Archive of Science & Technology
An official Journal of Precious Cornerstone University Ibadan Nigeria
ISSN:0189-3548
Journal Homepage: https://pcujournals.org.ng

Cloud Security Concerns: Assessing the Fears of Service Adoption

Paschal Uchenna Chinedu [1,*]; Wilson Nwankwo[2]; Daniel Aliu[1]; Saliu Mohammed Shaba[3] and Muyideen Omuya Momoh[4]

[1]*Department of Computer Engineering, Edo University Iyamho, Edo State, Nigeria*
[2]*Department of Computer Science, Edo University Iyamho, Edo State, Nigeria*
[3]*Federal College of Freshwater Fisheries Technology, New Buss, Nigeria*
[4]*Faculty of Air Engineering, Air Force Institute of Technology Kaduna, Nigeria*

ARTICLE INFO

Article history:
Article history:
Received September 2020
Received in revised form November 2020
Accepted December 2020
Available online December 2020

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

ABSTRACT

Like most business owners and individual consumers, many small and midsized businesses still undecided on migrating sensitive data or classified information from in-house servers to the cloud due to their lack of trust in the existing information security strategy adopted by cloud service providers (CSPs). The concerns among prospective cloud consumers include risk of unauthorised data access, network traffic and/or account hijacking, data losses, data privacy, dependability and availability, CSP's stability ratings, etc. pose a reasonable concern for the customers on the path to cloud deployment. In preparation for the next wave of cloud adoption which leverages on the enormous business and security benefits of cloud computing, this paper re-assesses these security issues and associated risks to cloud computing adoption. The paper adopted a quantitative approach that surveys the mindset of key IT Professionals in the Nigerian computing ecosystem. The survey was aimed at identifying and ranking the various security and forensic issues plaguing fears to the full cloud adoption and deployment. Following the findings, this paper prescribes the adoption of a mutually-beneficial strategy by CSPs which include incorporating hybrid cloud services with advanced threat computing model. This model is considered relevant across all virtualized environments. Going forward, this paper advocates the need for customer-centric implementation of all cloud security and forensic strategies which would ensure users exercise control over their data at rest or in transit within the network.

*Corresponding author.
E-mail address: (chinedu,paschal@edouniversity.edu.ng)

https://doi.org/10.xxx.

1.0 Introduction

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 return 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 within the constituencies of various consumers of cloud services along with some information security professionals have expressed fears on the path to the cloud, stating their unflinching consciousness on security and privacy issues associated with this new computing platform for the next generation of the Internet.

In view of the foregoing concerns, this paper is focused on assessing the merits of these plaguing hierarchies of security and privacy issues and associated risks responsible for the prevalent operational concerns around this modern computing paradigm. It is also aimed at evolving strategies that would promote awareness on the evolution of cloud service options which would reduce or eliminate the various concerns of potential cloud subscribers.

The specific objectives of this paper are to:

a. Unveil the anatomy of fear in the adoption of "cloudy" environment.
b. Prescribe suitable solution in a bid to remedy the fears of cloud adoption
c. Describe and evaluate the steps in the cloud computing threat model for a purposeful security solution
d. Explain the cloud computing operational concerns and measures for meaningful solutions
e. Analyse the cloud security and privacy issues among the IT professional in the Nigerian constituency.
f. Re-assess cloud computing security challenges, and make reasoned conclusions for progressions in the new direction.

1.1 Cloud Computing

A cloud is a pool of virtualized computer resources (Ullah et al. 2018). It is more than a collection of computer resources; hence it provides a mechanism to manage those resources. By means of provisioning, change requests, re-imaging, workload rebalancing, de-provisioning, and monitoring. Cloud computing is a term that describes 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 (Roy and Jain, 2015).

SoftwareTestingHelp (2021), and Chinedu and Osuagwu (2018) have described cloud computing as nothing but a way for renting the Software, Platform and/or Infrastructure hosted by a provider. The word *Cloud* implies that services provided by the service provide is accessed over the Internet. Thus, it is the cloud service provider that installs, maintains, scales and monitors hardware and/or software services for its customers who access these services via the Internet. Chinedu and Osuagwu (2018) noted that cloud computing also includes applications extended to be provisioned through the Internet. These cloud applications are run in large data centres driven by distributed servers. Accordingly, anyone who has Internet access or connection could access a cloud application following subscription. However, security pervades technology (Nwankwo, 2020) and by extension the security issues in a cloud computing environment are better grasped through adequate assessment of the risks and threats associated with the three computing models that come under its canopy (Chinedu et al, 2013). According to Harkut (2020), the service or delivery models are:

a. Software as a Service – SaaS
b. Platform as a Service – PaaS also called **Hardware as a Service (HaaS).**
c. Infrastructure as a Service – IaaS (Chinedu et al, 2013; Harkut,2020).

1.2 Risk Assessment of the Cloud Model

The cloud model comprises three basic service models (see Table 1), four deployment models (see Table 2) and five essential characteristics (see Table 3). Overall, the risks and benefits differ from model to model and it is important to note that when considering different types of service and deployment models, enterprises consider the risks that accompany them (ISACA, 2009).

Table 1. Cloud Computing Service Models

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.	• Availability • Confidentiality • Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) • Data ownership • 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).	• Who owns the applications? • Where do the applications reside?

Table 2. Cloud Computing Deployment Models.

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private cloud	• Operated solely for an organization • May be managed by the organization or a third party • May exist on-premise or off-premise	• Cloud services with minimum risk • May not provide the scalability and agility of public cloud services
Community cloud	• Shared by several organizations • Supports a specific community that has shared mission or interest. • May be managed by the organizations or a third party • May reside on-premise or off-premise	• Same as private cloud, plus: • Data may be stored with the data of competitors.
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud Services	• Same as community cloud, plus: • 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)	• Aggregate risk of merging different deployment models • Classification and labelling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.

As may be observed in the characteristics presented in Table 3, there are many approaches and challenges to cloud computing. The benefits to the enterprise, as well as the risks, will vary depending on the types of service and deployment models subscribed to (ISACA, 2009).

Table 3. Cloud Computing Essential Characteristics

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.

1.3 Anatomy of Fear: Need for Cloud Security

Historically, enterprises and users feel more comfortable and confident in storing and maintaining their data on their private computers located in their private network environments. The present concern expressed by Siddiqui (2011) with the advent of cloud computing where the data storage would 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 the origin of the concerns for security.

The concern is that total control is maintained where the data infrastructure are housed within the boundaries of the organization and for which appropriate security mechanisms could be implemented. Installations of hardware and trusted software could be done with ease to create secure perimeter around the internal network; 'security-by-complexity' could be affected by adding multiple layers of security, etc. However, once the data leaves the private network into the cloud, the owner loses control over it as well as the security around it. In the cloud, total dependence as to the security of the data is on the provider to offer these services (Siddiqui, 2011).

The fears based on the concern of where the data emanated from (traditional standalone/ network environment), and where it is going (cloud computing- "cloudy") have been examined and hence outlined by Hasan (2011), against the following security, privacy and forensic issues:

A. Confidentiality
    a. Will the sensitive data stored on a cloud remain confidential? Will cloud compromise leak confidential client data (i.e., fear of loss of control over data)
    b. Will the cloud provider be honest and won't peek into the data?
B. Integrity
    a. How does the data owner know that the cloud provider is doing the computations correctly?
    b. How would the subscriber ensure that the cloud provider really stored his data without tampering with it?
C. Availability
    a. Will critical systems go if the provider is attacked in a Denial of Service attack?
    b. What happens if cloud provider goes out of business?

D. Privacy issues raised via massive data mining
    a. Cloud stores data from a lot of customers, and can run data mining algorithms to get large amounts of information on clients

E. Increased attack surface
    a. The entities outside the organization store and compute data, and so attackers can target the communication link between cloud provider and clients
    b. Cloud provider employees could be involved in phishing attacks

F. Auditability and forensics
    a. It is difficult to audit data held outside the organization in a cloud
    b. Forensics is made difficult since clients don't maintain data locally

G. Legal quagmire and transitive trust issues
    a. Who is responsible for complying with regulations (SOX, HIPAA, GLBA,etc.)?
    b. If cloud provider subcontracts to third party clouds, will the data still be secure? (Hasan, 2011)

The foregoing are practical issues that are militating 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.

1.4 Cloud Computing Threat Model

According to Metri et al. (2011), it is difficult to build a secure platform without taking a major preliminary step such as appreciating and identifying the various threats to the proposed online platform. A threat model is a model which helps in analyzing a security problem, design mitigation strategies, and evaluate solutions (Hasan, 2011; Cho,2010; Metri et al.,2011).

Metri et al. (2011) further described this model as a theorem which incorporates the following steps reach the solution to 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

1.5 Cloud Data Security Concerns and Solutions

In a survey, IBIS Technology (2020) ranked security as top concern among 81% of business owners, and equally admitted that the cloud is one of the most secure environments to protect data. However, IBM Research (2011), highlights five key concerns about cloud computing. These gave foremost priorities to the issues of "less control" of user to their 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-tenant environment respectively.

Ghani et al (2020) further argued that with increase in size of the data, there is also an increase in data attacks and interceptions in the virtual environment. According to the submission, vitalized environment of cloud computing presents storage services where a user has no control over their data. Under such circumstance, a consumer's concern borders on questions as to: where exactly his data are located, what happens if he deletes his data and whether or not the deleted data were really permanently deleted. These concerns were debunked in a report by IBM Research (2011); Chinedu and Nwankwo (2018). Chinedu and Nwankwo (2018) had proffered the following solutions:

1. Less control: Provider become fully security transparent and offer sophisticated control
2. Data security, wherein the following are implied:

a. Implement secure authentication, authorization, and identity management
b. Isolate multiple tenants from each other
c. Encrypt critical data and ensure they are integrity-protected by client. Encryption involves using a cryptographic algorithm and a cryptographic key in order to transform a plaintext into a ciphertext or not obvious text (Al Beshri, 2013). Thus, encryption is an information security measure that renders data unintelligible to unauthorized readers. According to Hellman (1980) "encryption is a coded transformation of data into a form unreadable to intruders and interlopers who lack the appropriate key to decrypt the encoded data". Encryption is gaining popularity as social and community computing (such as the cloud) is gaining momentum.

Data are the most important resource to a user, and in a public cloud where communal computing and multitenancy are practiced, encryption must be inevitable to ensure confidentiality and integrity of data and data bank. Encryption is implemented to curb impersonation, wiretapping, piracy, spoofing and data diddling which are common abuses in a multi-user environment. There are different encryptions algorithms such as Blowfish, Rijndeal, AES, Crypt,etc to combat some of the known threats.

Chinedu and Nwankwo (2018) had argued that the increasing adoption of the virtualized environment have resulted in the recent rise in cloud computing such that the security of the virtual world is now the primary concern of cloud security. However, they noted that the virtual environment does have some pitfalls particularly security. Security is the foundation upon which the service (SaaS) lies. In the investigation, there are several areas of concern regarding the virtual environment and the ability to provide sufficient security (Chinedu and Nwankwo, 2018). Violino (2018) elucidated on thirteen (13) key areas of security concerns to include:

a. Data breaches
b. Insufficient identity, credential, and access management
c. Insecure interfaces and application programming interfaces (APIs)
d. System Vulnarabilities
e. Account hijacking
f. Malicious Insider
g. Advanced persistent threats (APTs)
h. Data loss
i. Insufficient due diligence
j. Abuse and nefarious use of cloud services
k. Denial of service (DoS)
l. Shared technology vulnerabilities
m. Spectre and Meltdown

2.0 Methodology

Research Design

This research adopted a quantitative approach which involves quantity and measurement as well as interaction with stakeholders. Questionnaires, structured interview and observation were used as instruments of the survey. Data were collected from a sample population including technology experts and professionals from the financial services industry.

The financial services industry included the banking and insurance companies. This industry subsector was selected through purposive sampling owing to its service delivery architecture, current prospects locally, contribution to the socioeconomic ecosystem as well as their dependence on information technologies. The technology experts were drawn from the local IT regulatory body-the Computer Professionals Registration Council of Nigeria (CPN) and the college of fellows of the Nigeria Computer Society (NCS). The random sampling technique was employed. The total population sampled was 180 respondents. 124 persons were selected. The 124 persons were considered a fair representation of the stakeholders. A structured questionnaire was constructed and distributed to the 124 respondents whereas 24 persons from the financial

services subsector were interviewed with respect to their information technology business strategy particularly the use of cloud services. The questionnaire was structured to reflect the qualification and experience of the respondents, cloud services benefits to the organization, risks, threats, security concerns and fears in respect of cloud adoption strategy in their respective organizations.

Statistical data were captured and sorted using MySQL database and later analysed with SPSS software. The frequency distribution and percentage methods were used to analyze the data. This was adopted based on the widely agreement that the percentage method is useful and could be validly used for studies including management, scientific and sociological researches (Ike, 2003; Saunders et al, 2007).

3.0 Results

3.1 Analysis of Results

3.1.1 Business and Security Benefits/ Expectancies

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

Majority of the participants indicate that three core drivers of cloud computing are relevant: flexibility (90 percent), cost savings (72 percent) and scalability of their IT infrastructure (62 percent) (see Figure 1). Some participants complained about the rigidity of their internal IT. Specifically, most large organisations (78 percent) with more than 100 staff indicated that improved flexibility is an essential motivation to migrate to the cloud (Chinedu, 2018).

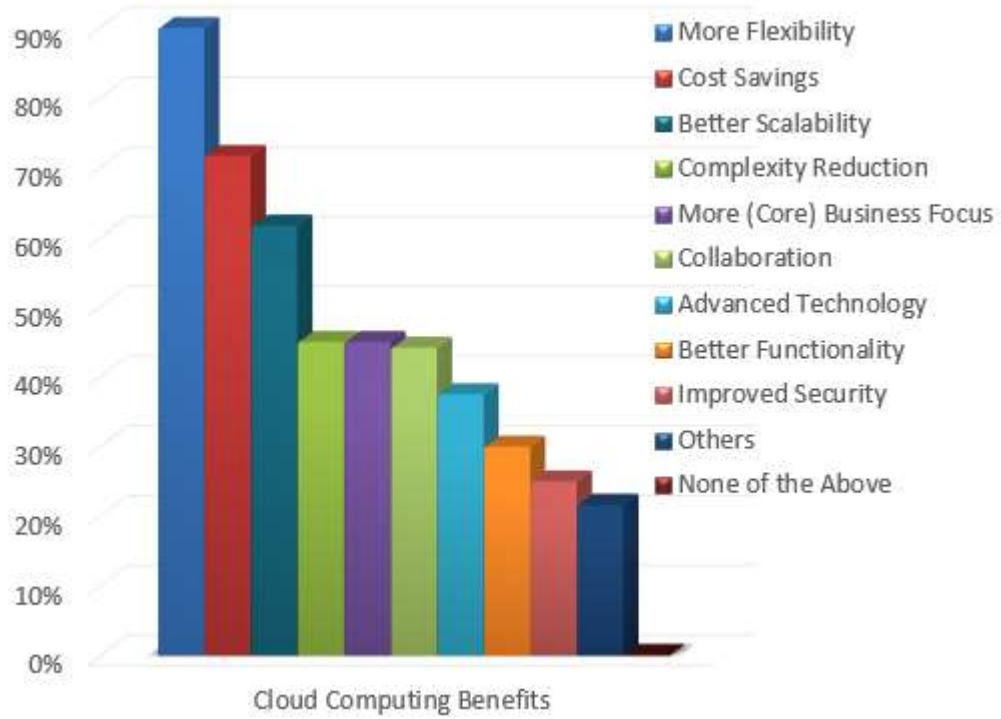

Figure 1. Percentage on business and security benefits.

Some 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 resources 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 is wasted) where as more efficiency could be attained.
The efficient use of IT resources from cloud computing vendors may well explain the resulting significant 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.

3.1.2 Security and Privacy Issues: Obstacles of Cloud Computing

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

An overwhelming majority of the participants (71 percent) consider security issues to be their main concern regarding the use of cloud computing. Privacy issues (60 percent) ranked second. Others such as legal (50 percent), and compliance issues (50 percent) are highlighted to be areas of risk. 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, 83 percent of participants agree that security concerns are a blocking issue when it comes to decision on migrating to the cloud. It appears that potential cloud subscribers are not worried about the lack of security measures, but about the lack of transparency on the side of vendors. 25 percent of participants indicated that improved security is one of the benefits they experience with cloud computing.

3.1.3 Fears on use of Cloud for mission-critical processes

The survey reveals that 49 percent are using or planning to use cloud computing storage services for managing their business-critical processes and for storing their extremely sensitive data. 45 percent maintained use or plan to use this computing paradigm for same purposes. While only a small fraction representing 6 percent prefers the cloud computing for their mission-critical applications (See Figure 2).

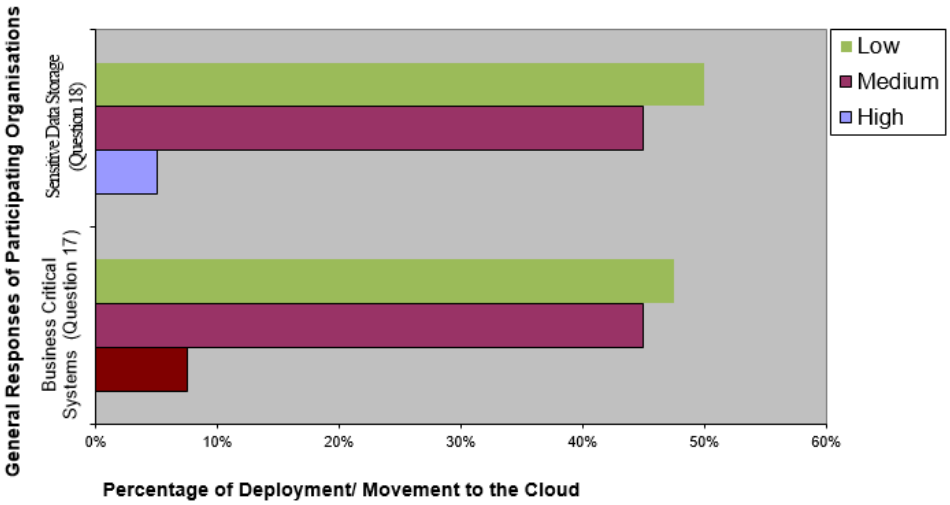

Figure 2. Degree of Deployment/ Movement to the cloud.

Greater concerns on adopting the cloud for business-critical systems and moving extremely sensitive data into the cloud have been made by many especially on the part of finance and banking businesses. This is evident from the responses of 40 percent of the respondents which indicated that they are virtually not considering cloud adoption and the rest (60 percent) participants which indicated they are fairly migrated or considering moving business critical processes and extremely sensitive data to the cloud. This aligns with a statement credited to a sales officer at Standard Chartered Bank which is captured thus:

> *"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 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 (Chinedu, 2018).*

None (0 percent) of the respondents showed affinity to high degree storage or intention to migrate highly classified data into the cloud as against those of the other businesses such as Education, Manufacturing, Service, and Development (see Figure 3).

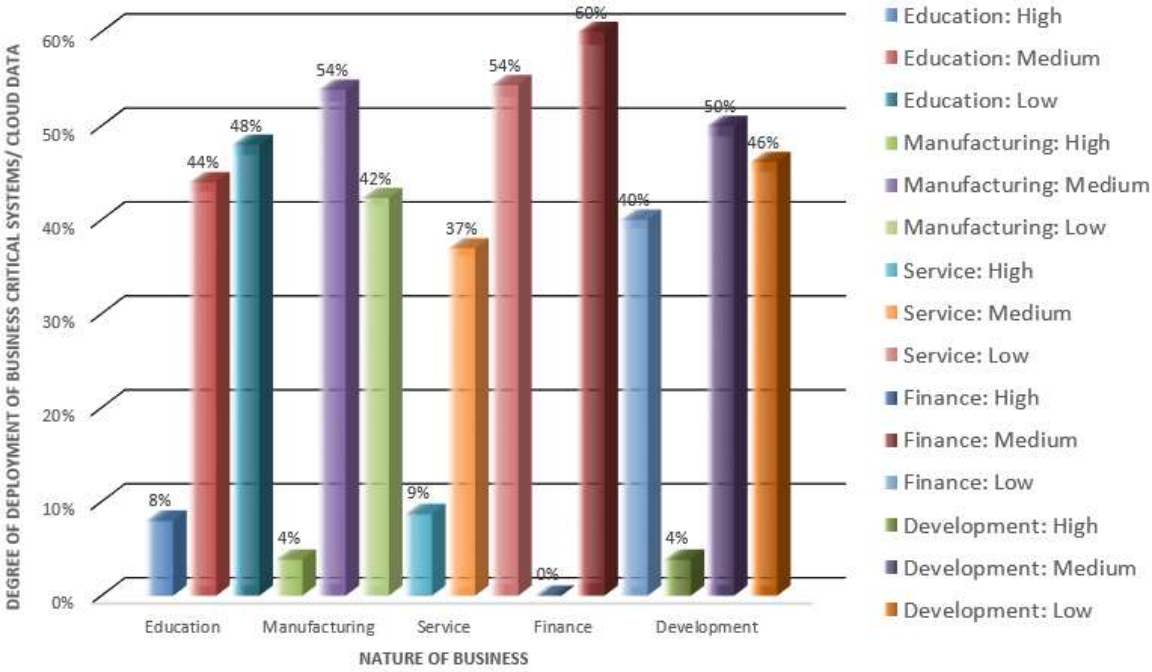

Figure 3. Measures of security concerns/ cloud dependency.

3.2 Debunking Cloud Security Challenges

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 worried about security and privacy concerning the use of cloud computing services as there appears to be no absolute assurance of protection against data breaches, data losses, service traffic hijacking, etc.(Ardagna et al,2015). Matching internal user security requirements with the security measures and controls employed by cloud computing vendors appears somewhat unrealistic at the moment due to discrepancies, lack of transparency, CSPs' non-readiness to guarantee absolute data privacy and protection against malicious attacks from hackers, service outage, etc. amidst the popularity of cloud computing deployment. The recurring event of data breaches appears to have heightened the decline in the enthusiasm especially among potential customers with highly classified missions or business critical systems from their plans to migrate sensitive data into the cloud. Besides, the enormous security benefits accruable from the cloud services, the respondents had 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 potential and prospective cloud customers.

Despite these security and forensic concerns expressed by banks, it would be strange to imagine a world without online banking and financial transactions. The respondents however noted that there is still enormous attraction of the organizations to cloud adoption owing to its economics and convenience such as enterprises long-term IT savings, reduced infrastructure costs and pay-for-service models; which makes cloud services adoption a constant business strategy while the CSPs are expected to revolutionize the existing cloud services to eliminate market concerns on security and data privacy.

Interestingly, not migrating to the cloud may imply paying more than your competitors for the same service (Chinedu, et al. 2015). However, cloud computing may not be for everyone. It is rational to agree that for critical security and risk concerns, a few organisations with highly classified missions and/or extremely sensitive data may opt out of cloud service adoption or better still deploy a private cloud where investment cost would not be considered a factor. However, for any business whose strategy includes reducing cost of infrastructure while remaining productive and competitive, deploying virtual private clouds may not be a viable option especially for small and medium scale businesses. Nevertheless, a virtual private cloud would enable cloud users exercise control over who uses the cloud infrastructure, where data is stored, who has access, etc. To a large extent this choice may satisfy the security assurances demanded by potential cloud users. The implication is that this choice would promote the deployment of hybrid cloud computing.

It is important to note that opportunities usually emanate from challenges, and cloud computing security is not an exemption. The identified concerns pose huge opportunities which CSPs could explore to develop cutting-edge solutions that would enable them win the trust of potential customers. Therefore, it would not be mind-boggling to assert that through developments in cloud security a CSP could gain a competitive advantage over others in the Nigeria marketplace as well as the global business environment. Finally, cloud security is part of the foreseeable evolution of IT. Any organisation intending to attain or sustain competitiveness must needs 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 forensics in the cloud are not as much a nightmare as compared to addressing them in-house.

4.0 Conclusion

Sequel to the outcomes of this study, this paper is a pointer towards progression in a new direction by appreciating that any new technological development may at first elicit fears among stakeholders. History has always had it that while change is permanent embracing the change may have some obstacles in its path. Such adjustments were once recorded against the Internet and e-commerce by financial institutions and their consumers, though those concerns still remain valid, technological advances in the domain of security has helped in reducing their extents.

As noted in the current study not many organisations in the Nigerian business ecosystem are zealous in deploying cloud computing facilities for their businesses. This is traced to the various uncertainties and barriers posed by the operational concerns among the prospective users which need resolution and assurance in the Nigerian marketplace. However, many respondents indicated their attraction to some benefits inherent in the cloud computing services. Thus, leveraging on the several economic and security benefits of cloud computing, it is believed that like other technologies which need time to evolve into maturity, the problems of cloud service delivery including legal, security assurance, data breaches, etc. would be reduced through the development and adoption of advanced strategies and policy frameworks that are mutually beneficial to all stakeholders. Thus, it is submitted that with the demonstration of such strategies by the CSPs, there would be increasing interest in the adoption of cloud services by prospective business owners and even private individuals.

References

Al Beshri, A. M. (2013) Outsourcing data storage without outsourcing trust in cloud computing. PhD thesis, Queensland University of Technology. Retrieved from http://eprints.qut.edu.au/61738/

Ardagna, C.A., Asal, R., Damiani, E., & Vu, Q.H. (2015). From Security to Assurance in the Cloud: A

Survey. ACM Computing Surveys, 2. https://doi.org/10.1145/2767005

Cho, Y. (2010). An overview of cloud security and privacy. Presentation, CS 590, Fall 2010. Retrieved from http://www.cs.purdue.edu/

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

Chinedu, P. U., Nwankwo, W. & Eze, U. F. (2013) Enterprise Cloud Adoption: Leveraging on the Business and Security Benefits. West African Journal of Industrial and Academic Research, 7(1).

Chinedu, P. U. & Nwankwo, W. (2018). Security of Cloud Virtualized Resource on a SaaS Encryption Solution. Science Journal of Energy Engineering, 6(1), 8-17. doi: 10.11648/j.sjee.20180601.12

Chinedu, P. U., Nworuh, Godwin E., Osuagwu, O. E., Onyesolu, M. O. & Ahaiwe, J. (2015). Overcoming the barriers to enterprise cloud adoption within Nigerian consumer constituency. British Journal of Mathematics & Computer Science, 8(1), 39-56.

Chinedu, P. U. & Osuagwu, O. E. (2018). Assessing and Mitigating the Security Concerns, Threats and Associated Risks with Cloud Adoption. Engineering Mathematics, 2(2), 95-106. doi: 10.11648/j.engmath.20180202.17

Ghani, A., Badshah, A., Jan, S. U., Alshdadi, A. A. & Daud, A. (2020). Issues and challenges in Cloud Storage Architecture: A Survey. Researchpedia Journal of Computing, 1(1), 50–65. Doi:10.1109/RpJC.2020

Harkut, D. G. (2020). Introductory Chapter: Cloud Computing Security Challenges. doi: 10.5772/intechopen. 92544

Hasan, R. (2011). Security and Privacy in Cloud Computing: Johns Hopkins University. https://www.cs.jhu.edu/~ragib/sp11/cs412/lectures/600.412.lecture01.pptx

Hellman, M. E. (1980). A cryptanalytic time-memory tradeoff. Information Theory. IEEE Transactions, 26(4)

IBIS TECHNOLOGY (2020). Demystifying the Fear of Cloud Computing https://ibistechnology.com/demystifying-fear-cloud-computing/

IBM RESEARCH (2011). Protocols for Secure Cloud Computing. http://www.zurich.ibm.com/~cca/talks/metis2011.pdf

Ike, K. R. (2003). Introduction to research method. Umuahia, Nigeria: Chudy Publications. ISACA (2009). Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives: Emerging Technology White Paper. http://www.isaca.org

Metri, P. et al. (2011). Privacy issues and challenges in cloud computing. International Journal of Advanced Engineering Sciences and Technologies (IJAEST), 5(1), 1 - 6

Morrow, T.(2018). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. Software Engineering Institute, Canergie Mellon University. https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

Nwankwo, W. (2020). A Review of Critical Security Challenges in SQL-based and NoSQL Systems from 2010 to 2019. International Journal of Advanced Trends in Computer Science and Engineering, 9(2).

Roy, N. & Jain, R. (2015). Cloud Computing: Architecture and Concept of Virtualization. International Journal of Science, Technology & Management, 4(1), Special Issue

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

SoftwareTestingHelp (2021, January 18). Introduction to Cloud Computing Services. https://www.softwaretestinghelp.com/cloud-computing-service-providers/

Ullah, A., Li, J., Shen, & Y. et al.(2018). A control theoretical view of cloud elasticity: taxonomy, survey and challenges. Cluster Computing, 21, 1735–1764 https://doi.org/10.1007/s10586-018-2807-6

Violino, B (2018). The dirty dozen: 12 top cloud security threats for 2018. https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html.