African Journal of Computing & ICT

www.ajocict.net

Security Management of Infrastructure as A Service in Cloud Computing

B.O. Lawal
Computer Science Department,
Olabisi Onabanjo University Consult, Ibadan, Nigeria
lawal5@yahoo.com

C. Ogude
Department of Computer Science
University of PortHarcout
Port Harcourt, Nigeria

K.K.A. Abdullah
Department of Computer Science
Olabisi Onabanjo University
Ago-Iwoye, Nigeria

ABSTRACT

Cloud Computing represents a new computing model that poses many demanding security issues at all levels, e.g., network, host, application, and data levels. The variety of the delivery models presents different security challenges depending on the model and consumers' Quality of Service (QoS) requirements. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. This paper presents a study of IaaS components' security and determines vulnerabilities and countermeasures. Finally, a Security Model for IaaS (SMI) was proposed to guide security assessment and enhancement in IaaS layer.

Keywords: Cloud Computing security, Infrastructure as a Service, IaaS Components, Threats, Security Management of IaaS.

African Journal of Computing & ICT Reference Format:
B.O. Lawal, C. Ogude & K.K.A. Abdullah (2013). Security Management of Infrastructure as A Service in Cloud Computing. Afr J. of Comp & ICTs. Vol 6, No. 5. Pp 137-146.

1. INTRODUCTION

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization [1]. Software, Platform, and Infrastructure as a Service are the three main service delivery models for Cloud Computing. Those models are accessible as a service over the Internet [2]. It's a pay-per-use model in which the Infrastructure Provider by means of customized Service Level Agreements (SLAs) offers guarantees typically exploiting a pool of resources. Organizations and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. From one perspective, cloud computing is nothing new because it uses approaches, concepts, and best practices that have already been established.

From another perspective, everything is new because cloud computing changes how we invent, develop, deploy, scale, update, maintain, and pay for applications and the infrastructure on which they run. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. IaaS provides simple provisioning of processing, storage, networks, and other fundamental computing resources over a network. With IaaS, IT services can be delivered as a subscription service, eliminating up-front costs and driving down ongoing support costs (enabling companies to make a strategic shift from a CAPEX to OPEX-based business model).

© 2013 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

As with managed hosting, IaaS providers keep costs low by pooling resources and giving customers access to a shared facility. But a major difference is that IaaS resources are elastic and available on a selfservice, on-demand basis. While IaaS providers often differ in their specific offerings, key features of all IaaS models include: Instant deployment, Ability to rapidly scale, Lower TCO and Predictable uptime. Infrastructure-as-a-Service (IaaS) represents a new consumption model for the use of IT resources. An IaaS provider offers customers bandwidth, storage and compute power on an elastic, on-demand basis, over the Internet.

Companies' reasons for choosing an IaaS environment differ, depending on the size of the organization and the nature of the business. Cost is often the primary reason. For Small and Medium Businesses (SMBs) with a limited capital budget, IaaS shifts the capital requirement to an operational expense that tracks with the growth of the business. Even among large enterprises, infrastructure costs are a driving force for considering IaaS.

IaaS' other key benefits include improved cashflow, accommodation of widely inaccurate provision planning, and exceptional transparency in utilization and costs.Traditionally, companies met their growing IT needs by investing in more capital equipment. Today, competitive pressures continue to demand improvements in quality of service despite growing numbers of users and applications. At the same time, the challenging economic environment has increased pressure on IT departments to keep costs down.

The convergence of those trends, with other advances of the last several years, has made it possible to take infrastructure outsourcing to a new level. Building on the foundation of managed services such as collocation, hosting, and virtualization services, Infrastructure-as-a-Service (IaaS) has emerged as an easily deployed service that enables companies to flexibly and cost-effectively anticipate and evolve with their customers' rapidly changing business requirements.

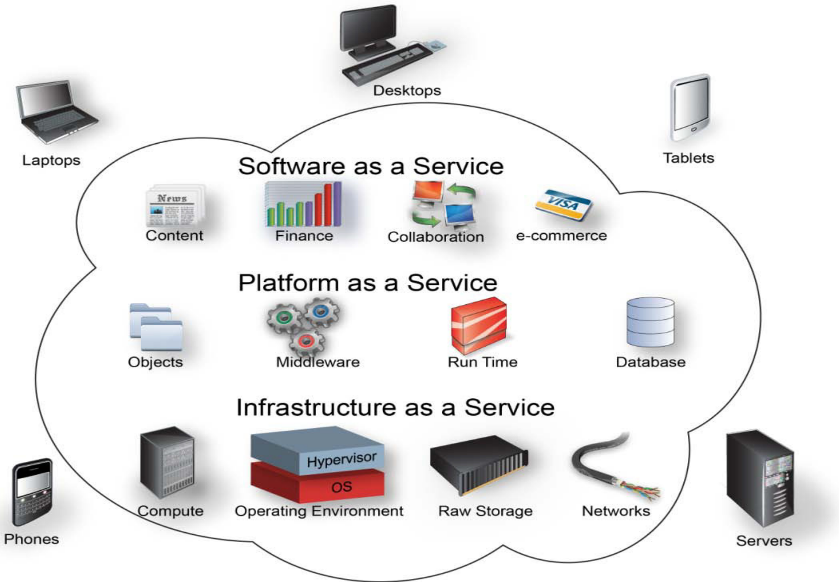

Figure 1. The three deployment methods for cloud computing environments are IaaS, PaaS, and SaaS [3]

The rest of the paper is organized as follows. Section 2 introduces IaaS platform within the cloud. Section 3presents a guide of choosing a cloud provider. In section 4 we present detailed components of infrastructure as a service. The challenges encountered in managing complexity were presented in Section 5. Section 6 presents the proposed security model for IaaS and conclusion in section 7.

2. IAAS: THE CORE OF CLOUD COMPUTING

Infrastructure can be considered as any hardware or software resource used to either execute and/or control the complete computational operations [4]. Infrastructure as a Service (IaaS), thus, can be explained as a mechanism of renting the infrastructure to the end user for carrying infrastructure dependent work on the said infrastructure without implementing infrastructure.

This helps user to concentrate on the work and frees user from the overhead of implementation of the required infrastructure to carry infrastructure dependent work. User is charged generally on pay per use basis or depending upon the contract conditions (Service level Agreements (SLA)) between user and infrastructure provider [4].

3. CHOOSING A CLOUD PROVIDER

Each provider serves a specific function, giving users more or less control over their cloud depending on the type. When choosing a cloud provider, it is important to compare the needs to the cloud services available. The cloud needs will vary depending on the intended use of the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if it will be used for business. Keeping in mind that the cloud provider will be pay-as-you-go, meaning that if the technological needs changes at any point more storage space (or less for that matter) can be purchased from the cloud provider [5].

Many people believe that cloud computing is just server virtualization, but cloud computing is much more than just server virtualization. Virtualization plays a huge role in cloud computing, and you can't have the cloud (at least not securely and cost effectively) without virtualization, but you can have virtualization without the cloud. Cloud computing is a delivery and consumption model, whereas virtualization is a technology that enables that model [5].

There are three types of cloud providers that you can subscribe to: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three types differ in the amount of control that you have over your information, and conversely, how much you can expect your provider to do for you. Briefly, here is what you can expect from each type [5].

1. Software as a Service - A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud [5].

2. Platform as a Service - A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.

3. Infrastructure as a Service - An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software, that they need.

Going down the list from number one to number three, the subscriber gains more control over what they can do within the space of the cloud. The cloud provider has less control in an IaaS system than with an SaaS agreement [5].

What does this mean for the home user or business looking to start using the cloud? It means you can choose your level of control over your information and types of services that you want from a cloud provider. For example, imagine you are starting up your own small business. You cannot afford to purchase and store all of the hardware and software necessary to stay on the cutting edge of your market. By subscribing to an Infrastructure as a Service cloud, you would be able to maintain your new business with just as much computational capability as a larger, more established company, while only paying for the storage space and bandwidth that you use. However, this system may mean you have to spend more of your resources on the development and operation of applications. As you can see, you should evaluate your current computational resources, the level of control you want to have, your financial situation, and where you foresee your business going before signing up with a cloud provider.

After you have fully taken stock of where you are and where you want to be, research into each cloud provider will give you a better idea of whether they are right for you.

4. COMPONENTS OF IAAS

Figure 1 show a reference architecture that roughly shows the components common to many Cloud Computing platforms [7]. The reference architecture shown takes into account the ideas in similar reference architectures, such as those used by NIST [8], IBM [9] and the Cloud Computing Use Cases Group [10].

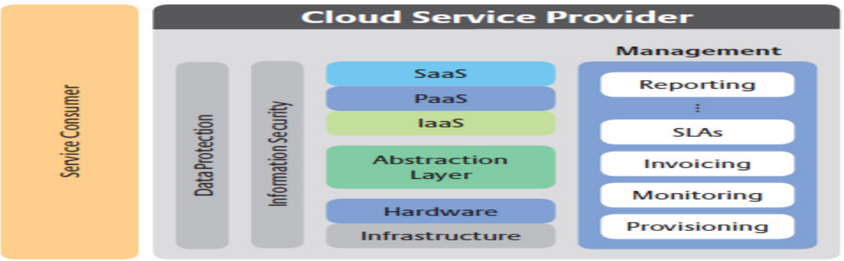

Figure 2: Reference Architecture for Cloud Computing Platforms [7]

IaaS delivery model consists of several components that have been developed through past years, nevertheless, employing those components together in a shared and outsourced environment carries multiple challenges. Security and Privacy are the most significant challenges that may impede the Cloud Computing adoption [11]. Breaching the security of any component impact the other components' security, consequently, the security of the entire system will collapse. In this section we study the security issue of each component and discuss the proposed solutions and recommendations.

A. Service Level Agreement (SLA)

Cloud Computing emerges a set of IT management complexities, and using SLA in cloud is the solution to guarantee acceptable level of QoS. SLA encompasses SLA contract definition, SLA negotiation, SLA monitoring, and SLA enforcement [12]. SLA contract definition and negotiation stage is important to determine the benefits and responsibilities of each party, any misunderstanding will affect the systems security and leave the client exposure to vulnerabilities. On the other hand, monitoring and enforcing SLA stage is crucial to build the trust between the provider and the client. To enforce SLA in a dynamic environment such Cloud, it is necessary to monitor QoS attributes continuously [12]. Web Service Level Agreement (WSLA) framework [13] developed for SLA monitoring and enforcement in SOA. Using WSLA for managing SLA in Cloud Computing environment was proposed in [14] by delegating SLA monitoring and enforcement tasks to a third party to solve the trust problem. Currently, cloud clients have to trust providers' SLA monitoring until standardizing Cloud Computing systems and delegating third-parties to mediate SLA monitoring and enforcement.

B. Utility Computing

Utility Computing is not new concept; it played an essential role in Grid Computing deployment. It packages the resources (e.g., computation, bandwidth, storage, etc...) as metered services and delivers them to the client. The power of this model lies in two main points: First, it reduces the total cost, i.e., instead of owning the resources, client can only pay for usage time (pay-as-you-go). Second, it has been developed to support the scalable systems, i.e., as an owner for a rapid growing system you need not to worry about denying your service according to a rapid increase of users or reaching peak in demand. Obviously, Utility Computing shapes two of the main features of the Cloud Computing (e.g., scalability, and pay-as-you-go).

C. Cloud Software

There are many open source Cloud software implementations such as Eucalyptus [15] and Nimbus [16]; Cloud software joins the cloud components together. Either Cloud software is open source or commercial closed source. We can't ensure the vulnerability and bugs in available software, furthermore, cloud service providers furnish APIs (REST, SOAP, or HTTP with XML/JSON) to perform most management functions, such as access control from a remote location [16]. For example, client can use the Amazon EC2 toolkits, a widely supported interface, to consume the services by implementing own applications or by simply using the web interfaces offered by the provider. In both cases, user uses web services protocols. SOAP is the most supported protocol in web services; many SOAP-based security solutions are researched, developed, and implemented [17]. WS-Security, a standard extension for security in SOAP, addresses the security for web services. It defines a SOAP header (Security) that carries the WS-Security extensions and determines how the existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages. Well known attacks on protocols using XML Signature for authentication or integrity protection [18] would be applied to web services consequently affecting the Cloud services. Finally, an extreme scenario in [19] showed the possibility of breaking the security between the browser and the clouds, and followed by proposal to enhance the current browsers security. Indeed, these attacks belong more to the web services world, but as a technology used in Cloud Computing, web services' security strongly influences the Cloud services' security.

D. Platform Virtualization

Virtualization, a fundamental technology platform for Cloud Computing services, facilitates aggregation of multiple standalone systems into a single hardware platform by virtualizing the computing resources (e.g., network, CPUs, memory, and storage). Hardware abstraction hides the complexity of managing the physical computing platform and simplifies the computing resources scalability. Hence, virtualization provides multi tenancy and scalability, and these are two significant characteristics of Cloud Computing.

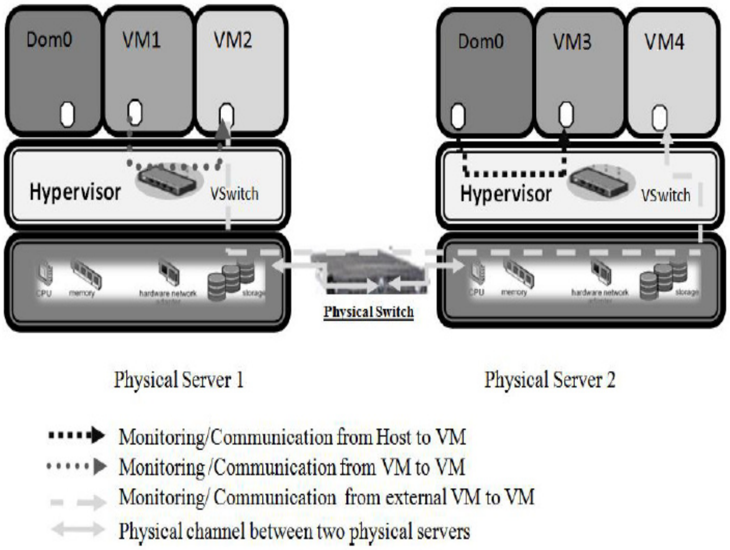
Dom0
VM1
VM2
Hypervisor
VSwitch
CPU
memory
hardware network
storage
Physical Switch
Dom0
VM3
VM4
Hypervisor
VSwitch
Physical Server 1
Physical Server 2
Monitoring/Communication from Host to VM
Monitoring /Communication from VM to VM
Monitoring/ Communication from external VM to VM
Physical channel between two physical servers

Fig. 3. The different types of interactions between VMs themselves and Host [2].

As the hypervisor is responsible for VMs isolation, VMs could not be able to directly access others' virtual disks, memory, or applications on the same host. IaaS, a shared environment, demands an accurate configuration to maintain strong isolation. Cloud service providers undertake a substantial effort to secure their systems in order to minimize the threats that result from communication, monitoring, modification, migration, mobility, and DoS.

Risks and vulnerabilities affecting particularly IaaS delivery model, according to [2], in addition to the recent proposed solutions to guarantee security, privacy, and data integrity for IaaS are here discussed.

1. Security threats sourced from host:
The threats sourced from host are result from monitoring, communication, or modification processes to VMs.

i. Monitoring VMs from host: Monitoring is considered an important procedure which includes control actions (e.g., start, shutdown, pause, restart the VMs), and VMs' resources modification. Unfortunately, the sysadmin or any authorized user who has privileged control over the backend can misuse this procedure. Xenaccess [20] is a tool allows sysadmin to run a user level process in Dom0 (i.e., a privileged domain in Xen) to access the memory of a customer's VM at run time. Here, it is important to know that Xenaccess is developed to run on Xen which was adopted by some of the initiative Cloud Computing providers (e.g. Amazon EC2 and Citrix7 are Xenbased).

ii. Communications between VMs and host: Communications between VMs and host flow between VMs through shared virtual resources (e.g., virtual network). Fig. 2 shows that all network packets coming from or going to a VM pass through the host, so the host is generally able to monitor network traffic of its hosted VMs. Attackers might exploit some useful features in virtual machine such as shared clipboard that allows data to be transferred between VMs and the host to exchange data between cooperating malicious program in VMs [21]. Nevertheless, the worst case occurs when a host is compromised, this puts all VMs in risk. Following the threats that originate from a host are the proposed solutions that prevent or mitigate these threats and vulnerabilities.

Solutions:
Terra [22] is an architecture presenting closed box execution environment for VMs to be protected from a user with full privileges (e.g., sysadmin), so VMs would not be inspected or modified by another VM running on the same platform even by a user with full privileges. Unfortunately, Terra is not suitable to be deployed in a complex dynamic environment like IaaS which comprises several hundreds of machines networked together. In IaaS environment, VMs are created and scheduled to dynamically run. Furthermore, serving huge number of consumers turns IaaS more vulnerable and less trusted. To overcome the drawbacks in traditional trusted platforms such as Terra, Trusted Virtual Datacenter (TVDc) [23],[24] technique is proposed to addresses both infrastructure and management security issues. (TVDc) manages the security in datacenter virtualization by enforcing a control access schemes to the networked storage based on security labels and by implementing management prototypes that demonstrate the enforcement of isolation constraints and integrity checking.

Similarly, Trusted Cloud Computing Platform (TCCP) [25] is proposed for ensuring the confidentiality and integrity of computations that are outsourced to IaaS services, the TCCP provides the abstraction of a closed box execution environment for a customer's VM. Like Terra, TCCP prevents the privileged administrator from inspecting or tampering VMs contents, on other words, TCCP is a solution for inside attacks that gain full privilege on systems. TCCP allows a customer to reliably and remotely determine whether the service backend is running in trusted environment before requesting the service to launch a VM. Moreover, this capability extends the notion of attestation to the entire service, and thus allows a customer to verify if its computation will run securely.

Using VLANs [26] to strengthen network isolation and enhance systems management capabilities was implemented by TVDs [23] and [24]. However, [27] described a technique to strengthen grid security by using Trusted Platform Module (TPMs) [28],[29]. TPM was proposed by The Trusted Computing Group (TCG) to provide cryptographic credentials, remote attestation, and integrity protection. It also could be employed in Cloud Computing to enable remote attestation like in Trusted Platforms [30] and [31].

2. Security threats sourced from other VM:

i. Monitoring VMs from other VM: As mentioned earlier, monitoring VMs could violate security and privacy, but the new architecture of CPUs, integrated with a memory protection feature, could prevent security and privacy violation. The hypervisor uses this to prevent a VM from monitoring the other VMs memory resources, and access other VMs' virtual disks allocated in the host. On the other hand, physical networking machines are connected by physical dedicated channel. However, in virtual networking, VMs are linked to the host machine by a virtual switch.

ii. Communication between VMs: The threats against the communication between VMs depend on how those machines will be deployed (e.g., Sharing a physical computer between multiple organizations). Sharing resources between VMs might expose security of each VM, for instance, collaboration using some applications such as a shared clipboard allows data to be transferred between VMs and the host assisting malicious programs in VMs to exchange data by which violate security and privacy.

[2] provided protecting *solutions* and techniques for securing communication between VMs as discussed below.

First, TVDc technique in [23] was extended in [24] to provide customer workloads isolation from each other to prevent data leakage, thus, it prevents VMs from spreading viruses and other malicious. Additionally, to prevent or mitigate the incidence of failed configuration management tasks, [24] proposed an isolation management policy for competing datacenter workloads and a continuous audit for dynamic cloud environment.

[31] proposed an IDS for Grid Computing and Cloud Computing environment. The proposed approach applies two intrusion detection techniques to the collected data from the cloud: (i) behavior-based method to verify user's actions correspond to known behavior profiles. (ii) knowledge based method to verify security policy violations and known pattern attacks.

A Security virtual machine (SVM) provides analysis of all virtual network traffic using Intrusion Prevention System (IPS) [32]. IPS, an advanced version of Intrusion Detection Systems, is capable of detecting and preventing both known and unknown attacks.

Also, Anti-DDoS Virtualized Operating System (ADVOS) [33] was recently proposed to secure networked computers against DDoS attacks. ADVOS integrates anti-DDoS capabilities in operating systems by performing packet filtering at the source computer itself to classify malicious traffic. Furthermore, the anti-DDoS was moved outside the host into independent domain to protect anti-DDoS from misbehaving by malicious code. ADVOS was not proposed to be used in Cloud, but we believe that ADVOS would be a feasible and an effective solution for DDoS in any virtualization environment especially for IaaS.

iii. Virtual machines Mobility: Mobility is an advantage feature that allows VMs to be transferred to other physical machines where the contents of the virtual disk for each VM are stored as a file. Mobility is essential for systems maintenance and load balancing, but it would be source of security risk (e.g., VM file can be stolen without physical theft of the host machine). The integrity of an offline VM might be compromised if the host is not secure and protected.

Denial of Service (DoS): Denial of Service (DoS) [7] attacks in virtual environment are a critical threat to VMs. These attacks can be an outcome of a hypervisor's misconfiguration that allows a single VM to consume all available resources, thus starving any other VM running on the same physical machine and avoiding network hosts to function appropriately due to the hardware resources shortage. However, Hypervisors prevent any VM from gaining 100% usage of any shared hardware resources, including CPU, RAM, network bandwidth, and graphics memory [11].

Additionally, an appropriate hypervisor's configuration enables extreme resource consumption detection to take the suitable solution, e.g., automatically restart the VM, nevertheless, restarting the VM has a smaller effect than restarting a physical machine, where VMs can usually be initialized much faster than physical machines because there is no need to initialize and verify hardware.

E. Networks & Internet Connectivity

To maintain availability and performance, cloud infrastructure spans multiple geographical sites to reduce the latency and the damage of unpredicted disasters. Each site connected locally as local area network is connected with the other sites by high speed Internet connections. These sites in total compose the cloud infrastructure which serves remote clients through the Internet. Thus, Cloud bequeaths both the conventional vulnerabilities of Internet and computer networks. IaaS model is vulnerable to DDOS, MITM, IP Spoofing, and Port Scanning.

For instance, a web-based code hosting service that uses both EC2 and the Amazon's Elastic Block Storage reported 19 hours of downtime as a result of a DDoS attack8. In addition to the external attacks (from the Internet), IaaS is exposure to internal attacks initiated from internal VMs against internal services. The internal attacks can be more severe than external attacks due to the system administrator's privileges on VMs that allow him to install and run any malicious applications. Furthermore, the dynamicity of IaaS environment (e.g., creating, removing, migrating VMs) adds more challenges to build defense plans against any attacks.

Solution:

Obviously, IaaS is more vulnerable to networks attacks than any other networked system; however, some of practical solutions and techniques for eliminating these attacks or reducing their impacts are listed as follows:

i. Logical network segmentation: A restrictive and a well planned network configuration should be applied in IaaS environment beside the hypervisor isolation power. VLAN offers isolated segments to prevent the external VMs from sniffing or monitoring internal traffic;

ii. Firewalls implementing: using firewalls enforce the organization's security policy by implementing rules to control the traffic based on protocol type, service port, and source IP address. Traditional three-tiered web applications architecture advised by Amazon AWS, could be a secure architecture for deploying applications such as in the next scenario. Port 80 (HTTP) and/or port 443 (HTTPS) should be accessible to the world and port 8000 should be accessible only to the web servers' group meanwhile port 3306 will be accessible only to the application servers' group. A well configured firewall for VMs instances level also is recommended to prevent all traffic except the required traffic.

iii. Traffic encryption: To access the outsourced infrastructure on the clouds, clients need secure channels to ensure privacy and integrity of the transferred data. VPNs provide encrypted tunnel between the client and the provider using Layer 2 Tunneling Protocol (L2TP) or Point-to-Point Transfer Protocol (PPTP), but, since these protocols are point to point, they cannot secure user's traffic inside the cloud.

iv. Network monitoring: In IaaS model, providers are responsible for network monitoring to sustain acceptable level of QoS. The monitoring process includes malicious activity, fault detection, and troubleshooting. In cloud, Network monitoring is not simple compared with traditional networks because cloud is geographically distributed and depends significantly on resources sharing. Furthermore, cloud infrastructure is a public environment containing multiple monitoring records refer to anonymous (users rent some resources for specific time then left). MapCenter and NetSaint are two examples of Grid monitoring systems.

F. Computer Hardware

IaaS offers an interface to a pool of distributed physical resources (e.g., Network Components, CPUs, and Storage Devices) and delivers a shared business model to serve multiple consumers. Virtualization, as seen previously, can keep a secure share of the computer resources and a controlled communication on hardware and network level. Even though the private organizations used to move the hardware components into locked rooms accessible only by the authorized and trusted persons to protect the resources, a study showed that over 70% of all attacks on organizations' sensitive data and resources occurred internally (i.e., from inside the organization itself) [34].

Computing resources: As discussed earlier, we consider that an attacker is able to access the machine physically. Depending on the goal of the attacker, we have multiple scenarios. First scenario is denying the service by turning off the machine or by removing any of hardware resources. This is not a common attack, but it can hurt the company's reputation. Hence, IaaS providers must carefully control the access to physical resources. Second scenario is accessing the physical machine to get or corrupt data for specific company benefit.

Storage resources: IaaS providers play an essential role in protecting clients' data. Whatever the level of the data security, it can be part of retired or replaced storage devices. Usually, companies don't have restrictive policy to manage the retired devices that could be accidentally devolved to untrusted people. Each organization is supposed to assure clients' data security along its life cycle. Encryption would be a good solution, but it might prevent the other users' accessibility to the data. To support multi parties' accessibility to encrypted storage, [35] propose architecture to mange encryption keys. Nevertheless, this approach increases traffic and degrade performance.

Transparent cryptographic file systems (NAS CFS) [46] provides a high security by using session ID and user ID for key management. The following table 1 summarises the discussion for IaaS threats and challenges and the proposed solutions by [2].

Table 1: Showing Threats/Challenges and Solutions of IaaS Components [2]

IaaS Component	**Threats / Challenges**		**Solutions**	
Service Level Agreement (SLA)	Monitoring and enforcing SLA. Monitor QoS attributes.		Web Service Level Agreement (WSLA) framework. SLA monitoring and enforcement in SOA.	
Utility Computing	Measuring and billing with Multiple levels of providers On-demand billing system availability.		Amazon DevPay.	
Cloud Software	Attacks against XML. Attacks against web services.		XML Signature and XML Encryption. SOAP Security Extensions.	
Networks & Internet connectivity	DDOS Man-In-The-Middle attack (MITM). IP Spoofing. Port Scanning. DNS security.		Traffic encryption. Network monitoring. Intrusion Detection System and Intrusion Prevention System (IPS).	
Virtualization Computer Hardware	Security threats sourced from host: -Monitoring VMs from host. -Communications between VMs and host. -VMs modification.	Security threats sourced from VM: -Monitoring VMs from other VM. -Communication between VMs. -Virtual machines Mobility -Resources Denial of Service (DoS). -VMs provisioning and migration.	Security threats sourced from host: - Trusted Cloud Computing Platform - Terra - Trusted Virtual Datacenter (TVDc) - Mandatory Access Control MAC	Security threats sourced from VM: -IPSec. -Encryption. -VPN. -Xen Security through Disaggregation. -LoBot architecture for secure provisioning & migration VM
Computer Hardware	Physical attacks against computer hardware. Data security on retired or replaced storage devices.		High secure locked rooms with monitoring appliances. Multi-parties accessibility to encrypted storage. Transparent cryptographic file systems. Self-encrypting enterprise tape drive TS1120.	

5. THE CHALLENGES OF MANAGING COMPLEXITY

In today's fast moving, highly competitive business environment, enterprises are running increasingly sophisticated and resource-intensive business applications (sometimes referred to in the IT industry as big compute, big data, and big pipe). The combination of comprehensive solutions and powerful IT technologies drives better business performance, helps customers optimize their IT investments, and use IT as a strategic differentiator. Since enterprise datacenters typically use a variety of operating systems and a mixture of server architectures running bare-metal and virtualized environments, datacenter managers frequently struggle with a fragmented management facility. Auch facility consisting of a variety of proprietary and single-purpose tools. These tools tend to be niche products and limited in scope, designed as they are to solve just one piece of a much larger puzzle [36]. Complicating the issue is the widespread use of virtualization technologies that help increase resource utilization and consolidate hardware resources in the datacenter. Virtualization imposes additional management requirements to handle dynamic resource allocation and often increases the number of systems to provision and support. Virtualization also blurs the lines between IT management responsibilities, making it less clear who handles storage, security, connectivity, and support when the server operating system is no longer tied to a unique hardware resource.

The result is a complex, hard-to-manage infrastructure that cannot scale to meet growing demand [36]. Furthermore, many of today's corporate departments and business units often lack the funding and resources to support their own IT infrastructure. As a result, a new paradigm for corporate IT is growing out of the recent wide-spread enthusiasm for cloud computing, specifically private clouds. IT managers, however, are concerned about the additional system management issues associated with the administration of clouds running mission-critical applications [36].

6. SECURITY MODEL FOR IAAS

Based on the research conducted by [1] and [2], a Security Model was proposed for IaaS (SMI) as a guide for assessing and enhancing security in each layer of IaaS delivery model as shown in Fig. 4. SMI model consists of three sides: IaaS components, security model, and the restriction level. The front side of the cubic model is the components of IaaS which were discussed thoroughly in the previous sections. The security model side includes three vertical entities where each entity covers the entire IaaS components. The first entity is Secure Configuration

Policy (SCP) to guarantee a secure configuration for each layer in IaaS Hardware, Software, or SLA configurations; usually, miss-configuration incidents could jeopardize the entire security of the system. The second is a Secure Resources Management Policy (SRMP) that controls the management roles and privileges. The last entity is the Security Policy Monitoring and Auditing (SPMA) which is significant to track the system life cycle. The restriction policy side specifies the level of restriction for security model entities. The level of restriction starts from loose to tight depending on the provider, the client, and the service requirements. Nevertheless, we hope SMI model be a good start for the standardization of IaaS layers. This model indicates the relation between IaaS components and security requirements, and eases security improvement in individual layers to achieve a total secure IaaS system.

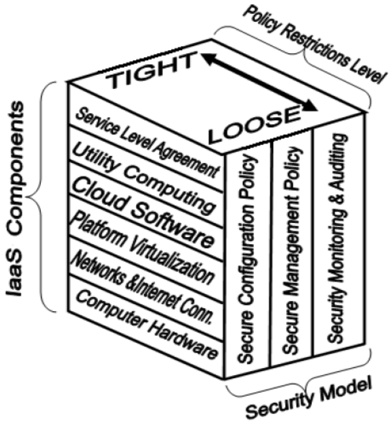

Fig. 4. Security Model for IaaS

7. CONCLUSION

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. Software, Platform, and Infrastructure as a Service are the three main services delivery models for Cloud Computing that are all accessible as a service over the Internet. Security professionals need to prepare to support internal and external clients. In This paper, focus was on the IaaS as a core area of cloud computing. We discussed the security issues of the components of IaaS within the cloud and proffered solutions to the threats and challenges of cloud infrastructure and proposed a security model for IaaS.

REFERENCES

[1] Pankaj A. et al (2012). Cloud Computing Security Issues in Infrastructure as a Service. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 1, January 2012, ISSN: 2277 128X. Available online at: www.ijarcsse.com.

[2] W. Dawoud, I. Takouna, C. Meinel. Infrastructure as a Service Security: Challenges and Solutions. Available at http://www.researchgate.net/publication/224136774_Infrastructure_as_a_service_security_Challenges_and_solutions/file/9fcfd50ead5ff22b8d.pdf

[3] An Oracle White Paper (April 2012). Making Infrastructure-as-a-Service in the Enterprise a Reality available at http://www.oracle.com/us/products/enterprise-manager/infrastructure-as-a-service-wp-1575856.pdf (visited 04-11-2013)

[4] Aniruddha S. R. and D.N.Chaudhari. Cloud Computing: Infrastructure as a Service. International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-3, February 2013

[5] N.Sainath, V. Narayandas, S.Jayakrishna and N. Aravind (2012) Analysis of Cloud Computing Security Considerations for Infrastructure as a Service. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622. Vol. 2, Issue 2, Mar-Apr 2012, pp.451-456. www.ijera.com

[6] Alexa Huth and James Cebula. The Basics of Cloud Computing. United States Computer Emergency Readiness Team-US CERT. Available at www.us-cert.govt /Tips _ US-CERT.htm.

[7] (Federal Office of Information Security White Paper. Security Recommendations for Cloud Computing Providers. Available at www.bsi.bund.de)

[8] Dr. Fang Liu, Jin Tong, Dr. JianMa, NIST Cloud Computing Reference Architecture, Version 1.0, March 2011. http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_CC_Reference_Architecture_v1_March_30_2011.pdf

[9] Mahesh Dodani: "Architected" Cloud Solutions Revealed, in Journal of Object Technology, vol. 9, no. 2, pages 27 – 36, March – April 2010. http://www.jot.fm/issues/issue_2010_03/column3/

[10] Whitepaper Cloud Computing Use Cases Version 3.0, produced by the Cloud Computing Use Case Discussion Group, February 2010. http://opencloudmanifesto.org/cloud_computing_use_cases_whitepaper-3_0.pdf

[11] P. Patel, A. Ranabahu, and A. Sheth, "Service Level Agreement in Cloud Computing," Cloud Workshops at OOPSLA09, 2009. [Online]. Available: http://knoesis.wright.edu/aboutus/visitors/summer2009/PatelReport.pdf

[12] SLA Management Team, SLA Management Handbook, 4th ed. Enterprise Perspective, 2004.
[13] G. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.
[14] P. Patel, A. Ranabahu, and A. Sheth, "Service Level Agreement in Cloud Computing," Cloud Workshops at OOPSLA09, 2009. [Online]. Available: http://knoesis.wright.edu/aboutus/visitors/summer2009/PatelReport.pdf
[15] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," Cluster Computing and the Grid, IEEE International Symposium on, vol. 0, pp. 124–131, 2009.
[16] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, 1st ed., 2009. [Online]. Available: http://books.google.com/books?id=BHazecOuDLYC&pgis=1
[17] R. Kanneganti and P. Chodavarapu, SOA Security. Manning Publications, 2008. [Online]. Available: http://www.amazon.com/SOASecurity-Ramarao-Kanneganti/dp/1932394680
[18] M. McIntosh and P. Austel, "XML signature element wrapping attacks and countermeasures," Workshop On Secure Web Services, 2005.
[19] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.
[20] B. D. Payne, "Xenaccess." Available: http://doc.xenaccess.org/
[21] J. Kirch, "Virtual machine security guidelines," 2007. [Online]. Available: http://www.cisecurity.org/tools2/vm/
[22] CISn VMn Benchmarkn v1.0.pdf
[23] T. G. Ben, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra:
[24] A Virtual Machine-Based Platform for Trusted Computing." ACM Press, 2003, pp. 193–206.
[25] N. Santos, G. P. Krishna, and R. Rodrigues, "Towards Trusted Cloud Computing," HotCloud'09, 2009. [Online]. Available: http://www.usenix.org/event/hotcloud09/tech/fullpapers/santos.pdf
[26] V. Rajaravivarma, "Virtual local area network technology and applications,"Proceedings The Twenty-Ninth Southeastern Symposium on System Theory, pp. 49–52, 1997.
[27] W. Mao, A. Martin, H. Jin, and H. Zhang, Security Protocols, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, vol. 5087.
[28] "Property-Based TPM Virtualization," Lecture Notes In Computer Science; Vol. 5222, 2008.
[29] V. Scarlata, C. Rozas, M. Wiseman, D. Grawrock, and C. Vishik, "TPM Virtualization: Building a General Framework," pp. 43 – 56, 2007.
[30] S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "vTPM:virtualizing the trusted platform module," USENIX Security Symposium, 2006.
[31] D. G. Murray, G. Milos, and S. Hand, "Improving Xen security through disaggregation," ACM/Usenix International Conference On Virtual Execution Environments, p. 9, 2008.
[32] X. Zhang, C. Li, and W. Zheng, "Intrusion Prevention System Design," CIT, 2004.
[33] S. Garg and H. Saran, "Anti-DDoS Virtualized Operating System," ARES, p. 7, 2008.
[34] E. Markatos, "Large Scale Attacks on the Internet Lessons learned from the LOBSTER project," Crete, Greece. [Online]. Available: http://www.ist-lobster.org/publications/presentations/markatosattacks.pdf
[35] L. Seitz, J.-M. Pierson, and L. Brunie, "Key Management for Encrypted Data Storage in Distributed Systems," SISW, 2003.
[36] An Oracle White Paper (April 2012). Making Infrastructure-as-a-Service in the Enterprise a Reality available at (visited 04-11-2013).

Author's Brief

Babatunde O. Lawal is a lecturer in Computer Science department at Olabisi Onabanjo University Consult, Ibadan, Nigeria. He received his Master of Computer Systems degree from University of Ibadan, Nigeria. He has worked as IT Support Officer and Database Administrator at Trans International Bank. His research interests are Database Management, Data Mining, Information Systems Management, Cloud Computing and Network Security. He can be reached at lawal5@yahoo.com or +2348038614477.