Enterprise Security and Privacy in Public Cloud Computing Environment -The African Case.

Okwor Anthony Nwachukwu
Department of Computer Science
Federal College of Education, Eha Amufu, Enugu State, Nigeria.
telltonee@yahoo.com.
+2348030916394.

Abstract: Enterprise security and privacy in public cloud computing environment in Africa is a burning issue that presents the concept of cloud computing and risk factors associated with it. With the advancement in Information technology, cloud computing has made access to computing resources a lot easier, but with that convenience has come a whole new universe of threats and vulnerabilities. The security challenges that cloud computing presents, especially for public clouds whose infrastructure and computational resources are owned by an outside party that sells those services to the general public, are formidable. Hence, this article presents the technological impacts and threats associated with cloud computing in Africa. Review method was used in this work. Works of different authors and bodies were collated and analyzed to help x-ray data accessibility, information dissemination, data integrity, privacy, and data security in a public cloud computing environment. Since cloud computing helps to keep businesses growing beyond boundary in Africa, it is recommended that more security measures should be adopted to improve data security.

Keywords: Cloud computing, computing models, public clouds, enterprise security.

INTRODUCTION

Cloud Computing is a technology which makes use of internet and central remote servers to maintain data and applications. Under this architecture, one can use applications without installation and access centralized storage space, networks, computer processing power, specialized corporate and user applications and bandwidth. Although various definitions of the cloud have been given, they all converge to give meaning to cloud computing as *a service on demand*: Software-as-a Service, Platform-as-a-Service, Infrastructure-as-a Service, security-as-a Service among other inclusions – "All-as-a-Service".

The National Institute of Standards and Technology (NIST) according to NIST(2009), defines cloud computing by five essential characteristics, three cloud service models and four cloud deployment models. A breakdown of this classification shows that the essential features are on-demand service, Broad Network Access, Resource pooling, Rapid Elasticity and Measured service.

Perhaps the interest shown in, and consequent adoption of cloud computing is further necessitated by some enticing provisions of the cloud service models: Software as a Service (SaaS) – which renders to the user the required application, software, hardware and network; Platform as a Service (PaaS) - which enables the user to develop and deploy applications on the cloud without the rigors of managing the servers, internet service and storage techniques; Infrastructure as a Service (IaaS) - which provides the hardware and network (infrastructure) to the consumers to access and deploy their stuff without the burden of equipment control, maintenance and repair.

The four deployment models of cloud computing according to NIST are: public, private, community and hybrid. While public models are cloud infrastructures available to the general public and owned by organization selling cloud services, a private cloud is a cloud

infrastructure for a single organization, and may be managed by the organization or a third party, on or off premise. Community model of cloud infrastructure is one shared by several organizations that have shared concerns, managed by an organization or a third party. Hybrid model is a combination of more than two clouds bound by standard or proprietary technology.
The development and the success of Cloud are due to the maturity reached by hardware and software virtualization, data transportation, dynamic extendibility and distributed computing. It promises to provide on-demand computing power with quick implementation, little maintenance, less IT staff, and consequently lower cost. Cloud computing aims to share data, calculations and services transparently, among users of a massive grid.

THE ENTERPRISE AND THE PUBLIC CLOUD

An enterprise refers to a business, non profit or government organization responsible for the production and/or distribution of goods and services. An enterprise is established to achieve certain aims and objectives. For a commercial enterprise, the cardinal objective is profit. As an enterprise strives to consolidate and achieve her target objectives, it encounters risks and challenges. Enterprise risk management (ERM) in business according to Wikipedia (2014), includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. The framework for this risk management, involves identifying, assessing and exploiting particular events, circumstances and opportunities relevant to the organization's objectives.

With the availability of up to four cloud deployment models, enterprises have the option to choose a Private, Public, Community or a Hybrid cloud. Admittedly, choosing the right cloud model for a business requirements is a tough task. The services offered by a particular model of interest, the security and privacy issues, as well as the overall cost-benefit analysis should be considered before a choice is finally made by the enterprise. From a risk perspective, Jansen and Grance (2011), stated that determining the suitability of cloud services for an organization is not possible without understanding the context in which the organization operates and the consequences from the plausible threats it faces.

In public clouds, resources are available to the general public over the internet for open use. These clouds are hosted and run fully on the premises of the provider. Analysts believe that public clouds are used widely by industries and businesses. With the public cloud offering a cost-effective model, Williams (2013) concludes that small and medium businesses are turning to this option. Its advantages, it adds, are cost-efficiency, flexibility, resilience and easy management, but on the other hand, has deficiencies in security by way of malicious attacks and easy access.
The characteristics of cloud computing that differentiates it from other traditional IT infrastructure and similar technologies is summarized by Mell and Grance (2011) as follow: broad network access**,** on-demand self-service, rapid elasticity, measured Service and resource pooling.

The enticing benefits offered by cloud computing technology in terms of: pay-as-you-go pricing model, on-demand- self-service, and location-independent operability have not only made it inevitable, but also irresistible for business to embrace this innovating technology. The offer of scalability without huge financial demand for infrastructure purchase, use and maintenance is seen as a welcome development in the business circle. This scenario according to Gallagher (2012) and Nkolwoudou (2010) is well suited to the African continent.

SECURITY AND PRIVACY ISSUES IN PUBLIC CLOUDS

Public clouds are owned and operated by third parties. They deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, Pay-as-you-go model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider (Jaydip, 2013).
In an enterprise such the banking sector, there is possibility that a fraudulent banker could alert criminals with vital information on a customer who has just withdrawn a huge sum of money from the bank with intent that he/she be robbed or duped. With this information the security and privacy of the customer is endangered, for mere being a customer and transacting business with the bank. On the other hand, a businessman who after a good sale for a day decides to go home with the huge sum of money realized, instead of depositing the money in the bank, stands the risk of losing the money or his life or both to hoodlums, other hazards notwithstanding. Insomuch as a customer succeeds in depositing his money in the bank, the bank consequently shoulders all security and privacy responsibilities and becomes accountable to the client for security breaches which it is expected by law, to provide. The above illustration mimics what obtains vis-à-vis transactions in the cloud. While there are inherent benefits, there are also associated risks.

Enterprises who key in unto the public cloud unarguably do enjoy the cost benefits associated with the economies of scale offered by the cloud at a fraction of the cost of having invested in the physical network and services. However, even with the obvious advantages, some large enterprises have migrated onto the cloud mostly onto the private cloud as companies still have security concerns about moving into the public cloud. This view by Gillwald (2013) is corroborated by Gartner (2008) who identified seven security issues that need to be addressed before enterprises should consider switching to any cloud computing model. These issues are: privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability.
Admitting that the internet is the best effort network, Gartner in Wikipedia (2013) laments that one of the greatest challenges to security professionals is the perception that the internet is a secure critical infrastructure. The internet being an open connection of diverse networks going by analysts, is risk ridden, and likewise the public cloud.

Data security is a fundamental issue for enterprises whether small, medium or large scale. With cloud computing, the service provider is largely responsible for security measures to ensure - data confidentiality and integrity, protection from data loss, continuity of service and quality of service. On the other hand, despite this inherent loss of control in public clouds, the cloud service consumer (here the enterprise) still needs to take responsibility for their use of cloud computing services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization. According to Cloud Standards Customer Council (CSCC) (2012), the consumer achieves this by ensuring that the contract with the provider and its associated service level agreement (SLA) has appropriate provisions for security and privacy. Specifically, it noted, the SLA must help to maintain legal protections for privacy relating to data stored on the

provider's systems. The consumer must also ensure appropriate integration of the cloud computing services with their own systems for managing security and privacy.

For an enterprise to optimize data security and/or maximize profit there must be tradeoffs. While the enterprise is trying to maintain water-tight security, a lot is spent financially. But while it tries to ward off many expenses so as to maximize profit, security might be jeopardized. The nature and goal of the enterprise therefore, becomes a deciding factor to the type and magnitude of tradeoff or compromise to be made.

It has been established that there are a number of barriers for cloud computing adoption. The barriers were identified by Mather et al. (2009) as security, privacy, connectivity and open access, reliability, interoperability, independence from cloud service providers (CSPs), economic value, IT governance, changes in the IT organization, and political issues due to global boundaries.

The security and privacy issues identified by NIST to be relevant in cloud computing are: (i) governance, (ii) compliance, (iii) trust, (iv) hardware and software architecture, (v) identity and access management, (vi) software isolation, (vii) data protection, (viii) availability, and (ix) incident response.

From the analytic point of view, there is a lot of convergence on issues of security and privacy in the cloud as identified by NIST, Marther et al. (2009), Jansen and Grance (2011), Williams (2013), Jaydip (2013) and CSCC (2012). Some of the issues are examined below.

Service delivery and deployment issues

The three main service models of cloud computing (Software-as-a-Service (SaaS), platform-as-a-service (PaaS) and Infrastructure-as-a-Service (IaaS) coupled with the deployment models (private, community, public and hybrid) are germane to security and control in the cloud. Given the *service* and *deployment* models of cloud computing, the ball is in the court of enterprises. Regardless of the service delivery model utilized, the choice of a deployment model automatically offers associated proviso and fixes the enterprise on a unique position in the security and privacy map.

From the NIST cloud computing model (Figure 1), the burden of security on the cloud service provider (CSP) decreases as we move from the **SaaS** end to the IaaS end, while that of the client (enterprise) increases.

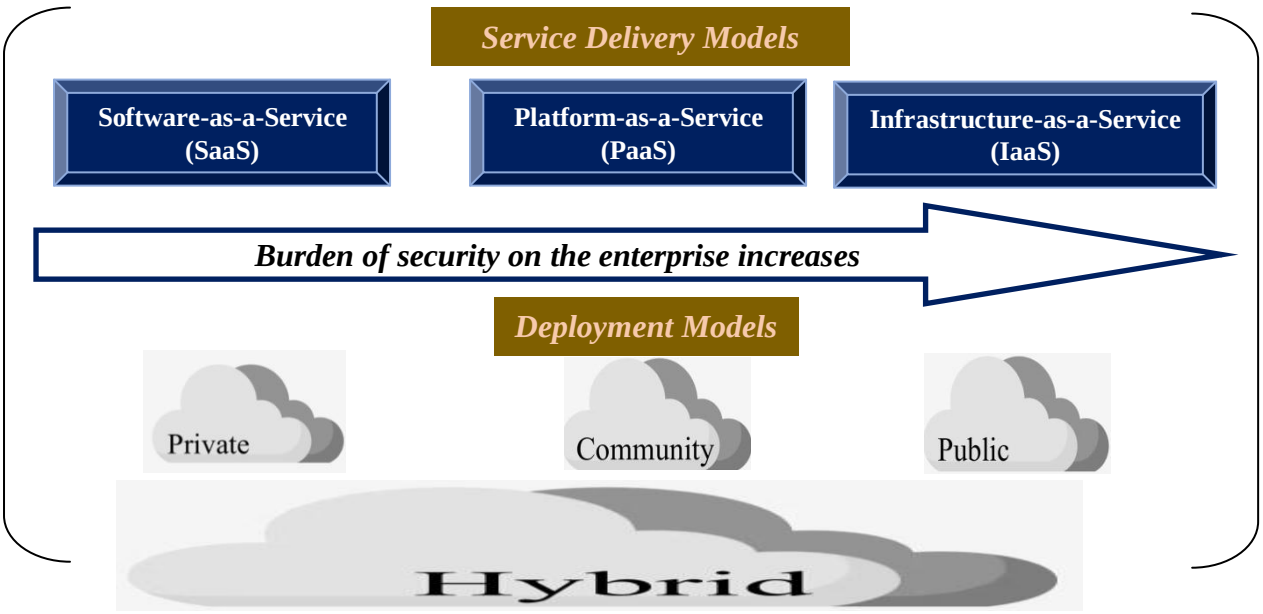

Figure 1: NIST Cloud Computing Model (Adapted from Winkler, 2011).

This is so because while SaaS provides a large amount of integrated features that confers a high level of security and/or responsibility for security on the part of the cloud service provider, PaaS offers less integrated features and less level of security. IaaS on the other hand provides little or no application-like features, however, it provides for enormous extensibility but generally less security capabilities and functionalities beyond protecting the infrastructure itself, since it expects operating systems, applications and contents to be managed and secured by the customers (Jaydip, 2013).
According to Jaydip (2013), the notion of private, managed, public and hybrid when describing cloud services really denotes the attribution of management and the availability of service to specific consumers of the services. As we move from private cloud towards public cloud, the enterprise/customer's control increases.

Although there is a general belief that the private cloud is best security-wise, what obtains in private cloud approximates that of the public cloud once the management and data center location (in the private cloud) are off-premise, since that scenario means *loss of control* of data and computation. To protect the enterprise, it is therefore necessary for IT organizations to develop strong monitoring frameworks over the SPI (SaaS, PaaS and IaaS) delivery model to ensure that their service levels and contractual obligations are met (Marther et al., 2009). Table 1 gives a summary of the various features of the four cloud deployment models.

Deployment model	Operating environment	Data center location/Variants	Infrastructure owned/Managed by	Security arrangement appropriate for
Private	Single tenant (dedicated)	On-premise Off-premise	Both organization and third party provider	Sensitive data
Community	Single tenant or Multi tenant (shared)	On-premise	Third party provider	Sensitive data common to group
Public	Single tenant Multi tenant (shared)	Off-premise	Third party provider	Non-sensitive data
hybrid	Both Single tenant and Multi tenant	On-premise and off- premise	Both organization and Third party provider	Sensitive data of a group concern and/or Non-sensitive data

Table 1: Summary of the various features of cloud deployment models (Adapted from Jaydip (2013).

Multi-Tenancy issues
Public cloud services are offered at an affordable price because resources are shared between multiple tenants. The multi-tenancy service is achieved by multiplexing the execution of virtual machines from potentially different consumers on the same physical server. The security implication of such an arrangement is however critical. This is because when CPU, memory and datacenter resources are shared by multiple users, there is a risk of unauthorized access of one's business networks especially when there is a flaw in the cloud network. Besides, according to Williams (2013), the Public Cloud allows people using the same hardware to hack each other's IP and MAC numbers thereby gaining unauthorized access to the other's business networks.

Data compliance issues

The scenario in public cloud computing environment is that data is stored at random locations across the globe. More often than not detailed information about the location of an organization's data is unavailable or not disclosed to the service subscriber. This situation according to Jansen and Grance (2011) makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met.

Governance

A handover of an organization's data and data management to a third party without adequate supervision and regulatory agreement backed by law is like a building without a pillar. To Ensure that effective governance, risk and compliance processes exist and in assessing the security provisions of cloud applications, the following questions according to CSCC (2012) are pertinent:

- Does the consumer have governance and compliance processes in place for the use of cloud services?
- Does the provider have appropriate governance and notification processes for their services, as required by the consumer?
- Is it clear whether responsibility for applications running on cloud infrastructure lies with the consumer or with the provider?
- Where the responsibility lies with the consumer, does the consumer have governance and policies in place that ensure the appropriate security provisions are applied to each application?
- Where the responsibility lies with the provider, does the SLA make the provider's responsibilities clear and require specific security provisions to be applied to each application and all data?

Data Protection

Data are at the core of IT security concerns for any organization and for an organization to opt for a public cloud implies all its data are in a shared environment. Being in the same environment, malicious users (co-tenants) can now legally be in the same infrastructure to cause havoc, hence the need for data protection. While Williams (2013) advocates mandatory data encryption using highly secure methods since unencrypted data can be vulnerable to hacking attacks, Jansen and Grance (2011) emphasizes that data isolation by provision of different layers of security for data at rest, data in transit and data in use is necessary. In addition the data sanitization method applied by the cloud service provider should be such that business data that is deleted or moved needs to be completely erased from the datacenter. However, the fear entertained by critics is that given the scenario in a public cloud, the client do not have the complete control on the datacenter infrastructure as to use proper data sanitization techniques, hence, if data is not properly erased, it can be accessed by other users and may be used in a harmful manner.

Availability

Once an enterprise gets subscribed to a cloud computing service, the expectation is that the organization's full set of computational resources will be accessible and usable. Jansen and Grance (2011), states denial of service attacks, equipment outages (temporal, prolonged or permanent), and natural disasters are all threats to availability which could impact the mission of the organization.

Incident response

All things being equal, is a saying, but all things cannot be equal. Systems and networks can fail at anytime, leading to partial or complete service withdrawal by the cloud service provider. But according to Vince Lombardi, an American football coach of the 1960's, 'the greatest accomplishment is not in never falling, but in rising again after you fall'. Hence, the most important thing needed in the event of a system failure or malfunction, or a hacker intrusion is prompt response, ability to identify the problem and fix it in record time. According to NIST report, a cloud service provider's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration (Jaydip, 2013). The CSCC concludes that the cloud provider is responsible for logging and timely data retrieval and provision to the consumer in an incident response scenario.

SECURITY BENEFITS IN PUBLIC CLOUDS

More often than not, once the issue of security and privacy in cloud computing is mentioned, thoughts get skewed to the negative aspects of the issues – that is, the security risks inherent in the cloud. This one sided-negative perception is however erroneous, since these issues in either the private or public cloud, is like a double-edged sword which could affect the service provider or the client or both, positively or negatively. The upside of these security and privacy issues is highlighted in this section.

A microfinance bank in one the first generation universities in Nigeria once got gutted by fire on a Thursday. Physical records and equipments including computer systems were burnt. Customers on getting to know this were greatly worried as to what has become their fate – who knows when the bank would come back to business? Perhaps, in months and months to come, they worried. Is their money safe? When can the bank resume normal operation? What of the records? Burnt! But the great surprise came on the Sunday following the Thursday as the announcements sent by the bank to various religious and social centers in the vicinity, says that *customers to the bank should come to the bank for their normal banking transactions the following day - Monday as the bank will resume normal operation on that day.*

Wow, what a technology! With such third party intervention by cloud or cloud-like computing, losing your data-laden laptop by fire or by theft leaves less to be desired, once you have your data in the *Dropbox*. But that is far off! A more user-friendly case is that whereby one could lose a handset today; do a *welcome back* today*;* pick another handset; and end well getting connected to all-contacts within 24 hours once a backup was performed.

Although Jansen and Grance (2012) agrees that the biggest obstacle facing public cloud computing is security, it noted that cloud computing paradigm provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations. It listed Potential areas of security benefits in public clouds as staff specialization, platform Strength, resource availability, backup and recovery, mobile endpoints and data concentration.

THE SITUATION OF CLOUD COMPUTING IN AFRICA

'The mobile-centric nature of Africa's future, its dicey current infrastructure, and the scattered and micro-entrepreneurial nature of much of its information technology industry all make the continent a prime candidate for cloud computing'. This assertion by Gallagher(2012) is corroborated by Nkolwoudou (2010) who is of the view that cloud

computing is suited to the African continent by reason of the concentration of infrastructures, availability of IT competencies and ease of implementation that abound in the proviso.

Although the advantages to be gained through access to the cloud are enormous, substantial challenges stand in the way of cloud computing in Africa. Critics are emphatic that the challenges go beyond the traditional obstacles seen in the current debate on cloud computing such as data controls, vendor 'lock-in', and sovereignty issues. Obstacles in Africa according to Laverty(2011), center primarily on infrastructure and government policy.
Apparently, the adoption of cloud computing in Africa is still associated with numerous challenges. Based on a survey conducted by International Data Corporation (IDC) in 2008, the major challenges that prevent Cloud Computing from being adopted as indicated by organizations are security, costing model, charging model, service level agreement, what to migrate and cloud interoperability issue (Kuyoro, Ibikunle and Awodele , 2011). Africa appears to be worst hit by those challenges for obvious reasons.

Report of Research ICT Africa survey:

A survey conducted in 2013 by Alison Gillwald of Research ICT Africa on "Households and individuals with Internet connection" shows the status of eleven African countries (**Gillwald, 2013)**. The result (figure 2), goes a long way to showcase the impact of the challenges, and the penetration of cloud computing in Africa as a whole.

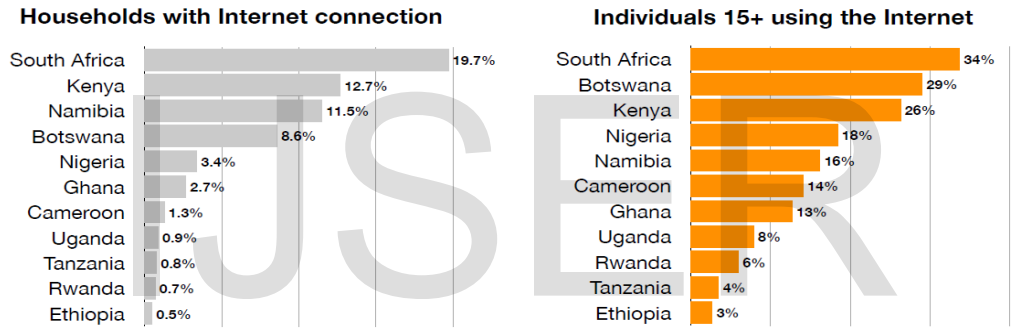

Figure 2: Penetration of Internet connections
Source: www.researchICTafrica.net

Africa's rankings in CISCO's Internet stages and ICT map:

Computer information system company (CISCO), a networking and internet multinational corporation developed two models- Internet stages and ICT map for assessing global Information and Communication Technology development (CISCO, 2009).
The purpose of the five "Internet stages" - proto-internet, early days, familiarization, extensive, and intensive—(with **Proto-internet as the lowest, and intensive - the highest and most advanced**), is to focus on key thresholds toward achieving nationwide connectivity. A total of 45 African countries have been placed and ranked accordingly in a sample survey of 157 countries. An analysis of the survey, by this author, is as summarized in Table 1 below.

	Proto-internet stage	Early days	Familiarization stage	Extensive stage	Intensive stage
ROACTO	31:45	11:32	3:39	0:18	0:23
African countries	Angola, Libya, …	Egypt, Kenya, Nigeria, Senegal, South Africa,	Mauritius, Morocco, Tunisia	-	-

		Algeria, …			
Internet usage rates	< = 5%	5% or slightly below	>=15%	-	-

Table 2 Countries by Internet Stage (157 worldwide, 45 of which are in Africa).
Source: Authors' tabulation, based on CISCO white paper, 2009.

ROACTO = Ratio of African countries to others in the category.

Placing a country in this context provides a useful perspective on where the country stands with respect to the benefits of broadband. It could be seen from the table that no African country is grouped either in the intensive or the extensive stage. The most advanced countries in Africa are Mauritius, Morocco, and Tunisia, and they are only in the "familiarization" stage. Eleven African countries are in the early stage while as many as thirty one are in the proto-internet stage. The parameter for such categorization is as given in Table 3 below.

Internet stage	Internet usage rates	Income	Average Urban habitation(%)	Internet access	Number of African countries
Proto-internet	<5%	low	35%	largely available only to larger businesses, universities, the government, and small, elite groups in the cities	31
Early age	5% or slightly below	Low to moderate	50%	Shared access: cybercafés	11
Familiarization	>= 15%	moderate	>= 50%	Home connections not less than 15%	3
Extensive	NA	NA	NA	NA	NA
Intensive	NA	NA	NA	NA	NA

Table 3 Parameters for classification of internet stage.
Source: Authors' calculations based on data from CISCO white paper, 2009.
NA – Not Available

From the 157 Countries captured by the survey – the following observations were made:
Proto-internet stage - Internet usage rates falls between 5 percent—or slightly below.
These are countries that have Internet usage rates between 5 percent—or slightly below but growing fast—and 15 percent, but the large majority of the population has yet to experience the Internet directly. South Africa is one of the 32 countries at this stage out of 157 countries that have been classified in the stages. Countries in "early days" generally have significant urban populations (on average, about half of the country's total population), and Internet use averages mask major differences between urban and rural areas. Many people in these countries use the Internet through shared-access connections (cybercafés or community

centers), so that the number of Internet users is a multiple of about five times the number of Internet connections in the country.

Internet and broadband facts: ITU 2013:

The term cloud is just a metaphor for the internet and by design and architecture, the internet cannot be dissociated from the broadband. Broadband—which simply means a fixed-line and/or wireless connection that enables the delivery of voice, video, and data at high speed to any node with a similar connection, has changed the way the world works. Internet services and information delivered over broadband networks provide the means, by which entrepreneurs and enterprises communicate, transact and offer services.

Cloud computing is considered by many to be the technological revolution of the twenty-first century.

Having been encapsulated in this digital suite, broadband penetration has become an important factor for the economic growth of any nation

A report on Internet usage habits in 157 countries around the world by the International Telecommunications Union (ITU) in its "*Measuring the Information Society 2013 report"* showcases the average IDI values of 38 African countries with that of the - world developing, global and developed countries for 2012 (ITU, 2013). An analysis of the ITU report on the average IDI values by this author, is as summarized in Table 4 below.

African countries	Developed: 6.5<AIDIV<7.0	Global(world): 4.5< AIDIV<6.5	Developing: 3.5< AIDIV<4.5	Africa: 2.0< AIDIV<2.5
Above AIDIV	0	2	3	12
Below AIDIV	38	36	35	26

Table 4. *Summary of the average IDI values of 38 African countries with that of the - world developing, global and developed country- averages for 2012.*
Source: *Authors calculation based on ITU data in "Measuring the Information Society 2013 report".*
AIDIV = Average Information and Communication Technology Development Index Value.

Based on a 10 point rating scale, developed-country average is greater than 6.5 but less than 7.0. No African country is in this category. The two African countries with an IDI above the global average are Seychelles and Mauritius. Seychelles tops African countries while Niger falls at the bottom in terms of ICT Development Index. The three African countries ranked above the developing country index average are Seychelles, Mauritius and South Africa. Countries in Africa with an IDI above Africa average are 12 in number - a fallback to the ITU document shows the countries are Seychelles, Mauritius, South Africa, Cape Verde, Botswana, Namibia, Gabon, Ghana, Zimbabwe, Kenya, Swaziland, and Nigeria. Besides, top five African countries with highest percentages of individuals using the internet are: Seychelles(47%), Mauritius(41%), South Africa (41%), Cape Verde (35%), Nigeria(33%), and Kenya (32%).

As could be seen from the table, developed countries, for obvious reasons, have the highest average followed by world, developing and African-country average, in that order.

The source document shows that the 26 African countries below African-country average has Senegal at the top and Niger at the bottom of the ladder, while countries with relatively high income levels but comparatively lower IDI values include Angola, Gabon, and Botswana.

Analyzing Africa's hope for low telecom tariffs, Abang (2007) noted that 'from Cape to Cairo, from Lagos to Nairobi, the problems plaguing Africa's telecom sector are hardly

different; only the degree may vary from country to country; also depending on the political depth and economic policies of the government'. The author was full of regrets that although African continent was reputed to be where civilization started, it is far behind in virtually every facet of human endeavor.

The power problem:

Computing be it cloud or non-cloud, cannot be done without power backing, and as such power is paramount to cloud service delivery. Aside broadband issues, enterprises in Africa face the problem of power availability. This has a grave negative effect on the accessibility of cloud services in Africa. The power problem poses great threat to the development of enterprises not only in Africa but globally, although Africa by statistics seems to be worst hit.

According to Abang (2007), "If you give some subscribers in Africa an opportunity for a moment to run amok, their first victim would most likely be their telephone or internet service provider. Poor services amid high tariffs", he asserted, "would be their first charge". He however noted that not many subscribers realize many of the underlying problems that make services on their continent poor. While subscribers point accusing fingers at service providers, service providers blame the government on the high cost of materials for power production and network sustenance. Blunt as it may sound, Abang was emphatic that no serious company in Nigeria relies on public power supply. Based on prevailing circumstances, it could be said that with the exception of a few African countries, while power availability is scarce, power outage is a norm.

Lamenting the deplorable situation, Barry Gill, an enterprise consultant for e-mail software-as-a-service provider Mimecast, remarked that although 'South Africa is very first-world in many things, electrical service is not one of them', resulting in people cursing the incumbent power provider all the time (Gallagher, 2012).

Africa is said to have an average electrification rate of 24% while the rate in the rest of the developing world lies closer to 40%(Wikipedia, 2014). The availability of electrical grid is however not the ultimate as the power is often unreliable - brownouts and power outages alternate with normal power supply. A situation where the manufacturing sector loses power on average 56 days out of the year does not help economic growth of any enterprise or nation. According to the analysis less than 2% of the rural populations of Malawi, Ethiopia, Niger, and Chad have access to electrical power while in Senegal power is out 25 days a year, in Tanzania 63 days, and in Burundi 144 days.

Frequent power outages no doubt cause damage to sales, equipment, and discourage international investment. Since the cost of deploying generators for 24 hours all-day for cloud computing is so high, enterprises in Africa would rather opt for a third party to bear that cost. The incidence of the high cost of sourcing power from third party providers retards growth of local enterprises in Africa.

CONCLUSION

Although worries about security and privacy issues have continued to mar people's minds with respect to public clouds, cloud providers however believe that the significant benefits coupled with substantial security and privacy improvements from the public cloud will induce customer migration into the cloud.

According to NIST report, 2011, the biggest beneficiaries from transitioning to public cloud computing environment are likely to be smaller organizations that have limited numbers of

information technology administrators and security personnel, and lack the economies of scale available to larger organizations with sizeable data centers.

Given the poor economic status of most African countries, the offer of scalability without huge financial demand for infrastructure purchase, use and maintenance is seen as a welcome development in the business circle.
To increase the level of reliability of public cloud services its capabilities for data security, backup, and disaster recovery need to be addressed in the organization's contingency planning. It is only when this is done that Enterprise Security and Privacy in Public Cloud Computing Environment will be guaranteed.
I acknowledge authors and bodies whose works were cited or referenced. The personal views, analysis and calculations expressed in this paper should not, however, be regarded as having been expressed by any of the individuals or sources mentioned. Works of the following bodies were cited: International Telecommunication Union (ITU), by International Data Corporation (IDC), The National Institute of Standards and Technology (NIST), United Nations Conference on Trade and Development (UNCTAD), Cloud Standards Customer Council (CSCC).

REFERENCES

[1] Abang M.(2007). Fiber optics: Africa's hope for low telecom tariffs. *IT and Telecom Digest.* September 2007 No. 69. P.16.
[2] CISCO (2009) CICSO case study: Broadband Across Africa. http://www.google.com.ng.
[3] CSCC (2012)http://www.cloudstandardscustomercouncil.org/2012 Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf.
[4] Gallagher, S. (2012) How Africa is embracing "the cloud" on its own terms. http://arstechnica.com/business/why-africa-embraces=cloud-computing/.
[5] Gartner (2008). "Seven cloud-computing security risks." *Infoworld*, http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks.
[6] Gillwald, A. (2013) Prospects, Challenges and Impacts of the Cloud: Perspectives from (South) Africa. Presentation to UNCTAD workshop on Cloud Economy, Geneva, February, 2013. www.researchICTafrica.net.
[7] ITU (2013). African internet and broadband facts from 'Measuring the Information Society 2013′ report October 14, 2013. http://www.oafrica.com/broadband/african-internet-a...mis-2013-report.
[8] Jansen W. and Grance, T. (2011) Guidelines on Security and Privacy in Public Cloud Computing. https://cloudsecurityalliance.org/.../NIST-Draft-SP-800-144_cloud-computing/ .
[9] Jaydip, S. (2013) Security and privacy issues in cloud. http://www.google.com.ng
[10] Kuyoro S. O., Ibikunle, F. and Awodele, O. (2011) "Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), 3, 5, 247-255.
[11] Laverty, A. (2011) The cloud and Africa - indicators for growth of cloud computing http://the africanfile.com/…/the-cloud-and-africa-indicators-for-growth.
[12] Mather, T., Kumaraswamy, S. and Latif, S. (2009) Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.
[13] Mell, P. and Grance, T. (2009) The NIST Definition of Cloud Computing, Version 15, October 7, 2009, http://csrc.nist.gov/group/SNS/cloud computing.

[14] Mell, P. and Grance, T. (2011) "The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), Special Publication Draft-800-145". http://csrc.nist.gov/drivers/documents/FISMAfinal.pdf.

[15] Nkolwoudou, R. (2010) L'Afrique courtisée, mais gare aux turbulences juridiques". *Les Afriques*. http://www.lesafriques.com/.../ .

[16] Wikipedia (2014). Energy in Africa. http://www.wikipedia.org/wiki/energy_in_Africa

[17] Williams Charly (2013). The public cloud is not always the most secure option for your business. Retrieved from http://www.2x.com/blog/author/charlesw.