Engineering Mathematics
2018; 2(2): 95-106
http://www.sciencepublishinggroup.com/j/engmath
doi: 10.11648/j.engmath.20180202.17
ISSN: 2640-0855 (Print); ISSN: 2640-088X (Online)

Assessing and Mitigating the Security Concerns, Threats and Associated Risks with Cloud Adoption

Chinedu Uchenna Paschal[1, *], Oliver Ebere Osuagwu[2]

[1]Department of Information Technology, National Open University of Nigeria, Abuja, Nigeria

[2]Department of Computer Science, Imo State University, Owerri, Nigeria

Email address:
drpuchinedu@gmail.com (C. U. Paschal), profoliverosuagwu@gmail.com (O. E. Osuagwu)
[*]Corresponding author

To cite this article:
Chinedu Uchenna Paschal, Oliver Ebere Osuagwu. Assessing and Mitigating the Security Concerns, Threats and Associated Risks with Cloud Adoption. *Engineering Mathematics*. Vol. 2, No. 2, 2018, pp. 95-106. doi: 10.11648/j.engmath.20180202.17

Received: October 2, 2018; **Accepted**: November 5, 2018; **Published**: December 4, 2018

Abstract: Cloud Computing Security is part of the foreseeable evolution of Information Technology (IT) which any organisation intending to attain or sustain competitiveness must need to embrace in order to play in the evolving digital economy. Evidently, companies who tackle cloud computing responsibly need not entertain fears of security concerns, threats and associated risks on the path to the cloud. This research paper unveils that the concerns of handling security, privacy or forensic in the cloud virtualised environment are not as much a nightmare as compared to addressing them in-house. In an environment where information systems security and privacy has become paramount concern to enterprise customers, the risk of unauthorized access to information in the cloud poses a significant concern to cloud stakeholders. In a bid to mitigate the inevitable threats concerns of the associated stakeholders, this research prescribes the deployment of a cloud computing threat model, relevant to all other computing environments. Further, the research undertook and accessed a survey which was designed to identify and rank the various security, privacy, and forensic issues plaguing fears to the full adoption and deployment of this new computing paradigm. The survey was geared at the Nigeria marketplace among practicing IT professionals and organisations. Consequently, the drive to underpin this new direction and computing paradigm was advocated where the research highlights and ranks some of the operational concerns for cloud users in Nigeria, and further suggests measures to raise the level of awareness and engagement around those concerns within the constituencies of various consumers of the services. However, the research further argues that proper implementation of security, privacy, and forensic measures should not just be seen as the cloud providers' sole concern, but the responsibilities of all consumers of the services. Thus, the paper prescribes techniques which could help cloud users maintain control of their data at rest or in transit within the cloud networks rather than outsource control to external vendors as usual.

Keywords: Cloud Computing, Cloud Security, Security and Privacy Issue, Operational Concerns

1. Introduction

It has remained almost unarguable that cloud computing is gaining centre stage and as such considerable attention in the emerging technology or digital economy. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort [1]. This definition unveils five characteristics of cloud computing, such as: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Accordingly, cloud computing presents enormous benefits to its adoption. However, there still exist some significant barriers to adoption. One of the most significant barriers to adoption is security [2].

Being relatively a new computing paradigm, fear of cloud adoption is entertained among prospective cloud customer and Cloud Service Provider (CSP), which have security and privacy concerns as the most critical. This implies that most organization with critical applications and sensitive data are experiencing drawbacks on their path to the cloud environment, which represents outsourcing control beyond their server room or data centers. The reoccurring event of data breaches of significant cloud services experience by many has declined the enthusiasm especially among potential customers or organization with highly classified missions or business critical systems from migrating extremely sensitive data into the cloud. To mitigate these concerns, a CSP must among all tactical, operational and managerial strategy to be deployed, ensure that customers will continue to have the same security and privacy controls over their applications and services, and provide evidence to customers that their organization are secured and they can meet their service.

1.1. Statement of the Problem

In view of these concerns, this research is concern on how to demystify these plaguing hierarchy of security and privacy issues and associated risks responsible for the prevalent operational concerns of this new computing paradigm as well as further raise the existing level of awareness and commitment to these concerns by cloud consumers so as to decline the fear to the full cloud service adoption and deployment. In suggesting answer to this, the research is not limited to the direct deployment of cloud services provider or vendor security solutions but instead, further emphasises a difference with deeper advocacy that proper implementation of security, privacy, and forensic measures should be considered as the responsibilities of all consumers of the services within the prescribed cloud computing model.

1.2. Objectives

The specific objectives of this paper are:

a To model a ranked cloud security threat model with relevant mitigation strategies and solutions which offers the need for progression in the new direction

b To demystify the fear and associated risks to cloud adoption among the various cloud constituencies

c To highlight the security expectancies and benefits accruable from the cloud vendors' services

d To analyse the threats impact and risk assessments to inform business leaders of the potential risks to their enterprise

e To appreciate the significance of cloud computing in the evolving digital society and offer the need for progression in the new direction amidst the perceived security concerns.

1.3. Introduction to Cloud Computing

A cloud has been defined as a pool of virtualized computer resources [3]. In their paper, Boss et al. [3] argued that a cloud is more than a collection of computer resources owing to the fact that it provides a mechanism to manage those resources. Management here includes provisioning, change requests, re-imaging, workload rebalancing, de-provisioning, and monitoring.

Cloud computing is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices [3].

In a paper, Siddiqui [4] described Cloud Computing as nothing but a way for renting the Software, Platform and/or Infrastructure hosted by a provider. The word *Cloud* in the name refers to the fact that most of the services could be accessed over the Internet. Thus, implying that it is *the Cloud Provider that installs, maintains, scales and monitors hardware and/or software services for its customers which access these services via the Internet* [4]. In support of this, Boss et al, [3] added that cloud computing also describes applications that are extended to be accessible through the Internet. These *cloud applications* use large data centres and powerful servers that host Web applications and Web services. According to them, anyone who has the appropriate Internet access or connection with a standard browser could access a cloud application.

Our understanding and appreciation of the security issues in cloud computing are better grasped through adequate assessment of the risks and threats associated with the three computing models that come under its canopy. These service models (also described as delivery models [5] are:

a Software as a Service – SaaS

b Platform as a Service – PaaS

c Infrastructure as a Service – IaaS [4].

1.4. Risk Assessment of the Cloud Model

The cloud model can be thought of as being composed of three service models (Table 1), four deployment models (Table 2) and five essential characteristics (Table 3). Overall risks and benefits will differ per model and it is important to note that when considering different types of service and deployment models, enterprises should consider the risks that accompany them [6].

Table 1. *Cloud Computing Service Models (Source: ISACA, 2009).*

Service Model	Definition	To Be Considered
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider.	(1) Availability (2) Confidentiality (3) Privacy and legal liability in the event of a security

Service Model	Definition	To Be Considered
		breach (as databases housing sensitive information will now be hosted offsite) (4) Data ownership (5) Concerns around e-discovery
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	(1) Who owns the applications? (2) Where do the applications reside?

Table 2. *Cloud Computing Deployment Models (Source: ISACA, 2009).*

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private cloud	(1) Operated solely for an organization (2) May be managed by the organization or a third party (3) May exist on-premise or off-premise	(1) Cloud services with minimum risk (2) May not provide the scalability and agility of public cloud services
Community cloud	(1) Shared by several organizations (2) Supports a specific community that has shared mission or interest. (3) May be managed by the organizations or a third party (4) May reside on-premise or off-premise	(1) Same as private cloud, plus: (2) Data may be stored with the data of competitors.
Public cloud	(1) Made available to the general public or a large industry group (2) Owned by an organization selling cloud Services	(1) Same as community cloud, plus: (2) Data may be stored in unknown locations and may not be easily retrievable.
Hybrid cloud	A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	(1) Aggregate risk of merging different deployment models (2) Classification and labelling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.

Table 3. *Cloud Computing Essential Characteristics (Source: ISACA, 2009).*

Characteristic	Definition
On-demand self service	The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service's provider.
Broad network access	According to NIST, the cloud network should be accessible anywhere, by almost any device (e.g., smart phone, laptop, mobile devices, PDA).
Resource pooling	The provider's computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence. The customer generally has no control or knowledge over the exact location of the provided resources. However, he/she may be able to specify location at a higher level of abstraction (e.g., country, region or data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in many cases automatically, to scale out quickly and rapidly released to scale in quickly. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service (Pay as you go)	Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and customer of the utilized service.

As can be observed in the characteristics listed in Table 3, there are many approaches and challenges to cloud computing. Benefits to the enterprise, as well as risks, will vary depending on the types of service and deployment models selected [6].

1.5. Anatomy of Fear - Need for Cloud Security

There have been high levels of comfort and confidence by enterprises (and individuals alike) in storing and maintaining their data on their private computers in their own network environments. The present concern expressed by Siddiqui [4] with the advent of cloud computing where the data storage will be provided (and controlled) by the provider is that the enterprises and individuals would have to part with their data if they want to enjoy the benefits of the cloud; and this is where the concerns for security originate from.

The concern pinged that we maintain complete control where the data and infrastructure are house within; we could implement any security mechanism we deem fit, we could install any hardware or software to create perimeter around our internal network, we could design "security-by-complexity" by adding multiple layers of security, etc. However, once the data leaves our network into the cloud, we lose control over it as well as the security around it. In the cloud we totally depend on the provider to offer these services; meaning that we have lost most of the control [4].

The fears based on the concern of where we are coming from (traditional standalone/ network environment), and where we are going (cloud computing- "cloudy") have been examined and hence outlined by Hasan [7] in a lecture, against the following security, privacy and forensic issues:

1.5.1. Confidentiality

(1) Will the sensitive data stored on a cloud remain confidential? Will cloud compromises leak confidential

client data (i.e., fear of loss of control over data)

(2) Will the cloud provider itself be honest and won't peek into the data? [7]

1.5.2. Integrity

(1) How do I know that the cloud provider is doing the computations correctly?

(2) How do I ensure that the cloud provider really stored my data without tampering with it?

1.5.3. Availability

(1) Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?

(2) What happens if cloud provider goes out of business?

1.5.4. Privacy Issues Raised Via Massive Data Mining

Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients

1.5.5. Increased Attack Surface

(1) Entity outside the organization now stores and computes data, and so

(2) Attackers can now target the communication link between cloud provider and client

(3) Cloud provider employees can be phished

1.5.6. Auditability and Forensics

(1) Difficult to audit data held outside organization in a cloud

(2) Forensics also made difficult since now clients don't maintain data locally

1.5.7. Legal Quagmire and Transitive Trust Issues

(1) Who is responsible for complying with regulations (e.g., SOX, HIPAA, GLBA)?

(2) If cloud provider subcontracts to third party clouds, will the data still be secure? [7]

These are practical issues that are advancing into a perpetual inefficient deployment of technology infrastructure and services, by obviously militate against the adoption of cloud computing. The onus lies with the providers, if they want to win the trust of incredulous potential customers and gain competitive edge in the marketplace, to speedily address the matters of security first.

1.6. Cloud Computing Threat Model

"You cannot build secure systems until you understand your threats." [8]

A threat model is that model which helps in analyzing a security problem, design mitigation strategies, and evaluate solutions [7, 9, 8].

Metri and Sarote [8] further described this model as a theorem which has the following step to evaluate and reach the solution to deal with the problem:

Step 1: Identify attackers, assets, threats and other components

Step 2: Rank the threats

Step 3: Choose mitigation strategies for the threats.

Step 4: Build solutions based on the strategies [7, 9, 8].

1.6.1. Identify Attackers, Assets, Threats and Other Components

Basically, we would advance by identifying the following three major components.

Attacker modeling

Choose what attacker to consider: Who are the attackers?

I. Attackers may be insider, like

(1) Malicious employees at client

They are capable of creating the following attack:

a Learn passwords/authentication information

b Gain control of the Virtual Machines (VMs)

(2) Malicious employees at Cloud provider

The attacks are reflected in the ability to:

Log client communication

(3) Cloud provider itself

Cloud providers may also be the attacker. What they could be up to include:

a Can read unencrypted data

b Can possibly peek into VMs, or make copies of VMs

c Can monitor network communication, application patterns

Their major motivation would include to either gain valuable information about the client data, or valuable information on client behavior. The essence may be to sell such information or use it to either create competitive advantage where the client could be seen as a rival to their business or any other intention. Usually, this is the case where the provider considers honesty as a cheaper option when compared with her main cooperate goal of existence. Third party clouds often fall victim as this kind of attackers in most cases.

II. They may also be outsider, like

(1) Intruders

(2) Network attackers (hackers)

These categories of attackers are capable of carrying out the following attack:

a Listen to network traffic (passive)

b Insert malicious traffic (active)

c Probe cloud structure (active)

d Launch DoS

These outsiders' attackers usually aim Intrusion, Network analysis, Man in the middle, or Cartography attacks as the case may be.

Assets / Attacker Goals

The attacker goal could be threatening on confidentiality of Assets. And such assets may include:

a Data stored (or transiting) in the cloud

b Configuration of VMs running on the cloud

c Identity of the cloud users

d Location of the VMs running client code

The threat could also impact on integrity of the following:

a Data stored in the cloud

b Computations performed on the cloud

Finally, the attack could hamper on availability of the following resources:

a Cloud infrastructure (IaaS)
b SaaS / PaaS
Vulnerabilities / Threats

1.6.2. Rank the Threats

We rank or prioritize the threats according to their impact on the privacy of cloud user and cloud server. This is actualized in Metri and Sarote, [8] by organizing threat using STRIDE Model.

(1) *Spoofing identity:* An attacker pretends to be another user or a machine takes the stance of a valid/trusted machine. A typical example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

(2) *Tampering with data:* Data tampering is the act of maliciously modifying data. This include unauthorized changes created on persistent data (e.g. data held in a database), and altering data flowing between computers over an open network, such as the Internet.

(3) *Repudiation*: Repudiation threats are linked with users who deny their execution of an action where other parties do not have any clue to prove otherwise—for example, where a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. On the other hand, Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package [8].

(4) *Information disclosure:* Information disclosure threats refer to the disclosure of information to individuals who are not meant to have such right of access. A typical example includes the ability of users to read a file that access was not granted them, or the ability of an intruder to access and read data transiting between two computers.

(5) *Denial of Service:* Denial of Service (DoS) attacks involves a scenario where service is denied valid users. A typical example includes where a Web server is made temporarily unavailable or unusable. In order to improve on the availability and reliability of system, efforts must be in place to protect against certain types of DoS.

(6) *Elevation of Privilege:* Elevation of privilege could be said to have occurred where an unprivileged user gains privileged access and thereby secures sufficient access to compromise or destroy the entire system. In this kind of threat as argued, situations arise in which an attacker effectively penetrated all system defenses and become part of the trusted system itself- a dangerous situation indeed [8].

In summing up, Metri and Sarote, [8] maintain you can reveal the threat targets from functional decomposition, determine types of threat to each component using STRIDE, use threat trees to determine how the threat can become vulnerability, and apply a ranking mechanism to each threat. These have been tabularized as given in Table 4:

Table 4. *Ranking of Threats.*

Threat Type	Affects Processes	Affect Data Stores	Affects Inter actors	Affects Data Flows
S	Y		Y	
T	Y	Y		Y
R		Y	Y	Y
I	Y	Y		Y
D	Y	Y		Y
E	Y			

1.6.3. Choose Mitigation Strategies for the Threats

This can be actualized by considering initial or existing solution together with new strategies to address the problem. Deploying a combinational approach could also help realize the expected solution as provided in Table 5.

1.6.4. Build Solutions Based on the Strategies

We build and apply solutions based on the strategies.

Table 5. *Types of Threats and Mitigation Techniques.*

Threat type	Mitigation technique
Spoofing identity	Authentication Protect secrets Do not store secrets
Tampering with data	Authorization Hashes Message authentication codes Digital signatures Tamper-resistant protocols
Repudiation	Digital signatures Timestamps Audit trails
Information disclosure	Authorization Privacy-enhanced protocols Encryption Protect secrets Do not store secrets
Denial of service	Authentication Authorization Filtering Throttling Quality of service
Elevation of privilege	Run with least privilege

In his presentation, Hasan [7] concludes that: *"A threat model helps in designing appropriate defenses against particular attackers."* Your solution and security countermeasures will ultimately depend on the particular threat model you are focusing on. Here the researcher shall be considering rendering maximal security solution to the data (at rest or transiting) the cloud network by combating such threat as "Tampering with Data", "Repudiation", "Information Disclosure", and "Denial of Service".

1.7. Cloud Data Security Concerns

Samson [10] publication of an RSA Conference of Cloud Security Alliance (CSA) showcases cloud vendors copiously hawking products and services that arm IT with controls to foster order to the threatening cloud chaos. The exercise requires for organization to identify and rank the greatest cloud related threats and where they occur. The report reveals the unanimous consensus among industry experts, focusing on shared, on-demand nature of cloud computing related threats which gave highest priority to data breaches such as data loss and data leakage.

Earlier work by IBM Research [11], highlights five key concerns about cloud computing. These gave foremost priorities to the issues of "less control" of user to their own data, and Data Security in a shared network and compute infrastructure to unveil threats on and discomfort by many companies and governments with the concept of locating data on systems not user controlled and the increasingly potential for unauthorized exposure in multi-tenants environment respectively. The research further addressed these concerns by proffering the following solutions:

Less Control:

Provider become fully security transparent and offer sophisticated control

Data Security:

Implement secure authentication, authorization, and identity management

Isolate multiple tenants from each other

Encrypt critical data and ensure they are integrity-protected by client.

Furthermore, in a blog post, Frye [12] describe a new open source project called CRYPTON, which development was said to be in-progress, which is hoped to put a reusable cryptographic solution in the hands of cloud app developers by providing easy, built-in encryption of user data.

Violino [13] has listed thirteen (13) cloud computing security concerns which are as follows:

i. Data breaches- these may involve data not intended for public access such as personal health data, financial data, trade secrets, intellectual property, etc.

ii. Insufficient identity, credential, and access management- whereby hackers may masquerade as legitimate users, developers, etc. to read, modify, and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source, CSA says.

iii. Insecure interfaces and application programming interfaces (APIs)- Cloud providers often expose APIs that enable customers to integrate interfaces that can communicate with cloud services. Since provisioning, management, and monitoring are conducted using the said APIs, the security of cloud services would inherently depend on the security of APIs.

iv. System vulnerabilities- These are exploitable bugs in programs that attackers may exploit to infiltrate a system so as to steal data, take control of the system, disrupt service operations.

v. Account hijacking- Attackers may gain access to a cloud user's credentials by eavesdropping on activities, transactions, data, etc.

vi. Malicious insiders- A malicious insider such as a system administrator can access potentially sensitive information, and can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on cloud service providers for security are at greater risk.

vii. Advanced persistent threats (APTs)- APTs are a parasitical form of cyber-attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Once in place, APTs can move laterally through data center networks and blend in with normal network traffic to achieve their objectives

viii. Data loss-Data stored in the cloud can be lost permanently through accidental deletion by the cloud service provider, physical catastrophes (e.g. fire, earthquake, flood, etc.)

ix. Insufficient due diligence -Business strategies must as a matter of due diligence take into consideration the cloud technologies and service providers. Available technologies and providers should be sufficiently evaluated so as to avoid a number of risks associated with low credibility and service delivery indexes.

x. Abuse and nefarious use of cloud services- It is submitted that insecure or poorly secured cloud deployments, free cloud trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models to malicious attacks. Attackers would often leverage on the said loopholes to target users, organizations, or other cloud providers. For instance, an attacker on gaining access to a cloud-based resource can launch distributed denial-of-service attacks, email spam, and phishing campaigns.

xi. Denial of service (DoS)- DoS attacks often prevent legitimate users of a resource from gaining access to the resource. Attackers can cause a shutdown of a cloud resource by bombarding a targeted cloud service with inordinate amounts of transactions which take up much resource such as processor power, memory, disk space, or network bandwidth, etc.

xii. Shared technology vulnerabilities- scalability is important in most cloud service delivery operations. In other words, the service providers often share infrastructure, platforms or applications at the expense of security in most cases.

xiii. Spectre and Meltdown- these two threats are mostly a lapse associated with modern microprocessors used in mobile devices, PCs, servers, Cloud, etc. whereby content, including encrypted data could be read from memory using malicious Javascript code. Meltdown breaks the isolation between user applications and the operating system thus allowing a program to access the memory including confidential credentials of other programs and the operating system. Spectre, on the other hand, breaks the isolation between different applications permitting an attacker to trick error-free programs, which follow best practices, into leaking their secrets.

Encryption is an information security measure that renders data unintelligible to unauthorized readers. It is a coded transformation of data into a form unreadable to intruders and interlopers who lack the appropriate key to decrypt the encoded data [14].

Encryption involves using a cryptographic algorithm and a cryptographic key in order to transform a plaintext into a ciphertext or not obvious text [15]. The figure 1 gives us diagrammatical illustration of a basic encryption system.

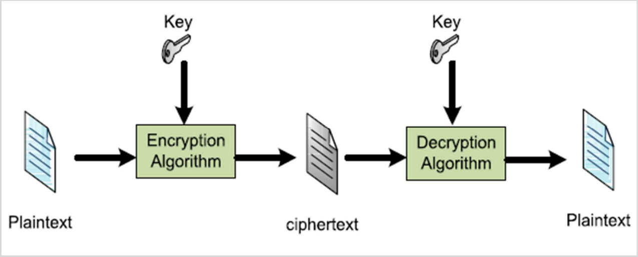

Figure 1. *Basic Encryption (Al Beshri, 2013).*

Encryption is gaining popularity as social and community computing (such as the cloud) is gaining momentum. According to Kelsey [16], Encryption Technique is important not just for the data but also for database controls and communication channels such as the Secure Socket Layer (SSL). In a public cloud where communal computing and multi-tenancy is practiced, encryption must be inevitable to ensure confidentiality and integrity of information and data store. As a mitigation technique that could sufficiently address the risk of information disclosure threat type, Wikipedia [17] elucidated that *Encryption is implemented to curb impersonation, wiretapping, piracy, spoofing and data diddling which are common abuse in a multitenant environment.*

The Cloud Standards Customer Council [18] has prescribed a ten-step solution to ensuring cloud data security:

i. Ensure effective governance, risk and compliance processes exist
ii. Audit operational and business processes
iii. Manage people, roles and identities
iv. Ensure proper protection of data and information
v. Enforce privacy policies
vi. Assess the security provisions for cloud applications
vii. Ensure cloud networks and connections are secure
viii. Evaluate security controls on physical infrastructure and facilities
ix. Manage security terms in the cloud service agreement
x. Understand the security requirements of the exit process

In a bid to adequately assess the varying concerns, threats and associated risks with adoption of this new computing paradigm so as to properly melt out mitigating measures, the research advanced into primary data gathering via a survey among the constituencies of consumers in the Nigeria marketplace.

2. Method and Analysis

2.1. Research Design

This research adopted Quantitative approach which has to do with quantity and measurement as well as interaction with stakeholders. The researcher used questionnaires, structured interview and observation instruments of the survey methods of research. This approach is considered competent as data collected was randomly sampled from the identified population. There was consistency in the characteristics of the population with regards to the research objective.

The population of this study comprises stakeholders from IT regulatory body such as Computer Professionals Registration Council of Nigeria (CPN) and association such as Nigeria Computer Society (NCS) tagged “college of fellows”.

The total population in this research was 180 respondents. These responded to the questionnaire instrument. Also, some selected organisations where reached to administer the structured interview questions. From the named population, 120 responses were further filtered from the selected 124 persons to constitute the required respondents based on the nature of organisation as highlighted in the previous heading. These will constitute a fair representation of the Stakeholders. The researcher used the probability sampling technique which was simple randomly selected to ensure probability of each case selected was known and same for all cases. This facilitated answering research question through statistical estimation of the characteristics of the sampled population [19].

Statistical data has been captured and sorted according to researcher’s interest using MySQL in the online Questionnaire database and later with computer software packages: Microsoft Office Excel and SPSS to facilitate further sorting, presentation and analysis. The frequency distribution and percentage method of analysis were used to analyze the data. Just as Ike [20] puts it “the percentage method is widely used in managerial and social researches”.

2.2. Analysis of Results

2.2.1. Business and Security Benefits/Expectancies

More flexibility, cost savings, and better scalability ranks high on benefits experiencing from cloud computing?

Participants in their largest number, indicate three core drivers of cloud computing: first is more flexibility (90 percent), then cost savings (72 percent) and followed by better scalability of their IT (62 percent). See Figure 2 for detailed representations. Some interviewees complained about the rigidness of their internal IT, combined with an unacceptable time to market. Cloud computing, by enabling the faster application deployment for less cost, can bring relief. Specifically, most large organisations (78 percent) with above 100 staff strength quote improved flexibility as an essential motivation to move to the cloud [21].

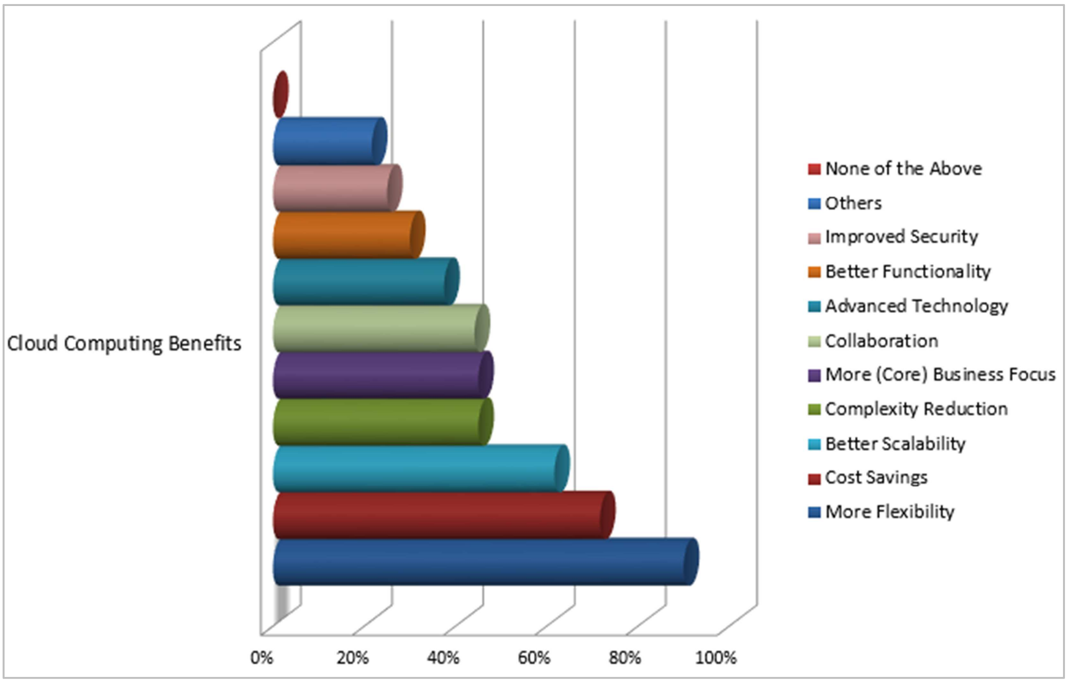

Figure 2. *Percentage on business and security benefits (Source: Chinedu, 2018).*

The rest of the participants expect such benefits as complexity reduction (45 percent), more (core) business focus (45 percent), collaboration (44 percent), advanced technology (38 percent), better functionality (30 percent) and improved security (31 percent) as accruable from the cloud.

The economics-of-scale the cloud computing vendors can realize usually have direct relationship with the accruing benefits of this IT innovation. Cloud computing solution create efficient use of IT resource by harnessing the multi-tenancy concept, where one available solution can deliver services to multiple organisations by sharing the IT resources rather than dedicating individual IT resources for each of these organization as in the case of on-premise IT. The utilization rate of most on-premise IT resources rarely exceeds 20 percent (implying that as much as 80 percent of its capacity remains a waste) where as more efficiency could be attained.

The efficient use of IT resources at cloud computing vendors may well explain the resulting much reduction in costs. Thus, cloud computing solutions are offered at lower prices than on-premise alternatives.

Cloud computing provisions at each delivery model (infrastructure, platform and software) already installed and instantly usable services which implementation is usually less time-consuming and less complicated compared to on-premise alternatives. Cloud computing solutions easily scales up and down using various types of virtualisation and load-balancing technologies. These technologies, if integrated with the popular cloud computing ‘pay-as-you-go’ or subscription models allows customers only to pay for what they use and the required IT capacity stays available. In contrary to on-premise IT, cloud computing IT capacity is never idle and never scarce.

2.2.2. Security and Privacy Issues: Obstacles of Cloud Computing

What are your main concerns regarding the use of cloud computing?

An overwhelming majority of the interviewed participants (71 percent) consider security issues to be their main concern regarding the use of cloud computing. Privacy issue (60 percent) ranked the second position. Others such as legal (50 percent), and compliance issues (50 percent) are highlighted to be areas of risks. Remarkably, very few participants (15 percent) believe that lack of functionality is an area of concern despite the standardised services that many cloud computing vendors offer. They also did not have many concerns when it comes to cloud computing’s immature technology (10 percent).

Focusing on the security issue, the total of 83 percent of participants agree (by answering “Strongly agree” and “Agree”) that security concerns are a blocking issue when it comes to their move to the cloud. It appears that they are not worried primarily about the lack of security measures in themselves, but about the lack of transparency on the side of vendors. This is owing to the fact that an appreciable 25 percent of participants answered to improved security as one of the benefits they are experiencing from cloud computing.

In an interview, it was argued that though cloud computing no doubt provided a centralized framework where security measures could be optimized, yet most users require sufficient trust on the providers to be able to outsource control of their valuable data to the third party. Thus, it would be deduced that where the threats to user data are mitigated with external parties' intruders or hackers, such data remains more than 70 percent vulnerable to internal threats or attackers from within the third-party cloud provider's premises.

2.2.3. Fears for Using the Cloud for Business-Critical Processes and Sensitive Data Storage

The survey reveals close to a half of all participating organisations (average of 49 percent) are to a low degree already using or planning to use cloud computing storage services such as for managing their business-critical processes and for storing their extremely sensitive data. And of the rest participants, 45 percent maintain medium degree use or plan to use this new computing paradigm for same purposes. While only a small fraction representing an average of 6 percent gives cloud computing a high option to the said use or plan. See Figure 3 for clearer representation:

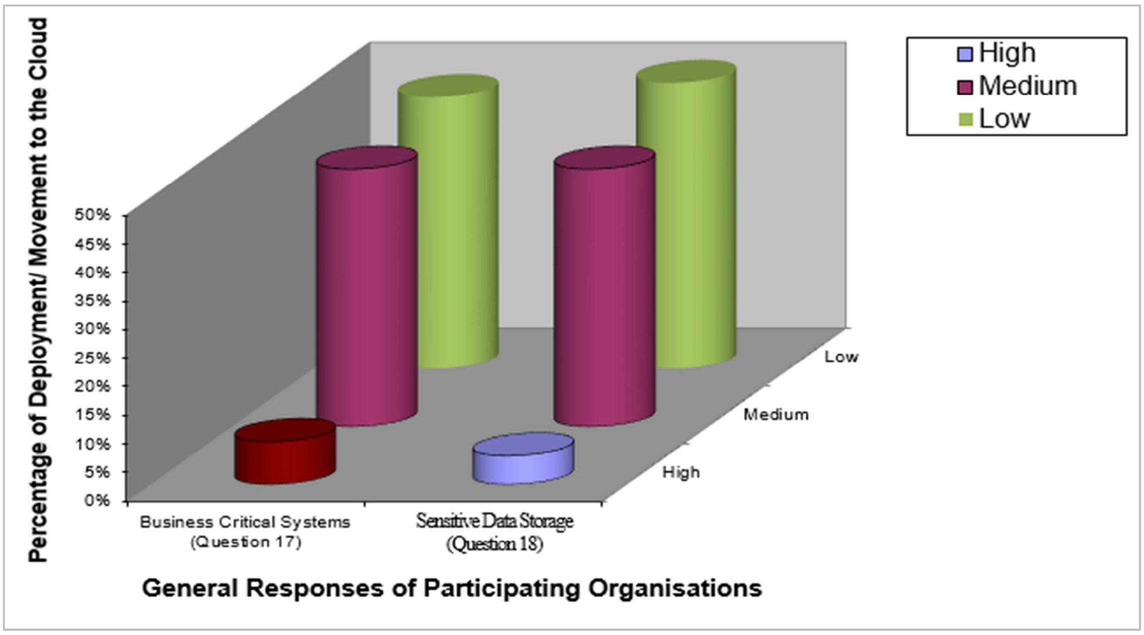

Figure 3. *Degree of Deployment/ Movement to the cloud (Source: Chinedu, 2018).*

Greater concerns on adopting the cloud for business-critical systems and moving extremely sensitive data into the cloud have been unveiled by most opposition on the part of the finance-based businesses as unveiled in Figure 4.

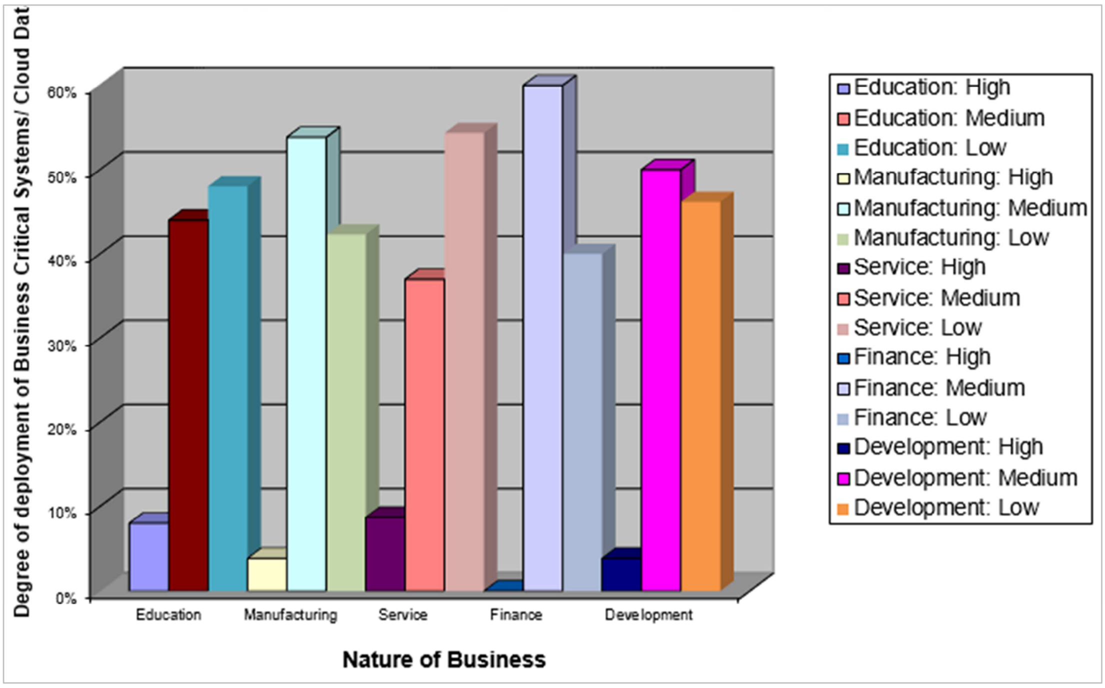

Figure 4. *Measures of security concerns/ cloud dependency (Source: Chinedu, 2018).*

This is evident from the 40 percent of these respondents which indicate that they are to a low degree (or virtually not) and the rest 60 percent participants which indicate medium degree (fairly) moved or considering moving business critical processes and extremely sensitive data to the cloud. None (0 percent) of the respondents showed high degree storage or intention to move highly classified mission or data into the cloud as against those of the other businesses such as "Education", "Manufacturing", other "Service" and "Development" unveiled in Chart 3.

"We are not actually certain how secure the cloud is at the moment, but so far, we can count on the availability as against those of our previously used on-premise business critical applications. We are said to be on business because of our cloud readiness."- Sales Officer of Standard Chartered Bank- a firm in the Financial services sector.

3. Discussions: Demystifying Cloud Security Challenges

There are major and notable concerns to data security in the cloud due to failure of service providers and malicious attacks from hackers, amidst the widespread eagerness on cloud computing deployment. The reoccurring event of Data breaches of significant cloud services experience by many has declined the enthusiasm especially among potential customers with highly classified missions or business critical systems from the plans to move extremely sensitive data into the cloud. Besides, the enormous security benefits accruable from the cloud vendors' services, the respondents to this survey, in the course of this research, argued on the matter of trust on a third-party provider, and the risks of outsourcing control of their data. Consequently, the cloud is inherently neither secure nor dependable from the perspective of some of the cloud customers.

Therefore, security of cloud data had been identified as the main obstacle that is encountered when implementing cloud computing. This is closely followed by issues regarding privacy, compliance, and legal matters. Among other areas of risk (such as dependency on the (public) internet, multi-tenancy and integration with internal security) on the path to the cloud, external data storage receives sufficient and the most highlight. Most Organisations are indeed worried about security and privacy concerning the use of cloud computing services as there is negligible assurance coming from the market. Matching internal user security requirements with the security measures and controls employed by cloud computing vendors or service providers proves to be impracticable due to discrepancies, lack of transparency and insufficient expertise inhibiting the trust from most cloud users.

4. Conclusion

4.1. Suggestions

While cloud security emerges as a critical concern among Information security professionals as well as all those who respond to cloud computing surveys, the basis to understanding security in cloud computing is to realize that the technology is not new, or untested. It signifies the logical evolution to outsourcing of commodity services to many of the same trusted IT providers we have already been using for years.

Cloud computing is the logical move for services to take as more established parts of IT are commoditized. Not moving to cloud computing will imply you are paying more than your competitors for the same commodity [22].

While cloud computing is certainly poised to deliver several benefits, sufficient business impact analyses and risk assessments to inform business leaders of the potential risks to their enterprise should be conducted by information security and assurance professionals. Regular reassessment of risks or reassessment based on event of change should be a part of planned risk management activities which must be managed throughout the information life cycle.

Enterprises that have been considering the utilisation of cloud in their business environment should estimate and match what cost savings the cloud can offer them against what associated and/or additional risks are incurred. Once this analysis is made, enterprises will be better positioned to appreciate how they can leverage cloud services.

Organisations should work with legal, security and assurance professionals to guarantee attainment and sustenance of appropriate levels of security and privacy within this new computing platform. The cloud represents a major paradigm shift in how computing resources will be utilized, and as such requires participation of a broad stream of stakeholders whose governance should initiate its deployment within adopting organizations.

Cloud security has to be a joint-venture between the provider and its customers; it ought to be a two-way street where providers are committed to providing the infrastructure and other services on the server-side and the customers should possess sufficient knowledge to take intelligent and safe cloud decisions on the client-side.

Your organisation is likely to be exposed to higher security risk than your cloud provider, unless you are in the business of implementing security. So, ensure you partner with your provider to determine its commitment to security. Match it against your current and actual security levels to ensure the provider is attaining parity or better levels of security.

Understand that proper risk assessment is the key to cloud security. Insist on having the risk assessment provided you by your cloud computing provider with details on how it plans to mitigate any issue identified. Further, mandatory discussions with the cloud provider's top security personnel should be on your monthly schedules. This discussion should encourage free flow of ideas from both ways with no hidden items.

The need for improved government regulations around cloud security cannot be over emphasised. Thus, these regulations should be very specific and well-targeted at cloud.

4.2. Progression in the New Direction

Despite the security privacy and forensic concerns expressed by banks along with other organization, it blows the mind to imagine a world without online banking and other forms of online financial transactions and systems. Correspondingly, the attraction due the economics and convenience of cloud computing (offering enterprises long-term IT savings, including reducing infrastructure costs and offering pay-for-service models) will make this technology innovation a commonplace while cloud computing vendors work vigorously to alleviate customers or market concerns about security … like ecommerce, online banking and other online financial transactions are today.

Obviously, regardless of the convenience and economic benefits, cloud computing may not be for everyone. For critical security and risk reasons, a few organisations with highly classified missions and/or extremely sensitive data may opt out of the idea of cloud computing or better still deploy a private cloud where investment cost was never a factor. However, for most (especially any business looking to enhance IT resources while controlling costs), the business and the security advantages of cloud computing discussed earlier together with the possibility to deploy virtual private clouds (allowing customers to control who is in the cloud, where data is stored, who has access, etc.) would contain the security assurances required to satisfy these organizations. Thus, giving rise to hybrid cloud computing deployment.

Certainly, with challenges come opportunities, and cloud computing security is surely not an exemption. Just as have been highlighted, these concerns pose huge opportunity that cloud vendors could seize to translate the enormous security ills of cloud computing into solutions to win the trust and the business of potential customers. Therefore, it would not be mind-boggling to assert that through developments in cloud security, a cloud provider or vendor could gain a differentiating advantage over others in the Nigeria marketplace as well as the global business environment at large.

Finally, cloud security is part of the foreseeable evolution of IT. Any organisation intending to attain or sustain competitiveness must need to embrace cloud computing and cloud security. Evidently, companies who tackle cloud computing responsibly need not entertain fears of security issues in the path to the cloud. The concerns of handling security, privacy or forensic in the cloud are not as much a nightmare as compared to addressing them in-house.

Sequel from the outcomes of this survey's analyses, the research offers the need for progression in the new direction by appreciating that any new technological development would definitely stir stakeholders fear in embracing the change from the usual to the unusual, or the known to the unknown as the case may be. Just like we find in the invention of the internet and then e-commerce as against their subsequent adoption by financial institutions and their consumers, the concerns and fear expressed almost appeared as a factor never to wave off. Subsequently, however, the demands and pressure of globalisation and digital society left every one with no other option than to accept the drive in this new direction and computing paradigm.

4.3. Concluding Statements

In practice, research data and observations from this study clearly indicates there are not many organisations that are fully virtualized and deploying cloud computing environment for organisation practices. This is as a result of various uncertainties and barriers posed by the operational concerns among the service-based users which need to be overcome first in the marketplace to warrant the researcher's suggestions earlier in this paper.

However, many organisations practices depict some features evident of a Cloud Computing service adoption. Thus, leveraging on the several economic and security benefits of cloud computing adoption (cost containment of the initial capital outlay and maintenance cost of such intense ICT infrastructural setup), we maintain that this major paradigm shift advocates all consumers' participation with legal, security and assurance professionals to guarantee attainment and sustenance of appropriate levels of security and privacy.

Thus, we forecast, there should be increasing interest in virtualisation or on the path to the cloud. Hence, adopting and deploying cloud services are relevant risk to manage or IT strategy to undertake.

References

[1] Rebollo, O., Mellado, D.: Systematic Review of Information Security Governance Frameworksin the Cloud Computing. Journal of Universal Computer Sc. 18(6), 798–815 (2012)

[2] Latif, R., Abbas, H., Assar, S. & Ali, Q. (2014). Cloud Computing Risk Assessment: A Systematic Literature Review. Springer-Verlag Berlin Heidelberg. Available online at DOI: 10.1007/978-3-642-40861-8_42,

[3] Boss et al. (2007). *Cloud Computing*: High Performance On Demand Solutions (HiPODS). Version 1.0, Available online at http://www.ibm.com/developerworks/websphere/zones/hipods / (Accessed: 20 May 2011).

[4] Siddiqui, M. (2011). *Cloud Computing Security:* Final paper submitted spring 2011. Available online at http://blogs.techconception.com/manny/content/binary/Manny%20Siddiqui%20%20Cloud%20Computing%20Security.pdf (Accessed: 20 May 2011).

[5] Reilly, D.; Wren, C. & Berry, T. (2011). *Cloud Computing: Pros and Cons for Computer Forensic Investigations:* International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011. Available online at http://www.infonomicssociety.org/IJMIP/Cloud%20Computing_Pros%20and%20Cons%20for%20Computer%20Forensic%20Investigations.pdf Accessed: 20 May 2011

[6] ISACA (2009). Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives: Emerging Technology White Paper. Available online at http://www.isaca.org/...Center/.../Cloud-Computing-28Oct09-Research.pdf Accessed: 08 June 2011

[7] Hasan, R. (2011). Security and Privacy in Cloud Computing: Johns Hopkins University en.600.412 Spring 2011, Lecture 1, 01/31/2011. Available online at http://www.cs.jhu.edu/~ragib/sp11/cs412/lectures/600.412.lecture01.pptx (Accessed: 20 May 2011).

[8] Metri, P. et al. (2011). *Privacy issues and challenges in cloud computing*. International Journal of Advanced Engineering Sciences and Technologies (IJAEST) Vol No. 5, Issue No. 1, 001 - 006

[9] Cho (2010). An overview of cloud security and privacy. Presentation, CS 590, Fall 2010. Available online at http://www.cs.purdue.edu/homes/bb/cs590/.../YounSun.pptx - United States. (Accessed: 08 June 2012).

[10] Samson, T. (2013) "9 top threats to cloud computing security. Conference processing by Cloud Security Alliance" [Online]. Available from http://www.infoworld.com/t/cloud-security/9top-threats-cloud-computing-security-213428?page=0,0 [Accessed: 05/06/2014]

[11] IBM Research (2011) "Protocols for Secure Cloud Computing: Christian Cachin, Zurich" [Online]. Available from http://www.zurich.ibm.com/~cca/talks/metis2011.pdf [Accessed: 21 May 2013]

[12] Frye, S. (2013) "Crypton for developers: Toward cryptographically- secure cloud apps" [Online]. Available at: http://www.techrepublic.com/blog/linux-and-opensource/crypton-for-developers-toward-cryptographicallysecure-cloud-apps/ [Accessed: 27/05/2014]

[13] Violino, B. (2018) "The dirty dozen: 12 top cloud security threats for 2018" [online]. Available at: https://www.csoonline.com/article/3043030/security/12-topcloud-security-threats-for-2018.html. [Accessed 7 March 2018]

[14] Hellman, M. E. (1980) "A cryptanalytic time-memory tradeoff. Information Theory", IEEE Transactions, Vol. 26, Issue: 4

[15] Al Beshri, A. M. (2013) Outsourcing data storage without outsourcing trust in cloud computing. PhD thesis, Queensland University of Technology. Available online at http://eprints.qut.edu.au/61738/ (Accessed: June 05, 2014)

[16] Kelsey et al (1997). RC2. Available online at http://en.wikipedia.org/wiki/RC2 (Accessed: June 14, 2014)

[17] www.wikipedia.com/cryptoanalysis/attacks, August 2013

[18] Cloud Standards Customer Council (2017). "Security for Cloud Computing: Ten Steps to Ensure Success" [online]. Available at: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf. [Accessed 7 March 2018]

[19] Ike, K. R. (2003). *Introduction to research method.* Umuahia, Nigeria: Chudy Publications.

[20] Saunders, M., Lewis, P., & Thornhill, A. (2007) *Research methods for business students* (4th Edition). (pp. 204- 246). Essex: Prentice Hall

[21] Chinedu, P. U. (2018). Secured Cloud-Based Framework for ICT Intensive Virtual Organisation. Approved by: Owerri, Nigeria, Federal University of Technology Owerri, Diss., 2008. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing. ISBN: 978-613-9-82456-4, Published: April 22, 2018

[22] Almond, C. (2009). *A Practical Guide to Cloud Computing Security: What you need to know now about your business and cloud security*: Avanade Perspective. Available online at http://www.avanade.com/Documents/Research%20and%20Insights/practicalguidetocloudcomputingsecurity574834.pdf (Accessed: 08 June 2011)