Wireko, Joseph Kofi; Azumah, Kenneth Kwame

Conference Paper

Who "owns" the cloud? An empirical study of cloud governance in cloud computing in Ghana

28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age", Passau, Germany, 30th July - 2nd August, 2017

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Wireko, Joseph Kofi; Azumah, Kenneth Kwame (2017) : Who "owns" the cloud? An empirical study of cloud governance in cloud computing in Ghana, 28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age", Passau, Germany, 30th July - 2nd August, 2017, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/169505

`WHO "OWNS" THE CLOUD? AN EMPIRICAL STUDY OF CLOUD GOVERNANCE IN CLOUD COMPUTING IN GHANA.

Joseph Kofi Wireko and Kenneth Kwame Azumah
Aalborg University-Copenhagen, Denmark

Abstract

Cloud Computing is being widely adopted globally due to its economies of scale, convenience and operational agility to organizations. With Cloud computing, organizations, institutions and companies no longer need to invest heavily in such resources, but instead have the option to migrate to a Cloud model enabling them to purchase or lease resources on line. In an economic context where companies are seeking to make the most from their investments and minimize operating costs, Cloud computing is seen as the solution for competitiveness. The benefits of Cloud computing are therefore of immense importance to the developmental needs of sub-Saharan African countries especially under the Information Communication and Technology for Development (ICT4D) program and the Smart Cities agenda. However, most developing countries, especially those in Sub-Saharan Africa stand the risk of not benefiting fully from the potential of Cloud computing service due to the absence of effective and well-structured decision making process of stakeholders and their accountabilities in Cloud implementation given that one of the basic principles of Cloud computing is that data may be posted or stored "anywhere in the world". This research is an empirical based study that elicited concerns on Cloud services governance and regulation militating against the rapid adoption and use of Cloud computing in Ghana. Respondents were made up of ICT officers who were in the decision making roles regarding the adoption and implementation of Cloud computing in their respective organizations. The results showed that the diversity of technology, service offerings and lack of coherent legislations and governance hindered Cloud service implementation. This has led to many organizations in developing countries sticking to their data centres and private Clouds in a bid to remain "safe" and "own" their data rather than venture into the "unknown" Cloud where ownership and governorship policies are unclear.

Keywords: Cloud governance, Cloud Computing; Data centres; Smart Cities.

1.0 Introduction

Cloud Computing is being widely adopted globally due to its economies of scale, convenience and operational agility to organizations. With Cloud computing, organizations, institutions and companies no longer need to invest heavily in such IT infrastructure, but instead have the option to migrate to a Cloud service model with little upfront costs. In an economic context where companies are seeking to make the most from their investments and minimize operating costs, Cloud computing is seen as the solution for tomorrow.

A prerequisite for a successful adoption of Cloud computing, with all its many benefits, is an understanding of this new phenomenon in IT services. Thus the presence of good Internet connectivity, good software and hardware market, trust in the security of the systems used, access, privacy, reliability and compliance, data location, liability and regulation in regard to Cloud computing are all key areas of concern for a successful Cloud computing implementation.

Notwithstanding the fact that a number of questions remain unanswered in Cloud computing especially in the areas of governance and regulatory conformance, this new mode of IT resource utilization is developing at a rapid and sustained pace, chiefly on account of its ease of use and direct service accessibility via the Internet, and above all to the productivity gains and cost savings it enables. This model now widely adopted by many companies, particularly small and medium-sized firms and very small firms across the world is gaining recognition and relevance in developing countries. Thus the key questions remain as to the ability of companies having adopted Cloud computing technology continue to comply with all the standards of governance in force and applied to the classic business IT environment.

1.1 Cloud computing in Ghana

The benefits of Cloud computing are of immense importance to the developmental needs of sub-Saharan African countries especially under the Information Communication and Technology for Development (ICT4D) program (Kelly Hill, 2015). In Ghana, with the relatively high mobile phone and mobile internet penetration rate of 139.09% and 69.83% respectively (NCA, 2017), Ghana stands to benefit enormously from an effective implementation of Cloud Computing infrastructure. Since the declaration of the government of Ghana Information Communication Technology for Development (ICT4D) program in 2012 and subsequently the launch of the Accra Smart city project, there has been an upsurge in interest in Cloud Computing by both public and private establishments, industry and academia (GSMA, 2016).

In spite of this growing interest, research in the area of governance in Cloud computing lags behind the other elements or characteristics of Cloud computing especially in developing countries. The lack of focus on governance in Cloud Cloud Computing can be traced historically to the way past IT experts and decision makers defined Cloud computing to exclude governance from its key characteristics and rather concentrated on the technical aspects. According to Mell and Grance (2009), Cloud computing built around the set of five essential characteristics: on-demand self-service, broad network access, resource pooling (multi-tenancy), rapid elasticity, and measured services, had been the reference solution for selling or renting different configurable computing resources.

The omission of governance in the original definition reflects the low level of perception of "governance" as a key element in driving and shaping the adoption and implementation of Cloud computing. Thus while there is a growing interest for Cloud management solutions, Cloud governance is left aside, with little or no attention paid to important data and security

concerns. In Ghana, a study conducted by Senya et al., in 2016 on Cloud computing adoption listed technology readiness, top management support and trading partner pressure as most important concerns by businesses in Cloud computing implementation. Curiously and conspicuously missing were the absence of governance and regulatory framework necessary in ensuring a robust and successful Cloud computing. There are also fewer studies done on the importance of governance in Cloud computing in developing countries, especially those in Sub-Saharan Africa. Given the importance of governance in Cloud computing, there is the need to examine why it has low awareness and importance in Cloud implementation, and hence a source of disincentive for rapid Cloud adoption.

1.3 Components (elements) of Cloud computing governance

The core of Cloud governance is based on the description of provider-consumer relationships over different business models. This model should define the way in which an offer is made and how it is consumed. In order to function at all Cloud service models (IaaS, PaaS, SaaS), the model has to be independent of the type of resources involved. O'Neill (2009), Kaisler and Money (2011) identified the components of Cloud governance to involve the definition of policies, parameters and processes that provide automatic aggregation of services. This involves defining and publishing a catalog containing services, managing access and generally assisting with service related operations. Cloud governance comes as a natural step from SOA governance. While migrating services to the Cloud involves several problems like provisioning, security and privacy (Kaisler and Money, 2011), migrating data into the Cloud give rise to problems like data confidentiality, integrity and availability (Cecere, 2011). Cloud governance, over the period has suffered from diverse interpretations and definitions with no clear focus on any specific elements.

However, a study done by Fortis et. al., (2012) identified four key elements or components of Cloud governance framework: Cloud security, Cloud privacy, Cloud Life cycle management and Cloud standards. They showed that the challenges with these four components of Cloud computing governance are what drive businesses (especially SMEs) away from adopting Cloud computing in order to compete favorably in the world market space.

According to Fortis et. al., (2012), Security is the number one concern that inhibits SMEs from adopting the Cloud. In the Cloud environment, the responsibility for security is shared between the Cloud vendor and the application developers. Core steps for creating a governance framework for Cloud security are to provide basic security features that include support for authentication, DoS attack mitigation, firewall policy management, logging, and

basic user and profile management. Even if Cloud providers are providing some minimal security features, they still need to adhere to industry standard frameworks such as an ISO certification. By disclosing their security policies, compliance and practices, Cloud providers can attract businesses and allow clients to evaluate Clouds and help prepare their security management. Also, providing tools (security APIs) for security auditing and management (log handling and management, user profile and privilege management, firewall policies, providing data in an enterprise format etc.) will drive the rate of Cloud adoption by enterprises.

Privacy is another important factor of Cloud adoption. Security and privacy is often a top nonfunctional requirement for Cloud based solutions, in large part due to Cloud topologies that distribute data and function across a dispersed decentralized computing landscape. It is therefore essential that privacy issues are adequately addressed in Cloud contracts and SLAs. In order for an enterprise to migrate to a Cloud environment it must trust its Cloud provider in terms of data privacy. One solution for an early adoption of Cloud from the privacy point of view is for enterprises to categorize the sensitivity of their data based in terms of privacy and confidentiality. Data with low sensitivity can be easier to migrate than one with high sensitivity.

Furthermore, privacy agreements offered by the Cloud providers must adhere to government privacy laws and that Cloud providers need to cover all bases by having a strong monitoring and internal audit (Sotto et. al., 2010). Cloud services have both functional and nonfunctional characteristics. Service Level Agreements (SLAs) between Cloud consumers and providers must fully address both. Life Cycle Management of Cloud governance architecture provides several aspects like the description and deployment of a service in the Cloud, the description of service offers and contracts between service providers and consumers, the management of services and their instances.

Cloud computing has led to a shift from isolated dedicated IT scenarios to scenarios that involve far more collaboration and cooperation among an assembled set of components and services, potentially provided by multiple Cloud service providers. That in turn has led to business and IT topologies that may be, and often are, distributed across multiple domains delineated by boundaries including architectural, design, geographical, cross-organizational, corporate and governmental. As a result, governance aspects of a Cloud topology are also more distributed.

Cloud computing governance has an ongoing obligation to make sure that Cloud service providers maintain compliance with its policies as expressed in SLAs. This includes ensuring the existence and use of an audit program covering all aspects of SLAs, including security

and privacy policies, as well as the existence and use of procedures and methods to carry out and verify that corrective actions take place to maintain compliance with those SLAs.

In Cloud governance framework, the element of standards must specify resource and scalability limits, resource discovery, tenant partitioning, session management, service levels, authorization, access entitlements, and identity. Other standardization areas include resource management protocols, packaging formats, identity protocols, key management protocols, audit formats, compliance formats, and security mechanisms to enable interoperability.

2.0 Literature and Theoretical Review

2.1 Literature Review

There is considerable controversy surrounding the definition of Cloud computing resulting in diverse definitions. For example, Vaquero et al. (2009) have derived a grounded definition of Cloud computing from a literature review and define Cloud computing "as aggregation of IT resources (hardware, platform and services), which can dynamically match the requested demand. Armbrust et al. (2009) define Cloud computing as an on demand solution, which serves at the end of the applications' layer to public customers. From technical point of view, Opitz et. al., (2012) have also provided a working definition of loud computing based on some key characteristics as:

The technology Cloud computing contains abstract, highly scalable and managed on demand infrastructure (server/computer, storage, networks) and on demand software (operation systems, applications, middleware, management and development tools), which can dynamically match the requirements and are paid per usage (2012).

As a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources Cloud computing can be deployed rapidly with minimal management effort or service provider intervention (Ramireddy et al. 2010, Unal & Yates, 2010). Common to the above definitions are certain key characteristics or elements of Cloud computing namely; On-demand self-service, ubiquitous network access, resource pooling, rapid elasticity, scalability, Public-Private collaboration and cost sharing benefits.

In many ways, Cloud computing or Cloud Services has been viewed by some analyst as simply an outsourcing of some IT services out of the firm or the organization due to its cost savings and ease of implementation. Thus Cloud computing is seen as an extension of the Service Oriented Architecture (SOA) which can be managed by the SOA governance, rules and procedures without any fear of security or loss of control. Vaquera et. al., (2009) have

also argued that the use of transparent Service Level Agreements (SLA) can ensure that Cloud service brokers and providers deliver a high level of risk-free Cloud computing services, although they acknowledge that the level of dependence varies strongly between the three service models of Cloud Computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), where the whole application lies in the hands of the provider (Jaster et. al., 2010). This perspective is predicated on the Principal-Agency theory that is supposed to govern the relationships with third parties, thereby ensuring effectiveness and efficiency in service delivery.

Notwithstanding, many IT experts are of the view that this type of "outsourcing" approach also comes with its own disadvantages that could be detrimental to the organization, particularly on the issue of loss of control, ownership and protection of company data from the prying eyes of competitors and unscrupulous users like hackers. For example, Ramireddy et al. [2010] arguing from the client's point of view identified and described the possible "loss of direct control of resources" as one of the negative key issues that create doubts in the minds of IT experts when it comes to Cloud computing. Koehler et al. (2010) described this concern by outlying the requirements of Cloud computing from customers view and concluded that "reputation of the Cloud service provider and the use of standard data formats are more important than those financial aspects such as cost reduction or pricing tariff choice. Other issues in IT security such as trust, multi-tenancy, encryption and compliance have all been identified as disincentives to Cloud Computing (Mell and Grance, 2009). Thus, the cost saving benefits (economies of scale) of Cloud computing (Ambrust et. Al., 2009) is being eroded when considered against the non-financial risks.

The issues of governance, regulatory and legislation represent challenges not only for companies directly involved in the provision and use of Cloud computing services, but also for governments. There is the fear that Cloud computing services in developing countries are not yet capable of complying with best governance practices for business information technology, because companies are unable to have control on who accesses their data, or on the location where their data are stored, given that one of the basic principles of Cloud computing is that data may be stored "anywhere in the world". Stantchev and Tamm in 2013, identified governance rather than technical reasons as the primary motivation for the adoption of Cloud computing by respondents in a survey of German enterprises. Compliance was also identified as an additional challenge and thus any efforts to encourage the rapid adoption of Cloud computing must first understand the fears of businesses regarding these elements and work to alleviate them if not minimize them.

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. One of the most common compliance issues facing an organization is the impact of data location on their ability to ensure compliance. However, a characteristic of many Cloud computing services is that data may be stored redundantly, and may exist in multiple physical locations. Detailed information about the location of an organization's data is potentially uncertain and could vary over time, or is possibly not even disclosed to the Cloud service consumer at all.

This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met, and in some cases even to be sure which of potentially multiple overlapping regulatory requirements take precedence. Even though, external audits and security certifications can alleviate this issue to some extent, they hardly provide the solution as a violation may incur severe penalties from national governments.

2.2 Theoretical Review

2.2.1 The Principal-Agency Theory in Cloud Computing

In Cloud environment, the Principal-Agent relationship is present: the Cloud service consumer is the principal and the Cloud service provider is the agent. When operational control is released from the principal and delegated to the agent (e.g., outsourced), a mechanism is required to minimize risks and costs. This shift of expectations and responsibilities presents a challenge that governance can help mitigate. The interests of a Cloud service consumer and Cloud service provider might initially differ, but need to be harmonized around the core objectives of reducing cost, supporting multi-tenancy, security, regulatory compliance and many other factors. These trusted relationships are essential to establish, maintain, and verify the underlying shared policies and standards required to support seamless operation of on- premise and off-premise enterprise and Cloud technology and services.

In some situations a Cloud service consumer may not know the physical location of a server used to store and process its data and applications. Regardless of whether data is in flight or at rest, physical location and transit between locations could potentially have an impact on the ability to meet enterprise policies and requirements, which in turn could be influenced by other spheres of governance including governmental statutes and regulations. Since these policies and requirements could vary from location to location and are established and applied by multiple entities, they form a critical issue for data governance and subsequently also for Cloud governance.

In addition to the issues surrounding physical location, Cloud scenarios that involve multi-tenancy also raise new data protection issues. Personally Identifiable Information (PII) typically requires imposing limitations on use and accessibility, based on policies, applicable regulations, and laws. Storing information securely and permitting access only by authorized users requires appropriate controls, which can be more challenging when data is stored within a Cloud service provider's infrastructure and not within the direct control of the data owning organization.

A robust Cloud governance framework that integrates and interlocks enterprise policies and standards with Cloud service providers is essential to maintaining a viable level of end-to-end consistency, reliability, and security across the distributed Cloud ecosystem. Establishing a strong framework of Principal-Agent relationship is an important aspect of encouraging Cloud computing adoption.

2.1.2 Global Diffusion of Internet (GDI) Theory

Cloud computing is a service or infrastructure that depends to a very large extent on the Internet to become successful. The ubiquitous presence of the Internet in all its forms in a country is therefore a driver for the adoption of many innovations happening across the globe. Thus for many successful implementation and adoption of technological services, the diffusion of the Internet must precede or go in tandem with their deployment. Cloud computing is not an exception. Cloud computing is no doubt synonymous with the Internet.

Global Diffusion of the Internet (GDI) is a framework developed by the MOSAIC Group (Wolcott et. al., 2001; Verna, 2014) which provides comprehensive framework for describing the diffusion of the Internet in a country. It is a multi-layer project that measures and analyzes the growth of the Internet in a country. The research approach uses the nation-state as the unit of analysis and includes the development of an analytic framework for capturing the state of the Internet within a country at a particular point in time. The framework characterizes diffusion of the Internet using six dimensions: pervasiveness, geographic dispersion, sectoral absorption, connectivity infrastructure, organizational infrastructure, and sophistication of use to highlight Internet diffusion determinants. The GDI is relevant to the adoption and usage of Cloud computing as it seeks to provide the framework for analysing the extent to which the Cloud computing services is largely dependent on the Internet and hence its successful implementation across the country. The role of Internet is paramount in ensuring the timely delivery and exchange of information and data within the network including user response and feedback. Therefore analysis of the six dimensions and the

determinants will help to know whether if the provision of internet infrastructure is concentrated in certain geographical location within the country or in terms of sectoral absorption, provide a measure of the degree of Internet utilization in education, commercial, health care, and public sectors which are seen as key to development. One of the other determinants is the sophistication of use, a measure characterizing usage from conventional to high sophistication that drives innovation and initiatives. The GDI is therefore relevant and useful to stakeholders in understanding the penetration of the Internet and how to invest in allied services and business such as Cloud computing in a country.

3.0 Research Methodology

This research is an empirical based study; designed to elicit concerns and perception on Cloud services governance and regulation militating against the rapid adoption and use of Cloud computing in Ghana. Specifically the study examined the roles of stakeholders and their accountabilities regarding the criteria and policies involved in the planning, architecture, acquisition, deployment, operation and management of Cloud computing in Ghana. Respondents were made up of ICT officers drawn from the list of "Ghana Club 100" companies and the "Enterprise Map of Ghana" (Sutton and Kpentey, 2012) which also contain both public and private organizations that have been profiled from different industries and sizes. Finally, the theory of Global diffusion of Internet (GDI), an extended version of TAM is used to analyse the stage of Ghana's Internet availability and readiness for an effective and successful implementation of Cloud computing (Wolcott et al., 2001).

The data collection method involved the distribution of an electronic survey using Survey Monkey as a collection tool through the mechanism of emails and social media. This method of distribution made it quicker to administer the questionnaire and have respondents make fewer errors in answering questions.

The questionnaire design focused on the subject of governance of Cloud adoption that targeted Chief Information Officers, Information Security Officers, Senior Network Administrators and generally IT directors of companies in Ghana. The sampling frame was purposive because the respondents were uniquely positioned to understand the subject at hand and could authoritatively provide answers for their organisations.

3.1 Results and Discussion

In all, 36 responses were received from 81 respondents, thereby achieving a response rate of 44%. Majority of respondents were from the Banking and Financial Institutions constituting about 34%, followed by Academic/Education and Healthcare (22% each). The bar chart in Fig. 1 shows respondent distribution by industry.

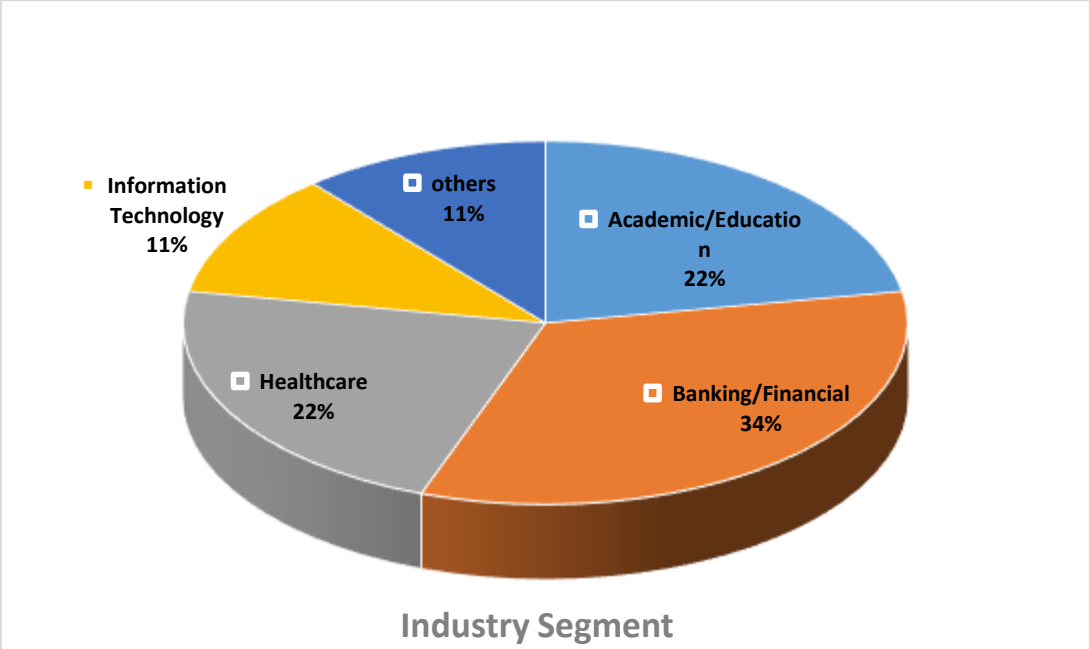

Fig. 1 Industry Segments of Respondents

When asked about where their corporate data are stored, only 22% indicated being stored on the Cloud. Majority of the corporate entities (67%) had their data on premises, an indication of possible fear associated with Cloud adoption (Fig.2). Inferring from Fig 1 and 2, it is observed that the the financial institutions that constitute the majority of respondents are the entities that prefer to store data on premise, hence lack of trust and confidence in Cloud adoption.

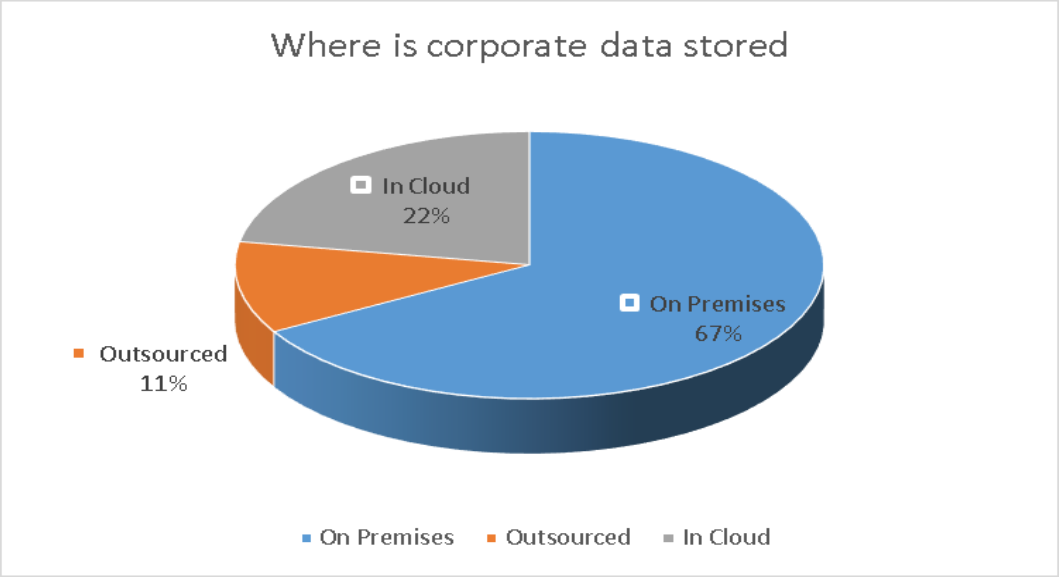

Fig. 2 Where is Corprate Data Store

For those that opted for or will consider Cloud computing implementation (Fig. 3), the private Cloud (56%) was preferred to the hybrid Cloud (44%).

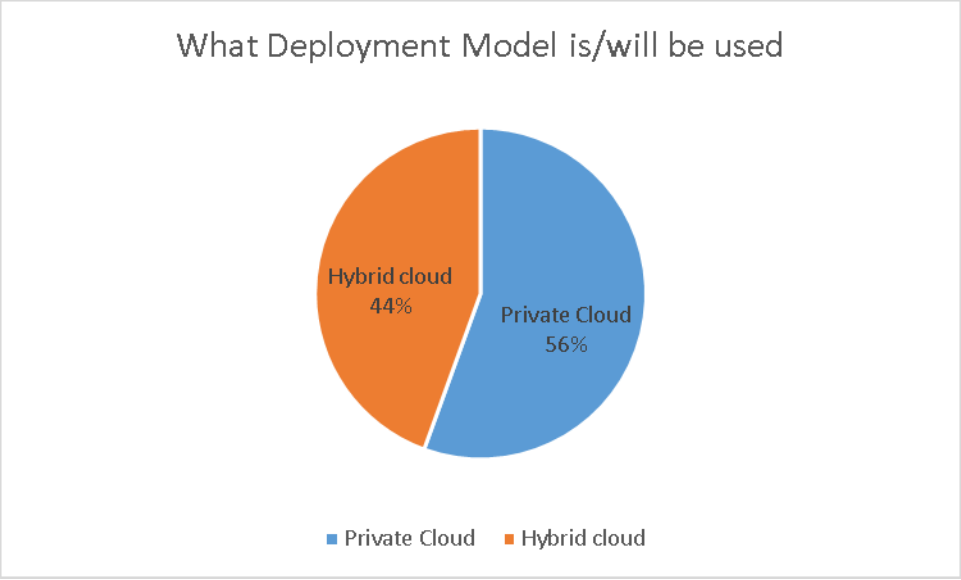

Fig. 3 What Deployment Model is/will be used

When probed further as to the reasons why there is low level of Cloud computing and/or the preferrence for private and on-premises data storage, the following key concerns or reasons were adduced (Fig. 4). All of the respondents did inidcate "fear of loss of data ownership" as important (100%). Risks associated with multi-tenancy in Cloud computing was also considered important, about 72% indicating it to be moderately to

extremely important. The issue of presence of administrative controls that may impede the operational efficiency and service delivery of Cloud users was considered important (over 99%.) while over 97% considered logging and monitoring of Cloud computing usage very and extremely important. Rsepondents also did indicate the importance of Cloud providers in managing access to their network and resources. Over 75% were of the view that access management is important in considering Cloud computing implementation. The importance of logging and monitoring by Cloud providers were also underscored with over 95% affirmation. Over 75.5% of respondents expressed concerns over government data protection regulations as very and extremely important. Regarding the privacy impact assessment 55.6% of respondents viewed it as very important to Cloud adoption and implementation. Regarding the fear and threat from hackers, only 44% considered it to be very important compared to 30% of those who view it as extremely important.

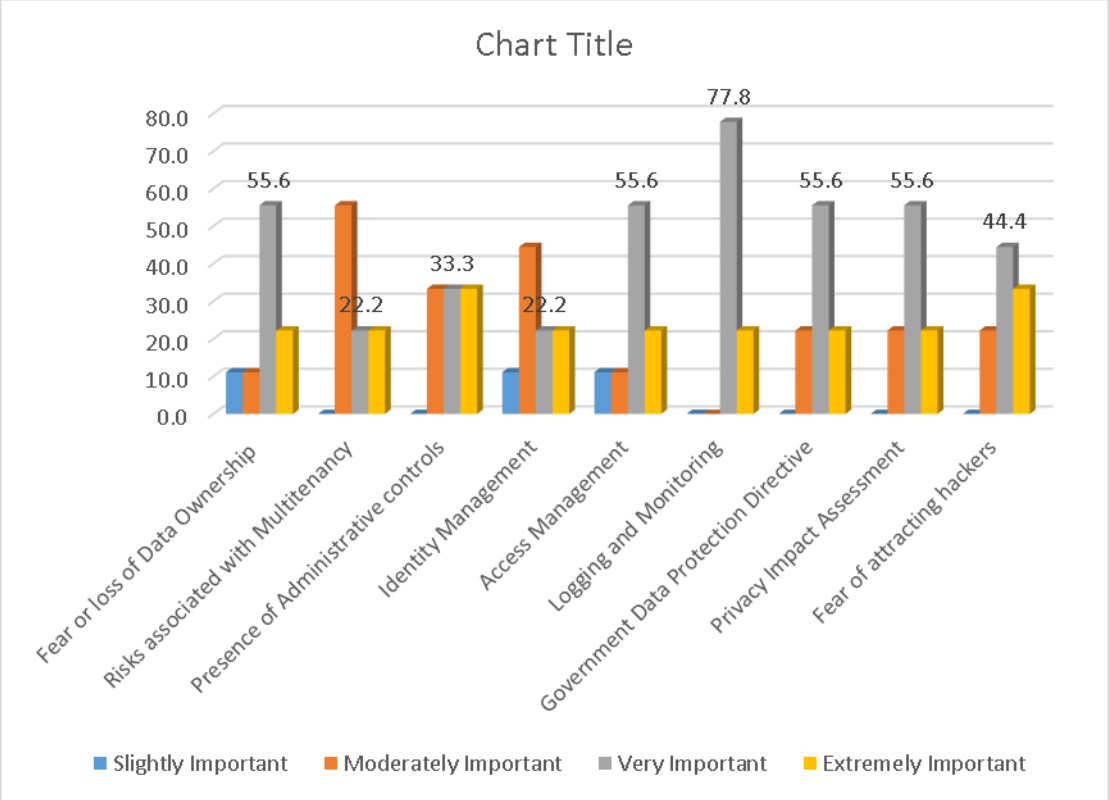

Fig. 4 Governance risks associated with Cloud Computing Adoption in Ghana

Within the IT department, the decision regarding who decides Cloud computing implementation was varied. About 34% indicated that the Head of Information Security decides followed by Chief Information and Network Administrator respectively constituting about 22%. (Fig. 5)

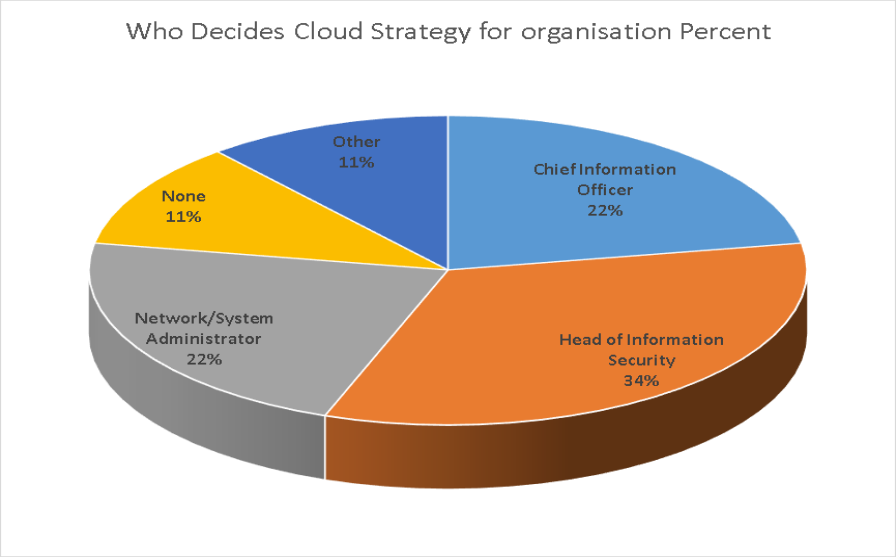

Fig. 5 Who Decides Cloud Strategy for Organisation

On breach detection measures, about 55% indicated that they do not have breach detection measures to identify violations and attacks on their networks in the Cloud (Fig. 6).

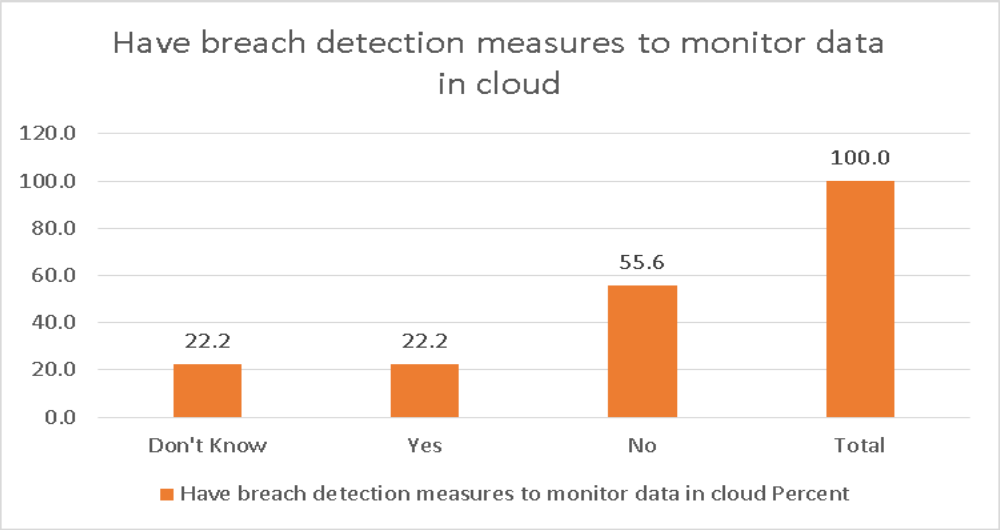

Fig. 6 Have Breach Detection Measures Monitor Data in Cloud

Regarding employee empowerment in adopting Cloud computing, about 66.7% did not have such policies in place (Fig. 7)

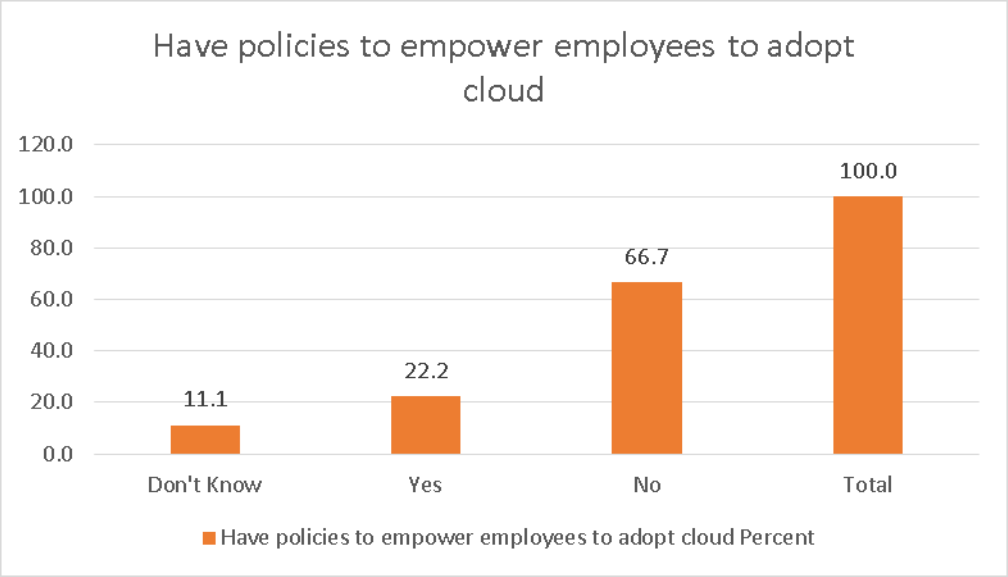

Fig. 8 Have Policies to Empower Employees to Adopt Cloud

In general, 55.6% respondents did indicate that the Information and security department were not consulted regarding the decision to implement Cloud computing.

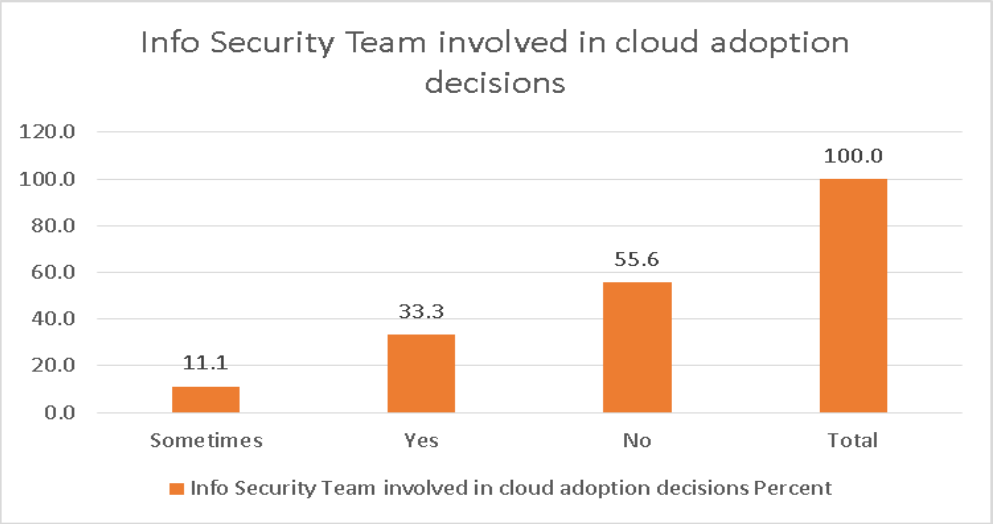

Fig. 9 Information Security Team Involved n Cloud Decisions

When it come to selecting service provider, only 33% indicated that there is a process in place. About 44% had no process in place (Fig. 10)

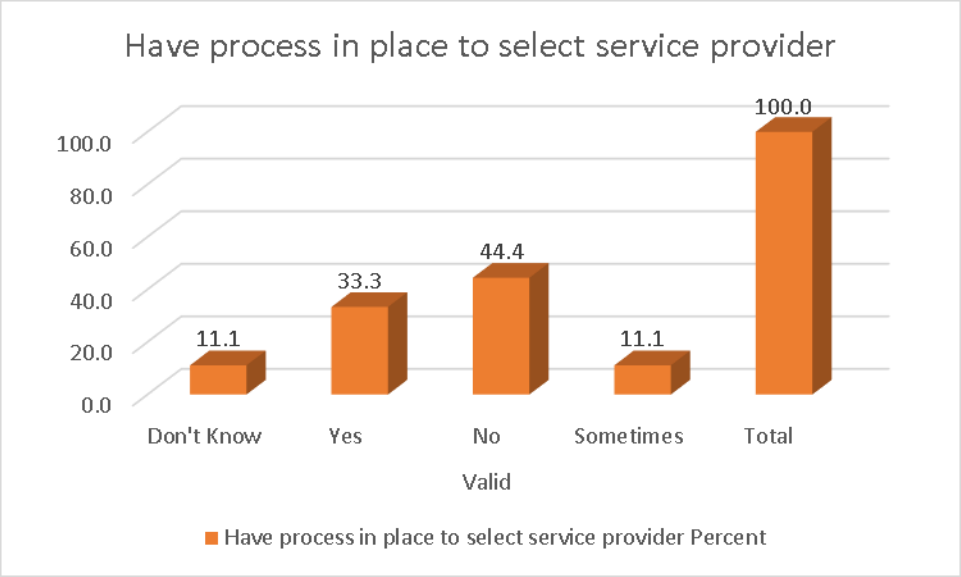

Fig. 10 Have Proces in Place to Select Service provider

About 55.6% were of the view that Internet availability was extremely important compared to about 22% who said was very important. In all 89% considered the availability of the Internet to be important for Cloud computing in Ghana (Fig.11).

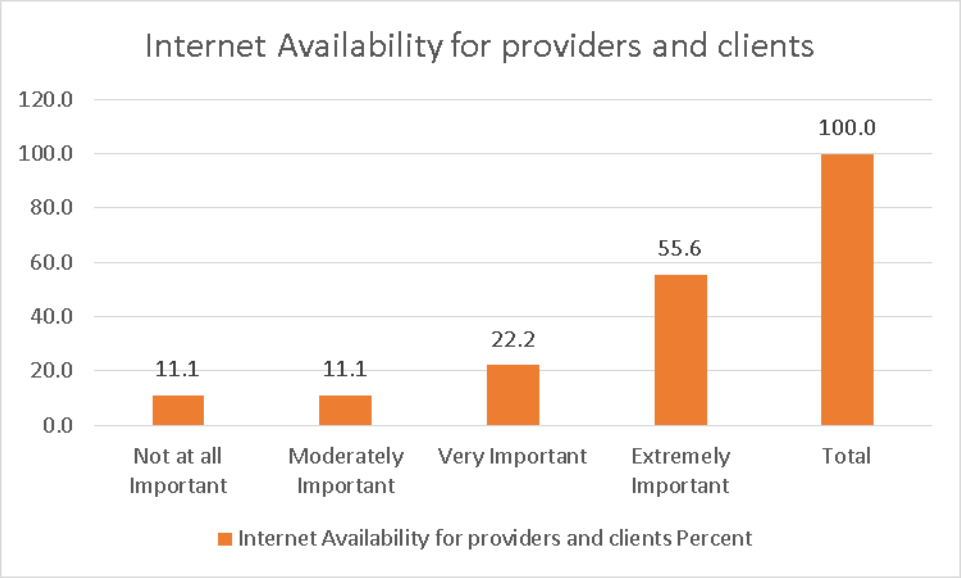

Fig.11 Internet Availability for Cloud providers and Clients

4.0 Conclusion and recommendations for further study

Cloud computing wields great potential for sub-Saharan African countries to reach global markets without expensive investments in building and maintaining data centers, and the

associated costs of running the traditional IT department of skilled personnel. To maximize the benefits of Cloud computing in a business, an understanding of the phenomenon is prerequisite especially in pertinent areas of concern including security, privacy, regulatory compliance and access management. However the lack of coherence in shaping Cloud governance has impeded the organizational understanding and preparedness towards the adoption of the phenomenon. The absence of standardized governance guidelines stems from the early definitions of Cloud computing which predominantly focused on technical elements of Cloud provision and had little mention of what to govern the trust between vendors and consumers.

Our study examined the matter of Cloud governance in relation to selected areas of concern to most Cloud consumers. Drawing from a sample of IT decision-makers in leading Ghanaian organizations, the responses to a survey on Cloud governance were analyzed in an attempt to gain more understanding of the mechanisms governing the Cloud adoption process in the sub-region. The findings revealed that organizations' concerns about security, privacy and loss of control largely linger owing mainly to the dearth of concrete governance structures, policies and guidelines. The study also sought to unpack the main factors of governance affecting Cloud computing adoption by organizations and found the chief hindering factors to be the low availability of human expertise to drive the processes of governance, and low level of awareness of data protection and privacy laws as far as Cloud computing was concerned. Given the level of Internet penetration in sub-Saharan Africa, it is clear from the analyses of the responses that Internet access was an important factor to an organization's implementation or adoption of Cloud computing. Governments' role in facilitating the policies and guidelines for the governance of Cloud computing should take cognizance of the level of Internet penetration and access.

From literature, lack of harmonization in Cloud governance persists chiefly due to vested interests such as depicted in the principal-agency theory where the combination of competition among vendors and bargain- chasing consumers fuel the growth of the Cloud in various directions. The diversity of technology, service offerings and national or regional legislations hinders the smooth implementation of standardized frameworks on Cloud governance. This has led to many organizations in developing countries sticking to their data centers and private Clouds in a bid to remain "safe" rather than venture into the "unknown" Cloud where ownership and governorship policies are unclear.

Being a recent phenomenon with just over a decade of widespread and evolving implementation, Cloud computing adoption has a lot to contribute to the growth of

developing economies. This can be achieved if there is a level of trust and transparency in the service offering of Cloud vendors, and the issues of security are addressed in the context of expectation of businesses in developing countries. Much of such trust and transparency will be possible if there are standard guidelines and policies that are in line with the perspectives of businesses in the developing world. Some work that can be done to further this agenda is enacting and harmonization of data protection laws to guide Cloud providers in their service offerings.

An area of focus to further probe the issue of Cloud governance is in the impact of Cloud service level agreements on existing IT security policies of organizations. This will help probe further the context of security, privacy, and access management expectations of organizations in developing economies.

References

Armbrust M., A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Paterson, A. Rabkin, I. Stoica, M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report UCB, EECS Department, University of California, Berkeley, 2009.

Cecere T. Five steps to creating a governance framework for Cloud security. Cloud Computing Journal; November 2011. http://Cloudcomputing.sys-con.com/node/2073041

Doherty, E. (2012). Broadband adoption and diffusion: A study of Irish SMEs, PhD Thesis, University of Ulster, Coleraine.

GSMA. (2016). GSMA Mobile Economy 2016. Retrieved December 20, 2016, from http://www.gsma.com/mobileeconomy/

Jaster B., J. C. de Mendonca, C. Slamka, and M. Radmacher, *Wer klaut in der Cloud?* Bonn, Germany: Detecon International GmbH, july 2010

Koehler P., A. Anandasivam, M. Dan, "Cloud Services from a Consumer Perspective", in Proceedings of the 16th Americas Conference on Information Systems, Lima, Peru, 2010, Paper 329.

Kaisler S, Money W. Service migration in a Cloud architecture. 44th Hawaii International Conference on System Sciences (HICSS); 2011 Jan. p.1-10.

Minges, M. (2016). *Exploring the Relationship Between Broadband and Economic Growth*. *World Development Report* (Vol. 1).

Mell P, Grance T. The NIST Definition of Cloud Computing. White paper; July 2009. http://www.nist.gov/itl/Cloud/upload/Clouddef- v15.pdf

Nationa Communication Authority-Ghana, February 2017: https://nca.org.gh/industry-data-2/market-share-statistics-2/data-3/ accessed 18th July 2017

Opitz Nicky , Tobias F. Langkau, Nils H. Schmidt, Lutz M. Kolbe (2012); Technology Acceptance of Cloud Computing: Empirical Evidence from German IT Departments. 45th Hawaii International Conference on System Sciences, 2012

O'Neill M. Connecting to the Cloud, Part 3: Cloud Governance and Security. IBM developer Works; 2009. http://www.ibm.com/developerworks/xml/library/x-Cloudpt3 [01/04/2012]

Ramireddy S, R. Chakraborthy, T.S. Raghu, H. Raghav Rao, "Privacy and Security Practices in the Arena of Cloud Computing – A Research in Progress", in Proceedings of the 16th Americas Conference on Information Systems, Lima, Peru, 2010, Paper 574.

Senyo, P. K., Effah, J., & Addae, E. (2016). Preliminary insight into Cloud computing adoption in a developing country. Journal of Enterprise Information Management, 29(4), 505–524. https://doi.org/http://dx.doi.org/10.1108/09564230910978511

Sutton J., Kpentey Bennet (2012): An enterprise Map of Ghana, Published by the International Growth Centre

Sotto L, Treacy B, McLellan M. Privacy and Data Security Risks in Cloud Computing. Electronic Commerce & Law Report; 2010.

Stantchev Vladimir and Gerrit Tamm (2013); Cloud Governance - The Relevance of Cloud Brokers in 2013 International Conference on Parallel and Distributed Systems

Teodor-Florin Fortis, Victor Ion Munteanu and Viorel Negru (2012): Steps towards Cloud Governance. A Survey. Faculty of Mathematics and Informatics, West University of Timis¸oara bvd. V. Pˆarvan 4, Timis¸oara, Romania

Unal E., D. Yates, "Enterprise Fraud Management using Cloud Computing: A Cost-Benefit Analysis Framework", in Proceeding of the 18th European Conference on Information Systems, 2010, Paper 144.

Vaquero M., L. Redero-Merino, J. Caceres, M. Lindner, "A break in the Clouds: towards a Cloud definition", Computer Communication Review (39:1), 2009, pp. 50 55.

Wolcott P., Press L., McHenry W., Goodman S., Foster W., (2001): "A framework for assessing the Global Diffusion of the Internet" in Journal of the Association for Information Systems, Vol. 2 Article 6 2001