1-1-2011

Cloud computing concerns in developing economies

Mathias Mujinga
University of South Africa

Baldreck Chipangura
University of South Africa

Recommended Citation

Mujinga, M., & Chipangura, B. (2011). Cloud computing concerns in developing economies. DOI: https://doi.org/10.4225/75/57b5486bcd8c8

DOI: 10.4225/75/57b5486bcd8c8
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

CLOUD COMPUTING CONCERNS IN DEVELOPING ECONOMIES

Mathias Mujinga[1] and Baldreck Chipangura[2]
School of Computing
University of South Africa
[1]mujinm@unisa.ac.za, [2]chipab@unisa.ac.za

Abstract

Cloud computing promises to bring substantial benefits to how organizations conduct their businesses and the way their services reach out to potential consumers. Cloud computing is a welcome initiative for small businesses that cannot afford to invest in ICT infrastructure but need to benefit from the rewards of conducting business online. In developing economies, there are challenges that face cloud services providers and their consumers. Broadband network access was identified as the main essential service for a successful cloud computing offering. The objective of this paper is to give background information on the security issues in cloud computing, and highlight the potential of cloud computing and the associated challenges in utilizing services on the cloud for small businesses in developing economies. We discuss security concerns specifically related to the small businesses, such as service availability, privacy and SLA terms.

Keywords
Cloud computing, Security, Cloud computing security, Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service

INTRODUCTION

Most small-, micro-and medium sized enterprises (SMME) businesses in developing economies and South Africa in particular find it difficult to invest in ICT. Given the advantages that come with participating in e-commerce in any business, this becomes a handicap that hinders such small businesses. Consequently, it put them at a disadvantage with more established organizations that have since taken their business online. Small businesses contribute to the economic growth of upcoming economies through employment creation and service delivery. At least two thirds of SMMEs are found in the informal sector and they participate in a variety of sectors from manufacturing, finance, mining, and hospitality (Al Berry, Cassim, Kesper, Rajaratnam, & van Seventer, 2002). According to Subashini & Kavitha (2010) small and medium business companies have started realising the benefits of cloud computing and they are boosting their businesses by tapping the cloud infrastructure to gain fast access to best business applications and infrastructure at negligible cost.

Cloud computing has the potential to bring significant benefits to these small businesses by reducing the costs of investment in ICT infrastructure. Since cloud computing allows users to make use of services such as computation, software, data access, and storage to end-users without the need to know the physical location and configuration of the system that delivers the services. Bakshi & Hemachandran (2011) identified these benefits of cloud computing; simplified cost and consumption model, faster provisioning of systems and applications, right-size to address business changes, ease of integration, highly secure infrastructure, and compliant facilities and processes.

Despite the advantages that come with cloud computing, its adoption and implementation in developing economies is faced by a variety of challenges. The objective of this paper is to shed light on the potential of cloud computing in Africa and the associated challenges in utilising services on the cloud. This paper begins by defining cloud computing, discuss deployment and delivery models, and discuss benefits that come with adopting cloud computing. Finally we discuss the potential and challenges faced by small businesses in developing economies when adopting cloud computing.

What is cloud computing?

The term cloud computing probably comes from (at least partly) the use of a cloud image to represent the internet or some large networked environment. Cloud computing according to Buyya, Yeo, Venugopal, Broberg & Brandic (2009) is increasingly being perceived as the 5th utility (after water, electricity, gas, and telephony) that will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community. There are a number of competing definitions of cloud computing. United States' National Institute for Standards and Technology (NIST) provided guidelines on defining cloud computing with this all encompassing definition (Mell & Grance, 2011):

> "Cloud computing is 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

The above definition is accompanied by these five essential characteristics as illustrated in Figure 1:

Broad network access: Capabilities and control of a cloud computing service must be available over the internet or other networks using standard protocols.

On-demand self-service: Customers can unilaterally provision computing capabilities, without requiring human interaction with the service provider.

Rapid elasticity: Near-immediate provisioning of capabilities, to quickly scale up, or down, according to demand.

Measured Service: Customers' use of the capabilities is monitored, controlled, reported, and charged; with complete transparency enabling a pay-as-you-consume metering arrangement.

Resource pooling: Physical and virtual resources are dynamically assigned and reassigned according to demand, resulting in cost savings to the customer.

Furht (2010) defined cloud computing as a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the internet on the other hand, Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Stoica (2010) sees cloud computing as both the applications delivered as services over the internet and the hardware and systems software in the data centers that provide those services.

CLOUD COMPUTING ARCHITECTURE

Cloud computing architecture consists of four deployment models and on top of the deployment models sits the three main service delivery models as illustrated in Figure 1. Each of these models brings about different security and other challenges that need to be taken into consideration when planning to move business processes to the cloud.

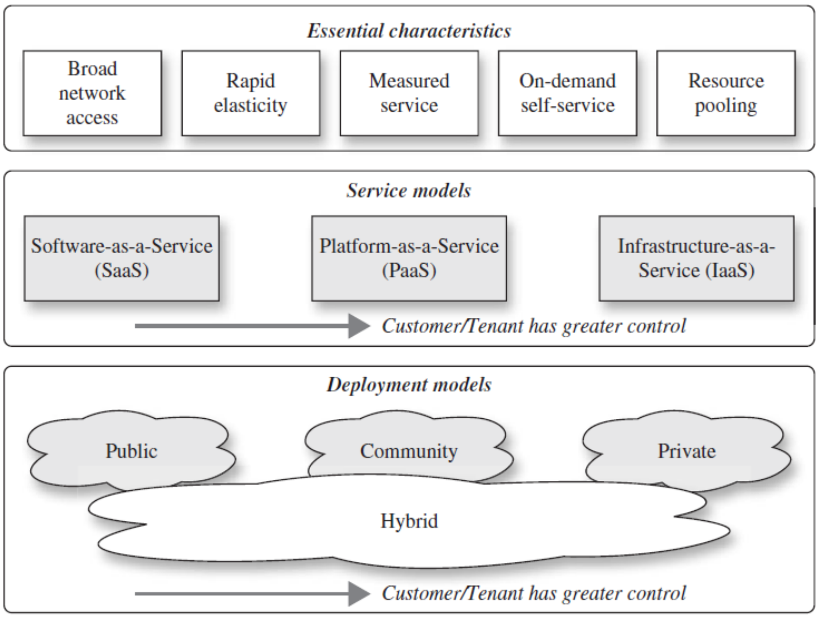
Essential characteristics
Broad network access
Rapid elasticity
Measured service
On-demand self-service
Resource pooling
Service models
Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)
Customer/Tenant has greater control
Deployment models
Public
Community
Private
Hybrid
Customer/Tenant has greater control

Figure 12: NIST Cloud Computing Model (Adapted from (Winkler, 2011))

Deployment Models

Cloud computing services can be deployed through four deployments models namely; private, community, public, and hybrid (Figure 1).

Private Cloud

In private cloud (or internal cloud), the infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Public Cloud

The public cloud (or external cloud) infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. A public cloud is hosted, operated, and managed by a third-party vendor from one or more data centers (Mather, Kumaraswamy, & Latif, 2009).

Community Cloud

Community cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns such as mission, security requirements, policy, and compliance considerations. It may be managed by the organizations or a third party and may exist on premise or off premise.

Hybrid Cloud

The hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (Mell & Grance, 2011).

Delivery Models

Cloud computing services are generally delivered through three main delivery models to the end-user, namely: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Apart from these main service delivery models a number of variations exists, namely Security-as-a-Service (SecaaS), Monitoring-as-a-Service (MaaS), Communication-as-a-Service (CaaS), Software Testing-as-a-Service (STaaS), Business Process-as-a-Service (BPaaS), IT-as-a-Service (ITaaS), Database-as-a-Service (DBaaS), and many more other variations being defined on a daily basis. Cloud computing enables the delivery of services through the on-demand service provisioning model to end-users on ‘pay-as-you-go’ basis over the network such as the internet.

Software-as-a-Service (SaaS)

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the internet. SaaS is dominant delivery model as an underlying technology that supports web services and service-oriented architecture (SOA). The SaaS model is associated with the pay-as-you-go subscription licensing model. Due to the increase in broad band accessibility and universal access to networked information, some companies have started incorporating the SaaS model in their businesses, notably IBM Lotus Live and Salesforce.Com. The dominance of SaaS has resulted in other models adopting it and they include Security-as-a-Service (SecaaS) and Communication-as-a-Service (CaaS).

Platform-as-a-Service (PaaS)

PaaS provides the development environment and it sits on top of Infrastructure-as-a-Service (IaaS). PaaS delivers operating systems and associated services over the internet without the need to download or installs applications on end-user computers. It provides an operating environment for delivering a variety of applications and is essentially an outgrowth of the SaaS application delivery model. Examples include the Amazon Web Services, Google's AppEngine and Windows Azure Platform.

Infrastructure-as-a-Service (IaaS)

IaaS provides the entire infrastructure stack that delivers the computer infrastructure and it leverages significant technology, services, and data center investments to deliver IT as a service to customers. IaaS differs from SaaS in that, instead of software, IaaS delivers hardware such as servers, memory, CPUs, disk space, and network connectivity. Examples include Flexiscale and Cisco Unified Service Delivery. Other notable models that are built on the basic foundation of IaaS are Computing-as-a-Service (CaaS) and Hardware-as-a-Service (HaaS).

The Cloud Security Alliance (CSA) (CSA, 2011) issued its first Security-as-a-Service (SecaaS) white paper in September 2011 that defines categories of service such as; identity and access management, data loss prevention, etc. In future, variations of delivery models are expected to be fully defined and be stand-alone models. The adoption of SaaS model is already high by enterprises of all sizes. But according to the Yankee Survey (2010) the two other areas of cloud computing; PaaS and IaaS are taking longer to develop. IaaS adoption is growing with 24% of large organizations already using IaaS and a further 60% considering it in the next twenty-four months (Yankee Survey, 2010)**.** But still the number one barrier for enterprises considering IaaS adoption is virtualization security, with those that have already deployed IaaS ranking regulatory compliance, data migration, reliability, employee use and quantitative benefits higher.

Cloud computing governance is another challenge that faces organizations that want to adopt cloud computing. Traditionally, most IT organizations govern the five technology layers shown in Figure 2. The two on-premises models indicate that IT has total control and responsibility for all five technology layers. However, as we move from IaaS to PaaS to SaaS, the IT organization's level of control diminishes as that of CSP increases. Although control increases for the CSP, responsibility remains with the IT organization. It is critical 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 (Mather et al., 2009).

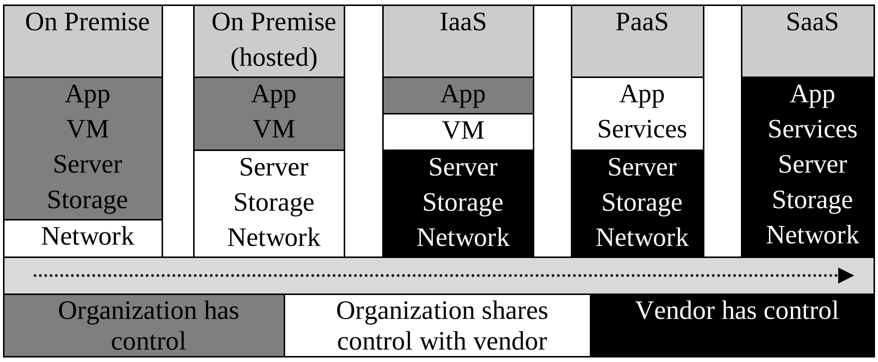

Figure 13: Cloud computing governance structure of IT organizations (Mather et al., 2009)

Figure 2 is also in line with the levels of abstraction of the SPI model as described by (Winkler, 2011). The SPI model has layers of abstraction that differ from one specific service model to the other. PaaS abstracts infrastructure to a greater extent and generally presents middleware containers that are tailored for different categories of usage. These containers provide tools to simplify application development and limit application interactions with the underlying systems. SaaS on the other hand abstracts even further and generally exposes narrow-functionality software-based services such as customer relationship management (CRM). In other words, from IaaS to SaaS underlying computing functions are more and more abstracted.

CLOUD ISSUES IN AFRICA

The cost-effectiveness offered by cloud computing has lead to a growth in cloud interest, but data security remains the main concern. Organizations have adapted an approach of migrating low risk business processes, until such time the cloud is considered safe. This is despite the fact that the cloud is more secure than most in-house networks. Since CSPs put security in the forefront because it's the main competitive advantage and a barrier to cloud computing growth (Deloitte, 2011).

Capobianco (2010) alluded that by definition, mobile devices that access the internet are performing mobile cloud computing, since handsets need to borrow storage and computing power from the cloud because of their limited resources or because it makes more sense. Accessing data in the cloud from mobile devices is becoming a basic need. There are successful initiatives that are using mobile cloud services such as M-Pesa an M-Banking service. M-Pesa (Swahili for M-Money) money transfer service was first a success in Kenya (Hughes & Lonie, 2007)and now has been launched in other countries like South Africa, Tanzania and Afghanistan. Other applications are in M-Health, M-Agriculture, and M-Education.

There a number of barriers for cloud computing adoption, (Mather et al., 2009) identified the following; security, privacy, connectivity and open access, reliability, interoperability, independence from CSPs, economic value, IT governance, changes in the IT organization, and political issues due to global boundaries. Below we discuss developing economies' problems when adopting cloud computing, especially for small businesses.

Infrastructure

Most rural communities in developing economies lack basic infrastructure such as roads, telecommunications, electricity, and water (Kauffmann, 2009). These infrastructures are the backbone of any development initiatives. This is not helping in the fight to bridge the digital divide. The absence of such infrastructure leads to the unavailability of internet infrastructure and escalating costs of such services and the cost of devices to access internet.

Devices

Most households in developing countries do not possess a personal computer and they rely on mobile devices to access the internet. Mobile service providers, in South Africa for instance, have rolled more advanced 3G network coverage in all of their access areas, with the mobile networks bringing internet access to many areas outside of the main cities for the first time (Lange, 2011). This provides the backbone for launching a wider range of services through mobile devices, e.g. M-Pesa. However, for SMMEs to maximize cloud computing benefits, services should not be limited to those only available through mobile devices but extend to computers. This is true for services offered by IaaS for instance, were appropriate devices might be personal computers not only mobile devices, hence the need to provide these devices and connectivity capacity.

Internet coverage

Internet courage in developing economies is still a challenge due to lack of infrastructure, in this case telephone network coverage, for dial-up internet, which does not cover most of the under developed communities such as rural areas (Jansen & Richardson, 1999). InternetWorldStats (2011) states that, Africa has 15% of the world population but it accounts for 5.7% of internet users in the world. According to Twinomugisha (2010) lack of infrastructure in Africa has resulted in low bandwidth and high costs. On 23 July 2009 the 17,000km SEACOM undersea fibre-optic cable went live; it provides broadband connectivity to a number of African countries (BBC, 2009). In the meantime internet cafés are the primary means of accessing internet in these under developed communities and they are playing a significant role in bridging the digital divide.

Physical location of data

Major CSPs are overseas companies such as, Google, Amazon, and Microsoft. Hence the infrastructure is usually not physically located in the premises of the consumer, let alone the same country, in case of most developing economies. Hence there is a lack of control of an organization's assets. First of all, cloud computing requires a higher bandwidth internet to be able to access Europe or USA servers. Secondly, in the South African context, there might also be exchange control implications for e-commerce transactions. Thirdly, IT expenditure may move from capital expenditure to operating expenditure on the balance sheet, which obviously changes the tax implications.

SECURITY IN THE CLOUD

Security in the cloud has been a thorny issue since the introduction of the concept, a joint survey by IEEE/Cloud Security Alliance (CSA) in 2010 indicated that the need for cloud computing security standards is important and urgent and it's hindering growth of cloud computing. Armbrust et al. (2010) also identified availability of the service or business continuity as the number one obstacle to growth of cloud computing. They also sighted data confidentiality and auditability as the third obstacle, this is despite companies entrusting sensitive services such as email and payroll to external providers. The loss of data and breach of privacy in the cloud can cause major disruption in the business operations of an organization. This is even worse in case of small organizations that could not afford alternative measures such as maintaining legacy systems in case of cloud failure. Subashini & Kavitha (2010) highlighted security issues that arise on each layer of the cloud computing environment as illustrated in Figure 3. Deployment models are more concerned with data storage security and for delivery models data transmission security is the main concern. In addition, security needs varies for each deployment or delivery model.

Cloud computing is faced with a number of challenges such as; secure data storage, high-speed access to the internet, and standardization. Privacy is still one area of security that concerns CSPs (Bristow, Dodds, Northam, & Plugge, 2010) and more so for the consumers and it is a threat to the success of cloud computing. When considering how to secure public versus private cloud architectures, the security concerns are more different than common. For instance, if a cloud is private, internal on a customer premises, and owned and managed exclusively by the organization utilizing it, the principles in securing it vary greatly from those of a public cloud hosted externally by a third party. A private cloud doesn't have the data confidentiality and legality concerns that a public cloud might (Winkler, 2011).

SaaS Security

In SaaS security, the burden of security lies with the cloud provider. This is due to the degree of abstraction, with the SaaS model having a high degree of integrated functionality with minimal customer control or extensibility (Winkler, 2011). Most enterprises are still uncomfortable with the SaaS model due to lack of visibility about the way their data is stored and secured (Subashini & Kavitha, 2010). Consequently, the risk of loss of data and breach of privacy is high in SaaS for organizations. Subashini & Kavitha (2010) identified key security elements directly related to SaaS, some of them are; data security, network security, data locality, data integrity, data segregation and data access.

PaaS Security

The PaaS model offers greater extensibility and greater customer control but fewer higher-level features (Winkler, 2011). The consumers are given some control to build applications on top of the platform but still any security below the application level will still be in the scope of the CSP. Extensibility means less complete built-in capabilities that extends to security features, but there is more flexibility to layer on additional security (Subashini & Kavitha, 2010).

IaaS Security

Due to relatively lower degree of abstraction, IaaS offers greater customer control over security than do PaaS or SaaS, as long as there is no security hole in the virtualization manager. This is mainly because the customer has less control over the IT organization as we move from IaaS to SaaS. IaaS security issues are based on the cloud deployment model through which it is being delivered. For instance, public cloud poses the major risk whereas private cloud seems to have lesser impact. Physical security of infrastructure and disaster management if any damage is incurred to the infrastructure is of utmost importance in IaaS (Subashini & Kavitha, 2010).

Security and Privacy Issues

This section looks at security and privacy issues of cloud computing and how they affect small businesses in developing economies. All security issues are mostly influenced by the fact that the CSPs are not locally available, hence the lack of specific guarantees and assurances make organizations hesitant to adopt the cloud and trust third parties. Security fears range from the loss of service availability to privacy breach at data centers and how all this affect the final SLA to be signed by both parties.

Service Availability

The cloud service can be unavailable due to a number of reasons; these may include security breaches at the physical location of data centers, failure of equipment at data centers, consumer site equipment failure, connectivity failure – this is a major issue in Africa due to distances between the provider's equipment and consumer site. It is made worse by the lack of reliable internet connectivity in developing economies, since cloud computing relies heavily on network connectivity. The pay-as-you-use model at least does not require the consumers to pay when the service way unavailable. Ultimately, measures need to be in place to manage not only risk of temporary service unavailability but also those situations when a CSP suddenly and unexpectedly stops delivering services. Reputable sites like Google, Amazon, and Microsoft have been known to have been down and unable to provide services for some time. The other issue to be considered is that in moving services to the cloud, the organization or individual no longer retains direct access and control (Bristow et al., 2010). In October 2011 Research in Motion's Blackberry network service was unavailable for days to users across the globe, causing a major backlog in their messaging service (New York Times, 2011). Therefore, business must have alternative means to deal with such failure if it affects business processes.

Identity Management

Over and above the smooth availability of the service, there is a need to have a reliable identity management to allow accurate pricing of cloud services usage. Identity theft is on the increase, hence cloud consumers need to be sure that reliable verification mechanisms are in place to verify that people are who they say they are and avoid the risk of paying for service consumption that was done by an intruder.

Data and Application Security

In cloud computing there is a need of multiple layers of security to ensure consumer comfort. Security need to applied from the infrastructure layer (hardware, operating system and storage), the network layer for data transmission and package applications must make sure all components of the final offering to the consumer has no security holes. Testing need to be done to assure operability in different environments and scenarios, such as, variable networks with low bandwidth. This will ultimately allow the provision of binding specific guarantees in the SLAs.

Privacy

The consumer's data need to be protected from access by the provider's other consumers, as this might jeopardize consumers' competitive advantages over the other. Guarantees are also needed to make sure that the provider will not use consumers' for any unintended purposes. When services are offered by providers from a different country, there is the risk of an organization's data being confiscated by the provider's authorities when the regulations of that country have been violated. Hence the consumer needs to trust the provider to ensure a workable trust relationship.

Service Level Agreement Negotiation

The process of negotiating the SLA is also a cause of concern, since it always results in a compromise between the needs and demands of both the provider and consumer. Some quality of service (QoS) aspects that are part of the SLA are difficult to enforce and monitor (Keller & Ludwig, 2003) and changes may be caused by external circumstances. For instance, metrics like response time and throughput might be affected by network connectivity that is controlled by third parties. Patel, Ranabahu & Sheth (2009) highlighted the need for a clear and formal methodology to handle the dynamic nature of cloud computing SLAs. Ultimately, the risk of security and privacy breaches plays a role in SLA negotiation, so does the reliability of the network connectivity.

CONCLUSION

Cloud computing offers major benefits, even if some areas are cause of concern but SMMEs and start-ups will ultimately benefit from using the cloud. For small organizations to consider adopting the cloud there is a need to address the infrastructure problem which to larger extent is the responsibility of government. Considering the contributions made by small informal business sector, developing economies' governments can benefit significantly through unemployment rate reduction and increased tax collections. The main inhibitor of cloud computing worldwide is security and in Africa this concern is more worrying. The loss of control over infrastructure, services, and data, once cloud models are adopted, are the key risks causing local business to take a guarded approached to cloud. Cloud providers need to guarantee some aspects of security in the SLAs for organizations to be more comfortable in service consumption. Service availability and business continuity are the major concerns of businesses in case of security and privacy breaches. Small businesses in developing economies need to take seriously the security issues in cloud computing when planning cloud migration and sufficient provisions must be in place to continue with business operations should there be a failure in the cloud services infrastructure.

REFERENCES

Al Berry, M. B., Cassim, R., Kesper, A., Rajaratnam, B., & van Seventer, D. E. (2002). *The economics of SMMEs in South Africa.* Unpublished manuscript. Retrieved 11 November 2011, from http://www.edgegrowth.com/Portals/0/Documents/Seminal%20Docs/THE%20ECONOMICS%20OF%20SMMES%20IN%20SOUTH%20AFRICA.pdf.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Stoica, I. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Bakshi, R. & Hemachandran, S. (2011), Transformative Benefits Driving Companies to Cloud Computing. Retrieved 11 November 2011, from http://www.virtual-strategy.com/2011/02/28/transformative-benefits-driving-companies-cloud-computing?page=0,0.

BBC (2009), East Africa gets high-speed web. Retrieved 11 November 2011, from http://news.bbc.co.uk/2/hi/africa/8165077.stm.

Bristow, R., Dodds, T., Northam, R., & Plugge, L. (2010). Cloud computing and the power to choose. *EDUCAUSE Review*, *45*(3), 14.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. & Brandic, I. (2009), Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599-616.

Capobianco, F. (2010). Five reasons to care about mobile cloud computing. *International Free and Open Source Software Law Review, 1*(2), 139-142.

CSA (2011). Cloud security alliance SecaaS defined categories of service 2011. Unpublished manuscript. Retrieved 11 November 2011, from https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf.

Furht, B. (2010). Cloud computing fundamentals. In B. Furht, & A. Escalante (Eds.), *Handbook of cloud computing*. USA: Springer.

Hughes, N., & Lonie, S. (2007). M-PESA: Mobile money for the "unbanked" turning cellphones into 24-hour tellers in Kenya. *Innovations: Technology, Governance, Globalization, 2*(1-2), 63-81.

InternetWorldStats (2011), Internet Usage Statistics for Africa. Retrieved 11 November 2011, from http://www.internetworldstats.com/stats1.htm.

Jensen, J. & Richardson, D. (1999), Wireless weaves to lessen the gaps in rural telecommunication coverage in Africa". Retrieved 11 November 2011, from http://www.fao.org/sd/cddirect/CDre0040.htm.

Kauffmann, C. (2009). Engaging the private sector in African infrastructure. Unpublished manuscript. Retrieved 11 November 2011, from http://www.oecd.org/dataoecd/39/41/41775965.pdf.

Keller, A. & Ludwig, H. (2003), The WSLA framework: Specifying and monitoring service level agreements for web services, *Journal of Network and Systems Management, 11*(1), 57-81.

Lange, P. (2011), Africa - Internet, Broadband and Digital Media Statistics. Retrieved 11 November 2011, from http://www.budde.com.au/Research/Africa-Internet-Broadband-and-Digital-Media-Statistics-tables-only.html.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance.* USA: O'Reilly Media, Inc.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *National Institute of Standards and Technology Special Publication.*

New York Times (2011), With Apologies, Officials Say BlackBerry Service Is Restored. Retrieved 11 November 2011, from http://www.nytimes.com/2011/10/14/technology/rim-struggles-to-overcome-blackberry-outages.html.

Patel, P., Ranabahu, A. & Sheth, A. (2009), Service Level Agreement in Cloud Computing, *Cloud Workshops at OOPSLA.*

Subashini, S., & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

Twinomugisha, A. (2010), Why Are African Internet Access Prices Still High? Retrieved 11 November 2011, from http://www.africabusinesssource.com/experts/why-are-african-internet-access-prices-still-high.

Winkler, V. J. R. (2011). *Securing the cloud: Cloud computer security techniques and tactics*. USA: Elsevier Science.

Yankee Survey (2010), The Anywhere Enterprise: 2010 U.S. Cloud Computing FastView Survey. Retrieved 11 November 2011, from http://www.yankeegroup.com/about_us/press_releases/2010-08-23.html.