International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

CLOUD COMPUTING SECURITY

[1]Ewulonu O. V [2]E. O. Nwachukwu

[1]Computer Science Department , School of graduate studies, University of Port Harcourt
Port Harcourt, Nigeria
anthonyvivian75@gmail.com

[2]Computer science Department, University of Port Harcourt, Port Harcourt, Nigeria
enochnwachukwu@uniport.edu

ABSTRACT:

Cloud computing does not bring about any new security issues or threats but still migrating onto Cloud may imply outsourcing some security activities to the Cloud provider. This may cause confusion between Cloud provider and users regarding individual responsibilities, accountability and redress for failure to meet required standards. There is high need for the users to have trust on the cloud provider and believe that the integrity of their information is highly preserved. This paper will focus on addressing some of the security issues to consider when moving our business to the cloud.

Keyword: cloud computing, security, cloud provider

1.0 INTRODUCTION

Clouds are large pool of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. It's a pay-per-use model in which the organizations, government and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [3] .

Security is a sensitive issue that requires adequate consideration in every area of computing of which cloud computing is not different. There is need to ensure that sensitive data items of an individual, government or organisation is well protected to avoid loss of data and unauthorised access to sensitive data items. As with other major technological change, the evolution of cloud computing has brought a lot of publicity though in many developed countries. It has also raised policy questions concerning how people, organizations, and governments handle information and interactions in this environment. Security of data in the cloud must ensure the following, [1]

Confidentiality: This refers to keeping data private. Privacy is of utmost importance as data leaves the borders of the organization. Not only must internal secrets and sensitive personal data be safeguarded, but metadata and transactional data can also leak important details about firms or individuals. Confidentiality is supported by, the following Continuity Disaster Recovery

- **Access control:** with access control you can control how and what information users can access. How could be by authentication through passwords and/or biometrics.
- **Passwords:** password is the basic authentication method and to make it even more secure it can be used alongside smart cards or biometrics.
- **Biometric:** biometrics concerns the use of humans physical characteristics for identification and authentication. It could be for example fingerprint scanning, retina scanning or face recognition.

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

- **Encryption:** by encrypting information from plain text to be unreadable prevents unauthorized users to access information. Encryption is performed through a mathematical algorithm to alter the information.
- **Ethics**: through policies employees can get the necessary guidance to know how to behave and prevent unethical use of for example an information system.

Integrity: This is a degree of confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. It also extends to the hurdles of synchronizing multiple databases. Integrity is supported by well audited code, well-designed distributed systems, and robust access control mechanisms.

To maintain the integrity of information you can use:

- **Configuration Management:** this is how you manage change when it comes to the information technology environment.
- **Configuration Audit:** this mechanism controls that information that is altered is allowed to be performed. The auditing can be done by monitor log changes either manually or through an automated system.

Availability: This implies being able to use the system as anticipated. Cloud technologies can increase availability through widespread internet-enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement. This can be achieved through the following:

- **Data Backup Plan:** to have a plan of how you backup your information is always important. It includes what information is being backed up and at which time interval. This depends on what type of business you run and how often information is altered.
- **Disaster Recovery Plan (DRP):** this includes the procedures for how a quick backup is performed with minimum impact on the business.
- **Business Continuity Plan or Business Resumption Design:** this is a part of the DRP and documents of how a business gets back to normal after a disaster has struck

2.0 Cloud service models

There are three cloud service models namely;

- **Infrastructure as a service (Iaas):** This service model contains all of the physical and virtual resources used to construct the cloud, and most closely corresponds to what exists in the most advance traditional IT operations. Resources are provided and managed in fairly chunky units- whole (physical or virtual) servers, storage pools and so on – and generally unaware of what applications are running on them [2]
- **Software as a Service (SaaS):** The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running [5].
- • **Platform as a Service (PaaS):** The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework.

2.0 Advantages of cloud computing

Cost saving: Organizations can reduce or eliminate IT capital expenditures and decrease ongoing operating expenditures by paying only for the services they use and, potentially, by reducing or redeploying their IT staffs.

Easy implementation: Without the need to purchase hardware, software licenses, or implementation services, an organization can deploy cloud computing rapidly.

Flexibility: Cloud computing offers more flexibility (often called “elasticity”) in matching IT resources to business functions than past computing methods. It can also increase staff mobility by enabling access to business information and applications from a wider range of locations and/or devices.

Scalability: Organizations using cloud computing need not scramble to secure additional, higher-caliber hardware and software when user loads increase, but

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

can instead add and subtract capacity as the network load dictates.

Access to top end capabilities: Particularly for smaller organizations, cloud computing can allow access to higher-caliber hardware, software, and ICT staff than they can attract and/or afford themselves. [4]

Greater mobility: Employees can access information wherever they are, rather than having to remain at their desks.

Shift of IT focus**:** No longer having to worry about constant server updates and other computing issues, organizations will be free to concentrate on innovation.

Cloud computing is still an evolving market. We can expect that, as it was the case for many other IT services, the exact realm of the Cloud services, its baseline technologies, but also the inherent risks and applicable rules will further evolve through the accelerated adoption of Cloud by the public and private stakeholders. Given its innovative nature compared to the standard model of service provision.

3.0 Security challenges of Cloud computing

Despite what Cloud providers and vendors promise, Cloud computing is not secured by nature. Security in the Cloud is often intangible and less visible, which inevitably creates a false sense of security and anxiety about what is actually secured and controlled. Accordingly, the security challenges related to Cloud computing are worth of a deeper attention and can relate to many different aspects.

Users control over Cloud resources - Cloud users typically have no control over the Cloud resources used and there is an inherent risk of data exposure to third

parties on the Cloud or the Cloud provider itself. From a security perspective, segregation of data containers within the technical infrastructure of Cloud computing may be a mean to ensure that each user can at best enjoy control over its data, information or other content he entrusts to the Cloud supplier.

Data secrecy & confidentiality - Encrypting data in transit has become common practice to protect secrecy and confidentiality of data in a hostile environment.

Contrary, encrypting data at rest - while only end-users may hold the decryption keys - still poses some technical challenges. New threats emerging from new technologies -Virtualisation and grid technologies expose cloud infrastructures to emerging and high-impact threats against hypervisors and grid controllers.

Access control and use of the data - the cloud computing architecture requires the adoption of identity and access management measures. When data are trusted to a third party especially for handling or storage within a common user environment, appropriate precaution must be in place to ensure uninterrupted and full control of the data owner over its data.

Application & Platform Security - General purpose software, which was initially developed for internal use, is now being used within the cloud computing environment without addressing all the fundamental risks associated to this new technology. Another consequence of the migration to Cloud computing is that the secure development lifecycle of the organisation may need to change to accommodate the Cloud computing risk context.

Security models on Cloud computing - Migrating onto a Cloud may imply outsourcing some security activities to the Cloud provider. This may cause confusion between Cloud provider and user regarding individual responsibilities, accountability and redress for failure to meet required standards. Means to clarify those issues can be contracts, but also the adoption of policies, “service statements” or “Terms and Conditions” by the Cloud provider, which will clearly set forth obligations and responsibilities of all parties involved. Lack of reference security standards - Currently there is still a lack of generally-admissible Cloud computing standards at EU or worldwide level. The consequence of this is uncertainty regarding the security and quality

levels to be ensured by Cloud providers, but also vendor dependency for Cloud users given that every provider uses a proprietary set of access protocols and programming interfaces for their Cloud services.

CRITICAL AREAS FOR CLOUD COMPUTING

The Cloud Security Alliance (CSA) has developed a 76-page security guide (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1) that identifies many areas for concern in cloud computing [6]. This environment is a new model which cannot be well protected by traditional “perimeter” security approaches. From this exhaustive document, we have selected six specific areas of the cloud computing environment where

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

equipment and software implementing TCG specifications can provide substantial security

1 - Securing data at rest.
Cryptographic encryption is certainly the best practice and in many countries worldwide, it's the law for securing data at rest at the cloud provider. Fortunately, hard drive manufacturers are now shipping self-encrypting drives that implement the TCG's Trusted Storage standards. Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Software encryption can also be used, but it is slower and less secure since the encryption key can be copied off the machine without detection.

2 - Securing data in transit.
Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit. Well-established protocols such as SSL/TLS should be used here. The tricky part is strong authentication, as described next.

3 - Authentication.
User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The TPM can easily provide stronger authentication than username and passwords. TCG's IF-MAP standard allows for real-time communication between the cloud provider and the customer about authorized users and other security issues. When a user is fired or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within seconds. If the fired user is logged into the cloud, they can be immediately disconnected. Trusted Computing enables authentication of client PCs and other devices, which also is critical to ensuring security in cloud computing.

4 - Separation between customers.
One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation. In addition, the TPM can provide hardware-based verification of hypervisor and VM integrity. The TNC architecture and standards can provide strong network separation and security.

5 - Cloud legal and regulatory issues.
To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, Trusted Storage and TPM access techniques can play a key role in limiting access to data.

6 - Incident response.
As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response or at least automated notification is the best solution. TCG's IF-MAP (Metadata Access Protocol) specification enables the integration of different security systems and provides real-time notification of incidents and of user misbehavior.

Security Controls
To adequately secure any system a lot of controls should be put in place. The table below describes several use cases and the security requirements for each.

Security Control	Description
Asset Management	It must be possible to manage all of the hardware, network and software assets (physical or virtual) that make up the cloud infrastructure. This includes being able to account for any physical- or network-based access of an asset for audit and compliance purposes.
Cryptography: Key and Certificate	Any secure system needs an infrastructure for employing and managing cryptographic

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

Management	keys and certificates. This includes employing standards-based cryptographic functions and services to support information security at rest and in motion.
Data / Storage Security	It must be possible to store data in an encrypted format. In addition, some consumers will need their data to be stored separately from other consumers' data.
Endpoint Security	Consumers must be able to secure the endpoints to their cloud resources. This includes the ability to restrict endpoints by network protocol and device type
Event Auditing and Reporting	Consumers must be able to access data about events that happen in the cloud, especially system failures and security breaches. Access to events includes the ability to learn about past events and reporting of new events as they occur. Cloud providers cause significant damage to their reputations when they fail to report events in a timely manner.
Identity, Roles, Access Control and Attributes	It must be possible to define the identity, roles, entitlements and any other attributes of individuals and services in a consistent, machine-readable way in order to effectively implement access control and enforce security policy against cloud-based resources.
Network Security	It must be possible to secure network traffic at the switch, router and packet level. The IP stack itself should be secure as well.
Security Policies	It must be possible to define policies, resolve, and enforce security policies in support of access control, resource allocation and any other decisions in a consistent, machinereadable way. The method for defining policies should be robust enough that SLAs and licenses can be enforced automatically.
Service Automation	There must be an automated way to manage and analyze security control flows and processes in support of security compliance audits. This also includes reporting any events that violate any security policies or customer licensing agreements.
Workload and Service Management	It must be possible to configure, deploy and monitor services in accordance with defined security policies and customer licensing agreements. Here are some standards that can be applied to these controls:

CONCLUSION:

Security is a sensitive issue in every area of information technology and cloud computing should not be an exception.

Cloud security is part of the inevitable progression of IT. It must be embraced by organizations to stay competitive. Companies who approach cloud computing in a mature manner need not be afraid about entering the cloud because of security concerns. Dealing with security in the cloud is no more difficult than addressing it internally. Cloud security can be as effective as the internal IT.

ISSN 2304-0777 www.jitbm.com

REFERENCES:

[1] Avizienis Et Al (2004): "Basic Concepts And Taxonomy Of Dependable And Secure Computing" Ieee Transactions On Dependable And Secure Computing.

[2] Eric A. Marks And Roberto R. Lazano (2010: Executive's Guide To Cloud Computing: Published By John Wiley & Sons, Inc., Hoboken, New Jersey

[3] Web 1 (2009), Mell And Grance: The National Institute Of Standards And Technology, U.S. Department Of Commerce; October, Http//Crsc.Nist.Gov

[4] Web 2: Http://Www.Cisco.Com/Go/Ibsgcisco

[5] Web 3: Http://Csrc.Nist.Gov/Groups/Sns/Cloud-Computing/. Retrieved 2011

[6] Web 4: Cloud Security Questions? Here Are Some Answers (Http://Cloudcomputing.Sys-Con.Com/Node/1330353)

[7] A White Paper On Cloud Computing Forcasting Change By Deloitte Retrieved November 2012