A Review of Adopter's Common Misconfigurations of Virtual Machines: The Case of Tanzania

S. Ally[1]., N.T. Jiwaji[2] and C. Tarimo[3]

[1]*The Open University of Tanzania, said.ally@out.ac.tz noorali.jiwaji}@out.ac.tz*
[2]*University of Dar Es Salaam, Tanzania, charles@udsm.ac.tz*

***Abstract**: Adoption and use of hypervisors and virtual machines have become heart of virtual server computing and are currently a primary choice to store and share data across different public and private sectors. However, one of the major security threats is on meager adopter's knowledge on proper handling of hypervisor installation, VMs creation and configurations. This paper exposes distinct security vulnerabilities of virtualized systems that are caused by the adopters due to various system misconfigurations such as use of unified installer across virtual infrastructure, level of security enhancement in type 2 hypervisors, presence of untouched default settings in open source hypervisors, usage of vendor lock in VMs file formats, ad hoc creation of VMs and allocation of computing resources especially virtual CPU, RAM and HDD. Furthermore, undecided size of key Linux directories including /home directory, /boot directory, /var directory, root (/) directory, /temp directory and swap have also been assessed. To undertake this study, server configurations in 15 public and 9 private organizations were screened. A total of 31 purposively selected server administrators were interviewed guided by a checklist of questions in a semi-structured questionnaire. A quick observation obtained from the findings of this study suggests that server virtualization adopters operate at high security risks due to existence of uncoordinated and unsecured VMs configuration due to lack of required expertise. Lack of regular system auditing and monitoring turn the adopters into vulnerable and target of attack at any time without the adopter's knowledge. The need for adopters to observe best practices towards adoption and use of virtualization software is vital.*

Keywords: *Adopter's malpractices, hypervisor, misconfigurations, security, virtual machine*

Introduction

Virtualization is one of the high growing computing technologies in the world. Virtualization of enterprise computing infrastructures provides

vast benefits to adopters. The most well-known benefits include efficient resource management and performance in a scalable and flexible way (Snyder *et al*., 2015). In terms of cost reduction as highlighted by Merrill and Heffernan (2011), Sgandurra and Lupu (2012), Fujitsu, (2013), by virtualizing server machines, adopters benefit from a significant cost reduction by up to 40% spent for physical space, power requirements, hardware, software licenses and personnel. Adopters have also witnessed security advantages as argued by Li *et al*. (2015).

Due to its vast benefits, server virtualization has received much attention among several technology adopters. Currently, the use of server virtualization is growing very fast where a big number of well-established million-dollar data centers of different sizes are now established everywhere on the globe. As pointed out by Bari (2013), the main catalysts for setting up these high performing computing infrastructures is the huge growth of data volumes and large variety of Internet applications. The acceptance and adoption of virtualization seems to grow consistently with no indication of any obstruction.
However, the move towards server virtualization has come with increasingly serious security concerns among researchers. As found from Shackleford (2015) when reviewing Verizon's 2011 data breach investigations report, 76% of all data breaches came from servers, with 29% of the breaches involving physical attacks. The report advocates that in 2012 about 60% of virtualized servers were less secure than the corresponding physical servers they replaced.

Attacks in hypervisors as engine part of virtualizing servers and their Virtual Machines (VMs) result from self-system design weaknesses or adopter's misconfigurations. For instance, hypervisor attacks due to adopter's misconfiguration of VMs that were discussed by Nazir and Lazarides (2016) include cloud burst and crisis malware. These VM attacks exist in virtualized computing environment and are determined to be the results of improper and unsecured practices towards VMs management. A crisis malware is a rootkit that uses fake installers to detect Operating Systems (OS) and spreads into VMs mostly using social engineering attacks. The penetration of malware is not due to security loopholes or vulnerabilities of the hypervisor in use; it is rather the use of the created VM forms which are just considered as files in disk of the host machine. A cloudburst on the other hand, is an exploit that causes a VM to attack its host hypervisor. This is also referred to as a VM escape, where attacker runs code on one VM and consequently causes an OS within VM to break out and interact directly with hypervisor, that is it provides access to the host OS and all other VMs running in the server.

Even though implementation of virtualization has proven to be particularly beneficial to information security, several ways have been used by attackers to compromise VMs (Li *et al*., 2015). Regardless of virtualization software applied and level of adopter's awareness, the trusted degree of security depends mostly on how adopters avoid configurations that attract malicious activities. Being a first-hand server infrastructure technology to most of the adopters, the adoption, configurations and usage of server virtualizations introduce clear security risks. Most studies have only focused on hypervisor systems security leaving VM misconfigurations to have not been dealt with in depth. So, in the light of managing virtual servers, concerns have been raised in identifying the most common VMs misconfigurations that would attract security attacks.

This paper assesses the pre-and-post virtualization processes by outlining all major issues from early hypervisor selection, creation and configuration of VMs and day-to-day management; all from the point of view of system security. This study has largely focused on assessing the adoption of open source-based hypervisors in which adopters are very flexible in changing VMs configurations and hypervisor settings compared to proprietary. It shows how open source-based server misconfigurations are prone to security attacks if not well handled. The wide range of constraints and security challenges can easily be witnessed in the usage of open source virtualized servers due to dynamicity, high dependency on the mobile patches and free online community support.

Hence, this paper outlines and discusses the common security vulnerabilities of the open source-based hypervisors at all stages of adoption and usage process focusing on the security threats due to adopter's inability to handle the entailed processes properly. With the aforesaid accomplished, the main contributions of the paper are three-fold: first, a review of VMs configurations threats; second, a comparative analysis of the VMs configurations for different adopters and highlight their security tradeoffs across multiple hypervisors in use. Finally, the identification of research gaps and provision of future research directions on matter in question. To the best of our knowledge, this work is the first to survey on the inappropriate server virtualization adoption processes and practices.

This work is based on a case study, whereby we outline and discuss key adopter's shortfalls in hypervisor adoption processes and configurations with respect to public and private adopters in Tanzania.

Related Works

More recent evidence reveals that hypervisors and VMs are prone to security attacks due to adopter's misconfigurations towards server management. Several studies, for instance Ramana *et al.* (2015) and Raz *et al*. (2015) have been carried out to assess possibility of security attacks due to configuration mistakes in virtualization systems. The attempt they have made justifies existence of misconfiguration issues in VMs and has drawn our attention to focus on finding out the key VM configuration issues that need proper handling.

The study by Mahjani (2015) and Lal *et al.* (2017) inform that some human mistakes may lead to configuration errors and consequently result in hypervisor vulnerabilities. The human mistakes are due to accidental or deliberate actions mainly characterized by low level of security awareness in virtualization software as studied by Ally *et al*. (2018) when reviewing security awareness status among public and private entities in Tanzania.

Security level in VMs is largely influenced by the type of hypervisor selected. Hypervisors exist in type 1 as a bare metal or native and type 2 as hosted. Normally hypervisor type depends on placement level on physical machine. Several studies have been conducted to assess security levels between two types of hypervisors. Researchers have always seen type 1 as more secured than type 2. For instance, Kim *et al*. (2017) concluded that type 2 is inherently less secure than type 1. A major defect of type 2 is because this type of hypervisor is typically managed by OS and does not have direct access with hardware as pointed out by Savage *et al*. (2016). While security level depends mostly on type of hypervisor selected, this raises many questions as to whether adopters are well informed on specific security configurations and trust level based on the type selected.

Considering well-grounded assumptions made by Kim *et al*. (2017), thorough security configurations might be seriously required for adopters of type 2 hypervisors. Some of the most common hypervisor products exist in the market include XenServer (Citrix, 2017), Xen (Xen, 2013), Proxmox VE (Proxmox, 2018), Nuxis (Eurotux, 2017), Window Server Hyper–V (Microsoft, 2018), and VMware ESX-ESXi (VMware, 2018) as type 1 hypervisors. The type 2 hypervisors include Oracle Virtual Box (Oracle, 2018), Kernel Virtual Machine (Chirammal *et al*. 2016; KVM, 2018), User Mode Linux (UML, 2018), Linux VServer (Linux VServer, 2017), Oracle VM Server for x86 (Oracle, 2017), and QEMU (2017).

A significantly high number of different type 1 and type 2 hypervisors in the field of server virtualization, one of the big challenges in VMs management especially across heterogeneous environment is on live migration process.

Practically, as explored by previous researchers, hypervisor adopters differ in knowledge level, techniques and usage of hypervisor technologies, thus possess different VMs file format. Consequently, managing diverse of VMs file formats is challenging. One of the pitfalls of managing multiple VMs file formats is in conversion process from one file type to another, a process which is time consuming and likely to introduce new security bugs if not well handled. A serious drawback has been principally discussed by Kargatzis *et al.* (2017) claiming that cloud providers differ in hypervisor types and image formats have their VMs tied up to a specific provider specification, hence becomes difficult in migration process to a provider of different infrastructure. Some of the common and well-known VM file formats include RAW, ISO, VHD, VMDK and QEMU Copy On Write (QCOW2) as listed by Kargatzis *et al*. (2017). This is one of the major issues that needs to be raised among researchers to assess whether adopters tend to downside VM configurations associated with file formats.

Another major drawback that may compromise hypervisor security performance is high number of created VMs with respect to amount of computing resources allocated such as virtual CPU, virtual HDD and virtual RAM. This setback was confirmed in the study of Garfinkel *et al*. (2005) by restating that total number of VMs created in any specific physical machine within organization can grow at an explosive rate, thus compromise security due to management challenges. Despite existence of automated functionalities in some administrative tasks, however a rapid growth of VMs has exposed number of security challenges especially those associated to upgrades, patch management, and configuration. As reported in the study by Wolke*et al*. (2015) the increase in number of VMs compromise security due to challenges in resource allocation especially if they are done in *ad hoc* way and not using proper decision support. There exist several decision support features that allows dynamic resource allocation. Some of these include algorithms such as First Come First Served (FCFS), Shortest Job First (SJF) algorithms (Sontakke*et al*., 2016), and Uncertainty Principle of Game Theory (Pillai*et al*., 2016) to mention but just a few. However, the use of dynamic resource allocation has also not received a required attention according to Wolke*et al*. (2015), thus attract attacks because most of the adopters do it manually.

Hence, security threats towards VMs can be looked at multiple perspectives; from early adoption and selection process, hypervisor configurations, and VMs creation and management. So, the parameters on which the security of these servers depend, vary from the existence and strict observance of the security principles and procedures guiding the adoption process and technical capability of the adopter on customizing and configuring the host and guest machines. The configuration threats depend mainly on the competency and skills required for handling the hypervisor default settings.

Materials and Methods

Sample and Sampling Techniques

The study was conducted in 15 public and 9 private organizations based in Tanzania to investigate a phenomenon that is adopter's proficiency towards implementation of virtualization. All 24 organizations have implemented virtualizations at different levels.

The major economic services of adopters include telecoms (mobile), finance, education, ICT firms and general social services. Table 1 shows a number of respondents for each adopter's category.

Table 1: Adopters Categories And Respondents

Adopter's Service	Adopters Category		Server Administrators
	Public	Private	
Telecoms (Mobile)	1	2	5
Finance	2	3	9
Education	3	0	3
ICT Firm	2	3	7
Social Service	10	1	7
Total	**18**	**9**	**31**

To ensure correct research data are gathered and maintained through flexibility in sampling process as presented by Silverman (2010), the selection of adopters and respondents was conducted based on theoretical and purposive sampling with main used criterion being virtualization usage.

To get high level of understanding on the likely hypervisor misconfiguration, 31 server administrators were interviewed in the study. The Admins are IT professionals involved in implementation of virtualization and have role of managing routine server operations in virtualized environment.

Demographic Profile of Respondents

Table 2 shows the experience of Admins in service and in using virtualization software based on the adopter's categories.

Table 2: Adopter's Experience In Virtualization Service

Adopter's Category	Experience (Years)	
	In Service	Using VMs
Telecoms (Mobile)	*8*	*4*
Finance	*10*	*5*
Education	*7*	*2*
ICT Firm	*6*	*4*
Social Service	*8*	*3*
Public	*8*	*3*
Private	*10*	*6*

Considering respondents experience in using VMs, the private adopters have more experience of twice as much compared to public adopters. Respondents from finance sector are mostly experienced in using VMs having average of 5 years followed by telecoms (mobile) and ICT firms both having average of 4 years. Results show that of the categories of respondents interviewed in the study, education sector has lowest experience of all, with average of 2 years. Table 3 shows the educational level of respondents.

Table 3: Educational Level Of Respondents

Educational Level	Adopters Category	
	Public	*Private*
Certificate	*0*	*0*
Diploma	*0*	*1*
Bachelor	*20*	*4*
Masters	*11*	*2*
PhDs	*0*	*0*

Educationally, majority of Admins possess Bachelor (24) and Masters' levels (13). While there was only one Admin with Diploma level, there was no respondent with either PhD or Certificate level. Despite of their educational levels, all respondents had computer science, IT or related disciplines.

Data Collection Methods

To undertake this study, data were collected using interview and in-depth discussion lasted for an average of 45 minutes. The interview was conducted using open ended checklist questions. Additionally, several

institutional reports were gathered and thematically analyzed. In some cases where permitted, a participant observation involving screening of server configurations was employed. Data collection exercise took four months from July to October 2017 with average of one week at each organization.

Findings

This section presents research results of various adopter's proficiency towards setting and configuration of hypervisors and VMs in public and private adopters in Tanzania.

Application Installations in Virtualized Environment

Under this aspect, the interest was to find out the mostly used approach for installing different software across virtualized servers. Two approaches used for assessment were the approach of straight application installation using a unified installer for all products, and the use of independent installer. The results are shown in Table 4.

Table 4: Installation Approaches In Virtual Infrastructures

Adopter's Category	Installer			
	In Service		Using VMs	
	N	%	N	%
Telecoms (Mobile)	2	22.2	3	16.7
Finance	3	33.4	5	27.7
Education	0	0.0	1	5.6
ICT Firm	2	22.2	5	27.8
Social Service	2	22.2	4	22.2
Total	**9**	**100**	**18**	**100**
Public	3	33.3	16	88.9
Private	6	66.7	2	11.1
Total	**9**	**100**	**18**	**100**

The results show that the unified installer for all VMs is used mostly in private organizations by 66.7% while the independent installer is mostly used in public organizations by 88.9% as indicated in Table 4. The motive behind private adopters to use a given installer over the other across multiple VMs is the perceived ease of use of the installer in simplifying system management task. This approach simplifies the task of server administrators especially if there are many VMs that require application installation. On the other hand, as shown in Table 4, the most common installation approach used in public organizations is the independent installer by 88.9%. Use of independent installer is a tedious

process for server administrators especially if there are a good number of VMs to be attended. From a security point of view, the two installation approaches possess different risk levels. While private adopters seem to enjoy simplicity in installation process, the chance that they operate with security risks is also high. This is due to the fact that unified installer across multiple VMs within the same virtual infrastructure brings possibility of introducing security bugs especially when the installer is not critically verified. With use of unified installer, adopters may easily suffer from VMs malfunctions due to attacks. The attacked VM turns to be a gateway of spreading bugs across network of VMs and their host machines.

The Hypervisor Types in Use and Security Comparison

Basically, the use of the two hypervisor types (type 1 and type 2) was assessed across different virtualization adopters. Table 5 shows the statistical usage for both types.

Table 5: Usage Of Hypervisor Types

Adopter's Category	Hypervisor Type			
	Type 1		Type 2	
	N	%	N	%
Telecoms (Mobile)	3	14.2	1	7.1
Finance	8	38.1	2	14.4
Education	1	4.8	0	0
ICT Firm	1	4.8	1	7.1
Social Service	8	38.1	10	71.4
Total	**21**	**100**	**14**	**100**
Public	12	57.1	10	71.4
Private	9	42.9	4	28.6
Total	**21**	**100**	**14**	**100**

From Table 5, while comparing extent of use of type 1 and type 2 hypervisors, type 1 hypervisor seen to be the most applied in both public and private sectors as well as in service-based adopters. For instance, in telecoms (mobile), finance, ICT firms and education sectors there is a more use of type 1 hypervisor than type 2. Surprisingly, type 2 hypervisors were found to be the most leading in other social service sectors. This result has further strengthened our confidence in use of type 1 hypervisor by most of adopters and is exactly in line with existing literature which claims type 1 to be highly secured compared to type 2. So, this finding confirms the usefulness of type 1 hypervisors over type 2 by Tanzanian adopters. Although high acceptance of type 1 hypervisors

assumes security advantages among adopters, it could nevertheless be argued that the trusted security level is only achieved by considering the way hypervisors are set and configured. This plays significantly major role in attaining the required security level. Hence, even though type 2 hypervisor is not widely used, however adopters may need to configure enhanced security settings to ensure created VMs are free from internal and external attacks. In line with this, the type of selected host OS is vital because type 2 hypervisors are structurally hosted by OS which possess different security levels of trust.

Comparing Hypervisor Software

As part of this study, identifying virtualization software currently in use in Tanzanian IT market is vital especially if adopters are concerned with security state of their VMs. Table 6 shows usage levels of different type 1 hypervisors across public and private sectors.

Table 6: Usage Of Type 1 - Hypervisor

Type 1 Hypervisor	Adopter's Category			
	Public		Private	
	N	%	N	%
Xen	7	25.9	2	10
Proxmox VE	2	7.5	5	25
Nuxis	0	0	1	5
Hyper – V	9	33.3	4	20
VMware ESX-ESXi	9	33.3	8	40
IBM System Z	0	0	0	0
Total	**27**	**100**	**20**	**100**

Generally, the results revealed that VMware ESX-ESXi leads in use by many adopters followed by Hyperv-V. However, in private adopters, the open source based Proxmox VE is a second leading after VMware. While, of the studied population, there is only one adopter of Nuxis, the IBM System Z hypervisor was also assessed but it is not used anywhere. Table 7 shows different type 2 hypervisors in use and their usage levels.

Table 7: Usage of Type 2 - Hypervisor

Type 2 Hypervisor	Adopter's Category			
	Public		Private	
	N	%	N	%
Oracle Virtual Box	5	29.4	2	18.2
KVM	9	52.9	4	36.4
UML	0	0.0	1	9.0
Linux VServer	1	5.9	2	18.2

Oracle VM Server for x86	1	5.9	0	0.0
MS Virtual PC	1	5.9	0	0.0
QEMU	0	0.0	2	18.2
Total	**17**	**100**	**11**	**100**

In contrast to results of type 1 hypervisors, for type 2 hypervisors there is a high usage of open source-based hypervisors in both public and private adopters. By comparing open source type 2 based hypervisors, we found KVM to be the most leading by far followed by Oracle Virtual Box (OVB). These results need to be treated with caution by adopters. Both KVM and OVB are type 2 hypervisors and are open source based, so a due care must be paid in throughout the adoption process and VMs configurations for adopters to attain a required security trust level.

The Number of VMs

Number of VMs is one of the determinants of server workloads. It is important for adopters to be sure of the number of VMs created on any single host. Understanding how the decision process is achieved for allowed number of VMs is also vital to avoid possibilities of *ad hoc* operations considering that VMs share computing resources. Given that the maximum number of VMs in any host machine depends on selected hypervisor and server specification for CPU, RAM and HDD, this does not preclude the importance of standardizing number of VMs on each host. This aspect is of unique importance especially when there is plenty of computing resources available to avoid unnecessary underperformance of VMs. Table 8 shows the current practices in creation of VMs among various public and private adopters.

Table 8: Number of Virtual Machines on Single Host by Adopters

Adopter	MEAN	MIN	MAX
Public	9	4	20
Private	31	7	100
Telecoms (Mobile)	34	6	100
Finance	16	7	30
Education	10	10	10
ICT Firm	10	4	15
Social Service	8	4	12

As seen from the Table 8, pubic adopters have VMs average number of 9 in any single host which is smaller compared to private adopters with

average of 31. Based on service role, the highest number of VMs in any single host has been observed from telecoms (mobile) companies with 100 VMs followed by finance/banks with 30 VMs. The smallest number of VMs per host is 4 observed from ICT firms and social service organization. What is surprising in our results is the high utilization of physical resources due to high number of created VMs per host. However, although our results signify maximum resource utilization by adopters, it was found that not all VMs were significantly required considering the size of organization and their workloads requirements.

So, it could nevertheless be argued that the number of VMs does not reflect the correct computing requirements by most of the adopters. As expected, although number of VMs on any single host depends on the available computing resources of the host machine, our results show that the *ad hoc* self-decisions made by server administrators play major role in VMs starvation due to resource scarcity

The VMs File Formats

Several VM file formats exist. The file types mostly depend on the type of hypervisor in use by adopting organization. Some of the file formats used for VMs storage include VMDK, VHD, VSWP, VMSS, VMEM, OVF, VMX, VMSD, VMSN and OVA. The results show that VMDK, VHD and VMX are generally the most used file types by public and private adopters investigated in the study. Of the studied organisations, the most common file format in private organizations is VMX followed by VMDK and VHD; while for public organizations, the most common VM file format is VMDK followed by VMX and VHD. The VMSD and VSWP file formats were not seen in any of the visited organizations. Furthermore, the file formats of VMSS, VMEM and VMSN are not at all used in any public organizations, while the same are used in at least one of the private organizations visited. Table 9 shows application of VM file formats across various adopters.

Table 9: Usage Of Virtual Machines File Formats

VM File Format	Adopter's Category			
	Public		Private	
	N	%	N	%
VMDK	12	41.4	4	19.0
VHD	6	20.7	4	19.0
VSWP	0	0	0	0
VMSS	0	0	2	9.5
VMEM	0	0	2	9.5
OVF	2	6.9	1	4.8

VMX	8	27.6	6	28.6
VMSD	0	0	0	0
VMSN	0	0	1	4.8
OVA	1	3.4	1	4.8
Total	**29**	**100**	**21**	**100**

The findings show that the common VM file format used in service providing organizations are VMX and VMDK. These are mostly used in finance/banks, followed by telecoms (mobile) companies and ICT firms. The VHD is mostly used by ICT firms and social service entities.

Assessing type of VM file format used by adopters is prime for facilitation of VM migration process between and within homogeneous or heterogeneous server infrastructures. It is apparently that in homogeneous infrastructure, VM migration is an upfront activity since file format is common for all VMs. However, there may be security risks during the file transfer between virtual servers of different hypervisors. The migration in heterogeneous environment requires VMs to be stored using an Open Virtualization Format (OVF) which ensures VM compatibility regardless of virtualization environment. When OVF is not deployed by adopters, the practices show that a special converter is used but rarely attain conversion of 100% accuracy. An OVF is an open standard for packaging VMs regardless of platform or processor architecture. Adopters may use OVFTool for VM conversion purpose. However, depending on converter type, the extent of retained accuracy level is not well known, hence lead to security concerns.

The VMDK files which are the most used formats in public organizations are compatible with MS Windows, Mac and Linux OS but the format works only for VMware and OVB hypervisors. The VMDK is well known as an open file format but it is not compatible with VHD format of Microsoft. Even though there is exceptional rapid expansion and growth of server virtualization and cloud computing technologies, the viable and foremost approach in setting up data centers uses heterogeneous server infrastructures with several hypervisors with different functionalities. Under this arrangement, the ideal way of securing VMs during migration process is to ensure VMs conform to OVF format. The evidence from this study points towards the fact that adoption of OVF is inevitable for wellbeing of virtualization security. To sidestep future VM migration challenges that adopters might face when hypervisor is no longer vendor-supported or when adopters fail to pay to renew software licenses, OVF is devised as an appropriate approach.

VMs Storage Methods

In this aspect, three main methods used for VM storage were assessed. These are the single storage/shared storage (SS/SS), multiple storage devices (MSD) and multiple storage devices with replication (MSDR).

A shared storage in virtualized environment is very important for attaining benefits of maximizing resources usage especially if there exist some applications which require less storage than others but the allocation during initial configuration was the same for all. So, with a shared storage, there is less need for direct-attached storage (DAS) in each physical server, which also simplify the management task; because storage is treated as a single logical resource that can be used by multiple servers based on demands. One of obvious management task simplified through use of shared storage is the automated VMs migration from one server to another without disrupting operations. Figure 1 below shows the structure of shared storage in virtualized environment.

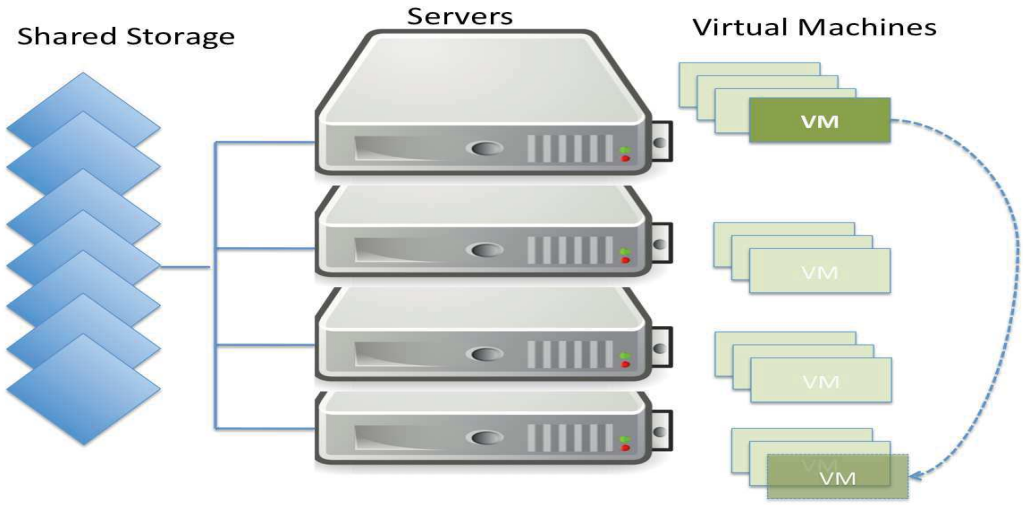

Figure 1: Shared Storage Structure

Based on the research results, the SS/SS storage approach is mostly used in public organizations by 50%, followed by MSDR with 31.8% and MSD 13.6%. In private organizations, the leading storage approach is MSDR by 38.5% followed by SS/SS 30.8% and MSD by 23.1%. For service organization, both MSDR and SS/SS are widely used in finance sector.

VMs Computing Resource Allocation: vCPU, vRAM and vHDD

Regarding aspect of computing resource allocation, the interest was to assess the adopter's practices towards allocation of virtual resources such as vCPU, vRAM, and vHDD and to check whether allocation is done

based on existing operational guidelines for VMs management and/or the available computing resources.

Generally, regarding allocation of vHDDs, data show that mean of virtual HDD size is 7065 GB in public and 2038 GB in private, but the average of maximum permissible virtual HDD in public institutions is 9 TB compared to 30 TB in private organizations. The highest allocation was captured in finance and telecoms (mobile) companies. For virtual RAM size, results show that the average between public and private adopters are the same but differ in minimum size where in public the minimum RAM size is 700 MB while in private is 4048 MB. Another most important aspect in allocation of virtual resources in VMs is the number of vCPUs. Results show that private adopters allocate higher average of vCPUs compared to public. The minimum number of vCPUs in public adopters is 2 while in private is 4. Through critical analysis of whole process of resources allocation on VMs by adopters, the practices show that resource allocations are generally done by server administrators with no consultation of technical decision committee, external experts or reference to any ICT related operational document. Surprisingly, adopters are less informed and are not sure whether allocation is done properly or not. This implies that there is *ad hoc* resource allocation process that may leads to server overloads or underutilization.

Furthermore, to find out whether there is association between the allocated size of vHDD for public or private adopters and for service-based organizations, a two-way ANOVA was computed as shown in Tables 10(a)–10(d):

Table 10(a): Allocated Virtual HDD (In GB)

Public Orgs.	**Mean**	**Std. Dev**	**N**
Finance	32108.00	36826.016	4
Education	30.00	.	1
Telecommunication	700.00	.000	3
Social Services	256.67	126.754	6
ICT	427.40	523.094	5
Total	**7065.21**	**20066.125**	**19**
PrivateOrgs.	**Mean**	**Std. Dev**	**N**
Finance	61.75	47.444	4
Telecommunication	8000.00	1414.214	2
ICT	30.00	14.142	2
Total	**2038.38**	**3718.376**	**8**

Both	Mean	Std. Dev	N
Finance	16084.88	29574.114	8
Education	30.00	.	1
Telecommunication	3620.00	4060.419	5
Social Services	256.67	126.754	6
ICT	313.86	469.099	7
Total	**5575.78**	**16969.122**	**27**

Table 10(b): Allocated Virtual HDD (in GB)

Tests of Between-Subjects Effects

Source	DF	Mean Square	F	Sig.
Corrected Model	7	487868598.198	2.277	.073
Intercept	1	239160133.364	1.116	.304
OrgType	1	310919574.749	1.451	.243
OrgService	4	358824506.886	1.674	.197
OrgType * OrgService	2	721489720.121	3.367	.056
Error	19	214297271.857		
Total	27			
Corrected Total	26			

a. R Squared = .456 (Adjusted R Squared = .256)

Table 10(c): Allocated Virtual RAM (in MB)

Public Orgs.	Mean	Std. Dev	N
Fin.	33500.00	59621.920	4
Edu.	4096.00	.	1
Tel.	8533.33	7685.687	3
Soc.	21088.00	23365.304	6
ICT	29759.20	31769.550	5
Total	23106.32	32681.742	19
PrivateOrgs.	Mean	Std. Dev	N
Fin.	12264.00	13798.776	4
Tel.	73000.00	77781.746	2
ICT	4048.00	.000	2
Total	25394.00	42686.184	8
Both	Mean	Std. Dev	N
Fin.	22882.00	41640.424	8
Edu.	4096.00	.	1

Tel.	34320.00	52809.282	5
Soc.	21088.00	23365.304	6
ICT	22413.14	28814.340	7
Total	23784.15	35087.784	27

Table 10(d): Allocated Virtual RAM (in MB)

Tests of Between-Subjects Effects

Source	DF	Mean Square	F	Sig.
Corrected Model	7	1119912049.134	.880	.540
Intercept	1	8657544066.273	6.806	.017
OrgType	1	150950022.435	.119	.734
OrgService	4	476873556.745	.375	.824
OrgType * OrgService	2	3416361586.094	2.686	.094
Error	19	1272135935.551		
Total	27			
Corrected Total	26			

a. R Squared = .245 (Adjusted R Squared = -.033)

Generally, a 2 (adopter's categories) by 5 (organization services) between–subject's factorial ANOVA was calculated comparing the size of the allocated virtual HDD (in GB) and virtual RAM (in MB) by virtualization adopters. From Table 10(b), the main effect for allocation of virtual HDD by adopter categories was not significant as value of $r = 0.243$ so, $(F(1,27) = 1.451, r > 0.05)$. As expected, size of the allocated virtual HDD on the side of the service based organization, the results show that the value of $r = 0.197$, hence, $(F(4,27) = 1.674, r > 0.05)$. However, interaction between organization type and organization service was slightly not significant $(F(2,27) = 3.367, r > 0.05)$ with value of $r = 0.056$.

From Table 10(d), the effect of allocation of virtual RAM by adopter categories was also not significant as value of $r = 0.734$ so, $(F(1,27) = 0.119, r > 0.05)$. This applied also when assessing adopters based on their services with value of $r = 0.824$, hence, $(F(4,27) = 0.375, r > 0.05)$. The interaction between organization type and organization service was also not significant $(F(2,27) = 2.686, r > 0.05)$ with value of $r = 0.094$.

These results appear to be surprising since neither value of allocated vHDD nor vRAM were found to have significant effects when assessed for adopter categories, organization services or combination of the two.

One clear interpretation of this result is the ad hoc allocation of computing resources in VMs. It cannot be ruled out that server administrators allocate virtual resources based on their will, determination and competency. This practice can easily compromise reliable VM performance and consequently circumvent a chance of one VM to control and consume all resources while leaving other VMs starving. This result suggests lack of clear guidelines for resource allocation and non-usage of virtualization calculator for better estimate of the required resources for each VM based on the hardware specification.

Linux Directories and VMs Creation

Another area where VM misconfigurations can be seen during installation process of the VMs in Linux environment. This involves allocation of virtual storage size in some important Linux directories which includes /home directory, /boot directory, /var directory, root (/) directory, /temp directory and swap. As seen from adopters, storage allocation of Linux directories is done in ad hoc method because majority of server administrators were found to possess less awareness of the criteria that guide allocation of storage size in /home, /boot, /var, root (/), /temp directories and swap. For instance, we found no correlation between size of /home directory and number of users the same as size of /var directory and number of running applications. Also swap size does not conform to specification of physical RAM, resulting into memory underperformance especially when the system runs out of memory.

Implication of these results offer vital evidence that some adopters still follow an old rule of thumb when deciding size of swap partition and physical RAM in which swap is twice size of RAM which works better for smaller RAMs of less than 2 GB. However, in a modern Linux system, swap space required depends mainly on memory workload whereby a memory between 2 GB and 8 GB, a swap size normally takes (equal) to RAM size while for all memories between 8 GB and 64 GB, at least 4 GB of swap space is required. This apparent lack of correlation between swap space and RAM size is justified by serious lack of proficiency where most adopters failed to associate them with whether hibernation is allowed or not.

Discussion

The results highlight that there is a little awareness of secure adoption and usage of hypervisor technologies by potential adopters in Tanzania. Our results demonstrated adopter's inability to properly carryout server

setup, hypervisor installation, VMs configurations and ad hoc allocation of virtual resources that does not consider the number of VMs. The current VMs configurations by most adopters are not ideal, instead we believe that they are exposed to VM hopping attack resulted from improper resource allocation which causes denial of service (DoS) attacks and consequently VMs starving. This analysis found evidence that creation of VMs is not controlled due to lack of virtualization security awareness by adopters.

Clearly, from this standpoint, adopters failed to provide proper monitoring of VMs performance. This happened because most adopters have not experienced VMs resource starvations due to vast available computing resources. Evidently, it is imperative to note that as computation demands expand, adopters will likely realize this problem. As seen from a two-way ANOVA statistical proof, allocation of vRAM and vHDD is not associated with adopters, thus justifying lack of a systematic way of resource allocation within studied organizations.

Another promising finding involved approach of application installation between public and private adopters. It is revealed that due to high usage of unified installers, private adopters are prone to attacks especially if they use un-trusted and unverified unified installers. This result suggests high VM vulnerabilities in VM escape attack where malicious VMs may attack the underlying host hypervisor after receiving security bugs from unified installers. On the other hand, high usage of type 2 hypervisor in public adopters (71.4%) implies low level of security skills for type 2 hypervisors. While security vulnerabilities of type 2 hypervisors are unquestionably, it remains unclear to whether adopters are aware or not of security risks associated with host OS. The fact that adopters of type 2 hypervisors cannot rule out security influence of host OS due to its high dependency, we found lack of a thorough security analysis of specific host OS by most of adopters.

Furthermore, based on research findings, although high usage of KVM and OVB as most leading type 2 hypervisors bring open source advantages, we still believe that adopters are highly vulnerable and operate in high risk of malicious attacks related to open source usage due to untouched default settings, hypervisor immaturity, and add-on patches and upgrading process. The evidence from this study points towards critical security concerns arises from vendor lock in based VM file format. The results indicate that adopters rarely use OVF system for VM flexibility during migration process. This goes in line with

configuration malpractices on deciding size of Linux directories such as /home directory, /boot directory, /var directory, root (/) directory, /temp directory and the swap. The criteria for deciding storage size are either unknown or not followed.

Conclusion

This paper has given an account of critical assessment of the adopter's proficiency in configuration of virtualized server systems by the Tanzanian organizations. The evidence from this study points towards the idea that Tanzanian adopters of server virtualization lack necessary skills required for secure implementation of hypervisor and VMs configuration. The upshot of this is the high security risk operation for both public and private adopters on one side, and service-based organizations on the other side, however, the results should be applicable to any developing country with similar computing infrastructures.

Based on the investigations from this study, adopters need to be aware of the security issues associated with their actions for them to gain intended benefits. Further study of this issue would be of interest and is still required especially on assessment of configuration issues for the specific used hypervisor. Extending this research appears fully justified in assessing suitability of various open source solutions in data sensitive applications. It also opens a variety of new research challenges in Tanzanian context where this field is largely taking control of the established data centers.

Acknowledgment

We would like to acknowledge The Open University of Tanzania for financial support.

References

Ally, S., Jiwaji, N. T. and Tarimo, C. (2018). Security awareness in virtualized server-based computing: A focus on threat sources and attack types in hypervisors, *Tanzania Journal of Science and Technology* – in Press.

Bari, F., Boutaba, R., Esteves, R., Granville, L. Z., Podslesny, M., Rabbani, G., Zhang, Q. and Zhani, M. F. (2013). Data center network virtualization: A survey, *IEEE Communications Surveys & Tutorials*, 15 (2), Second Quarter 2013 909; DOI: 10.1109/SURV.2012.090512.00043

Chirammal, H. D., Mukhedkar, P. and Vettathu, A. (2016). Mastering KVM virtualization, 1st Edition, ISBN 978-1-78439-905-4, PACKT Publishing, Birmingham, UK.

Citrix (2017). XenServer Open Source Virtualization, Citrix Systems https://xenserver.org/, Date Accessed 8/9/2017

Eurotux (2017). Nuxis-integrated solutions-Nuxis hypervisor, http:// nuxis.com Date Accessed: 12-Nov-2017

Fujitsu, (2013). "*Desktop Virtualization with Citrix*", White Paper, www.fujitsu.com/fts,

Garfinkel, T. and Rosenblum, M. (2005). When virtual is harder than real: security challenges in virtual machine-based computing environments. In HotOS. 2005.

Kargatzis, D., Sotiriadis, S. and Petrakis, E. G. (2017). Virtual machine migration in heterogeneous clouds: from openstack to VMWare. *In Sarnoff Symposium*, 2017 IEEE 38th, pp. 1-6. IEEE, 2017.

Kim, G., Lim, J. and Kim, J. (2017). Mobile security solution for sensitive data leakage prevention.*In Proceedings of the 5th International Conference on Communications and Broadband Networking* (pp. 59-64). ACM.

KVM (2018). Kernel Virtual Machine-Type 2 OSS hypervisor, https://www.linux-kvm.org/, Date Accessed: 22-Jan-2018

Lal, S., Kalliola, A., Oliver, I., Ahola, K. and Taleb, T. (2017).Securing VNF communication in NFVI.*In Standards for Communications and Networking (CSCN)*, 2017 IEEE Conference on, pp. 187-192. IEEE

Linux (2017).Linux VServer-OSS type 2 hypervisor, http://linux-vserver.org/, Date Accessed: 22-Nov-2017.

Li, S., Yen, D. C., Chen, S., Chen, P., Lu, W. and Cho, C. (2015).Effects of virtualization on information security, *Computer Standards & Interfaces* 42 pp. 1–8, Computer Standards & Interfaces.

Mahjani, M.(2015). Security issues of virtualization in cloud computing environments. Master Thesis for award of Master of Science in Information Security degree at Lulea University of Technology, Sweden. 62pp.

Merrill, D. and Heffernan, M. (2011). Hypervisor economic-Aframework to identify, measure and reduce the cost of virtual machines. Hitachi Data Systems, [https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/partners/hitachi/vmware-hypervisor-economics.pdf] site visited on 15/06/2017

Microsoft (2018). Window Server (Hyper–V hypervisor), Type 1 proprietary hypervisor, https://www.microsoft.com/en-us/cloud-platform/server-virtualization, Date Accessed: 22-Jan-2018

Nazir, S. and Lazarides, M. (2016). Securing industrial control systems on a virtual platform-How to best protect the vital virtual business assets", White Paper, FIRSTCo

Oracle (2017).Oracle VM Server for x86- Application-Driven Virtualization, https://www.oracle.com/virtualization/vm-server-for-x86/index.html, Date Accessed: 22-Nov-2017

Oracle (2018).Oracle Virtual Box - Type 2 OSS hypervisor, https://www.virtualbox.org, Date Accessed: 22-Nov-2017

Pillai, P. S. and Rao, S. (2016). Resource allocation in cloud computing using the uncertainty principle of game theory. *IEEE Systems Journal* 10 (2) (2016): pp. 637-648.

Proxmox, V.E. (2018). Proxmox - powerful open-source server solutions-Type 1 OSS hypervisor, https://www.proxmox.com/en/, Date Accessed: 12-Jan-2018

QEMU (2017).Open SourceQuick machine emulator, https://www.qemu.org, Date Accessed: 22-Nov-2017

Ramana, V. V., Reddy, Y. S., Reddy, G. R. S. and Ravi, P. (2015). An assessment of virtual machineassails.*International Journal of Advanced Technology in Engineering and Science,*www.ijates.com, 3 (1),.315–320

Raz, O., Amnon P. and Erez, B. (2017).Methods for effective network-security inspection in virtualized environments. *U.S. Patent* 9,672,189.

Savage, B. C., Kellam, S. L. and Grant, E. A. (2016). System, method, and computer-readable medium for performing automated security validation on a virtual machine." U.S. Patent 9,516,063.Washington, DC, U.S. Patent and Trademark Office.

Sgandurra,D. and Lupu, E. (2012). Evolution of attacks, threat models and solutions for virtualized systems*, ACM Computing Surveys*, 48(3),1-35, DOI: http://dx.doi.org/10.1145/0000000.0000000

Shackleford, D. (2015). Learn the essentials of virtualization security, *HY Trust, Cloud Under Control*, White Paper

Silverman, D. (2010). Doing qualitative research – A practical handbook. 3rd edition, ISBN: 978-1-84860-033-1, SAGE Publications Ltd

Snyder, B., Ringenberg, J., Green, R., Devabhaktuni, V. & Alam, M. (2015).Evaluation and design of highly reliable and highly utilized cloud computing systems. *Journal of Cloud Computing,* 4(1), 11.

Sontakke, V., Patil, P.,Waghamare, S., Kulkarni, R., Patil, N. S., Saravanapriya, M., and Scholar, U. G. (2016).Dynamic resource allocation strategy for cloud computing using virtual machine environment. *International Journal of Engineering Science* 4804.

UML (2018).User mode Linux - Type 2 OSS hypervisor, http://user-mode-linux.sourceforge.net, Date Accessed: 22-Jan-2018

VMware (2018).VMware Cloud-Type 1 proprietary hypervisor, https://www.vmware.com, Date Accessed: 22-Jan-2017

Wolke, A., Tsend-Ayush, B., Pfeiffer, C. and Bichler, M. (2015). More than bin packing: Dynamic resource allocation strategies in cloud data centers. *Information Systems* 52 (2015): 83-95.

Xen (2013).Open Source Virtualization - Xen Project, https://www. xenproject.org, Date Accessed: 22-Nov-2017