Vol 8. No. 1 – March, 2015
African Journal of Computing & ICT

www.ajocict.net

Imperatives for Security and Integrity Frameworks In Cloud Computing Environments

G.O. Odulaja & O.B. Alaba
Computer Science Education Department
College of Science & Technology
Tai Solarin University of Education
Ijagun, Ogun State, Nigeria
goddyseyi@gmail.com;; alabaob@tasued.edu.ng

O. Awodele & S.O. Kuyoro
Computer Science Department
School of Computing and Engineering Sciences,
Babcock University
Ilishan Remo, Ogun State, Nigeria.
delealways@yahoo.com; afolashadeng@gmail.com

ABSTRACT

Of note is the fact that lately, with the conspicuous presence and domineering influence of cloud computing (cloud for short), virtual computing resources, Information technology Services, data usage and storage are all undergoing paradigm shift as several of these resources and services move from on-premises to public cloud environments. As Cloud Computing Service Providers (CSP) take advantage of virtualization technologies, combined with Do-It-Yourself (DIY) capabilities, to offer to clients cost-effective access to computing resources via the internet, one consistent but major issue in cloud computing is security and integrity and they are interrelated. Security and integrity are serious issue here because they can determine level of acceptability and success of the emerging phenomenon. An insecure outlet cannot claim to have integrity. The converse is also true. This paper reviews security and integrity concerns associated with cloud computing services and environments and offers suggestions to maintain compliance with data security and integrity using a proposed model as virtual resources move from on-premise to public cloud environments.

Keywords: Cloud, Integrity, On-premise, security, Service Providers, Third Party Auditor (TPA)

African Journal of Computing & ICT Reference Format:
G.O. Odulaja, O. Awodele, S.O. Kuyoro & O.B. Alaba (2015). Imperatives for Security and Integrity Frameworks In Cloud Computing Environments Afr J. of Comp & ICTs. Vol 8, No. 1. Pp 69-.78 .

1. INTRODUCTION

Cloud computing can be described as online computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Virtualization (Hypervisor) and virtual appliances are the main features on which the cloud rides. Clouds can be classified as public, private or hybrid. The cloud is private if its infrastructures, services and other resources are entirely owned, controlled and meant to serve a particular enterprise exclusively. A private cloud allows the organization to manage its resources over its own private network. The company owns the service and defines which users can access it and how. Firewall secure and prevents external intrusion into the private cloud. Security risks are thus reduced since everything is managed inside the enterprise firewall allowing a fair use of the applications and the network bandwidth. Enterprises can deploy security protocols and monitor the levels of access to the information and resources available in private cloud. Users of private cloud, the tenants have relative flexibility on policies and procedures for provisioning, usage and security. The owner also controls the maintenance schedule and the upgrades. If hardware fails, the server is automatically booted on the remaining node. It provides direct access to the support team and helps to avoid the downtime. The private cloud works well for infrastructure when it comes to virtualizing servers. It is a good platform for organizations that want to implement the compliance. (Ngongang, 2011)

On the other hand in public cloud computing, the provider makes the resources available to the customers over a public network like the Internet. It owns and runs the technology to deliver the service and the consumers have no control over the operations of the service. Usually the documents of the company which uses the public cloud are stored outside its premises by a third party which they trust and this comes at a cost (Ngongang, 2011).

Hybrid cloud combines the features of both private and public clouds in that its functions, ownership and maintenance responsibility resonates between that of private cloud and public cloud. It is the combination of some private and or community clouds functioning collectively as one cloud and can be seen by the clients as a single entity. Hybrid cloud computing is a platform which interoperates between private cloud and public cloud. It is deployed by organizations, which do not want to put everything in the external cloud (public cloud) while hosting some servers in their own internal cloud infrastructure. The cloud providers are able to process applications which can work seamlessly between those boundaries [9].

In a case where the public cloud fails to handle an application, the request can be forwarded to the private cloud as shown in figure 1. The hybrid cloud validates the fact that not all information technology resources should remain in the public cloud today. When considering the security restrictions and the performance, the need of a private cloud is a fact today. It is imperative that enterprises know which kind of data can be kept locally and what can be processed remotely.

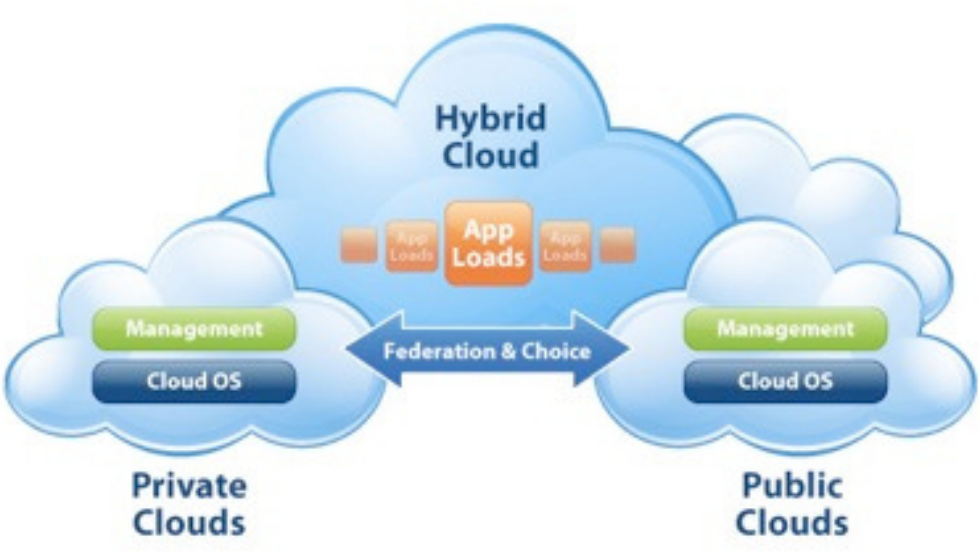

Fig. 1. Hybrid cloud computing (Source: Acute System Consulting)

1.1 Why the Cloud gains more Attraction

1. ***Infrastructural Convergence Benefits***
   Cloud computing relies on restricting sharing of resources to achieve coherence and economies of scale, over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.
2. ***No Requisite Knowledge of Technical Details before Deployment***
   The goal of cloud computing is to allow users to benefit from existing computing and communication technologies and paradigms without the need for deep knowledge about or expertise with each one of them.
3. ***Cost Effective***
   It can prove to be cost effective when enterprises take advantage of offers made by Cloud Service Providers. The clients can enjoy the flexibility and possibility of selecting from several available cloud computing resource options offered by the cloud. The cloud aims to cut costs, and help the clients focus on their core business instead of being impeded by IT obstacles. (Hamdaqa, 2012). Put simply, cloud computing, extends an enterprise's ability to meet the computing demands of its clients and everyday operations at much less cost. The time required to acquire, install and maintain IT infrastructure needed to run the enterprise is drastically reduced, thus saving the enterprise both time and money which can be used to improve and expand the business in other ways.

1. ***Reduced Fear of Failure and Redundancy****:* Fear of system failure or crash as a result of unanticipated or unpredictable down time or internal or external attack, malware attack and other probable dangers are also imperatives for leveraging unto cloud computing.
2. ***Wide Range of Network Access*****:** Cloud Services can be accessed using desktop computer and

mobile devices such as laptop, PDA, mobile phone, smart phones, tablets etc.

3. ***Resource Pooling*:** Provider resources are pooled to serve multiple clients
4. ***Regulated and Well-Controlled Service* –** there are standards established for measuring and billing services rendered.
5. ***Virtualisation Benefits***
   The main enabling technology on which the cloud rides is virtualization. Virtualization software multiplexes a physical computing device into one or more virtual copies of the same device, each of which can be easily used and managed independent of others to perform computing tasks. At operating system level, virtualization essentially brings about a scalable system of multiple independent computing devices, idle computing resources can thus be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization.
6. ***Autonomic Service on Demand* -** Autonomic computing automates the process through which the client is provided near real-time services on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors. (Hamdaqa, 2012).
7. ***Service-Oriented Architecture Benefits***
   When clients face difficult business tactical, strategic and IT problems, they could benefit from the Cloud's adoption of concepts from Service-Oriented Architecture (SOA) that can help the clients break these problems into services that can be integrated to provide a solution.
8. ***Service is Globally Available on Pay-Per-Use Model***
   Cloud computing offers all its resources as services, and follows the well-established standards and best practices of SOA to allow global and easy access to cloud services in a standardized way. Cloud computing also leverages concepts from utility computing to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models.
9. ***Flexibility and Scalability***
   Cloud offers flexibility and choice, mobility and scalability, all coupled with potential cost savings. Since measured services are an essential part of the feedback loop in autonomic cloud computing, this allows services to scale on-demand and to perform automatic failure recovery.
10. ***Dynamic and Mutually Beneficial***
    Cloud computing being a kind of grid computing that has evolved by addressing the QoS (quality of service) and reliability problems is able to provide the tools and technologies needed to compute intensive parallel applications real time at affordable prices to the benefit of the client. Resources are optimized and effectively shared resources with distance as no barrier. According to Hamdaqa (2012), "cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand." Consequently, both service providers of cloud services and patronizing individuals and enterprises can benefit from the coalition.
11. ***Capacity on Demand Offer***
    One of the significant benefits of leveraging to cloud computing include the fact that on-premise computing infrastructure can be expanded by adding capacity on demand. The model in the figure below from Wikipedia illustrates what the cloud can look like and can offer. (See figs. 2 & 3.)

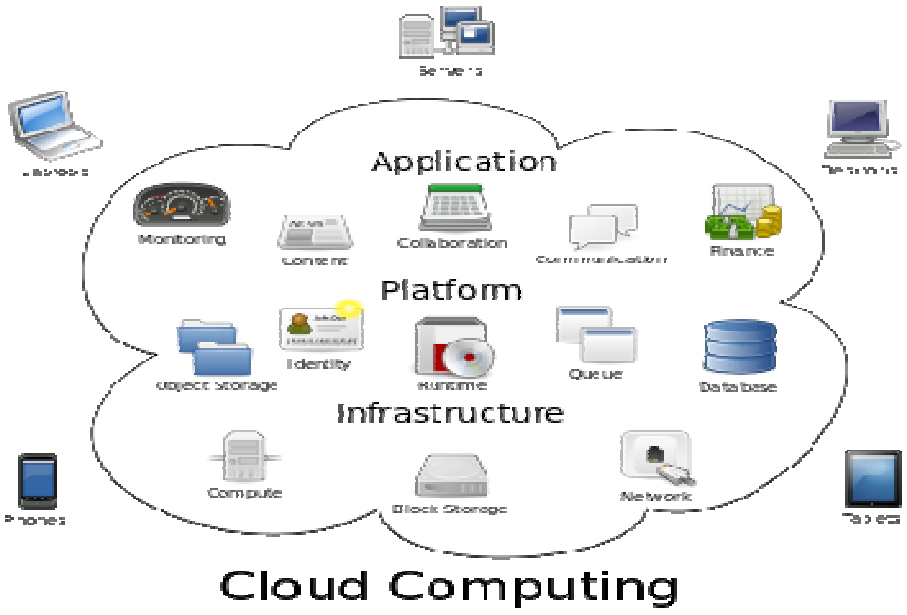

Fig. 2. Cloud Computing Model (Source: Wikipedia)

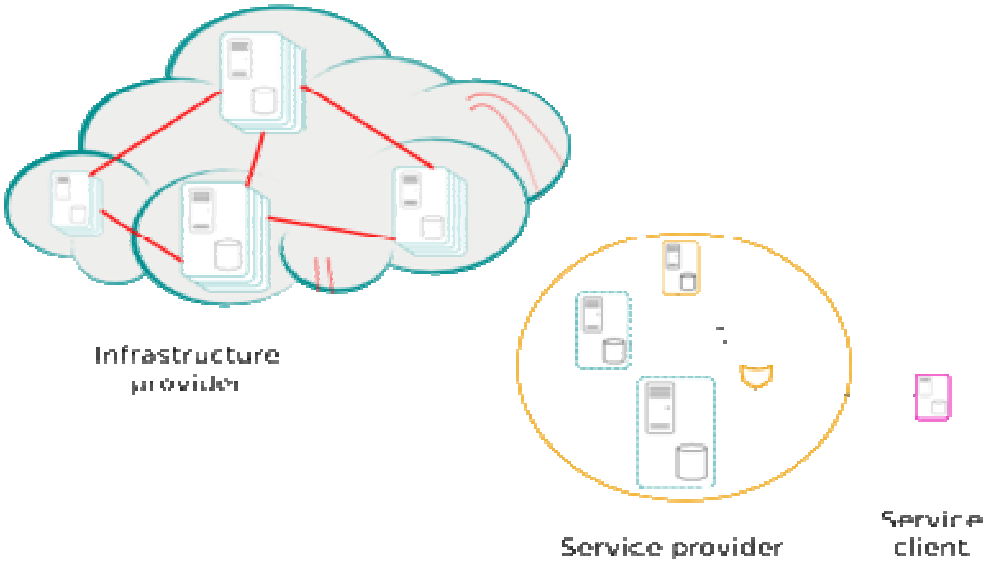

Fig. 3. Another representation of the cloud computing model. (*Source: Wikipedia)*

2. RELATED WORKS

Saranya (2012) acknowledge that there is no guarantee that data stored in the cloud is secured and not altered by the cloud or Third Party Auditor (TPA) and suggested, in order to overcome the threat of integrity of data that the user must be able to enlist the service of a TPA. He stressed that the TPA has experience in checking integrity of the data unlike clouds users. He also suggested that for the data in the cloud to be correct, consistent, accessible and of high quality data integrity provision of cryptographic key to secure the data is necessary.

Gondaliya, 2011 confimed that security is the major issue in cloud Computing. He identified security concerns arising in cloud computing environments and outlines methods to maintain compliance, integrity and preserve security protection. He provided a checklist of key questions to be considered by enterprise and service provider for cloud computing deployment.

Hamdaqa (2012) observed that Cloud computing extends an enterprise's ability to meet the computing demands of its everyday operation. Offering flexibility and choice, mobility and scalability, all coupled with potential cost savings, leveraging many enterprises to cloud computing. He however noted that the area of concern, causing hesitation on the side of enterprises most when it comes to moving business workloads into public cloud is ***integrity*** and ***security*****.** He spoke extensively on the several cloud services available such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) and UcaaS (Unified Communications as a Service), and offered some best practices suggestions to service providers and enterprises.

Ngongang (2011) recognized the security issue associated with the cloud. He stressed that the security in the cloud is a concern nowadays and security professionals are still grappling for the solution. According to him, the virtual servers have permanently in-use operating systems and applications that hold valuable data that make them attractive to malware and intruders. To him, the intruders are permanently looking for vulnerabilities in the applications and networked system to steal and destroy sensitive data.

He suggested the use of **Snort,** an open source Network Intrusion Detection system to help prevent malware and intruders who through invasion, wants to take advantage of the security weaknesses found in the applications and the operating system. The snort sensor can be configured in order to monitor the network activity. It sends an alert when it founds malicious traffic with the same pattern as those stored in its signature database. Using a network intrusion detection system, one can track down individual hacker after the investigation by watching the attacks that occur and the vulnerabilities that need to be addressed.

According to Smith, although cloud computing has attained a stage of technological maturity, indicating that most of the main issues with cloud computing have been addressed to a degree that clouds have become interesting for full commercial exploitation. This however does not mean that all the problems listed above have actually been solved, only that the attendant risks can be tolerated to a certain degree but there are some integrity and security concerns for the enterprises and organization (Smith, 2014.)

All these boils down to the fact that security and integrity are recognized issues of the cloud demanding serious attention.

3. UNDERSTANDING THE PLACE OF INTEGRITY AND SECURITY IN THE CLOUD

While there had been much emphasis on cloud's delivery of service, one area of concern however that might be causing deployment hesitation on the side of enterprises when it comes to moving business workloads into public cloud is the sensitive issues of **security** and ***integrity***. Security has variously been defined as "precaution taken to keep somebody or something safe from crime, attack or danger"; "something that provides a sense of protection against loss, attack or harm" and as "Freedom from worries of loss"(Microsoft Encarta Dictionary). All these definitions are considerable when it comes to enterprise moving business workloads into public cloud. While**,** the cloud offers various services such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) and UcaaS (Unified Communications as a Service) to the public, the important and relevant issues of Security and Integrity must be objectively considered by those desiring to deploy any of them. This paper looks at the security and integrity challenges and its implications on cloud deployment and offers best practice suggestions to service providers and enterprises. According to Webster's New Collegiate dictionary (2012), integrity is defined as "steadfast adherence to a strict moral or ethical code", with regards to data encryption, "integrity ensures that information is not altered by unauthorized person in a way that is not detectable by authorized users".

3.1 Dimensions of Security and Integrity Issues in the Cloud

Integrity and security issues in cloud computing are multidimensional. Amar (2011) identified the following non-trivial issues:

a. **Data Location :** Different countries have different requirements and controls placed on access.
b. **Data Access :** Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been interested with approved access to the cloud.

c. **Regulatory Requirements :** Organizations operating in the US, Canada, or the European Union have many regulatory requirements that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT).
d. **Auditing:** This particular item is no small matter; the cloud provider should agree in writing to the terms of audit.
e. **Employees' Training:** This is actually a rather important item, because people will always be the weakest link in security. Knowing how your provider trains their employees is an important issue of integrity to consider.
f. **Data classification:** Is the data classified? How is your data separated from other users? Encryption should also be discussed.
g. **Data Interference:** one needs to know: Is my data being used while at rest or in transit? **Service Level Agreement (SLA) Terms:** The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.
h. **Service Provider's Historical Record:** How long has the cloud provider been in business and what is their track record. If they go out of business, what happens to your data? Will your data be returned, and if so, in what format?
i. **Security Breach Eventuality:** While many providers promote their services as being unhackable, cloud based services are an attractive target to hackers.
j. **Disaster Recovery Plan (DRP):** All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising?

Since the cloud principally offers three major services namely: Software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), as depicted in the figure below, this paper examines each of them in details in the light of data security and integrity each can offer.

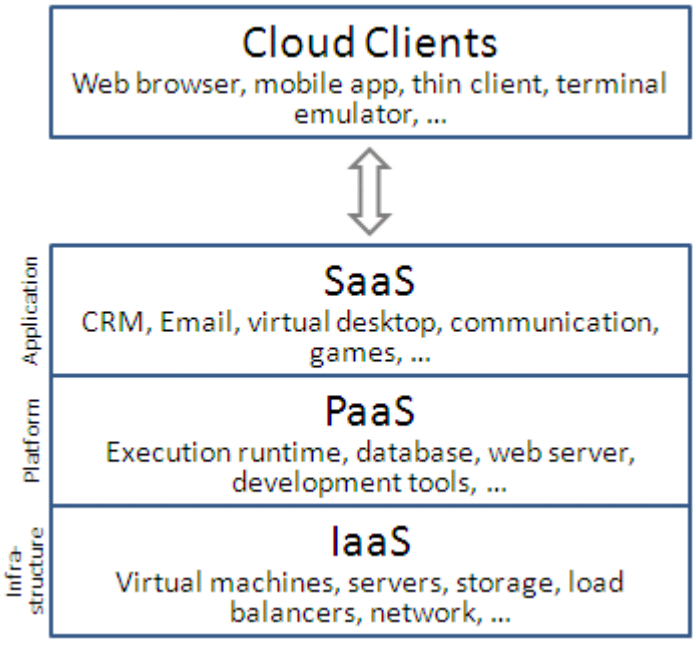

Fig. 4. Cloud Computing Services – Fundamental Model (Source: Wikipedia)

3.1 Considerable Security Issues in SaaS

As identified by Amar(2011), before deploying to Cloud's SaaS, it is necessary for an enterprise to consider the following key security and integrity issues that are integral to SaaS deployment process: Data Security, Network Security, Data Locality, Data Integrity, Data Access, Data Segregation, Authorization and Authentication, Data Confidentiality, Web Application Security, Data Breaches, Virtualization Vulnerability, Availability, Backup, Identity Management on sign-on process.

3.2 Considerable Security Issues in PaaS

a. In PaaS, the provider might give some control to the people to build applications on top of the platform. Realistically however, the client must admit that any security below the application level (such as host and network intrusion prevention) will still be within the scope of the provider.

b. Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, requiring leveraging a protocol such as Web Service Security(WSS) (Oracle, 2009). Meanwhile the ability to segment ESBs is not available in PaaS environments. Therefore metrics should be in place to assess the effectiveness of the application security programs.

c. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

3.3 Considerable Security and Integrity Issues in IaaS

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies. Operating System Security is also a major issue in IaaS. Below are some IaaS specific integrity issues.

3.3.1. Security and Integrity Issues in Cloud IaaS

a. ***Denial of Service (DoS) Attacks***: Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. A reference point is that of Twitter. Twitter suffered a devastating DoS attack during 2009.

b. ***Side Channel Attacks***: An attacker could attempt to compromise the integrity of the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

c. ***Authentication Attacks***: Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows (e.g ATM PIN), has (such as ID card), or is (Biometrics). The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

d. ***Man-in-the-middle Cryptographic Attacks***: This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

e. ***Network Security:***

- Network penetration and packet analysis
- Session management weaknesses
- Insecure SSL trust configuration.

f. ***Web Application Security:***

- Injection flaws like SQL, OS and LDAP injection
- Cross-site scripting
- Broken authentication and session management
- Insecure direct object references
- Cross-site request forgery
- Insecure cryptographic storage
- Failure to restrict URL access
- Insufficient transport layer protection
- Un-validated redirects and forwards

3.4. Non-Software Cloud Security Challenges

3.4.1 Administrative Access to Servers and Applications

One of the most important characteristics of cloud computing is that it offer "***selfservice***" access to computing power, most likely via internet. In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in the system control.

3.4.2 Vulnerability of Dynamic Virtual Machines: VM State and Sprawl

Virtual machines (Cloud Servers) are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can readily be cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In the cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

3.4.3 Vulnerability Exploits and VM-to-VM attacks

Cloud computing servers use the same operating systems. Enterprise and web applications as localized virtual machines have physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition, co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention system need to be able to detect malicious activity at the VM level regardless of the location of the VM within the virtualized cloud environment.

3.4.4 Data Integrity: Co-location, Compromise and Theft

According to the *2008 Data breach Investigation Report* conducted by Version Business Risk Team, 59% of data breaches resulted from hacking and intrusions. Dedicated resources are expected to be more secure than shared resources. The attack surfacing in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are not being tempered with nor compromised, particularly when residing on shared physical infrastructure. Operating system and application files and activities need to be monitored.

4. SUGGESTED SOLUTION APPROACHES - FACTORS TO CONSIDER BEFORE DEPLOYING ONTO THE CLOUD

1. **Identify the Offer:** it is essential to identify the assets in the cloud computing and their importance.
   Basically, cloud offers three major services:
   a) Platform as a Service (PaaS) – which covers various operating system platforms, database, web server, execution runtime, development tools and others
   b) Software as a Service (SaaS) – which comprises of applications (email, virtual desktop, CRM), functions and processes, games
   c) Infrastructure as a Service (IaaS) – these encompasses the necessary infrastructures of the cloud that drives the cloud (such as the technologies, virtual machines, servers, load balancers, RFID, SOA, WSN, networks protocols,), and network broadband etc. (See figure 3 below).

2. **Evaluate the Offer:**
   Importance - Determine how important the service is to your organization by considering the following factors:

   a) **Vulnerability –** What obtains if the asset became widely public and widely distributed or an employee of your cloud provider accessed the asset, and the process or function was manipulated by an outsider, or your information or data was unexpectedly altered?

   b) **Down time, Service / Network failure** - if the service failed to provide expected results what then? Or perhaps the assets were unavailable for a period of time what becomes of your business?

   c) Integrity and Security Implications of Cloud Reality
      a) Users are not fully aware of how cloud services are provided
      b) There is no well demarcated network security border
      c) Cloud computing implies loss of control
      All these will affect their response to change and work output and this is the crux of this paper.

Amar (2011) in a white paper on Security in Cloud Computing suggested the exploitation of the following four distinct security technologies –firewall, intrusion detection and prevention, integrity monitoring and log inspection- that can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environment can convince cloud clients of a more secure service of integrity.

3. Prevent / Reduce Vulnerabilities

Decreasing the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall, deployed on individual virtual machines can provide centralized management of server firewall policy. It should include predefined templates for common enterprise server types and enable the following:

1. Virtual machine isolation
2. Fine-grained filtering(Source and Destination Address, Ports)
3. Coverage of all IP-based protocols (TCP, UDP, ICMP, …)
4. Coverage of all frame types (IP, ARP, …)

5. Prevention of Denial of Service (DoS) attacks
6. Ability to design policies per network interface
7. Location awareness to enable tightened policy and the flexibility to move
the virtual machine from on-premise to cloud resources

4. Intrusion Detection and Prevention (IDS/IPS)

It is mandatory to shield vulnerabilities in operating system and enterprise applications until they can be patched, to ascertain timely protection against known and unknown attacks. Since virtual machines and cloud computing servers use the same operating systems, deploying intrusion detection and prevention software on virtual machines shields newly discovered vulnerabilities of applications and OSs and do provide protection against exploits attempting to compromise virtual machines.

Integrity Monitoring

Integrity monitoring of critical operating system and application files (files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

5. Log Inspection

Log inspection collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a Security Information and Event Management (SIEM) system or centralized logging server for correlation, reporting and archiving. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level. Log inspection software on cloud resources enables:

- Suspicious behavior detection
- Collection of security-related administrative actions
- Optimized collection of security events across your datacentre

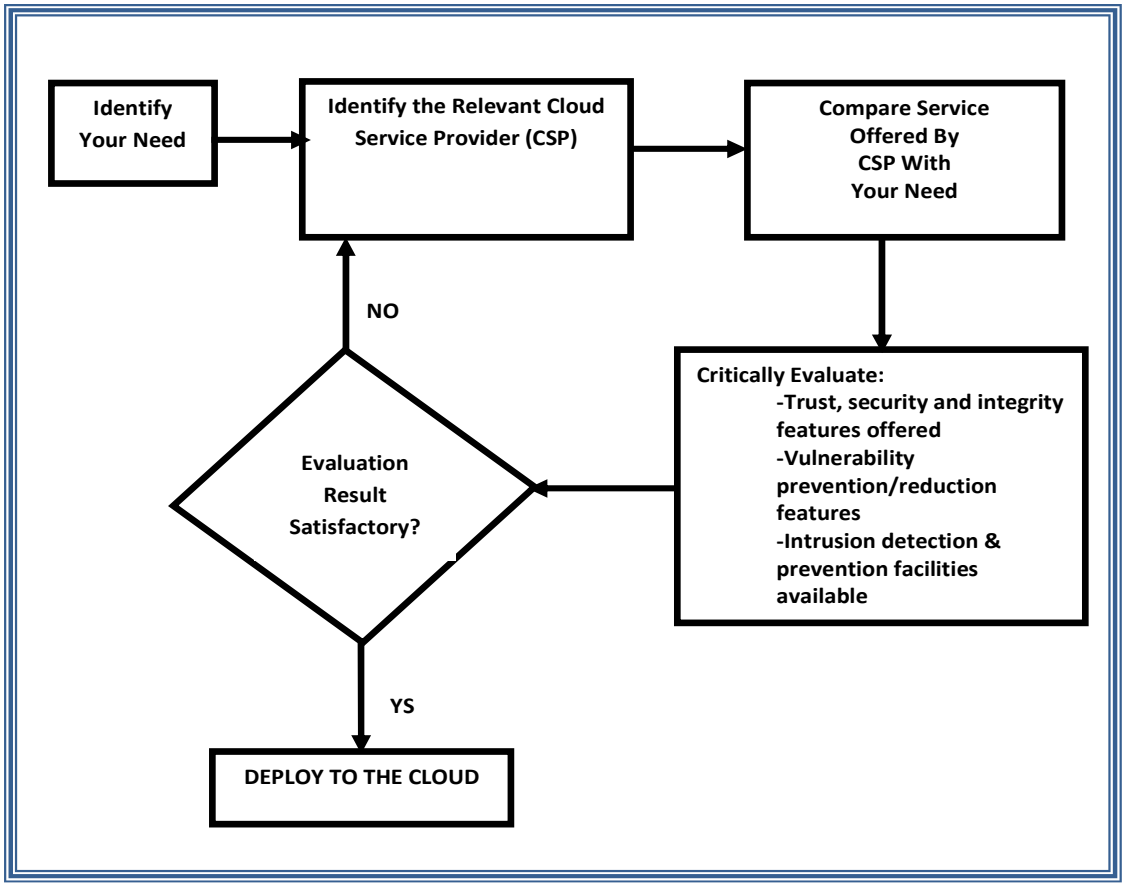

Fig. 5. Cloud Security and Integrity Model (CSIM) (*Source: Odulaja 2014*)

6. CONCLUSION AND RECOMMENDATION

This paper gives an appraisal of the attractiveness of deploying to the cloud vis-à-vis the security and integrity challenges associated with such deployment. Relevant suggestions were offered both to the service providers as well as the client enterprise, as well acknowledged in cloud analytics by several cloud analysts. After discussing the security issues, the paper concludes that we should be careful about the security concerns while putting our business on Cloud. A model (Cloud Security and Integrity Model) that will ascertain the security and integrity of the deployment was developed.

REFERENCES

1. Amar Gondaliya (2011). Security in Cloud Computing *UniSYS technical Paper Contest*
2. Hamdaqa Mohammad (2012). *Cloud Computing Uncovered: A Research Landscape*. Elsevier Press. pp. 41–85. ISBN 0-12-396535-7.
3. He, Sijin; L. Guo; Y. Guo; C. Wu; M. Ghanem; R. Han. "Elastic Application Container: A Lightweight Approach for Cloud Resource Provisioning". 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA). pp. 15–22. doi:10.1109/AINA.2012.74. ISBN 978-1-4673-0714-7.
4. Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing". In R. Buyya, J. Broberg, A.Goscinski. *Cloud Computing: Principles and Paradigms*. New York, USA: Wiley Press. pp. 1–44. ISBN 978-0-470-88799-8.
5. Mills, Elinor (2009-01-27). "Cloud computing security forecast: Clear skies". CNET News. Retrieved 2010-08-22.
6. Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "*Infrastructure as a Service Cloud Concepts*". ***Developing and Hosting Applications on the Cloud***. IBM Press. ISBN 978-0-13-306684-5.
7. Snort [online]. Sourcefire : 2010 URL: http://www.snort.org/ .Accessed March 17,2011
8. Ngongang Guy Mollet (2011), Cloud Computing Security, Helsinki Metropolia University of Applied Sciences, Bachelor Of Engineering Degree, Information Technology Thesis. April 11, 2011
9. Computing Use Cases White Paper [online]. SA(shared alike): July 2,2010. URL: http://www.scribd.com/doc/18172802/Cloud-Computing-Use-Cases-Whitepaper.
10. Cloud computing [online]. Infosys Technology limited: 2010. URL:http://www.infosysblogs.com/cloudcomputing/2009/05/hybrid_approach_for_cloud_comp_1.html.
11. Reprinted from Acute system consulting [online]. Acute system consulting: 2010. URL:http://www.acutesys.com/wp-content/uploads/2009/10/virtualize-why-choosehybrid-cloud-dg-en-full.jpg.

Other Sources:

www.cloudreadysecurity.com
www.cloudsecurityalliance.org/guidance
www.malwaredomainlist.com/
blogs.zdnet.com/security
www.programmableweb.com
securitylabs.websense.com/content/Blogs