

BARRIERS TO GOVERNMENT CLOUD ADOPTION

Samuel Tweneboah-Koduah¹, Dr. Barbara Endicott-Popovsky² and Anthony Tsetse³

¹iSchool, University of Washington, 4311 11th Ave. NE, Seattle, Washington 98105

²iSchool, University of Washington, 4311 11th Ave. NE, Seattle, Washington 98105

³State University of New York, Fredonia, USA, 280 Central Ave, Fredonia, NY 14063

ABSTRACT

Besides the benefits are there possible challenges government agencies are likely to encounter should they decide to adopt cloud computing? What strategies should be deployed to overcome the inhibitors of cloud computing? These are but few questions this paper aims to investigate. Studies have shown that, cloud computing has become a strategic direction for many government agencies and is already being deployed in many critical areas of the government's cyber infrastructure. The benefits and the challenges of cloud adoption have heightened interest of academic research in recent times. We are however uncertain, per literature factors that hinder successful cloud adoption especially in the Ghanaian context. We posit that, understanding the challenges of cloud adoption and overcoming them must accompany the use of the technology in order to prevent unwanted technical consequences, and even greater problems from government information management. This study is based on unstructured interviews from selected government agencies in Ghana. The study is grounded on the theory of technology, organization and environment (TOE) framework. Major inhibiting factors identified include lack of basic infrastructure for cloud take-off, data security, unreliable internet connectivity, and general lack of institutional readiness.

KEYWORDS

Cloud-computing, adoption, challenges, deployment-models, virtualization

1.0 INTRODUCTION

Cloud computing, which allows for highly scalable processes, storage, and communication, is increasing in importance throughout government information technology (IT) strategy [1]. Cloud Service providers (CSPs) offer variety of services to individuals, companies, and government agencies. Cloud consumers (users) usually employ cloud computing for storing and sharing information, database management and mining, and deploying web services, which can range from processing vast datasets for complicated scientific problems to using clouds to manage and provide access to medical records [2] in (Hand, 2007). Whilst the overall benefits of cloud adoption seem seductive, it is important that decision-makers factor in the very significant antecedents that might thwart its implementation and deny its success. In a government context, both tangible risks and intangible risks are introduced along with the functionality and benefits provided by cloud applications [1]. The institutions' ability to manage these challenges will be a key determinant in the success of cloud computing. Understanding challenges of cloud adoption and strategies to overcome the challenges must accompany the use of cloud model in order to prevent unwanted technical consequences, and even greater problems from government information management perspective.

Currently, there exist very few studies that investigate migration of existing public agencies' IT systems to the cloud in the Ghanaian context, concern that motivated the call for this study. Furthermore, little has been published about the implications of cloud computing from an enterprise or organizational perspective[3].

This is how the rest of the paper is structured: The next section provides background study on cloud computing, we provide data on global government cloud adoption in section III. Section IV looks at the research method and results of the study while section V discusses our findings with conclusion.

1.1 BACKGROUND

The rapid advancement of information technologies (IT) has contributed to the downward trend of the cost of computing resources. While prices of computing resources keep slumping, the technologies that depend on these resources are becoming more powerful, sophisticated and ubiquitously available than ever before. This advancements in network and Internet technologies have led to a computing model known in as cloud computing. The model enables services providers known as Cloud Service Providers (CSPs) to provide computing resources as utilities through the Internet to Cloud Service Consumers (CSCs). Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[4]. The three most common cloud services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). The model is also described by how it is deployed. The most popular among them are private, community, hybrid and public clouds (figure 1).

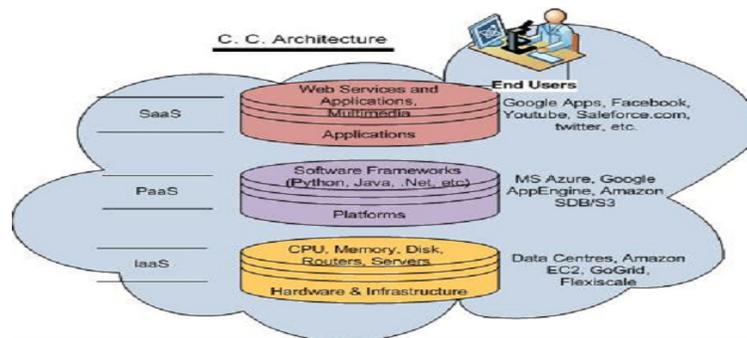


Figure1: Cloud architecture

The emergence of cloud model has made a tremendous impact on the IT industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-effective cloud platforms. Below are few compelling features that have made cloud model attractive to business and government agencies all over the world:

- i. No up-front investment: Because cloud computing operates like the traditional utilities, pricing of cloud services is based on pay-as-you-use. For this reason CSCs do not need to invest in technology infrastructure to start gaining the benefit of cloud computing. Consumers simply pay for the resources they use according to their needs and requirements.
- ii. Lowering operating cost: Because resources in cloud environment can be rapidly allocated and de-allocated, service providers rent cloud resource according to their needs.

With this feature, consumers are able to request resources based on their own needs preventing unwanted or under/over utilization of computing resources saving considerably on IT cost.

- iii. High scalability: Scalability is the ability of a system to expand to meet internal and external demands. This enables cloud infrastructure providers to pool large amount of resources from data centres sometimes across different geographical locations and make them accessible to meet rapid demand from consumers.
- iv. Easy access: Cloud services are internet and web based, making them accessible through variety of internet enabled devices such as phablets, tablets, cell phones, laptops and the traditional PCs.

The three key benefits government agencies could derive from well implemented cloud models include (but not limited to): increase productivity, ease scalability and overall cost cutting (figure 2).

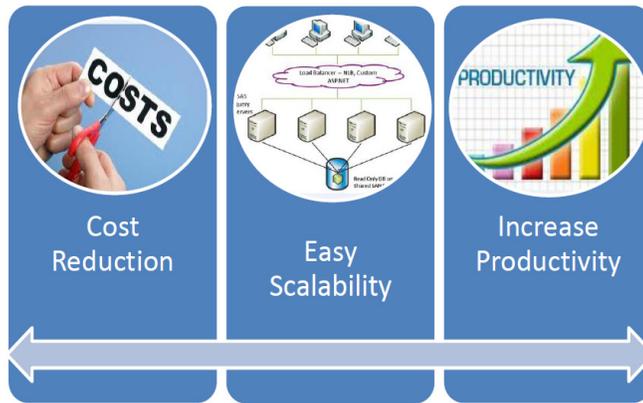


Figure 2: Key Benefits of Cloud Adoption

Cutting cost: SaaS enables government agencies to minimize costs on software acquisition and maximize operational performances. This allows CSCs to pay for software according to their needs. For instance, if clients need an application for a short period of time, they only pay for application that is needed instead of paying for complete licensing for software that might not be needed. As service providers own and host software, users benefit from ongoing upgrades and updates as well as maintenance without the associated costs and time constraints. Moreover, since CSPs use multiple redundant sites, they are able to provide reliable and secure locations for data storage which provides greater security which is ideal for disaster recovery and business continuity. Government agencies are therefore not worried about the loss of data and creating recovery backups.

Easy Scalability: Depending on services needed, cloud users are able to scale back the amount of storage space needed, or raise it according to the pattern of growth. This is especially helpful for agencies that are trying to save money at every possible turn. If an agency is a SaaS user, the user can also request to adopt PaaS or IaaS whenever required. With an on-demand integration of cloud services, CSCs can quickly and easily increase or decrease connections, transactions, or the number of companies in their integration community, and then scale up when resources

requirement increases. The elimination of an up-front commitment by CSCs enables agencies to start small and increase hardware resources as and when the needed.

Increased Productivity: There has been an upsurge in the demand for services by citizenry in both developed and developing economies. To meet this demand, both private and public institutions around the world need to communicate, collaborate and share data. Cloud enables government services to be accessed by citizens anytime anywhere. With the use of cloud applications, citizens can access government services (taxes, pensions, medical records, transport information, forms, view updated orders or transactions) anywhere anytime as long as they have internet access. This enables public organizations to deliver effectively and efficiently, making them more productive, leading to improved services and overall satisfaction.

1.2 CLOUD COMPUTING IN GOVERNMENT

According to International Data Corporation[5], worldwide spending on public cloud services reached \$47.4 billion in 2013 and is expected to be more than \$107 billion in 2017. Moreover, over the 2013–2017 forecast period, public cloud services have a compound annual growth rate (CAGR) of 23.5%, five times that of the IT industry as a whole[5]. Cloud computing certainly seems to be the phrase “*du jour*” in much of the computing world today, many experts now think that cloud computing will be “the next big thing”[6]. The promise of cloud computing is that, it can bring together practices, tools and technologies that will better position a public organisations to operate in a significantly more efficient, predictable, flexible, and accountable manner. From literature reviewed, most government cloud adoption strategies include the use of cloud-based productivity and project management tools that are also popular with businesses. As well as gaining significant cost savings, governments also use cloud technology to increase the quality and innovation in the services they provide to citizens, businesses and other governments.

Government use of cloud computing is gradually increasing in areas such as transport services, health services, education, contracting and now managing of utility services [5]. Countries leading the way in cloud adoption in terms of Government institutions are USA, Japan, Australia, Finland, Denmark, Sweden and United Kingdom[6]. Table 1 below provides examples of cloud adoption, planned adoption, and cloud model use by selected government agencies.

Table 1: Global cloud adoption from selected countries

Country	Services	Details
United Kingdom	Digital Britain (G-cloud)	An important aspect of the Digital Britain strategy is to improve governmental IT and allow for more services to migrate online [7]
Finland	Cloud Software Program	The four-year Cloud Software Program (2009-2013). This seeks to support business developing cloud solutions[8].
Spain	‘Un alcorque, un árbol’	Adopted by Madrid City Council to help manage more than 245,000 trees around the capital cared for by 300 maintenance workers[9].
Japan	The “Kasumigaseki Cloud”	This project allows for greater information and resource sharing promoting more standardization and consolidation in the government IT resources
Hong Kong	GovCloud	This is government private cloud which is used to host common apps for shared by Hong Kong government departments. Services such as e-procurement, e-invoicing, human resource management and electronic information management, among others, are placed

		on GovCloud.
USA - General Services Administration	USA.gov and its Spanish-language companion site, GobiernoUSA.gov	With the shift to cloud-based hosting, the GSA can use “cloudbursts” to increase capacity as needed, rather than having to host server capacity (and the costs—in personnel and energy—necessary to support this largely idle capacity) to handle the web traffic experienced only at peak times[5],[10],[11].
The White House - USA	Google Moderator	The cloud-based application allowed for hundreds of thousands of votes to be cast on the almost ten thousand questions that were submitted for possible use in the live event with the president. Moreover, Office Management and Budget using cloud based applications to interact with state and local agencies receiving stimulus funding[10].
NASA, USA	NEBULA cloud computing platform	Designed to allow for greater transparency and public involvement with space efforts, while serving as a “seamless, self-service platform” that consolidate the agency’s web offerings into a single portal, and provide NASA personnel with “high capacity computing, storage, and network connectivity and a virtualized, scalable approach to achieve cost and energy efficiencies” (Martin K 2012) .
SLOVENIA	KC Class program	Collaborating platform that brings together researchers and developers from six small businesses, four middle-sized enterprises, and seven research organisations, who work to develop local solutions, services and products in the field of cloud computing [12]
EU Initiatives	EU Cloud Strategy	In addition to setting-up internal, private cloud environments, European nations were beginning to explore the use of cloud-based computing in the following areas: management of public sector housing, transportation service, census, health services, contracting and education services.

2.0 THEORETICAL REVIEW

Multiple theories exist in literature for the research of information systems adoption[13]. In order to achieve our goal, we borrow some theoretical concepts from one of these theories which epitomize our understanding and shape the direction of the study. From the theory, we posit that internal and external organisational factors, available technologies and environmental factors are key drivers for successful cloud adoption in Ghana. From these contexts, we attempt to holistically review and investigate the antecedents that might hinder the successful adoption of cloud computing in Ghana. To do this, we adopt technology, organization and environment (TOE) framework by Tornatzky and Fleischer (1990). The TOE framework was adopted due to its philosophical constructs. Moreover, the framework has been used for studying adoption of different types of IT innovation especially at the organisational level. It provides theoretical basis, consistent empirical support and the potential application to IS innovation domains, even though specific factors within the three contexts may vary across different studies[14].

Developed in 1962 by Rogers with further work on it in 1990 by Tornatzky and Fleischer in 1990, TOE identifies three key constructs that influence the process by which organization adopts and implements technological innovation. First, the technological context refers to characteristics

of the technologies which are available for possible adoption by the organization, and the current state of technology in the organization. This current state of technology can be expressed in both

material (e.g., equipment owned by the organization) and immaterial (e.g., methods currently in use). Second, the organizational context; this consists of the organization’s structure, presence of innovation–enabling processes such as informal communication and strategic behaviour of top management, slack resources, and the size of the organization. Third, the environmental context combines elements such as market structure, the external support available for adopting new technologies and government regulations. These elements interact with each other to influence technology adoption decisions[15]. Although, many important issues involves in the theory, this research chiefly focuses on the discussion about the key variables influencing technology adoption.

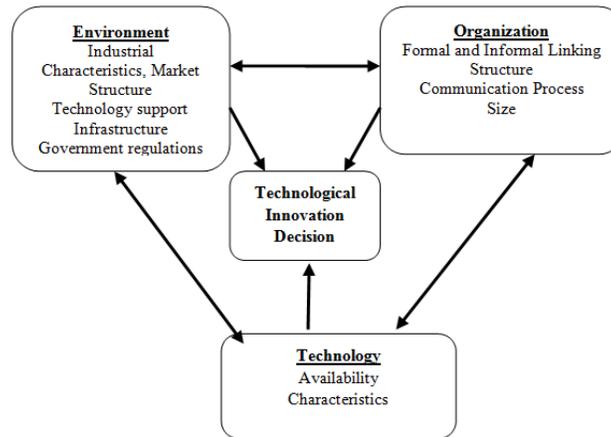


Figure 3: TOE framework (Tornatzky and Fleischer 1990)

Several authors have used the framework to study different IT adoption strategies. The following examples exist in literature: [16], [17], [14], [18] and [19]. Although it has primarily been used to study adoption of technology and/or innovations, it does not provide concrete model describing the factors that influence the organizational adoption decision; it rather provides taxonomy for classifying adoption factors in their respective context [15]. The model therefore encourages the researcher to take the broader context in which innovation takes place into account why applying it.

2.1 METHOD

Using a semi-structured interviews we explore the challenges agencies could encounter should they decide to adopt cloud computing. The interviews were conducted with key IT personal across twelve public (state funded institutions). They are made up of three government ministries, three public universities, three regional hospitals and three district assemblies located in three different regions in southern Ghana. These are institutions which annual budgets are financed by the central government. This means, the decision to adopt or not to adopt cloud models with the exception of the universities might have to get an approval from the sector minister. Thirty-six personnel took part of the study. Interviews were one-on-one. Each interaction session was preceded with an overview of cloud computing, the purpose of the study and clearly defined study expectations. Those involved in the discussions were IT managers, Director of IT, Head of IT and Head of System. With the exception of the Directors of IT who was found to report directly to the respective sectors’ minister, the rest have the same functions with different titles

per functional documents reviewed. This was however different at the universities. The study data is analysed using MS Excel Macro scripts.

Guided by the theory, our focus of discussion was to ascertain and understand the environmental, organisational and technical challenges that might hinder the institutional adoption of cloud computing. We defined ‘challenge’ as any technical, operational, social-economic and environmental antecedents that may hinder successful adoption of cloud computing by these agencies. The details of the result are the subject of the next section.

2.2 RESULTS

With the exception of the district assemblies, all other institutions visited had well structured IT infrastructure consisting of Database Systems, Networks and Data communication tools, Software and well trained IT staff. What was visibly missing among all but two institutions, were IT user policy, data protection and confidentiality agreement, service level agreement and overall institutional IT policy framework. About 95% of the IT resources reviewed have no documentations covering their operations and most users don’t have adequate formal training on how to use techie tools that they use for their day-to-day operations.

Over 55% percent (21/36) of those interviewed had heard of cloud computing but their agencies have no immediate plans to migrate their services or operations to clouds. The three public universities have implemented google(g)mail (SaaS) but were not sure or ready to add other cloud services. The entire respondents had not discussed the issue in their last or the current budget and they have no immediate plans of adopting or implementing cloud modules. Having explained the cloud concept, we asked participants to rank factors that might influence their organisation’s cloud adoption using the following factors as exist in the study’s framework (Technology, Organization and Environment). The chart below (figure 3) shows their responses.

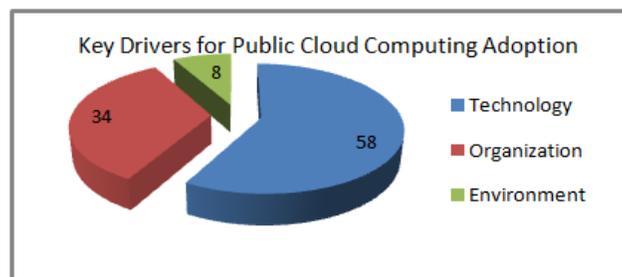


Figure 4: Institutional Drivers for Cloud Adoption

Using the response above, we developed the following follow-up questions to understand the top challenges or inhibitors of each of the above drivers. First, what do you believe are the top technical challenges or concerns your agency faces in adopting cloud computing?

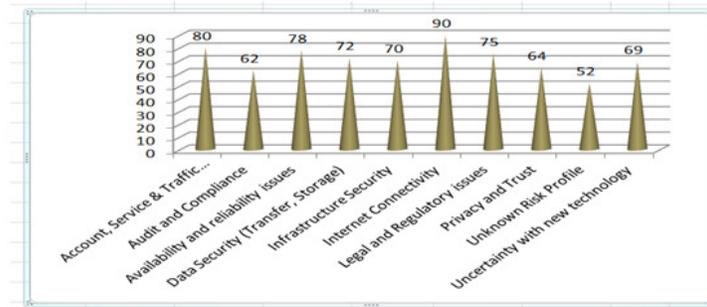


Figure 5: Top technical challenges of adopting a cloud environment

Second, what do you believe are the top institutional challenges or concerns your agency faces in adopting cloud computing?

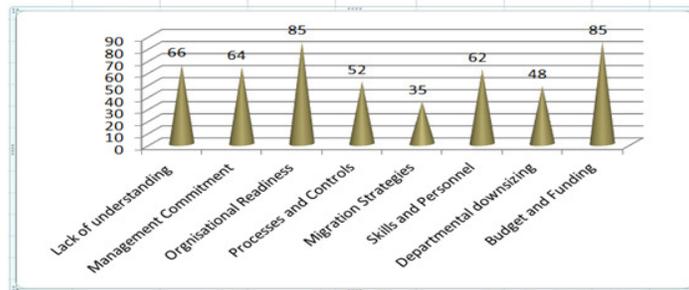


Figure 6: Institutional barriers to public cloud adoption

Third, what do you believe are the top environmental challenges or concerns your agency faces in adopting cloud computing?

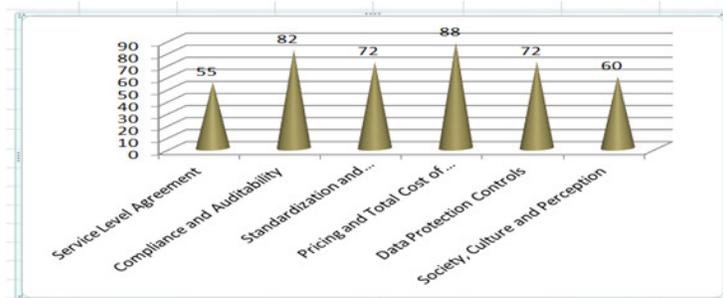


Figure 7: Environmental barriers to public cloud adoption

Inferring from figure 7, we generate the eight-factor concerns considered to be the key inhibitors to government cloud adopting in the study context (figure 8). The next section discusses our findings.

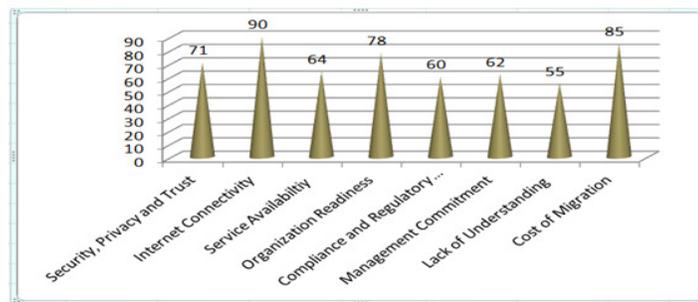


Figure 8: Challenges of public cloud adoption

In the next section, we provide detailed discussions of the above concerns and provide our eight-point strategies to address them.

2.3 DISCUSSION

Most of the challenges of government cloud adoption relate to its apparent newness and the relative underdevelopment of the marketplace for cloud services,[20]. At the national level,

information is the lifeblood of government, for this reason, decision to manage information can have far-reaching political, social, and economic considerations. Cloud computing has been welcome as a new model capable of helping government manage its information resources. Despite the ever increasing interest of cloud computing in the public sectors across the globe, various factors continue to slow down its migration, and in Ghana the situation is not different. We provide below the discussions on the key challenges that potentially create barrier between adopting and adopters.

Cost of migration - According to the survey, the key performance indicators include those relating to cost, productivity, and revenue in most public agencies in Ghana. In the finance ministry, the concern was to cut down the cost of operations and how cloud could help improve revenue generation. Nearly 85% of our respondents mentioned cost associated with cloud adoption as a key determining factor. The costs associated with cloud adoption include (but not limited to) building new technology and security infrastructure that are cloud compatible and redesigning existing ones, training and retraining, institutional realignment, policy and standards formulations in addition to the cost of cloud services which in most cases are not known until the services have been consumed. It was not surprising, when we spoke to one sector Minister about cloud adoption in his ministry, his first reaction was “Yes, I know cloud computing is good but who is going to fund its implementation?”

Security and Data Sovereignty - The major critiques against public cloud adoption to date, has been the issue of security, privacy and trust ([21], [6], [22], [22], [23], [24], [25],[26]). Government has an onus to protect citizen data and ensure availability of critical infrastructure such as power, water, health, communications, and banking. This might not relate to only data owned by government but those entrusted to her by others. Over 80% of our respondents mentioned the issue of security and privacy as the major concern for government cloud adoption. Besides, most studies relating to the subject, do mention security, trust and privacy as majors concerns for both public and private adoption. A survey conducted by department of Economic and Scientific Policy under EU, 63% of government CIO consider security and privacy as the major concern for public cloud adoption. Report by KPMG on public cloud adoption across Europe, America and Asia Pacific indicates that, security and privacy concerns are the most significant barriers to public sector cloud adoption.

Equally important is the impact of data storage on national sovereignty. This is because most CSPs have storage servers in multiple countries sometime far away from their regional boundaries. Whether cloud services are provided on or offshore, governments will need the assurance that sovereignty is not threatened, especially, where overriding effect of laws in the jurisdiction of CSPs application or data storage. Public managers are also concerned about challenges in preserving the integrity or privacy of government information held offshore and in having it repatriated, if required, in instances of natural disaster, political instability, civil or industrial unrest, criminal activity, terrorism, or any instance of “casus fortuitous”. Data security risks arising from cloud computing relate to: 1) an increase in threats to data confidentiality, integrity and accessibility due to the concentration of data on common cloud infrastructure, 2) loss of control and governance by organisations using cloud services, 3) and an increased risk of data interception in authentication and transmission procedures that are mostly hidden from CSCs.

Privacy - Privacy in cloud environment is the ability of a user or a business to control what information they reveal about themselves over the cloud or to a cloud service provider, and the ability to control who can access that information[27]. This is an important issue for cloud computing users and most importantly Government, both in terms of legal compliance and user trust. This needs to be considered at every phase of design and implementation. Cloud

environment is beset with complex privacy and confidentiality issues due to lack of appropriate laws that block users from information disclosure to the cloud providers or other cloud users. Government may not be interested in sharing her information but such information may be already placed in the cloud and this may lead to adverse impacts on their services and sometimes the state as a whole. Privacy and data protection laws (regulations of EU countries and US Safe Harbour Program), require knowledge of where data is stored at all times but these laws are not known to exist in Ghana, making it almost impossible for Government to protect itself in case of breach by CSP or other CSC.

Internet Connectivity- Virtually all Cloud deployment services are assessed over the internet using hypertext transfer protocols (http). Any agency planning to adopt cloud must ensure reliable and stable internet connectivity and accessibility not only to the agency but its service consumers. Indeed, universal connectivity is a panacea for successful cloud adoption and cloud usage. Available statistics show that nearly 85% of Ghanaian population don't have access to reliable and stable Internet both at home and public offices. Besides, Ghana as a nation has not done much in digitizing public services. Most countries that have adopted cloud services have long had digital services making the migration quite easier and faster. E-government services in Ghana are still not matured [28]. Out of the thirty-six public institutions observed only three (less than 8%) of them have some kind of e-services. The graph below shows population per internet usage (%) in major economies that have adopted cloud services compared to that of Ghana (coloured).

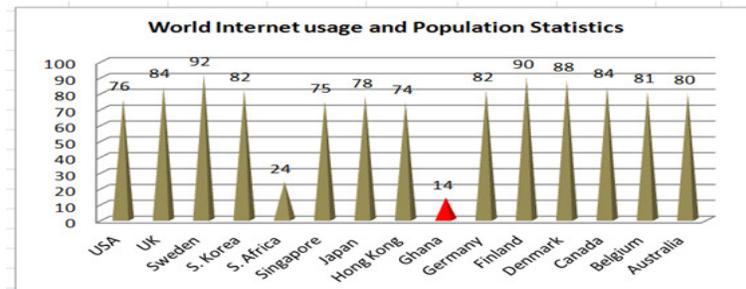


Figure 9: World Internet usage statistics (source: <http://www.internetworldstats.com/stats.htm>)

Institutional Readiness - Cloud migration requires that certain basic services be cloud ready, up and running. E-government services, government data centres and digital service are but few examples. These services pave way for smooth cloud migration. Only three out of thirty-six (8%) of the agencies observed have their e-services working perfectly. Though government over the years has managed to improve its LAN and Internet connections, this infrastructure development are mostly found at the regional capitals especially in the national capital, Accra. Studies have shown that, organisations that have successfully migrated to cloud environment, did build on existing digital or e-services and well managed data centres. Cloud migration requires institutional re-alignment. It requires administrative, operational, cultural and managerial reforms including training and retraining. In Ghana, public organisations are beset with bureaucratic processes. General perception was that, digitization is a panacea for institutional downsizing especially for most system and network administrators who feel threatened should government adopt cloud.

In a related development, nearly 89% of the leaders and administrators interviewed stated the issue of funding. The concern is that, in Ghana most government agencies get their budget approved from the Ministry of Finance which in most cases approve institutional expenditure. For this reason any project they intend to finance must get approval from the ministry making it difficult to implement cloud project on their own without financial tussle from the ministry of finance.

Business Continuity and Service Availability - A key selling point to cloud computing has been the potential for 100% non-interrupted availability to the customer. For large vendors and most essential government services, maintaining 24/7 up time is crucial to businesses and the citizens in general, as customers demand no less to support their mission-critical efforts. Outages do occur, and can be unexpected and costly to a customer [21]. Concern was whether CSPs will have adequate capabilities and effective business continuity plans (BCP) to handle emergencies and disaster situations. This makes some wary of cloud computing. Though existing cloud services have set a high standard in this regard, records show however, there have been instances where cloud services have gone down making the concern a legitimate one. Most government agencies depend on reliable data for their day-to-day operations. The absence of such data brings government business to a halt. Table 3 shows recorded outages for Amazon Simple Storage Service (S3), AppEngine and Gmail in 2008.

Table 2: Outages in selected cloud services

Provider	Services	Duration	Date
AWS	S3: authentication service overload leading to unavailability (Siegele 2008)	2 Hours	15/02/08
AWS	S3: Single bit error leading to gossip protocol blow up (Armbrust et al. 2010)	6-8 Hours	20/07/08
AppEngine	AppEngine partial outage: programming error (Paquette, Jaeger, and Wilson 2010b)	5 Hours	17/06/08
Gmail	Site unavailable due to outage in contacts system (Canedo et al. 2012)	1.5 Hours	11/08/08

Standardization, Legal, Compliance and Audit - Cloud standards are an agreed-upon approach to ensure interoperability, so a customer can take data, tools, applications, virtual images, etc., and use them in other cloud environments with minor rework in case provider's system goes

down¹. Standards and policies regulating cloud computing have been a great concern to date. Equally challenging, is the legal requirement with respect to trans-border information flow relating to cloud adoption. The following legal questions need to be answered to clear the doubts and concerns on legal and governance issues: what kind of liability will a company that provides cloud services expected to assume in the event that there are serious outages? What are the requirements with regard trans-border information flow? What are the minimum criteria for service termination (including data, asset return, data privacy, destruction and migration) in a contractual arrangement? Another thorny issue related to the cloud may be electronic surveillance, particularly when it spans international borders[29]. In the United States, citizens are protected by the constitution against unreasonable search and seizure. In most cases, the police must get a search warrant to examine data on someone's home computer. It is not clear if the same data is protected when backed up in a data centre in the Cloud, particularly if that data centre is in another country[29]. It is even less clear how and when intelligence services in Ghana can access data stored in the cloud for security and protection purposes.

3.0 THE WAY FORWARD

No organization wants to spend time, money or resources needlessly. When it comes to cloud computing, the same is true – organizations do not embark on cloud strategies just to have a

“Cloud”. It is critical therefore to understand the driving factors behind such a move and whether it is a standalone activity or part of a more transformational move toward delivering IT as a service. Agencies must assess and re-assess themselves if they are cloud ready. Below is our seven-point migration strategy for government cloud adoption in the context of the study.

Education, Training, and Engagement - Adopting any technology must begin with learning the basics of the technology by attending seminars, networking, talking with vendors and other institutions that have the experience. Given that cloud computing represents a new paradigm in information technology, it will be important for technology and knowledge transfer to occur—the “techies” in and outside of government will need to go the extra mile to educate and inform the “non-techie” policymakers (agency executives, staffers, and lawmakers) as to the merits and value of cloud computing[6].

Government should collaborate with universities to expand their courses and revise their existing curricula to build knowledge and skills needed in cloud computing. They should seek the support of cloud service providers to offer short courses for industry, government and university researchers on cloud computing, including its data-parallel programming, virtualization and big data models. Where possible, government should negotiate internships and exchange programs for fresh graduates and newly recruited IT staff as a form of re-training. As it is being done in the Pacific Northwest of US, the engagement should include colleges, the military and other training institutions. Besides, both technical and non-technical IT personnel should be retrained, encouraged and/or supported to take certifications in cloud computing and other related programs to build local capacity.

Institutional Assessment - Cloud computing is a new way of managing IT infrastructure. It is not a magic wand. Adopting it, impacts on the organization's operations and processes. Organisations that have successfully adopted it have had existing structures and services that were cloud compatible which facilitated the migration. IT managers should conduct an overall IT cloud-readiness assessment to determine if their organization have services, data and applications that could readily move to a cloud environment. The assessment will help

¹ EU Directorate General for Internal Policies

establish which services, data and applications can - and cannot be housed in any form of cloud environment. In doing so, they will discover a definite field of “cloud-eligible” and “cloud-ineligible” data and applications[30]. Equally, agencies must ensure they have personnel with the right skills and experience level for successful move to the cloud. Internal staff must be assessed of their current roles and responsibilities, change management needed, and how well current skills will map to the cloud model being designed or implemented. The organization network capability must also be assessed to test its capability of supporting additional network traffic that will result from assessing applications over cloud environment.

Security Risk Assessment - As with adoption of new processes or technologies, there exist some associated risks. As we stated above, security, privacy and trust issues have been suggested and documented to be one of the major risks to cloud adoption. However, cloud providers and end-users are increasingly working together to use cloud in ways that actually enhance the ability to manage key risks in areas such as trusted platforms, data privacy and security. In short, says Ian Gravestock, “Government agencies should be aware of risks, but they should not be using the mere existence of risk as an excuse for doing nothing” in [30]. IT managers should ensure their IT and security infrastructure has been tested and verified to be cloud compatible. They should conduct security risk impact assessment for the services and information they intend to move to the cloud environment. It is suggested, IT managers must be retrained on cyber security issues and be abreast of the threats in cloud environment and cyber infrastructure in general. Moreover, users must ensure to have secured authentication protocols. Other non-technical solutions such as awareness creation, provision of IT user acceptability policies and safety cultural practices should be encouraged across government agencies.

Universal Connectivity (broadband) - All Cloud deployment services are internet dependent tunnelling through hypertext transfer protocols (http). Successful cloud adoption strategy must ensure reliable and efficient internet connectivity and accessibility to both the institution and the end-users. Government agencies must build and ensure local and wide area networks are well connected and are compatible with cloud architecture. Government could liaise with National Communication Authority (NCA) and perhaps with the Commonwealth Department of Broadband Communications and the Digital Economy to review existing broadband pricing and policies of providers to ensure that unnecessary impediments to the uptake of cloud computing are minimised. In particular, ensuring internet prices do not increase the cost of users accessing cloud services.

Infrastructure Setup for Cloud take-off - Cloud computing is a network centric application with storage, information processing, multi tenancy and virtualization technologies being the key backbone. Government must invest in new networks infrastructure and improve the existing ones. Government can partner with local network providers and major partners in the industry (Amazon, IBM, Microsoft and google) to build data centres and reliable energy source that is capable of supporting the centres. Network and security infrastructure must be secured, tested and verified to be cloud compatible. Lack of integration between networks makes it difficult for organizations to combine their IT systems with the cloud and realize the gains from the technology. Organizations need to automatically provision services, manage virtual machine instances, and work with both cloud-based and enterprise-based applications using a single tool set that can function across existing programs and multiple cloud providers[31]. Government could liaise with the Open Grid Forum, an industry group, which is working on the Open Cloud Computing Interface, which provides an API for managing different cloud platforms.

Regulations, Accountability and Standardization - Cloud standards are an agreed-upon approach to ensure interoperability, so a customer can take data, tools, applications, virtual images, and more, and use them in another cloud environment with minor rework or in case

provider's system goes down [32]. Standards and policies regulating to cloud are major concerns of cloud adoption to date. The issue has been discussed on several platforms and other international forums. These however, can be addressed by establishing a new taskforce to review the adequacy of current regulations, standardization, and legislation and identify what steps are needed to be taken to ensure a supportive regulatory environment in Ghana. Local taskforce could liaise with other international bodies such as National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA), Federal Information Processing Standards (FIPS) and the European Network and Information Security Agency (ENISA) for support and guidance. Regarding service level agreement (SLA), government should engage with CSPs to determine their business continuity and disaster recovery plans. These should be factored into government cloud migration strategies. Besides, the contracting process, the degree of flexibility (contract length, scope and coverage, liabilities, indemnifications and policies) regarding cross border data migration need to be discussed with CSP.

Cloud Piloting - Concluding, IT managers should pick one area, a process or one specific project to "cloud pilot" and assess their ability to manage and bring such project to fruition using internal resources where possible. This can also be used to test the capability and efficiency of cloud provider should managers decide to use public cloud for the pilot process. For government, it is recommended to start with locally built private cloud for data and time sensitive resources. Less sensitive and more general services could be piloted with either hybrid cloud or public cloud. IT managers can use this time to roll-out their cloud migration strategies by gaining buy-in from

both organizational leadership and IT staffers. The trial period can be used to communicate to both internal and external stakeholders as to the goals, progress, and costs/benefits of the project. This is where the cloud goes from being a test effort to become a mainstream, in the way the agency manages its data, operations, services and its people in the new cloud environment.

4.0 CONCLUSION

We should all think of what we do on the Internet on a daily basis. We check mails, "social networking – Facebooking, once, twice,...ten times a day and now Twittering", and the like. We post and view photos (selfies), we store files online (dropbox, Google drive, etc.) Yes, there can be real work done as well, creating documents, spreadsheets and presentations entirely online. Indeed, a lot of people are in the cloud yet they are not realising it. Cloud computing has come to stay. It is already at work today reducing operating costs, in some cases substantially. They are enabling optimization of asset utilization and flexibility in both the scale and scope of IT services and hardware². Many government agencies are exploring a host of new services and are interactions with other groups within government as well as citizens[6]. Cloud computing is set to change (if it has not done that already) how IT systems are deployed both in business and in government because of its apparently cheap, simple and scalable nature. The question isn't whether government will migrate to cloud or not, but how far and how fast will it go?

The main concerns about adopting cloud services are security, privacy data location, universal connectivity, applicable law and jurisdiction over data and uncertainty about the cost of migration as this study has shown. It also appears that most organisations lacked a full understanding of the complexity of cloud computing including inadequate IT and security infrastructures for cloud take-off. Having identified what cloud is and its key characteristics, the benefits, adoption inhibitors and the way forward of adopting cloud, further research work is needed to establish clear strategies to overcome adoption inhibitors in the case of Ghana. Moreover, government should partner with key stakeholders to strategise and develop workable solutions to address the

² <http://www.kpmg.com>

challenges identified in this study. Finally, we provide figure 10 below as the general overview of the cloud environment as discussed in the study.

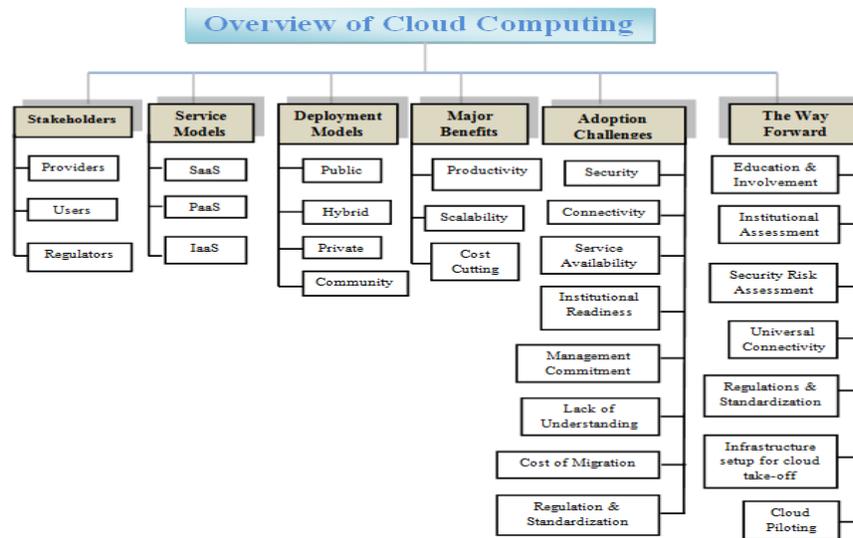


Figure 10: Overview of cloud environment

ACKNOWLEDGEMENT

The authors would like to send our appreciation to the Directors, IT Managers and especially all the personnel who took part in our interview sections. We would also like to thank Professor Knud Erik Skouby of CMI, Aalborg University, Associate Professor Gamel Wiredu at School of Technology GIMPA and Ruth Ayanful-Torgby of Ghana Health Service & Nuguchi Momorial Institute for Medical Research, Ghana for your comments and reviews. Finally, the comments from two anonymous reviewers are very much appreciated.

BIBLIOGRAPHY

- [1] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Gov. Inf. Q.*, vol. 27, no. 3, pp. 245–253, 2010.
- [2] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?," *J. Inf. Technol. Polit.*, vol. 5, no. 3, pp. 269–283, 2008.
- [3] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud migration: A case study of migrating an enterprise it system to iaas," in *Cloud Computing (CLOUD)*, 2010 IEEE 3rd International Conference on, 2010, pp. 450–457.
- [4] P. Mell and T. Grance, "The NIST definition of cloud computing," *Natl. Inst. Stand. Technol.*, vol. 53, no. 6, p. 50, 2009.
- [5] F. Gens, M. Adam, D. Brandshaw, and C. A. Christiansen, "Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast," *International Data Corporation, Market Analysis 38*, Aug. 2013.
- [6] D. C. Wyld, "THE cloudy future of government IT: Cloud computing and the public sector around the world," *Int. J. Web Semantic Technol.*, vol. 1, no. 1, pp. 1–20, 2010.
- [7] P. Black, T. Byron, F. Caio, and A. Chitty, "Digital Britain," The Secretary of State for Culture, Media and Sport and the Minister for Communications, Technology and Broadcasting, United Kingdom, London, United Kingdom, Parliamentary Report, Jun. 2009.
- [8] Finish Cloud Software Program, "Cloud Software (Finland) Guide," 2013.
- [9] L. Boch-Andersen, *Cloud Help the City of Madric stay Green, one tree at a time*. 2011, p. 1.

- [10] A. Rastogi, "A model based approach to implement cloud computing in e-Governance," *Int. J. Comput. Appl.*, vol. 9, no. 7, pp. 15–18, 2010.
- [11] D. Beizer, "USA.gov will move to cloud computing," *The Business of Federal Technology*, p. 1, 23-Feb-2009.
- [12] S. EuroCloud, "KC Class," Eurocloud Slovenia, Regional Report, Sep. 2012.
- [13] T.-P. Liang and J. J. You, "Resource-based View in Information Systems Research: A Meta-Analysis," in *PACIS 2009 Proceedings*, 13, 2009, vol. 72, p. 13.
- [14] T. Oliveira and M. Fraga Martins, "Literature Review of Information Technology Adoption Models at Firm Level," *Electron. J. Inf. Syst. Eval.*, vol. 14, no. 1, pp. 110–121, 2011.
- [15] B. Ranjit and X. Luo, "Integrative framework for assessing firms' potential to undertake Green IT initiatives via virtualization – A theoretical perspective," *J. Strateg. Inf. Syst.*, no. 20, p. 17, 2011.
- [16] P. Y. Chau and K. Y. Tam, "Organizational adoption of open systems: a 'technology-push, need-pull' perspective," *Inf. Manage.*, vol. 37, no. 5, pp. 229–239, 2000.
- [17] T. Oliveira and M. F. Martins, "A Comparison of Web Site Adoption in Small and Large Portuguese Firms.," in *ICE-B*, 2008, pp. 370–377.
- [18] T. S. Teo, C. Ranganathan, and J. Dhaliwal, "Key dimensions of inhibitors for the deployment of web-based business-to-business electronic commerce," *Eng. Manag. IEEE Trans. On*, vol. 53, no. 3, pp. 395–411, 2006.
- [19] R.-Z. Kuo and G.-G. Lee, "KMS adoption: the effects of information quality," *Manag. Decis.*, vol. 47, no. 10, pp. 1633–1651, 2009.
- [20] M. Sedaghat, F. Hernández, and E. Elmroth, "Unifying cloud management: Towards overall governance of business level objectives," in *Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on*, 2011, pp. 591–597.
- [21] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Gov. Inf. Q.*, vol. 27, no. 3, pp. 245–253, 2010.
- [22] J. Joshi, A. Ghafoor, W. G. Aref, and E. H. Spafford, "Digital government security infrastructure design challenges," *Computer*, vol. 34, no. 2, pp. 66–72, 2001.
- [23] K. Curran, S. Carlin, and M. Adams, "Security issues in cloud computing," *Elixir*, vol. 38, pp. 4069–72, 2011.
- [24] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing," *ArXiv Prepr. ArXiv11095388*, 2011.
- [25] J. L. Duffany, "Cloud Computing Security and Privacy," in *10th Latin American and Caribbean Conference for Engineering and Technology*, 2012, pp. 1–9.
- [26] F. S. Gharehchopogh and S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy," *Int. J. Sci. Technol. Res.*, vol. 1, no. 6, pp. 49–54, 2012.
- [27] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. B. Othmane, and L. Lilien, "An entity-centric approach for privacy and identity management in cloud computing," in *Reliable Distributed Systems, 2010 29th IEEE Symposium on*, 2010, pp. 177–183.
- [28] S. Tweneboah-Koduah, "Knowledge Management: Critical Factor for Successful Implementaion of e-Government applications in Ghana," in *12th European Conference on eGovernment, Barcelola, Spain, 2012*, pp. 713 – 721.
- [29] M. R. Nelson, "The cloud, the crowd, and public policy," *Issues Sci. Technol.*, vol. 25, no. 4, pp. 71–76, 2009.
- [30] J. Herhalt and K. Cochrane, "Exploring the Cloud: A Global Study of Governments' Adoption of Cloud," *KPMG Global, Industrial Report*, Jan. 2012.
- [31] S. N. Brohi and M. A. Bamiah, "Challenges and benefits for adopting the paradigm of cloud computing," *Int. J. Adv. Eng. Sci. Technol.*, vol. 2, pp. 286–290, 2011.
- [32] L. Schubert, K. G. Jeffery, and B. Neidecker-Lutz, *The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010:–expert Group Report*. European Commission, Information Society and Media, 2010.