12-4-2013

# Privacy and Legal Issues in Cloud Computing - The SMME Position in South Africa

Mathias Mujinga
*University of South Africa*, mujinm@unisa.ac.za



DOI: 10.4225/75/57b5658ecd8e4
11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013

# PRIVACY AND LEGAL ISSUES IN CLOUD COMPUTING – THE SMME POSITION IN SOUTH AFRICA

Mathias Mujinga
School of Computing, University of South Africa, South Africa
mujinm@unisa.ac.za

**Abstract**
*Cloud computing (CC) brings substantial benefits to organizations and their clients. Information technology (IT) users in developing countries, especially those in underdeveloped communities, are gaining easy and cost-effective access to a variety of services, from entertainment to banking. South Africa has outlined a national e-strategy that aims to improve those communities, by providing frameworks for access to information and communications technology (ICT). The products and services of small-, medium and micro-sized enterprises (SMME) are now reaching a wider audience through the use of technology. CC can go a long way to help government realize the national e-strategy. There are numerous barriers to CC adoption; among the main concerns are security, privacy and availability. CC adoption is rising globally, but in South Africa it hasn't penetrated the mainstream operations of small and large organizations. The major inhibitor is security, though it is losing ground to other factors, especially privacy concerns, and The absence of security and data privacy legislation in South Africa makes it difficult for organizations to adopt CC. The objective of this paper is to highlight CC inhibitors especially privacy and legal issues in the context of South African SMMEs and how they contribute to low rate of CC adoption.*

**Keywords**
Cloud computing, legal, security, privacy, South Africa, SMME.

## INTRODUCTION

Cloud computing has the potential to bring significant benefits to organizations by reducing the costs of investment in ICT infrastructure. CC allows users to make use of services such as computation, software, data access, and storage without the need to know the physical location and configuration of the system that delivers the services. CC has entered the mainstream enterprises in the United States of America (USA). According to North Bridge (2013), half of the USA organizations now have implemented CC in some of their business processes. The South African National Small Business Act defines SMME broadly as follows; micro-enterprises (up to 5 employees), very small enterprises (up to 20 employees), small enterprises (less than 50 employees) and medium enterprises (up to 200 employees) (NSB Act, 1996). South Africa has a National Small Business Support Strategy for the development and promotion of small businesses. The primary objective of the national policy framework is to create an enabling environment for small enterprises (DTI, 1995).

Most SMMEs 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 puts 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, including manufacturing, finance, mining and hospitality (Berry et al., 2002). According to Subashini & Kavitha (2010), SMMEs have started realising the benefits of CC, and they are boosting their businesses by tapping into the cloud infrastructure to gain fast access to the best business applications and infrastructure, at negligible cost.

South Africa has undertaken to assist SMMEs to participate in e-commerce through provision of ICT infrastructure under the auspices of the national e-strategy. SMMEs have a crucial role to play for the strategy to success as highlighted by (Farelo & Morris, 2006). CC has the potential to bring significant benefits to these small businesses. Broadly the benefits of CC are; simplified cost and consumption model, faster provisioning of systems and applications, right-size to address business changes, ease of integration and compliant facilities and processes (Bakshi & Hemachandran, 2011). Additionally, Desai & Mock (2012) identified benefits of CC as; easy and fast deployment of ICT infrastructure, pay-as-you-go model, benefits of scale and less in-house and IT staff and costs. It has since, however, been realised that security and system availability have turned out to be more problematic, and are now the top inhibitors to adoption.

Despite the advantages that come with CC, its adoption and implementation in developing economies is faced with a variety of challenges. The objective of this paper is to shed light on the potential of privacy and legal issues as inhibitors of CC in South Africa, and the associated challenges contributing to a low rate of adoption. The paper begins by defining CC followed by a brief discussion on deployment and delivery models. The barriers to CC adoption are discussed followed by privacy and legal issues as inhibitors of CC in South Africa. Finally the support for SMMEs is discussed and the paper is concluded.

## 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. CC, according to Buyya et al., (2009), is increasingly being perceived as the 5th utility (after water, electricity, gas and telephony), that will provide the basic level of computing service which is considered essential to meet the everyday needs of the general community. There are a number of competing definitions of CC. The United States' National Institute for Standards and Technology (NIST) provides guidelines on defining CC 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 definition consists of five essential characteristics, three service models and four deployment models. The five characteristics are essential to the realization of service and deployment models, as they are the enablers. The models are briefly discussed in the following sections.

### Deployment Models

CC architecture consists of four deployment models, and, on top of the deployment models, rest 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:

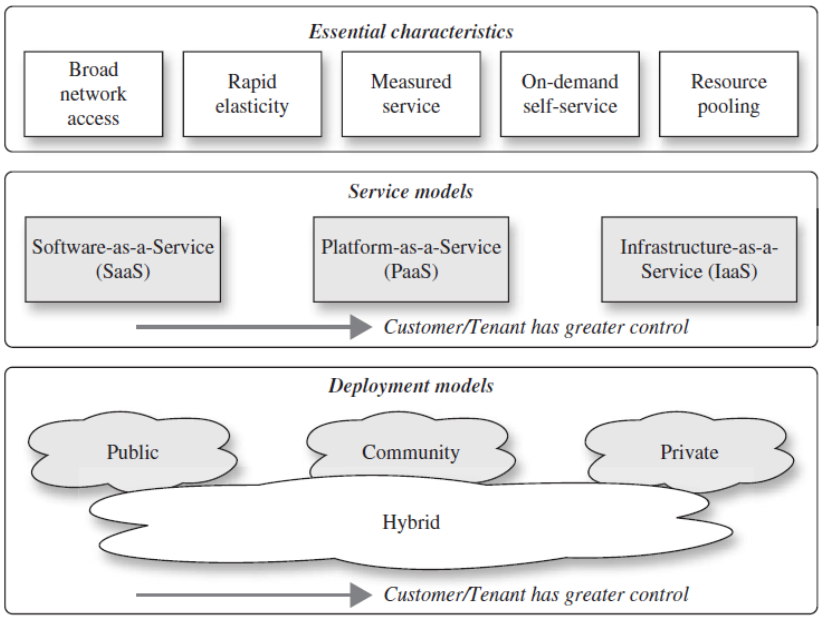


*Figure 2: NIST Cloud Computing Model (adapted from Winkler, 2011).*

Organizations planning to adopt CC services can choose from four main deployment models (Figure 1). Firstly, there is the 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-site or off-site. Usually, large organizations with multiple sites implement this model to service their office locations that might be scattered across the globe. At the other extreme, there is the public cloud (or external cloud) model, that is made available to the general public or a large industry group, and is owned by an organization offering cloud services for a fee. A public cloud is hosted, operated and managed by a third-party vendor from one or more data centres (Mather et al., 2009). The community cloud model is shared by multiple organizations that have a common objective, and supports a specific community that has shared concerns such as mission, security requirements, policy and compliance considerations. It may be managed by the organization or by an assigned third party. The hybrid cloud model 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).

CC services are generally delivered through three main delivery models to the end-user, as illustrated in Figure 1. *SaaS* 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 has emerged as the dominant delivery model and 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. North Bridge (2013) identifies SaaS as the leading model, with a 63% share of the market, while according to the Yankee Survey (2010), PaaS and IaaS are taking longer to develop. Some of the major players in this area are IBM Lotus Live, Google Apps, Oracle, Facebook, Netsuite and Salesforce.com.

*PaaS* provides the development environment and it rests on top of Infrastructure-as-a-Service (IaaS). PaaS delivers operating systems and associated services over the internet, without the need to download or install 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. Sub-types of PaaS include Desktop-as-a-Service (DTaaS) and Testing-as-a-Service (TaaS). Vendors in this area include Amazon Web Services, Google App Engine, Windows Azure Platform, Force.com and Caspio.

*IaaS* provides the entire infrastructure stack that delivers the computer infrastructure, and it leverages significant technology, services, and data centre 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. Service providers in this model include Flexiscale, Rightscale, Gogrid, Amazon Web Services and Cisco Unified Service Delivery. IaaS is the fastest growing model, and is expected to give way to PaaS in five years' time.

**Cloud Computing Inhibitors**

There a number of barriers to CC adoption. Mather et al. (2009) identify the following: security, privacy, connectivity and open access, reliability, interoperability, independence from cloud service providers (CSP), economic value, IT governance, changes in the IT organisation, and political issues due to global boundaries. Other CC adoption problems in developing economies for SMBs are the following: poor basic infrastructure, access to ICT devices, poor internet coverage and geographical location of cloud data (Kauffmann, 2009; Mujinga, 2012). This section highlights some of the top inhibitors of CC adoption.

Security concerns have since been the top inhibitor of CC adoption, as identified by a number of surveys. A 2008 survey of senior IT executives by International Data Corporation (IDC), a market research and advisory firm, in IT, telecommunications and consumer technology, identified security and performance as top two challenges of cloud computing (Gens, 2008). A follow-up survey in 2009 identified security still as the top concern with performance replaced with availability on second spot and performance a close third (Gens, 2009). Figure 2 shows the results of IDC 2009 survey (Gens, 2009). The non-existence of well-developed security standards for the cloud has also been identified by surveys in Subashini and Kavitha (2010) and CSA (2011), as it is hindering the growth of CC. Armbrust et al. (2010) also identify availability of the service or business continuity as the number one obstacle to the growth of CC. According to a number of current surveys, security and interoperability are issues that are detrimental to seamless migration and are emerging as top inhibitors (Gartner, 2012; Oracle, 2013; North Bridge, 2013; Microsoft, 2013; Moyo, 2013). Even though security is often cited as a weakness, Kim et al. (2009) posits that from a technical and practical perspective, data hosted in-house is less secure than cloud data. This is even more so for SMMEs who lack security staff with relevant expertise.

The next top inhibitor has to do with reliability issues. Organizations are worried about downtime due to the non-availability of the cloud infrastructure. CC integration needs seamless system migration that avoids disruptions. The task becomes insurmountable when an organisation needs to migrate multiple systems to the cloud. In a Microsoft (2013) survey conducted in the USA, it emerged that small to medium businesses (SMBs) that have already adopted CC, are more concerned with reliability issues (42%). Data security is the main concern for SMBs yet to adopt CC at 60%, while it comes second to reliability for adopters. Non-cloud users (32%) felt there is a need for industry standards in cloud security, as that might persuade them to consider adoption (Microsoft, 2013). In the context of SMME, service availability depends significantly on the internet infrastructure that is often unreliable, especially in underdeveloped communities where there is bandwidth shortage. (Dörflinger, 2009; Kshetri, 2010). Performance of cloud infrastructure is also a CC challenge, with respondents of IDC survey asking for service level agreements and service level assurances (Gens, 2009). With limited bandwidth, small businesses experience performance degradation during peak times when a large number of users send simultaneous data-intensive requests (Kim et al., 2009). Since SMMEs have legacy ICT infrastructure integration with cloud infrastructure is also a concern. In the context of SMMEs, as much as ICT infrastructure costs are identified as a benefit for CC adoption, cost is still a barrier since bandwidth is still low and expensive in South Africa (Dörflinger, 2009).

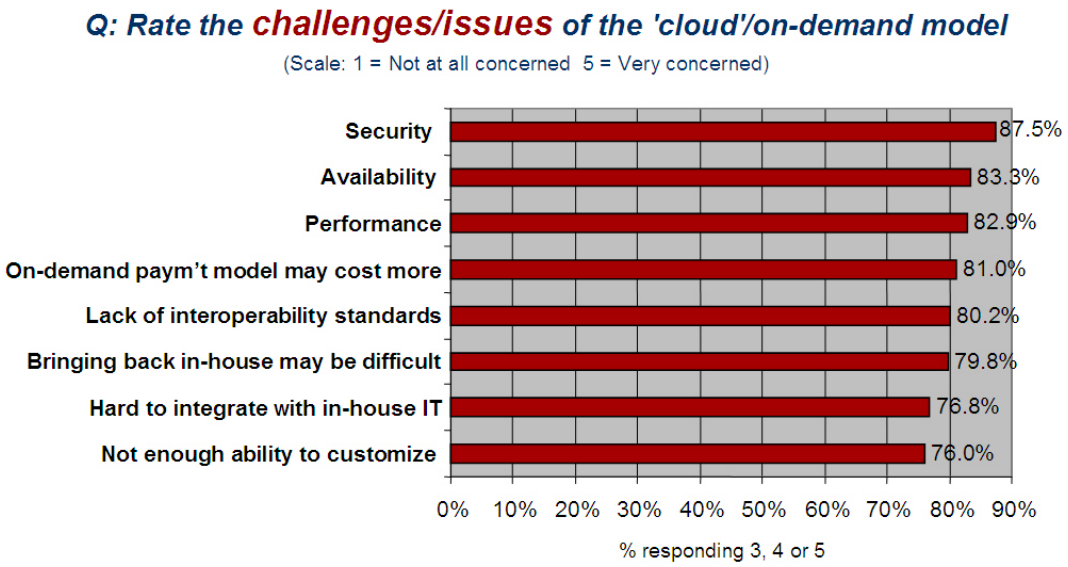


*Figure 2: IDC Cloud Computing Challenges and Issues (Gens, 2009)*

The lack of adoption is more worrying in developing countries – in South Africa, for instance, where the adoption rate is very low. According to Dimension Data, one of the major cloud vendors in South Africa that have gone global, China (36%) is the biggest CC adopter from the BRICSS (Brazil, Russia, India, China, South Africa and South Korea) states, followed by South Korea (29%), India (16%), Brazil (13%) and Russia (4%), with South Africa at a lowly rate of 3% (Moyo, 2013). In South Africa, top inhibitors are security and privacy concerns, together with governance issues such as inadequate, inflexible or non-existent cloud service level agreements (SLAs) and migration complexity (Moyo, 2013). Globally, Patel et al. (2009) also highlight the need for a clear and formal methodology to handle the dynamic nature of CC SLAs.

The South African cloud market is still immature, and vendor transparency is still poor – accompanied with the inability to assess risks and audit the claimed security measures. Dimension Data also noted a lack of service interoperability, as well as poor service migration. These issues expose organizations to insurmountable operational and security risks, in the event of an SLA breach and data loss. Data loss can potentially expose the organization to legal and social risks. It has also been observed that some quality of service (QoS) aspects that are part of the SLA, are difficult to enforce and monitor (Keller & Ludwig, 2003). Changes may be caused by external circumstances, and both parties must be clear on what the other party can deliver. According to Dimension Data, SLAs should include proper security terms, as many cloud vendors claim provision of secure cloud services, but few actually deliver acceptable levels of security. Putting such commitments into SLAs, coupled with choosing reputable vendors, might put organizations at ease. Dimension Data identified a number of SLA considerations for South African organizations adopting CC. Some of them include availability guarantees, the liability the service provider takes for data loss that the service provider can secure and guarantee data retention and backup guarantees, and disaster recovery provisions (Moyo, 2013).

Locally, a recent Oracle (2013) survey has revealed that poor cloud application integration hampers the productivity of more than 50% of businesses. The results for South Africa indicated that 69% of businesses experienced staff downtime, due to poor cloud integration. Half of the survey respondents attributed missed project deadlines or similar problems to poor cloud integration, and 86% indicated that

they considered cloud integration vital to their business. Globally, 54% of survey respondents cited downtime due to cloud integration. The downtime did not only affect cloud adopters, but also those non-adopters doing business with adopters. The 2013 Future of Cloud Computing Survey by North Bridge (2013) in the United States found that security is losing the label as the primary inhibitor to cloud adoption, with 46% listing the management of IT as more complex, reflecting the immaturity of the cloud stack together with vendor lock-in (35%), interoperability (27%) and reliability (22.3%). Additional inhibitors include regulatory compliance (30%) and privacy (26%). The survey also reported that 75% of SMEs are already using cloud services, and that number is expected to grow in 2014.

IDC (2010) and North Bridge (2013) surveys both predict a significant increase in CC spending by 2014. The projected spending on public IT cloud services is expected to increase by 347% from $16 billion in 2009 to $55.5 billion in 2014 (IDC, 2010). Gartner (2012) predicts that the worldwide market for CC will grow by 18.5% in 2013 to $131 billion, and is expected to rise to $158.8 billion by 2014 (North Bridge, 2013). The increase in CC spending suggests that organizations are benefiting from its adoption regardless of some challenges. This indicates that CC is the way forward and organizations are better placed putting in place migration plans.

**PRIVACY AND LEGAL ISSUES IN SOUTH AFRICA**

The South African Constitution (1996), through the Bill of Rights, enshrines that everyone has the right to privacy, be it with some limitations, but it is one of the fundamental human rights. Governments across the globe often have such rights in their respective constitutions. Many have enacted privacy laws that encompass digital privacy and data protection. Unfortunately, South Africa does not yet have privacy and data protection laws; the draft bill is still under discussion (Privacy and Data Protection, 2006). Currently, the Electronic Communications and Transactions (ECT) Act (2002) and the Personal Protection of Information (POPI) Bill (2009) set out the universally accepted data protection principles describing how personal data may be collected and used.

Privacy is identified as top barrier for CC adoption in numerous studies and surveys (Yankee Survey, 2010; CSA, 2010; IDC, 2012). Regulatory responses to these concerns are resulting in increasing complexity with different compliance requirements across industry sectors and legal jurisdictions. These trust and compliance complexity issues are further exacerbated by the nature of businesses operating in the cloud, often characterised by a chain of service provision and trans-border data transfers (Lynn et al., 2013).

IDC (2012) identified legal jurisdiction as the main barrier of CC adoption in the European Union (EU) and IDC recommended harmonising and clarifying personal data protection and privacy protection rules across the EU to protect citizens' rights. At the same time they identified simplifying bureaucratic requirements, regardless of where the data is stored and favouring the identification and removal of local laws and regulation that limit the use of cloud services. Governance issues were also highlighted as barriers to CC adoption in (CSA, 2010). Given this background it is important for governments to define the legal framework that specifically addresses CC issues, so as to allow organizations to adopt CC without holding back due to uncertainties. We believe legal and governmental aspects should form the foundation, with these defined only then can organizations start to address other barriers such as security and availability.

CC is a complex technology that has no boundaries, and governing its operations from the point of view of the government, is a monumental task. The government is needed to put parameters on how organizations can adopt and use certain technology, especially those ventures that yield a potential of bringing in revenue. Organizations need to understand tax and legal implications in implementing CC in

their mainstream operations. Given this background, a sound legal framework is a necessity; otherwise companies will not be in a position to take advantage of new advances in technology to improve their competitive advantage and, ultimately, contribute towards economic growth. These laws include security, privacy and electronic communications. Privacy concerns in CC are largely based on trust issues associated with entrusting third party organizations with sensitive and valuable data that can disrupt core business processes in case of a breach (Bristow et al., 2010).

**The Electronic Communications and Transactions Act, 2002**

South Africa has a range of legislation that governs the digital, electronic and internet fraternity. Among these is the ECT Act that deals with any form of electronic communications. It governs issues such as the facilitation of electronic transactions, e-government services, cryptography and authentication service providers, consumer protection and protection of personal information. The Act outlines the national e-strategy that is mandated to provide for ways of maximising the benefits of electronic transactions to historically disadvantaged persons and communities. Among the ECT's purposes is to promote universal access to electronic communications and transactions and the use of electronic transactions by SMME. In particular, it facilitates the establishment of electronic communications centres and the development of websites for SMMEs. This mandate gives encouragement to the adoption of CC from the government, as the technology can facilitate these initiatives to service those underdeveloped areas.

Consumer protection can also be extended to CC services obtained from cloud vendors. This chapter stipulates, among other issues, the return and refund policies of goods and services acquired through electronic channels. A customer is entitled to cancel a purchasing agreement within seven days, and be awarded a full refund. The 'protection of personal information' chapter governs the collection, collation, processing and disclosure of personal information obtained through electronic channels. Personal information refers to any information that identifies an individual, and collectors must have written permission that allows them to obtain such information. A party controlling personal information may use that personal information to compile profiles for statistical purposes, and may freely trade with such profiles and statistical data as long as the profiles or statistical data cannot be linked to any specific data subject by a third party (ECT Act, 2002).

**Protection of Personal Information Bill (POPI), 2009**

This Bill (POPI) aims to regulate the collection and processing of personal information by both private and public bodies, including the state. POPI redefines personal information as any information relating to an identifiable natural person, such as, race, sex, name, ID number, views and opinions. The Bill sets out eight principles for the processing of personal information – namely, accountability, processing limitation, purpose specification, further processing limitations, information quality, openness, security safeguards and data subject participation. The Bill regulates the transfer of personal information to parties outside South Africa, as it requires personal information to be transferred to a party in a foreign jurisdiction where the information will enjoy similar protection to that afforded in terms of the Bill. This requirement holds serious implications for CC adopters, who sometime do not get necessary guarantees from respective CSPs.

**CLOUD COMPUTING SUPPORT FOR SMME**

Given the above-mentioned barriers to CC adoption, SMMEs need support structures to be in place for them to flourish and realize their potential in a developing economy. In South Africa SMMEs contribute to the economy in terms of revenue, employment and economic growth, even if quantifying such contributions has been unsuccessful since most SMMEs are found in the informal sector, consequently different sources offer varying statistics (Berry et al., 2002; Rogerson, 2004). There are a number of

initiatives to support small businesses (NCR, 2011) but the awareness is very low and most potential beneficiaries are not aware of such programmes (DTI, 2008).

The need for a legal framework that clearly addresses CC complexities security and data privacy protection in the cloud is needed for organizations, regardless of size, to be comfortable in adopting CC. The government is also responsible for providing or facilitating the provision of reliable ICT infrastructure that enable successful CC adoption. The government can facilitate access to affordable high-speed internet through promoting competition in the internet market and attracting potential investor, as well as properly regulating the industry. Currently the price of high-speed internet in South Africa is significantly higher compared to the developed world (Dörflinger, 2009). This can be costly for SMMEs since CC requires transmission of high volumes of data to and from cloud storage servers.

The cloud infrastructure need to allow applications to be ported between different cloud infrastructures as this allows for backup in case of access issues. Interoperability is needed to integrating legacy systems into the new cloud infrastructure (Marston, 2011), since in most cases organizations do not migrate all business processes at once. There is need for cloud and legacy infrastructures to work together during the transitional period. Standardization will increase and accelerate the adoption of CC as users will have a wider range of choices in cloud without vendor lock-in, portability and ability to use the cloud services provided by multiple vendors. (Parameswaran & Chaddha, 2009).

SMMEs need financial support and the government of South Africa have a number of initiatives as part of the small business support strategy that facilitates SMMEs access to low-cost micro-finance loans (DTI, 1995; von Broembsen, 2005; NCR, 2011). CC significantly reduces initial ICT infrastructure setup costs but finance is still needed initially to successfully adopt CC. The South African National Treasury also identified the need to increase support for small businesses and cooperatives in their 2013-17 strategic plan (National Treasury, 2013). Firms expressed concern about accessibility and bureaucracy around SMME support. A low level of awareness and knowledge of government support programmes was disclosed. Interactions between firms and staff running programmes were unsatisfactory. DTI's promotion of programmes was rated as poor or very poor. Programme management in terms of processing time of applications was seen as less than satisfactory (Rogerson, 2008).

**CONCLUSION**

Successful adoption of CC will undoubtedly bring major benefits, especially for developing communities where ICT infrastructure is poor. In South Africa, the majority of the population lives in underdeveloped areas, but the mobile telephone coverage covers almost the whole country. CC, through mobile devices and services, can help in bridging the digital divide. CC adoption is rising globally, but in developing countries the adoption rate is very low. A number of inhibitors have been identified in literature and in a global survey. Among the top inhibitors are security and complexity of integrating the legacy system. In other countries, South Africa in particular, security concerns are largely based on privacy issues and the lack of a government privacy framework that addresses specific CC privacy issues. Currently, the privacy regulations that exist are not tailor-made to address CC, and this is contributing to the low adoption rate. The loss of control over infrastructure, services and data, once cloud models are adopted, is the key risk causing local business to take a guarded approached to cloud.

Cloud providers need to guarantee some service level assurances with regard to security and availability in SLAs, for organizations to be more comfortable in service consumption. Another area of concern is the disruptions caused by failure of cloud migration. Small businesses need to take the security issues in CC seriously, 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.

The government need to play a significant role in setting up the basic infrastructure and an environment conducive for smooth operation for cloud providers and users. This includes defining the legal framework for protecting personal and sensitive information that will be stored on third party servers. The framework also needs to define penalties for violation of security and privacy laws in the cloud. Ultimately, CC adopters needed to plan and prepare before migrating to the cloud as the cost of unplanned migration might significantly outweigh the perceived benefits, due to lost productivity due to downtime and more importantly, a damaged corporate brand.

**REFERENCES**


Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., …& Zaharia, M. (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 November 12, 2013, from the Virtual Strategy Magazine website: http://www.virtual-strategy.com/2011/02/28/transformative-benefits-driving-companies-cloud-computing?page=0,0.

Berry, A., von Blottnitz, M., Cassim, R., Kesper, A., Rajaratnam, B. & Van Seventer, D. E. (2002). The Economics of SMMEs in South Africa. Johannesburg: Trade and Industrial Policy Strategies.

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, 25*(6), 599-616.

CSA. (2011). Cloud Security Alliance SecaaS defined Categories of Service 2011. Unpublished manuscript. Retrieved November 12, 2013, from the Cloud Security Alliance website: https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf.

Desai, A. M. & Mock, K. (2012). Security in Cloud Computing. In *Cloud Computing Service and Deployment Models: Layers and Management*, 208.

Dörflinger, J., Friedland, C., Merz, C. & de Louw, R. (2009). Requirements of a mobile procurement framework for rural South Africa. In *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems,* 3. ACM.

DTI. (1995). The White Paper on National Strategy for the Development and Promotion of Small Business in South Africa. Retrieved November 12, 2013, from the Department of Trade and Industry website: http://www.dti.gov.za/sme_development/docs/White_paper.pdf.

DTI. (2008). An Annual Review of Small Business in South Africa, (2005-2007). DTI, South Africa.

ECT Act. (2002). Electronic Communications and Transactions Act. Retrieved November 12, 2013, from the South African Government Information website: http://www.info.gov.za/view/DownloadFileAction?id=68060.

Farelo, M. & Morris, C. (2006). The status of e-Government in South Africa. Retrieved November 12, 2013, from http//www.researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf.

Gartner. (2012). Gartner's 2012 Hype Cycle for Emerging Technologies. Retrieved November 12, 2013, from Gartner website: http://www.gartner.com/newsroom/id/2124315.

Gens, F. (2008). IT Cloud Services User Survey, Part 2: Top Benefits & Challenges, IDC eXchange. Retrieved November 12, 2013, from http://blogs.idc.com/ie/?p=210.

Gens, F. (2009). New IDC IT Cloud Services Survey: Top Benefits and Challenges, IDC eXchange. Retrieved November 12, 2013, from http://blogs.idc.com/ie/?p=730.

IDC. (2010). Through 2014 Public IT Cloud Services Will Grow at More Than Five Times the Rate of Traditional IT Products, New IDC Research Finds. Retrieved November 12, 2013, from http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22393210.

IDC. (2012). Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake, *IDC*.

Kauffmann, C. (2009). Engaging the private sector in African infrastructure. Unpublished manuscript. Retrieved November 12, 2013, from the Organization for Economic Co-operation and Development (OECD) website: 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.

Kim, W., Kim, S. D., Lee, E. & Lee, S. (2009). Adoption Issues for Cloud Computing. In *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*, ACM Press, 2-5.

Kshetri, N. (2010). Cloud Computing in Developing Economies: Drivers, Effects, and Policy Measures. In *Proceedings of 32nd Annual Pacific Telecommunications Conference 2010,* 17-20 January, Honolulu, Hawaii, USA.

Lynn, T., Healy, P., McClatchey, R., Morrison, J., Pahl, C. & Lee, B. (2013). The Case for Cloud Service Trustmarks and Assurance-as-a-Service. Retrieved November 12, 2013, from doras.dcu.ie/18357.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. (2011). Cloud Computing—The Business Perspective. *Decision Support Systems*, *51*(1), 176-189.

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

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing, National Institute of Standards and Technology. *NIST Special Publication*, 800-145.

Microsoft. (2013). Small and Midsize Businesses Cloud Trust Study: U.S. Study Results. Retrieved November 12, 2013, from Microsoft website: http://www.microsoft.com/en-us/news/download/presskits/security/docs/TwCJune13US.pdf.

Moyo, A. (2013). *SA cloud adoption behind BRICSS*. Retrieved November 12, 2013, from ITWeb website: http://www.itweb.co.za/index.php?option=com_content&view=article&id=65786.

Mujinga, M. (2012). Developing Economies and Cloud Security: A Study of Africa. *Journal of Emerging Trends in Computing and Information Sciences*, *3*(8), 1166-1172.

National Treasury. (2013). Strategic Plan 2013/2017. Retrieved November 12, 2013, from http://www.treasury.gov.za/publications/strategic%20plan/Strat%20Plan%202013-2017.PDF.

NCR. (2011). Literature Review on Small and Medium Enterprises' Access to Credit and Support in South Africa, National Credit Regulator. Retrieved November 12, 2013, from http://www.ncr.org.za/Literature Review on SME Access to Credit in South Africa_Final Report_NCR_Dec 2011.pdf

North Bridge. (2013). Future of Cloud Computing Survey 2013. Retrieved November 12, 2013, from North Bridge website: http://www.northbridge.com/2013-cloud-computing-survey.

NSB Act. (1996). Department of Trade and Industry. National Small Business Act, Pretoria, 27 Nov 1996. Retrieved November 12, 2013, from http://www.dti.gov.za/sme_development/docs/act.pdf

Oracle. (2013). Cloud for Business Managers: the Good, the Bad, and the Ugly. Retrieved November 12, 2013, from Oracle website: http://www.oracle.com/us/corporate/press/1946764.

Parameswaran, A. V. & Chaddha, A. (2009). Cloud Interoperability and Standardization. *SETLabs Briefings*, 7(7), 19-26.

Patel, P., Ranabahu, A. & Sheth, A. (2009). Service Level Agreement in Cloud Computing. Fairborn, OH: Wright State University, Kno.e.sis Center. (OOPSLA Cloud Workshop).

POPI Bill. (2009). Protection of Personal Information Bill. Retrieved November 12, 2013, from the South African Department of Justice website: http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf.

Privacy and Data Protection. (2006). Retrieved November 12, 2013, from the South African Department of Justice website: http://www.justice.gov.za/salrc/dpapers/dp109.pdf.

Rogerson, C. M. (2004): The Impact of the South African Government's SMME Programmes: A Ten-Year Review (1994-2003), Development Southern Africa, *21*(5), 765-784.

Rogerson, C. M. (2008). Tracking SMME development in South Africa: issues of finance, training and the regulatory environment. In *Urban Forum*, Springer Netherlands, *19*(1), 61-81.

South African Constitution. (1996). Bill of Rights. Retrieved November 12, 2013, from the South African Department of Justice website: http://www.justice.gov.za/legislation/constitution/bill-of-rights.html.

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.

von Broembsen, M., Wood, E. & Herrington, M. (2005). Global entrepreneurship monitor: South African report 2005. *The UCT Centre for Innovation and Entrepreneurship*.

Winkler, V. J. R. (2011). Securing the cloud: Cloud computer security techniques and tactics. *Waltham, MA: Syngress*.

Yankee Survey. (2010). The Anywhere Enterprise: 2010 U.S. Cloud Computing FastView Survey. Retrieved November 12, 2013, from Yankee Group website: http://www.yankeegroup.com/about_us/press_releases/2010-08-23.html.