# Overcoming the Barriers to Enterprise Cloud Adoption within Nigerian Consumer Constituency

**Chinedu Paschal Uchenna[1*], E. Nworuh Godwin[1], E. Osuagwu Oliver[2], O. Onyesolu Moses[3] and Ahaiwe Josiah[1]**

[1]*Department of Information Management Technology, Federal University of Technology, Owerri, Nigeria.*
[2]*Department of Computer Science, Imo State University, Owerri, Nigeria.*
[3]*Department of Computer Science, Nnamdi Azikiwe University, Akwa, Nigeria.*

*Original Research Article*

## Abstract

The impact of globalization coupled with the pressure by recent economic downturn have stirred increased customer outlook on availability, scalability and efficiency to enterprise information technology (IT) solutions. The increasing interest of a broad based business leaders and organisations centre on how best cloud computing can contain these requirements to reduce or eliminate the huge capital outlay for infrastructure ownership, increase efficiency, ensure higher returns on investment (ROI), dynamic provisioning and utility – such as pay-as-use services. However, the slow adoption of cloud computing by many organizations such as those with high business economic drives and those with very sensitive security concerns raises huge concerns. A number of these enterprises along with some information security professionals have expressed fear of the cloud, stating their unflinching consciousness on security and privacy issues associated with this new computing platform for the next generation of the Internet. Thus, this research paper analyses the level and nature of cloud service adoption and deployment among IT practitioners and organizations in Nigeria. It further identified the various barriers (security, privacy and forensic issues) generating fear and inhibiting the full adoption and deployment of this new IT paradigm. The methodology takes a quantitative approach and the results of which analysis were discussed and interpreted in relation to the key issues of cloud service adoption and deployment to achieve the research aim of the paper. The results of the research survey conducted provisions the research outcomes which attempts to demystify cloud computing and most associated risks in the virtualized cloud environment by pining the

*Corresponding author: puchinedu@yahoo.com; Profoliverosuagwu@gmail.com;*

issues of outsourcing data and its control via external data storage as top ranking among others. Further, Proper implementation of security, privacy and forensic measures were advocated to be seen not just as the cloud providers' sole concern, but the responsibilities of all consumers of the services. Finally, arguments to back-up the need for progression in this new paradigm shift were elucidated.

*Keywords: Cloud computing; cloud security; cloud forensic; security benefits; business benefits.*

# 1 Introduction

**What is a Cloud?** A cloud has been defined as a pool of virtualized computer resources [1]. A cloud has the following attributes:

- Hosts a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications.
- Allows workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines
- Supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures
- Monitors resource use in real time to enable rebalancing of allocations when needed [1].

In their paper, [1] 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.

## 1.1 Cloud Computing

*Cloud computing* is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and de-provisions 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 [1].

In a paper, [2] 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* [2]. In support of this, [1] 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.

Cloud computing environments support grid computing by quickly providing physical and virtual servers on which the grid applications can run [1]. According to his lecture, mid to late '90s, Grid computing was proposed to link and share computing resources [3]. However, Cloud computing should not be confused with grid computing. Grid computing involves dividing a large task into many smaller tasks that run in parallel on separate servers. Grids require many computers, typically in the thousands, and commonly use servers, desktops, and laptops [1].

Clouds also support non-grid environments, such as a three-tier Web architecture running standard or Web 2.0 applications [1].

## 1.1 Cloud Computing Models and Characteristics

Our understanding and appreciation of the security issues in cloud computing are better grasped through adequate discussion of the three computing models that come under its canopy. These models also described as delivery models [4] are:

- Software as a Service – SaaS
- Platform as a Service – PaaS
- Infrastructure as a Service – IaaS [2]

In highlighting the place of these models, [3] in a lecture described Cloud computing to mean selling "X as a service". Thus, exerting:

- **IaaS:** Infrastructure as a Service – as "Selling virtualized hardware"
- **PaaS**: Platform as a service – as "Access to a configurable platform/API"
- **SaaS**: Software as a service – as "Software that runs on top of a cloud"

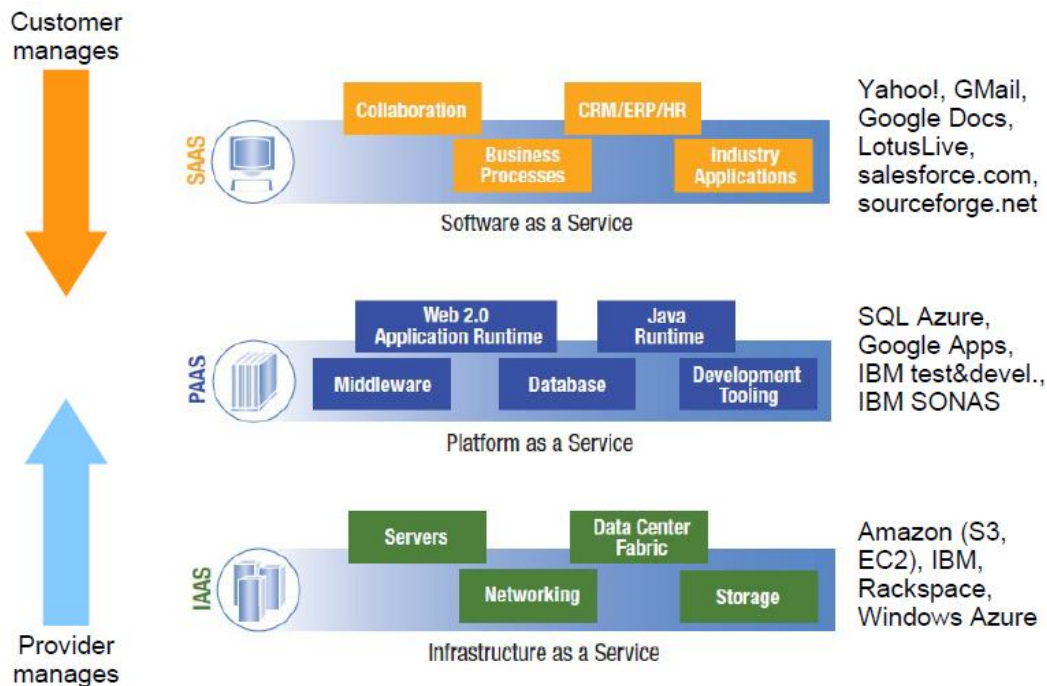The cloud computing stack of Fig. 1.3 shown below would be beneficial in revealing the place of these services.



**Fig. 1.3 Cloud computing service models showing the three delivery models [5]**

The demonstration of adequate understanding of these three delivery models has significantly shed light on creative ways a few companies had implemented cloud services at the different levels. Obviously, organizations could conveniently go virtual or collaborate in virtual organizing by leveraging on the any or the entire cloud service provision. Thus rather than concern itself on the huge initial capital and maintenance cost of owing such cloud services, could allow the cloud service provider to provide the needed intensive ICT resource support to help her concentrate on

core business in a virtual organization. In some case, the said cloud service provider becomes a participating company of the virtual organization.

In order to be considered "cloud" [4] maintained that these delivery models must be deployed on top of cloud infrastructure that satisfies the following five characteristics:

1. On-demand self-service
2. Ubiquitous network access
3. Location independent resource pooling
4. Rapid elasticity
5. Pay per use [4]

Thus, the four deployment models are:

1. **Private (internal) cloud**: enterprise owned or leased, behind a firewall
2. **Public (external) cloud**: sold to the public, mega-scale infrastructure (e.g. Amazon EC2)
3. **Hybrid cloud (virtual private cloud)**: composition of two or more clouds (e.g. Amazon VPC)
4. **Community cloud**: shared infrastructure for specific community (e.g. academic clouds) [4].

# 2 Research Methodologies

A hypothetic deductive methodology (quantitative approach) involving survey design, distribution, collation and computational analysis using, frequency distribution and percentage method; Discriminant Analyses using statistical packages such as Excel, and SPSS. The results of such analysis has been discussed and interpreted in relation to the key issue of this research paper. This research adopted Quantitative approach which has to do with quantity and measurement as well as interaction with stakeholders [6]. 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.

## 2.1 Sampling Frame

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). The researcher accessed these populations of respondents, tagged "college of fellows" with expert opinions via the identified professional bodies and associations to which the researcher's registration and membership exists. This facilitated some friendly responses and reliability of data. The population, therefore, was made up of fellows of CPN and NCS, which comprises stakeholders from the following IT collaborative or related background:

| | |
|---|---|
| • Virtual organizations | 11 |
| • Outsourcing (project outsourcing/ BPO) | 22 |
| • Network organizations | 63 |
| • Cloud/ internet vendors | 15 |
| • Other IT firms | 9 |
| **Total** | **120** |

The total population in this research was 180 respondents. These represents licensed CPN members who at the time of study maintained active and fellow membership status with NCS. Also, some selected organisations where used to administer the structured interview questions.

These represent organisations which maintain corporate membership status with CPN and/or NCS, or whose interviewed staff are registered and practicing professionals.

### 2.1.1 Respondents

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.

Among those who were interviewed in the course of the field work include a staff of an IT company- New Horizon, Ikeja, Nigeria, two employees of a telecommunication company- MTN, Lagos, Nigeria, and staff of some randomly selected commercial bank in Lagos, Nigeria: These include Standard Chartered Bank, Agidingbi, Ikeja, EcoBank, Awolowo Way, Ikeja, Skybank, First Bank and Zenith Bank PLC.

### 2.1.2 Sampling size

The researcher employed the use of Yaro Yammeh's standard formula as cited by [7] for the determination of the sample size from the population. This is given by Fig. 2.1.2 as shown:
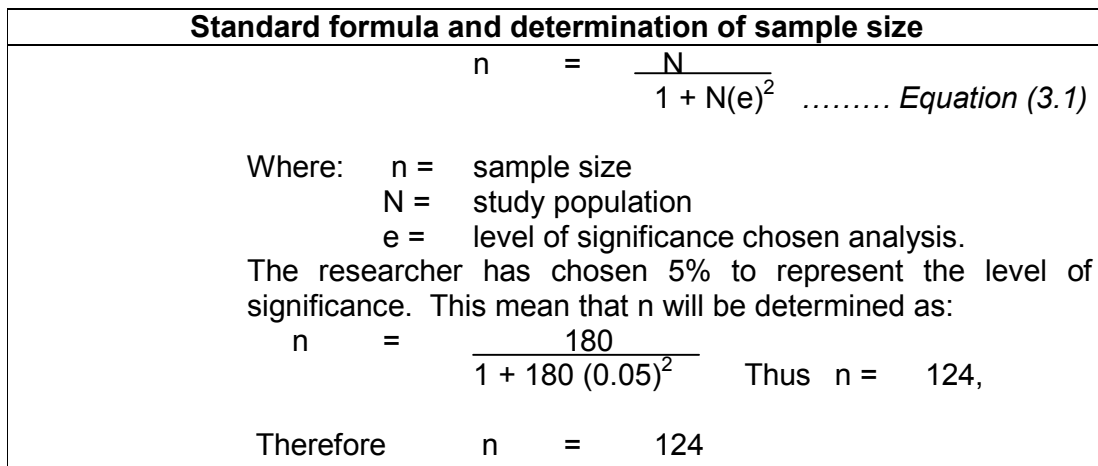
| Standard formula and determination of sample size |
|---|
| $$n \quad = \quad \frac{N}{1 + N(e)^2} \quad \text{……… Equation (3.1)}$$ <br><br> Where:  $n =$  sample size <br> $N =$  study population <br> $e =$  level of significance chosen analysis. <br> The researcher has chosen 5% to represent the level of significance.  This mean that n will be determined as: <br> $$n \quad = \quad \frac{180}{1 + 180\,(0.05)^2} \quad \text{Thus } n = \quad 124,$$ <br><br> Therefore  $n \quad = \quad 124$ |

**Fig. 2.1.2 Showing standard formula and determination of sample size [7]**

## 2.2 Sampling Techniques

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 [8].

## 2.3 Statistical Treatment of Data

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 [9] puts it "the

percentage method is widely used in managerial and social researches". According to him the formula is as represented in Fig. 2.3 below:
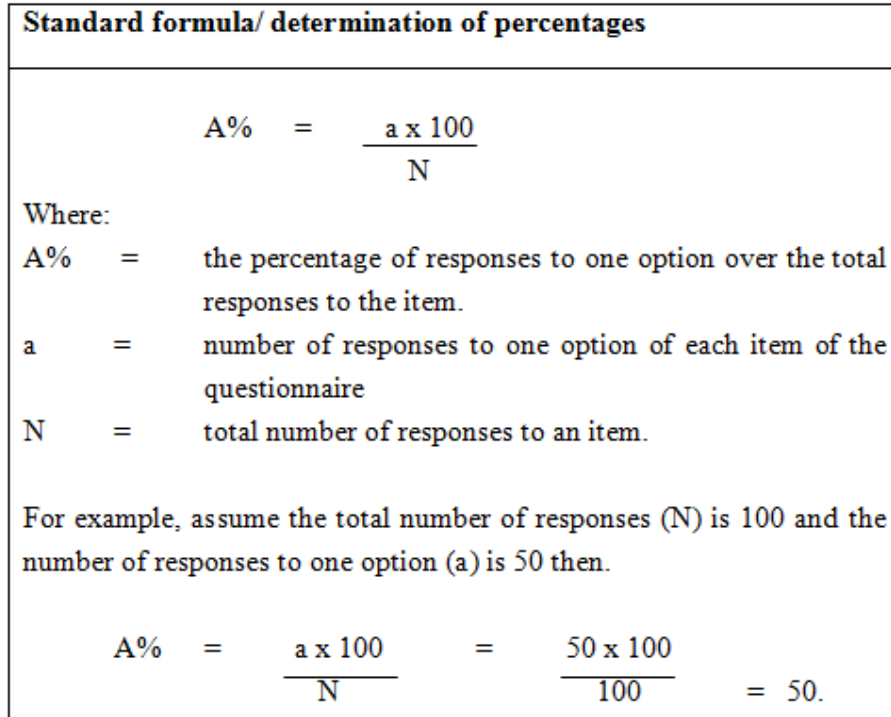
---

**Standard formula/ determination of percentages**

$$A\% = \frac{a \times 100}{N}$$

Where:

$A\%$   =   the percentage of responses to one option over the total responses to the item.

$a$   =   number of responses to one option of each item of the questionnaire

$N$   =   total number of responses to an item.

For example, assume the total number of responses (N) is 100 and the number of responses to one option (a) is 50 then.

$$A\% = \frac{a \times 100}{N} = \frac{50 \times 100}{100} = 50.$$

---

**Fig. 2.3 Showing standard formula and determination of percentages [9]**

# 3 Data Presentation and Analysis of Results

## 3.1 Respondent's Characteristics and Classifications

There were a total of one hundred and eighty (180) active fellows from the College of Fellows; representing IT professionals in the focus groups (CPN and NCS) which constituted the research population. One hundred and twenty four (124) of this representing sample size from the named population received a web link to the online questionnaire form distributed by the researcher via their respective email addresses. A total percentage of 97% of these (representing a total of 120 respondents) properly filled and submitted the survey instrument.

The respondents selected were made up of approximately 62% employees, 13% service providers, 8% customers, and 17% strategic partners pulled from within organisations identified or believed to be participating in some form of collaborative projects or businesses with others. These organisations include those whose business or project activities have some degree of advance ICT support both in and out of the organisations. Based on their nature of organisation, these respondents represent stakeholders from organisations of 53% network groups, 18% outsourcing firms, 9% virtual firms, 13% Internet/ Cloud Vendor and 8% of others. Similarly, and as previously highlighted, accessing responses based on the nature of business, 21% respondents represent stakeholders from educational sector, 11% Manufacturing, 38% Service, 8% Finance, and 22% Development sectors. A vast majority of these 60% indicated to operate under small sized organization (between 10 to 50 employees), 25% are medium sized (50 to 100 employees), while the rest 15% come under large sized organization (100 employees above).

## 3.2 General Presentation and Analysis of Data

The research work presents an in-depth analysis of the results of the survey, together with some comments based on the findings.

### 3.2.1 Nature of business

Cloud computing is metamorphosing from topic of discussion into real world implementation among many organisations biding to stay globally visible and competitive in the digitized marketplace. Conversely, of all those whose nature of business are generally information-based, finance (20%) showed highest degree of strong disagreement to this paradigm shift. However, on the overall, manufacturing based businesses (46.15%- disagree and 7.69%- strongly disagree) followed by the financial sector (20%) which constituted only 8% of the total participants among others (see chart 3.2.1 below) indicated a striking pull back from this evolving paradigm as they by this percentages disagreed to the deployment of cloud computing as the future IT model of their organizational businesses. Further concern expressed by one of the interview respondent pinned the Human Resource and their corresponding legal implications as blocking issues to the pathway to cloud computing by some of these organisations. The idea of relieving these IT personnel responsibilities so as to outsource public data containing personal organizational details for service provider infrastructure storage raised fear and so should be subject to strict regulations. Therefore, cloud computing adoption will probably only receive stakeholders' implementation at a slow pace.
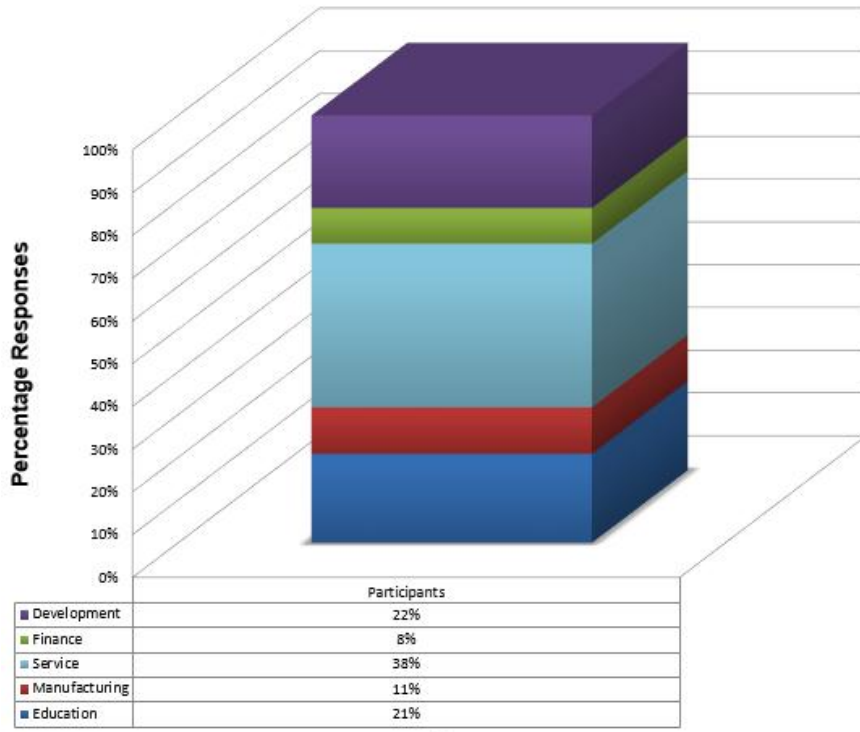


| | Participants |
|---|---|
| ■ Development | 22% |
| ■ Finance | 8% |
| ■ Service | 38% |
| ■ Manufacturing | 11% |
| ■ Education | 21% |

**Chart 3.2.1 Response based on the nature of business (Source: Field work, 2014)**

Financial services organisations, among the pool of our surveyed cloud and virtual organization stakeholders, tend to be more risk-averse when it comes to the innovation of taking the pathway to the cloud- "go cloudy". The risks associated with using cloud computing services are still hard to

assess and presently, very few organisations in this sector are eager to take further risks, despite the potential benefits that includes reducing their IT expenditure. Although many others aside the financial based organisations appear to be using or planned using cloud computing for business critical processes, or for storage of their extremely sensitive data to an appreciable degree (Refer to Section 2.2.5 of this paper for detailed analysis), the overall adoption rate should be taken into perspective. Where a vast majority of software and hardware are still locally installed within these financial organizations Information Systems, declining the total cloud computing share of the total IT spending to be less than 5 percent, the current success of cloud computing is still threatened.

Leveraging on the most optimistic scenarios, the estimated cloud computing's share of total IT spending bridges up at no more than 15 percent. The researcher anticipate that Cloud Computing will definitely remain and even accelerate its growth by 2020, but, for the meantime, on-premise IT will still dominate the IT market until cloud stakeholders are assured of personal control of their confidential data.

### 3.2.2 Cloud computing: from hype to future

*3.2.2.1 Cloud computing is the future model of IT*

There has being several IT concepts and trends that have come and gone at a very fast pace. Some of our respondents positions cloud computing as probably next inline. In the survey, participants strongly concur to the fact that cloud computing is not hype that will subside (in responding to Question 12 in the questionnaire set) as revealed in the Chart 3.2.2 below:
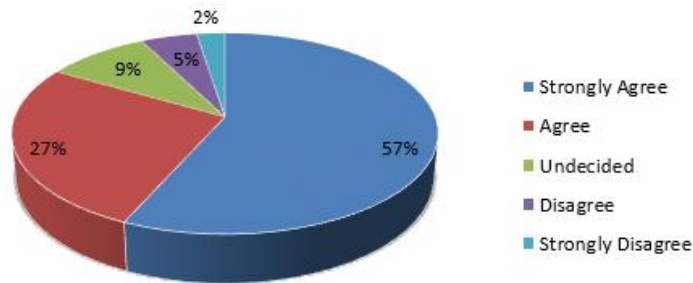


**Chart 3.2.2 Response on cloud computing as IT future model (Source: Field work, 2014)**

While 7 percent of the participants opinions imply they do not agree (with 5 percent- disagreeing and 2 percent- strongly disagreeing), and just 9 percent of them are undecided with the statement that **"cloud computing is the future model of IT"**, yet an overwhelming 84 percent of these agree (by indicating strongly agree- 57 percent and agree- 27 percent) with the statement that cloud computing is the future model of IT.

Obviously, cloud users' maintain remarkably high expectations towards cloud computing. A number of interviewees hold strongly that cloud computing is the next stage of evolution in IT. They feel that the current on-premise IT is highly inefficient and too complex for individual organisations to manage. Cloud computing is the model of choice to shift the complexity to professional vendors and to benefit from their economies-of-scale.

*"In the same way we do not generate our own primary energy source via individual power generators anymore but now receive distributed electric energy from a central power source to our buildings, in the near future, IT resources will be commoditized and delivered from huge IT factories. While the Nigerian market gradually gets more mature, cloud computing will*

*obviously replace our local IT. With this in view, the thought that we still deploying on- premise IT resources becomes quite unreasonable."*

**- Developer of an international servicing firm to the oil and gas sector**

### 3.2.3 Business and security benefits/expectancies

*Application hosting is the most popular use of cloud computing*

In this survey, the respondents from those organisations that are already or plan using cloud computing identified that the most commonly used type of services are application hosting/ development (73 percent), data storage (53 percent), and e-mail and messaging (56 percent). Finance and ERP (18 percent) and BPM/ Project Outsourcing (24 percent) offerings are yet to become commonplace in the cloud in the Nigerian IT market. The Chart 3.2.3A on the percentage response on usage of various cloud services following provides graphical representations:
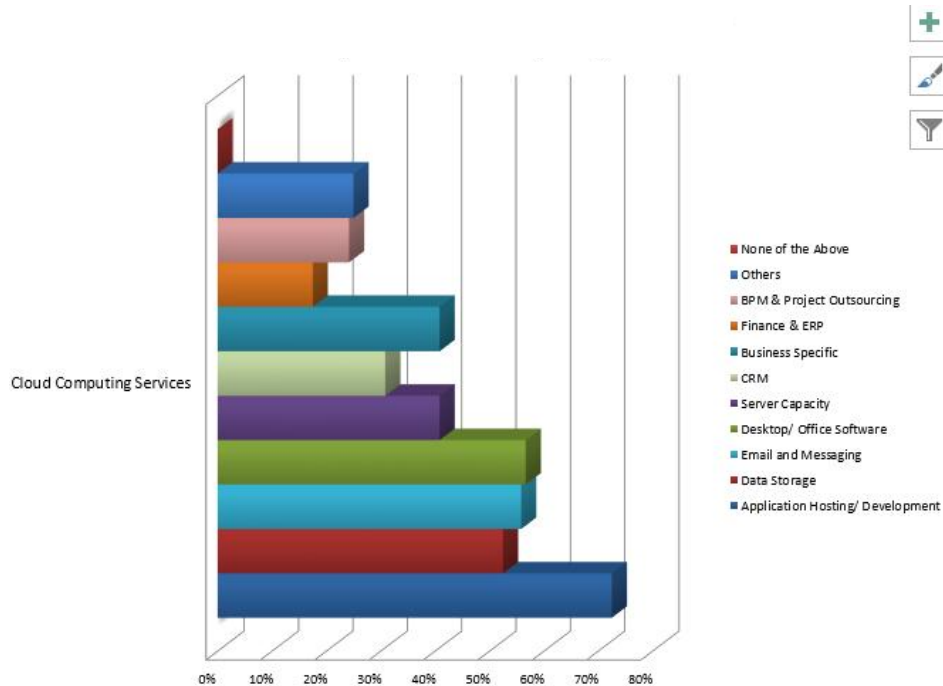


**Chart 3.2.3A Response on usage of cloud computing services (Source: Field work, 2014)**

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

Participants in there 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 Chart 3.2.3B on the percentage response on the business and security benefits below for detailed representations. Some interviewees complained about the rigidness of their internal IT, combined with a delayed 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.
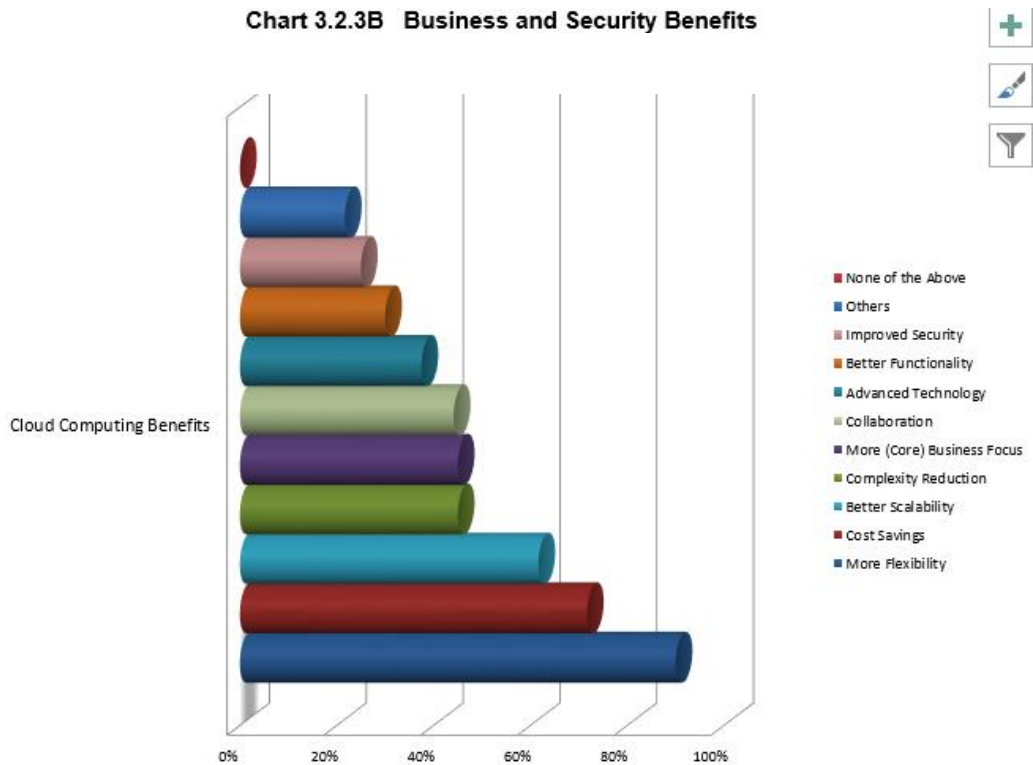
## Chart 3.2.3B  Business and Security Benefits

**Chart 3.2.3B Response on business and security benefits (Source: Field work, 2014)**

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 exceed 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. This 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.

### 3.2.4 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.

### 3.2.5 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 Chart 3.2.5(a) on the degree of movement of business critical systems and storage of sensitive data in the cloud:

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.

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 3.2.5(b) which represent response on measures of security concerns/cloud dependency.

> *"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.***
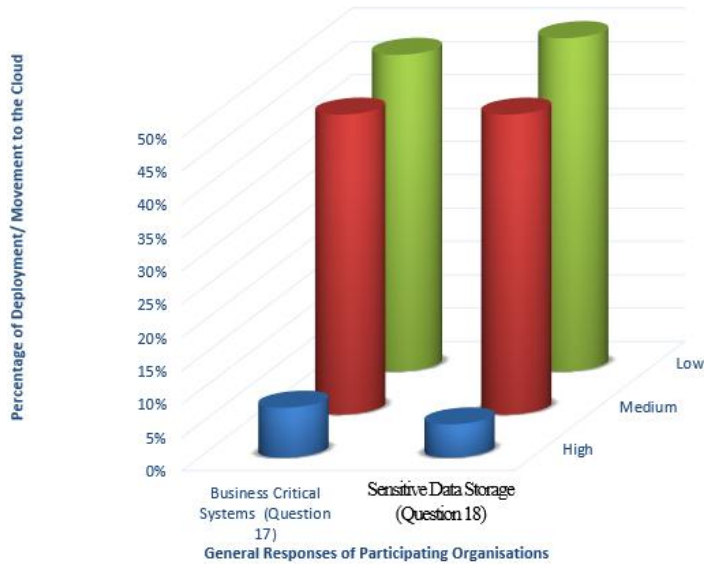
**Chart 3.2.5(a) Response on degree of movement to the cloud (Source: Field work, 2014)**
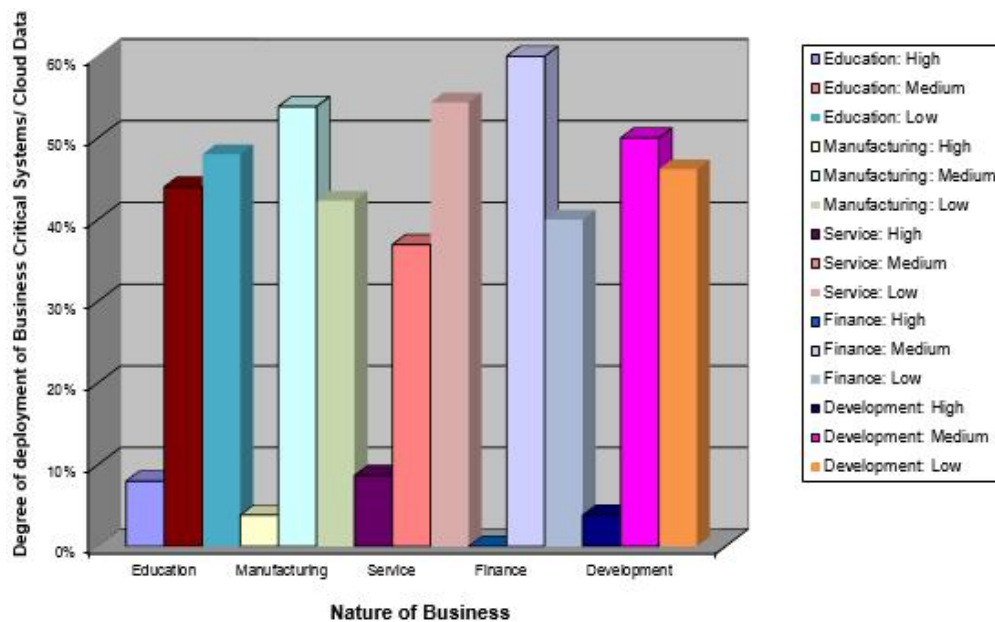


**Chart 3.2.5(b) Response on measures of security concerns/cloud dependency
(Source: Field work, 2014)**

## 3.2.6 Further Comments from the cloud computing market

*"The impact of cloud computing are not just measurable in the lives of individuals. Todays' employees are now on the outlook for the same access flexibility and ease of use at work as they have with applications in their personal lives. This suggests the need for sharing information as well as collaborating on projects just as they are engaged chatting on social networks and invite people to participate or comment on their blogs. As information sharing is*

*vital to these individuals, its need cannot be over emphasized within organisations. But availing the needed time, money or infrastructure to provide this experience for most staff are difficult with many organisations. This is where cloud computing becomes your only alternative."*

*"We are not in doubt that the cloud computing is here to stay and is already impacting heavily on IT world. Where there is increasing flexibility and responsiveness of web applications to meet user needs, thereby reflecting increasingly on the fact most people are collaborative whether at home and in the workplace, innovations in information creation and distribution are definitely a big challenge to traditional notions and boundaries."*

*-Israel Akujobi, Project Director, Jemak Consulting, Nigeria.*

*"It is not a news that most companies in reality are already accustomed with moving data outside of their organization. Consider the present rise of mobility, hosting, outsourcing needs of these organisations."*

*-Timothy, IT Infrastructure Architect, New Horizon Nigeria.*

*"Where Standards are perceived to be an issue, however, also take into cognizance that a cloud is basically built on TCP/IP, HTTP and HTML. So interoperability is available in its most basic form. We know most people are freely using such cloud services like Google doc, Skype and Facebook without known concerns or fear. Moreover, as appropriate standards gradually converge based on the SOA architecture principles, more and more needs would evolve for cloud users to exploit in the IT marketplace."*

*- Victor Ezeliorah, Developer, Intels Nigeria.*

*"Just like what we now find with most software and web development where already made templates simplifies the job for developers, cloud computing is not intend to replace the need for a customer's or organization's IT department but instead transforms its role. Rather than focusing on technical issues and architecture, IT departments can now associate better and nearer to the business and help in translating all business requirements into cloud computing solutions, their configuration, change management, integration, implementation and governance within the provisioned IT landscape. This would imply providing IT departments an unusual level of responsiveness to any IT matter."*

*- John Akpukpu, Infrastructure Support Engineer, MTN Nigeria.*

*"Here at Expertech we are not unaware of the challenges or possible findings of the survey with our own valued customers. Cloud computing is not a hype. Moving up the service layers from IaaS to real SaaS we are faced with the way forward for computing in the coming years; especially SaaS, with software upgrades and licenses on a 'pay-what-you-use' basis."*

*- Emma Nwachukwu, Systems Engineer, Expert Technologies (Nig.) Ltd.*

*"We can see, from what is real or perceived, as well as from the questions, that the survey truly reveals the present atmosphere in today's marketplace. Cloud computing is swiftly invading than is generally anticipated. To be candid, most of us are already using cloud without being conscious of it." "Based on our experience, we could overcome most of the fears knowing that the issues of security and privacy are justified for any evolving IT innovation. However, the cloud providers, users and legislative bodies should objectively examine the available options."*

*- Fredrick, IT Sales Engineer, Jumia, Nigeria.*

# 4 Challenges to Cloud Adoption and Deployment

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 move to 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 and VO participants.

There are major and note worthy concerns to data security in the cloud due to failure of service providers and malicious attacks from hackers, a midst 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 our interview, 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. Therefore, the cloud is inherently neither secure nor dependable from the perspective of some of the cloud customers.

# 5 Suggestions and Conclusion

## 5.1 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 [10].

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.

## 5.2 Discussions and 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 given 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 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 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 digitalised society left every one with no other option than to accept the drive in this new direction and computing paradigm.

## 5.3 Conclusion

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 which need to be overcome first in the Nigeria market 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 economic benefits of cloud computing adoption (cost containment of the initial capital outlay and maintenance cost of such ICT intensive setup) as well as inherent potential benefits for the corporate value creation, we forecast that there is increasing interest in virtualisation or the process of becoming "Cloudy". Hence, adopting and deploying cloud services are relevant strategic assets for ensuring corporate visibility, sustained competitiveness, customer satisfaction, shareholder wealth creation and overall stakeholder value creation.

# 6 Recommendations and Directives for Further Research

## 6.1 Recommendations

Upon the bedrocks propounded to promote cloud-based virtualised environment among organisations, this research seeks to proffer the following recommendations which implementation would greatly ameliorate the existing barriers to enhance effective deployment and adoption of cloud computing in Nigeria as a future IT model among the constituencies of the various consumers of the services:

- Deploying cloud computing backbone in Nigeria require the steady supply of electrical power both to assure the cloud users' reliable network connectivity and to manage the service providers' data centers.
- There should be accelerated effort by the federal government to effectively develop a national broadband strategy and roadmap as a measure towards stimulating the rate of adoption and degree of deployment of cloud computing in Nigeria.
- More data centers should be established within the federation to help beef up the state of awareness, level of deployments and dependency on cloud computing among consumers. The availability will also not only help to reduce cost of access, but promote monitoring for security purposes and protection of local contents by relevant regulatory or legislative bodies.
- Thus, legislative bodies in Nigeria should follow the internationally known best practices to advance a strong legal framework on data protection with the clearly enhanced Service Level Agreements (SLA) in place.

- Finally, developers should demystify cloud to relief fears to its adoption by developing dependable and trusted platforms and apps which promotes user data outsourcing with user data control rather than user outsourcing their

## 6.2 Directives for Further Research

It is recommended that the follow-up of this research be conducted with the analysis of how to handle cloud security, privacy and forensic challenges.

Further, researches are recommended to investigate into overcoming fears to the cloud service adoption through the use of dependable and Trusted Computing and applied cryptographic techniques. The outcome would help enterprises and individuals gain assurance around their cloud computing provider's internal controls and security.

Finally, researches on appreciating the role of virtual world security as a strategy for securing information systems (IS) in a global project. This could also carry along the focus on the cloud computing as an IT strategy for global IS project management.

# Competing Interests

Authors have declared that no competing interests exist.

# References

[1]     Boss, et al. Cloud computing: High performance on demand solutions (HiPODS). Version 1.0; 2007. Available: http://www.ibm.com/developerworks/websphere/zones/hipods/ (Accessed: 20 May 2011).

[2]     Siddiqui M. Cloud computing security: Final paper submitted spring; 2011. Available:http://blogs.techconception.com/manny/content/binary/Manny%20Siddiqui%20-%20Cloud%20Computing%20Security.pdf (Accessed: 20 May 2011).

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

[4]     Reilly D, Wren C, Berry T. Cloud computing: Pros and cons for computer forensic investigations. International Journal Multimedia and Image Processing (IJMIP). 2011;1(1). Available:http://www.infonomics-society.org/IJMIP/Cloud%20Computing_Pros%20and%20Cons%20for%20Computer%20Forensic%20Investigations.pdf (Accessed:  20 May 2011).

[5]     IBM Research (2011). Protocols for Secure Cloud Computing: Christian Cachin, Zurich; 2011. Available: http://www.zurich.ibm.com/~cca/talks/metis2011.pdf ( Accesse:  May12 2013)

[6]     Mitchell S. Studies in history and philosophy of science. Philpapers: Philosophical Research Online Part A. 1993;24(4):565-583.

[7]     Alugbuo CC. A practical guide to project writing. Owerri, Nigeria: Credo Publication; 2002.

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

[9]     Ike KR. Introduction to research method. Umuahia, Nigeria: Chudy Publications; 2003.

[10]    Almond C. A practical guide to cloud computing security: What you need to know now about your business and cloud security. Avanade Perspective; 2009. Available:http://www.avanade.com/Documents/Research%20and%20Insights/practicalguide tocloudcomputingsecurity574834.pdf (Accessed: 08 June 2011).