats have become common for cloud hosting companies. This has necessitated the movement from relational database management

systems to fully object oriented database management systems.

- Network related threats. The communication environment that facilitates the virtual environments is also a security threat. In this case you may have a robust virtual system but weak network policies and access credentials. The attackers would still compromise on the poor network and its related hardware to cause security breaches to the virtual environment.
- Authentication: most cloud providers do not take into consideration security policies around authentication and authorization. This can be security threat if the cloud providers do not take measures towards authenticating VMs and even VMMs while structuring the virtualization. The access matric and frameworks may also be weak to allow a hacker to be able to gain control and compromise the virtual environment for a business.
- Lock-in: transfer of services between cloud providers exposes customer's data to unauthorized access.
- Inter-virtual communication: where necessary, the VMs may need to communicate with each other and share information such as threads resources and registers. This may cause a security breach where caution is not considered especially the operating system's kernel and system calls.
- Attacks between VMs or between VMs and VMM: an attack can occur if the VMs are not well structured and isolated. This may also happen to VMs and VMMs. The virtualization practitioners must put in place well-structured access policies to prevent inter attacks between these entities.
- Virtual machine escape: is the process of breaking out of avirtual machine and interacting with the host operating system. A virtual machine is a "completely isolated guest operating system installation within a normal host operating system. This gives the user a chance to take advantage and attack the operating system and thereby putting to risk all the other VMs accessing the system.

- Virtual machine isolation: The primary benefit of virtualization is isolation. If it does not deploy correctly then it can be a threat to the environment. The workload is separated amongst the VMs is one of the important issues in implementing the cloud. It can lead to data leakage and cross-VMs attack. So the isolation process should be configured carefully while deploying virtual machine in cloud infrastructure [15].
- VM Monitoring: In a virtual environment, the host machine considered as a control point and designed for monitoring the application running on the VMs. In general, all the traffic data is passing through the monitor host. There are many techniques that influence the host monitor machine, for example, the host can restart or shutdown the VMs, it cannot monitor the traffic in this span of time. Another way is that the host itself can sniff, alter, change, copy or delete the resources that are available in VMs (Li et al., 2012).
- Network security: In cloud computing, communication is via the internet and it is the backbone of the cloud environment. Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network. [17]focuses on the virtual network in a Xen platform by discussing and analyzing its security problems.

Virtual machine isolation: The primary benefit of virtualization is isolation. If it does not deploy correctly then it can be a threat to the environment. The workload is separated amongst the VMs is one of the important issues in implementing the cloud. It can lead to data leakage and cross-VMs attack. So the isolation process should be configured carefully while deploying virtual machine in cloud infrastructure [15].

VM Monitoring: In a virtual environment, the host machine considered as a control point and designed for monitoring the application running on the VMs. In general, all the traffic data is passing through the monitor host. There are many techniques that influence the host monitor machine, for example, the host can restart or shutdown the VMs,

it cannot monitor the traffic in this span of time. Another way is that the host itself can sniff, alter, change, copy or delete the resources that are available in VMs [16].

Network security: In cloud computing, communication is via the internet and it is the backbone of the cloud environment. Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network. According to [17] focuses on the virtual network in a Xen platform by discussing and analyzing its security problems.

All these security threats 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 evaluate security threats and vulnerabilities present in the virtualized environments in SMEs. Based on the objective under study the researcher describes the following threats and vulnerabilities.

According to [15] present a novel virtual network framework aimed to control intercommunications and provide high-security level. Some attacks like DoS or DDoS, DNS, ARP spoofing, IP spoofing phishing attack and port scanning are aimed to gain access to the resources in a cloud network.

Security is the biggest concerns for IT businesses who are considering to join the virtualized systems and environments and by extension cloud users. Currently, security is one of biggest obstacles for cloud computing service adoption.

Security issues in the cloud environment are caused by its essential characteristics such as resource pooling, virtualized nature, elasticity, and some measured services.

There was an increase of 70% Advance Persistence Threat (APT) attacks [18], 68% suspicious activities, and 56% brute force attacks on a cloud environment in 2015. APT attack is network attack in which an unauthorized identity gain access to a network and remain undetected for a long period. The International Data Center (IDC) is an analysis and research firm that takes the opinion of companies' chiefs on cloud challenges. The results show that security is most

concerned topic for 87% of respondents [19]; [30].

Some business organizations are reluctant to completely believe the third party service providers. Security in cloud computing is managed through policy and Service Level Agreement (SLA) which is the foundation of expectation of service between consumer and provider [31]. It is the common belief too many IT professional that cloud computing distributes the data openly at much higher risk [20].

Many researchers have studied and discussed the security issues of virtualization and cloud computing. Fernandes et al. (2014) suggested making comprehensive reviews on cloud security issue, it addresses many several key topics namely threats, vulnerability, attacks proposing and taxonomy for their classification. According to [22] explained the security survey highlighted on communication, architectural, contractual and legal aspects. It also discusses the countermeasure for communication issues, it also surveys on the vulnerability of virtual machine like VM migration, VM image, hypervisor, and discusses security in future direction. According to [15] gave the detailed knowledge on critical infrastructure for the secure cloud. Moreover in [21] has emanated the security issue in service delivery models of cloud computing system and provide some solution regarding these issues.

According to [22] surveyed the most relevant privacy and trust issue and analyzing privacy, security and trust threats and provide solution a secure trustworthy and dependable system.

According to [23] surveyed critical privacy and security challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations, and envisioned future research directions.

According to [24] discussed recent developments in cloud computing, various security issues and challenges in cloud computing environment, various existing approach and solutions provided for dealing with these security threats and will deliver a comparative analysis of these approaches.

According to [25] provided a systematic review of security issues in clouds based on an attribute-driven

methodology. The attributes used were confidentiality, integrity, availability, accountability, and privacy-preservability. For each attribute, a few threats were reviewed along with the corresponding defense solutions.

The researches for virtualization have considered the unique advantages of empowered computing system, and a wide range of potential cloud applications have been recognized in the literature. One of the major drivers of cloud computing acceptance is economies of scale. It provides a pay-per-use type of service, thus eliminating the upfront investment in many cases.

Despite of all advantages, the lack of enthusiasm in other investigation topics shows that researchers are focused on the first mitigating security risks in virtualization instead of digging into their wide area of potential applications. Security practitioners must first address the security issues and concerns in virtualized environments first before a lot of investments can go into wide applications. This would allow a better and more secure deployment of clouds over the industry. Despite all security measures available nowadays to counterattack the many security issues, one should always have in mind that no system is 100% secure. Previous security researches and events have proven that, no matter what kind of new technology is invented, it may be flawed due to human error. This was the main motivation of this survey.

In this section, the researcher proposed a scheme in virtualization as far as security is a concerned. Virtualization is the important key component of cloud technology. It makes more efficient the system for a user who is sitting at a remote location. According to the CSA recommendations against the vulnerability in virtualization is as follow:

i. Securing each virtualized OS running on guest VMs
ii. That Virtual machine which is at rest should be encrypted.
iii. Evaluating risk associated with virtual technologies
iv. Securing all element of the virtual machine and restrict and protect the administrator to the virtual machine.
v. Awareness of security tools and techniques while deploying virtualization in cloud computing.

vi. Configuration, installation should be carefully planned while deploying it.

vii. Evaluate the hypervisor technologies and harden the hypervisor (VMM) and another component.

Evaluate the virtual network security feature and recognize dynamic nature of VMs. According to [26] considered the virtualization is the key element in future. The paper shows a lack of data control mechanism, hypervisor vulnerability, and the isolation solution virtual cloud environment. The author provides most popular isolated virtual machine is Xen, KVM, and VMware aiming to verify their security concern and availability solution. The privacy, encryption, and integrity check has been used to provide secured VMS runtime environment in the cloud [27]. The author proposed a scheme named a hardware- software framework in short Hyper Coffer which focuses integrity and privacy to tenant's VMs. Hyper Coffer retains the transparency between existing virtual machine and it can only trust the processor chip and assume no security in any external devices. Hyper Coffer architecture protects cache data, memory data, and CPU context when execution transfers from VM to the hypervisor. It also protects EPT-Extended page table of VMs and VM table for multiplexing. It introduces VM-Shim that runs between guest machine and hypervisor. For secure processor design, two techniques were reviewed AISE-based encryption and Bonsai Markely tree. Both used for encryption and integrity respectively.

According to [28] considered the complications of enabling a secure VM-vTPM migration protocol in a private cloud. The author used trusted computing technology to secure intra-cloud migration of VMs. It ensures data integrity, privacy, the freshness of data and secure mitigating information to the communication channel. Virtual trusted platform module vTPM key structure combined with the virtual machine to certify the integrity of VMs. Literature implements to evaluate the feasibility of proposed scheme on Xen Hypervisor and it is successful and securely migrated to the existing hypervisor.

A novel security solution of virtualization, which provides a widespread protection to the virtual environment, proposed in [32]. The author combines basically three technologies: first is Mandatory Access Control (MAC)-access of

resource is controlled and determined by administrator by the help of reference monitor, access enforcement hook, and access policy. Second one, Linux Security Module (LSM) – gives a function hooks which can place within kernel and run as kernel module without causing any compatibility issue with the main Linux kernel. The third one is SELinux developed by NSA and works alongside DAC to provide fine-grained access of resources. The proposed solution also protects against guest VMs and hypervisor attack.

Live migration is an indispensable feature of a virtual machine that allows the movement the VMs from one physical host to another without halting the VMs. A framework is proposed in [29] for secure live migration in virtualization in cloud computing. The approach uses four next doors level of privilege covers starting, stopping, pausing, executing, or getting information status information of VM. L4 defines end users who have no authority to access VMs command. The framework protects against unauthorized access, breach of confidentiality, integrity of live migrated data and network attack.

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 researcher evaluated the security threats, attacks, concerns and vulnerabilities in virtualized environments in SMEs. Later it proposed solutions that if well implemented would reduce the security risks involved in the virtualized environments.

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

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

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

[6] 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.

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

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

[2] 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.

[7] Emerson, Network Power white paper, Power Management Strategies for High-Density IT Facilities and Systems,

http://www.EmersonNetworkPower.com, 2007.

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

[11] 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.

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

[6] 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.

Singh A., An introduction to virtualization. Available at: http://www.kernelthread.com/publications/virtualization/ 2004.

Liu S., Z. Cai, H. Xu, and M. Xu, "Security-aware virtual network embedding," in 2014 IEEE International Conference on Communications.

[26] Gonzalez N, Miers C, Redígolo F, Carvalho T, Simplício M, Naslund M, Pourzandi M: **A quantitative analysis of current security concerns and solutions for cloud computing.** In *Proceedings of 3rd IEEECloudCom*. Athens/Greece: IEEE Computer Society; 2011.

[28] Danev, B., et al. (2011). Enabling secure VM-vTPM migration in private clouds. Proceedings of the 27th Annual Computer Security Applications Conference, ACM.

[29] Anala, M. R., Kashyap and G. Shoba, 2013. Application performance analysis during live migration of virtual machines. Proceedings of the 2013 IEEE 3rd International Conference on Advance Computing.

[30] Singh Vaishali and Pandey S.K., International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013

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, a Master of Science degree 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.