A Study into Privacy and Legal Issues in Cloud Computing: The Mozambican Context

Ambrósio Patricio Vumo
Universidade Pedagogica, Maputo, Mozambique
Technische Universität Dresden, Department of Computer Science, Germany

ambrosio_patricio.vumo@mailbox.tu-dresden.de

Abstract: During the last 10 years, Cloud computing has become an evolving technology providing several benefits such as cost reduction and high flexibility. However, one of the main challenges related to cloud computing is related to data security and privacy. Despite this, worldwide many countries, specially developed countries have adopted cloud computing technology. In Africa, specifically in the Southern African Development Community (SADC), Mozambique is one the countries who has recently adopted cloud computing technology. However, on the contrary to countries such as Mauritius and South Africa, Mozambique still does not have a national strategy for cloud computing in place, including security and privacy issues. International organizations such as ENISA and NIST as well as ITU have published frameworks related to cloud computing adoption covering data security and privacy issues. Therefore, in this paper we first analyze the cloud computing frameworks published by these international organizations. In addition, the paper also analyses the adoption of cloud computing in developed and developing countries, such as USA, UK, Germany, Mauritius and South Africa. From these analyses, the paper presents some recommendations for Mozambique to adopt best practices and follow international frameworks related to cloud computing including data security and privacy.

Keywords: Cloud computing, Data protection, PRIVACY, LAws, Mozambique

1. Introduction

Cloud computing and the emergence of a cloud economy based upon it is becoming increasingly important considerations for governments and enterprises (UN, 2013). A recent study has described cloud technology as one of the most significant disruptive technologies which will develop over the next two decades, with major implications for markets, economies and societies. It predicts that, by 2025, most information technology - IT and web applications and services could be cloud delivered or cloud enabled, and that most enterprises might be using cloud facilities and services. In simple terms, cloud computing enables users, through the Internet or another digital network, to access a scalable and elastic pool of applications, data storage and computing resources (Nelson Fonseca, 2015). Despite of the numerous benefits that cloud computing promises, its adoptions face numerous challenges such as (ITU, 2012): i) data security, the trust, reliability and dependency in moving data and applications to a remote third party; ii) availability of connectivity and sufficient bandwidth; iii) legal and regulatory uncertainty; and iv) in additional in developing countries there are varying challenges in their socio-economic and political development leading to low investments in advanced technologies for government, academic, industry and private. Many African countries have seen development and integration with the global economy limited due to lack of high performing technological infrastructures. Cloud computing has emerged as a new computing paradigm that will revolutionize the way we buy and use computing equipment and services in many countries of the African continent (UN, 2013). While it is always difficult, even risky, to predict the development of IT so far ahead, policy makers and business leaders should start examining the opportunities and potential risks of this growing phenomenon. The Internet infrastructure and connectivity today are providing a ubiquitous access to shared applications, software and hardware across the globe allowing users to quickly and easily get information whenever and wherever they might be. Cloud computing is taking this ubiquitous access to another level be providing users with access not just to information available on the Internet but also to their business applications and network wherever there is Internet connectivity using any compatible device such as a personal computer, laptop, tablet or smartphone. Users can have access to programs, storage, applications, processing and software development environments that are provided through cloud computing. The best of our knowledge there are no articles or research works on data security and privacy protection in cloud computing environment in Mozambique.

2. Theoretical Background

2.1 Cloud Computing Definition and Models

The National Institute of Standards and Technologies (NIST) of the United States of America, the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) together with the

International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) are widely used to define Cloud computing where both definitions establish the fundamental nature of the concept such as "self-services" and "on-demand" through "access network":

- **NIST (**NIST, 2019), defines cloud computing as a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resource such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction;
- **ISO/IEC together with ITU-T** (ITU, 2014), define cloud computing as a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on demand service provisioning and administration.

According to (NIST, 2019) (ITU, 2014), there are three classic or three well-known cloud service models in the cloud computing paradigm, namely: i) Software as a Service -SaaS; ii) Platform as a Service - PaaS; and iii) Infrastructure as a Service - SaaS and four deployment models, namely: i) private cloud; ii) public cloud; iii) Community cloud; and iv) hybrid cloud.

2.2 Contributions and Opportunities of Cloud Computing

According to Varnika (Varnika, 2018), the on-going adoption of cloud computing services and potential for the future will have significant impacts on wide-ranging aspects of developing economies. Varnika stated that the cloud computing in the developing world is in its infant stage and is an attractive proposition to organizations due to the benefits that come with adopting it, they include (Varnika, 2018):

- **Enterprises Applications**: Utilizing the cloud significantly reduces the barriers to entry for entrepreneurs in the developing world by providing customized and scalable computing, storage, and development solutions without the need for significant capital outlays. Developing businesses can purchase only what they need at the time while being able to accurately forecast future costs in the face of growth. Similarly, developers and software engineers in these regions benefit from access to the same computing power availability as those they are competing with in the West, allowing them to produce applications and services that are better tailored to their local and regional market due to their increased understanding of the cultural and economic needs of the area.
- **Health Applications:** Cloud technologies are able to match patients with medical providers in ways that were previously impossible at the turn of the millennium. In areas that are often underserved by qualified medical facilities and providers, the future potential of the cloud to jump start the implementation of telemedicine is enormous. Effective telemedicine would allow providers to access remote patients, track disease outbreaks, and reduce the burden on physical hospital resources by prioritizing care.
- **Government Applications:** The most striking example of the benefits of cloud technology is the reduction in infrastructure required, including electrical, computing, storage requirements. Similar to applications in healthcare record management, the utilization of cloud computing and storage could greatly expand the quality, reliability, and affordability of government services. This would also greatly improve the redundancy of record keeping in areas prone to conflict, reducing the time required to return to normalcy following fighting.

2.3 Defining Security, Privacy, Trust and Personal Data

Nayak (Nayak, 2012) within his research entitled understanding the security, privacy and trust challenges of cloud computing has defined security, privacy and trust as following:

- Privacy concerns the expression of or adherence to various legal and non legal norms regarding the right to private life. In the European context this is often understood as compliance with European data protection regulations. Although it would be highly complex to map cloud issues onto the full panoply of privacy and personal data protection regulatory architectures, the globally accepted privacy principles give a useful frame: consent, purpose restriction, legitimacy, transparency, data security and data subject participation (Nayak, 2012).

- Trust revolves around assurance and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine, human to machine or machine to human. At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives (Nayak, 2012).
- Security concerns the confidentiality, availability and integrity of data or information. In accordance with this author, security may also include authentication and non-repudiation (Nayak, 2012).
- Personal Data is defined as information of any kind referred to identified and/or identifiable individuals and/or entities. It is a very broad definition which encompasses almost any sort of information linked to a subject. In turn, data treatment is also widely defined as the systematic operations or procedures, by electronic means or others, allowing storage, conservations, modifications, relationship, evaluation, lock, destruction and in general data processing of personal data, as well as assignment to third parties through communications, interconnections or transfer (Lisandro Frene, 2019).

2.4 Challenges of Data protection to address new technologies

According to (UN, 2013), Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. The relationship between data protection and ICT developments changes all the time and can be demonstrated by three recent developments: i) Cloud computing; ii) the Internet of Things; and iii) Big Data analytics. Each of these technologies presents new challenges to data protection, particularly in the areas of the definition of personal data and the management of cross-border data transfers.

3. Privacy and Legal Issues in Cloud Computing

3.1 Privacy Issues in Cloud Computing

According to (Benameur, 2011) (Dlodlo, 2011), privacy is a fundamental right enshrined in the UN Universal Declaration of Human Rights. There are various forms of privacy, including the right to left alone and control of information about ourselves. There are different types of information that need to be protected. These include any information that can be used to identify or locate an individual such as Name, address, credit card number and IP address. Sensitive information such as personal financial information and job performance information is considered private. Behavioral information such as viewing habits for digital content, users recently visited websites or product usage history need to be protected as well. According to Siani and Azzedine (Benameur, 2011) in the commercial, consumer context, privacy entails the protection and appropriate use of the personal information of customers, and the meeting of expectations of customers about its use. For organizations, privacy entails the application of laws, policies, standards and processes by which Personally Identifiable Information (PII) of individuals is managed. According to (SG, 2019) data privacy is one of the most important components which individuals/business organizations take into consideration before hiring the services of any third-party cloud computing service provider. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure. Privacy and confidentiality are regarded as the major problems in cloud computing. Individuals to a large extent do not have any problem in sharing their information with the cloud service provider, but when it comes to business organizations, they are very anxious about sharing proprietary data. There are certain categories of businesses that are by specific laws prohibited from sharing certain data. For instance, for a healthcare company in the United States, the Health Insurance Portability and Accountability Act (HIPAA) lays down certain restrictions in relation to the sharing of medical records of individuals. In cloud computing environment, services can be aggregated and changed dynamically by customers and service providers can change the provisioning of services anytime. Nomusa (Dlodlo, 2011) has stated that violation of privacy occurs as a result of a number of cloud computing dynamics. In the cloud computing the infrastructure is shared between organizations and is off-premise. Therefore, there are threats associated with data being stored remotely and because of virtualization. Virtualization is a method of running multiple independent virtual systems on a less physical resource making on computer act as many, and sharing the resources of hosts across multiple environments. Sensitive data may move around within an organization and across organizational boundaries. Thus, Legal compliance and adequate protection has be maintained therefore.

3.2 Legislative and Regulatory Issues in Cloud Computing

Nomusa (Dlodlo, 2011) stated that in cloud computing there are a number of issues that need to be regulated. Potential physical location of data centers could be anywhere, with geography-blind distribution of applications and data. As a practical commercial matter, national regulations should be able to influence the actual deployment of cloud computing services in countries around the globe. SG (SG, 2019) also stated that Legislative and regulations is another aspect of cloud computing which is largely uncertain as cloud computing is an unregulated field with a mixture of legislation and regulations present in limited countries. The problem arises when the jurisdiction where the customer resides requires a certain standard for the data which may not be required by the jurisdiction where the data centre is located. For instance, the customer's country might have certain data privacy, data retention and data access enforcement laws, but these might not be the same as the laws of the service provider's country, and the laws might conflict with each other. For instance (Dlodlo, 2011), in the US and Europe the regulations require some cloud computing offerings to allow users to stipulate the country in which their data will be stored. Non-US firms whose servers are located in the US can have their information accessed by the US government under the US Patriot Act and Homeland Security Act. This impact on information privacy policy.

3.3 Data Location, Law and Jurisdiction Issues in Cloud Computing

According to (sg, 2019), in cloud computing environment the location of data is usually uncertain. Customers at times are unaware as to the region where the cloud infrastructure is located. The data stored or processed by any individual or business organization travels over the internet network to various data centers located in multiple locations of the world. This gives rise to various legal issues as the cloud infrastructure is located elsewhere, not in the country where the customers reside, and different countries have different laws pertaining to data storage/transfer. Thus, it is the contract of service that determines the applicable law and the courts who should decide matters in the case of disputes. With cloud computing, the applicable laws governing your data could include the laws where your organization is headquartered, where your cloud provider is headquartered, where your cloud provider's data centers are located, where the subjects of the data reside, and potentially the laws of the countries that your data pass through on their way to, from and among the cloud provider's data centers. For these reasons it is essential for a cloud computing contract to identify the geographic region within which the data centers hosting your data, and potentially the headquarters of the cloud provider, may be located, and to specify the cloud provider's obligations to keep your data in those regions. Otherwise, the overlaps and potential conflicts between the possible governing laws could make legal and data access compliance impossible. According to [UN], Data protection regulation is high on the political agenda as evidenced by a number of current developments:

- The United Nations in 2015 appointed a Special Rapporteur on the right to privacy.
- The African Union in 2014 has developed the African Union Convention on Cyber security and Personal Data Protection.
- A new General Data Protection Regulation has replaced the European Directive on Data Protection, which has been a prominent source of regulation for twenty years.
- Data protection has been included in several international trade agreements.
- Data protection regulation has been considered in several high-profile court cases in relation to national surveillance.
- Numerous countries are drafting new data protection laws or are reviewing existing ones.
- The European Union and the United Stated have re-negotiated a long-standing cross-border data protection agreement.
- Several global and regional organizations have issued (or are developing) multiparty agreements and /or guidelines on data protection.

4. Privacy and Legal Issues in Mozambique

According to Dla Piper (2024), in Mozambique there is no specific legislation on data protection or privacy. Vumo et al (2019) stated that the Constitution of the Republic of Mozambique outlines some aspects related to protection of personal data. For instance, pursuant to Article 41 of the constitution of republic of Mozambique

states that all individuals are entitled to intimacy of their private life (Joao Luis Traca, 2016). Further, Article 71 of the Constitution grants all individuals the right to privacy, prohibiting the use of electronic means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives (Joao Luis Traca, 2016). Moreover, Data Protection is referred on the Electronic Transaction Law approved in 2017. But it provides only some degree of personal data protection and privacy. Still today, Mozambique does not have a full regime for data protection and privacy (UN, 2013). However, there are other sources of law that impose some privacy obligations such as: i) The Civil Code (Decree-Law no. 47344, of November 25, 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967); ii) The Penal Code (Law no. 24/2019, of December 24, as amended by Law no. 17/2020 of 23 December); iii) The Labour Law (Law no. 23/2007, of August 1) and the new Labour Law (Law no. 13/2023, of 25 August) which has entered into force on 22 February 2023; iv) The Regulations on Registration and Licensing of Intermediary Electronic Service Providers and Operators of Digital Platforms (Decree no. 59/2023, of 27 October) Dla Pipel (2024).

Despite the Constitution of the Republic of Mozambique outlines aspects related to data protection and privacy, Mozambique is among the least committed countries in cybersecurity within five designated areas, namely (ITU, ITU, 2019): i) legal; ii) technical; iii) organizational; iv) capacity building; and v) cooperation. In this context, Mozambique could be viewed as a permissive environment for cyber criminals due to a lack of security capabilities, absence of specific legislation on data protection and privacy and other cyber related legislations. Currently several governmental and non-governmental organizations have been discussing data protection and cyber security issues but there is a lack of coordination between these organizations and concrete actions are missing. Thus, due to the dynamic nature of cyberspace, there is a need for these actions to be unified under national level with an integrated vision and a set of sustained and coordinated strategies for their implementation. Despite this cloud computing is reality in Mozambique. However, the absence of relevant laws and regulations to regulate this environment for data storage, conservations, modifications, lock-in, destruction and in general data processing of personal data, as well as assignment to third parties through communications, interconnections or transfer could pose risks and lack of trust to cloud consumers.

5. Addressing Privacy and Legal Issues in Mozambique

5.1 National Considerations

As previously presented issues related to privacy, trust and legal issues in cloud computing and based in theoretical evidence, we present some initial steps that help address these concerns. We proposed that, the government of Mozambique should:

- **Develop Laws:** Jacques Rousseau (2012) explained in the social contract, or principles of political right, the rules that the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called laws. Laws are rules mandate or prohibit certain behavior; they are drawn from ethics, which define socially acceptable behaviors. In Cloud computing environment, laws are needed to governing the issues related to data protection and privacy. This can be addressed mainly by the geographical location of the stakeholders involved, and the rights and obligations of each stakeholder are determined by applicable regulations. In this context, it is very important to develop specific Personal Data Protection Law.
- **Include the core principles of Data protection:** According to (UN, 2013), recommend for countries that do not yet have laws in place, or countries that are updating or reforming their laws, should look to include the core principles in their new/amended legislation as following: i) openness, organization must be open about personal data practices; ii) collection limitation, collection of personal data must be limited, lawful and fair; iii) purpose specification, purpose of collection and disclosure must be specified; iv) use limitation, use of data must be limited to specific purposes; v) security, personal data must be subject to appropriate safeguards; vi) data quality, personal data must be relevant, accurate and up-to-date; vii) access and correction, people must be able to access and correct their personal data; and viii) Accountability, data controllers must comply with the data protection principles. Accountability in the cloud is a very important concept that needs to be supported from both a legal and technical viewpoint. The way to achieve accountability in such a dynamic and worldwide infrastructure is to have a strong emphasis on auditing. Audit should be able to keep track of where the data has been outsourced, who processed it and for what purpose.

- **Establish Data Protection Authority:** The data Protection Authority is an independent supervisory authority ensuring that privacy is protected when personal data are processed. Ensuring that a cloud deployment meets the requirements imposed by the applicable laws, regulations and contractual obligations, the National Data Protection Authority must take responsibility for ensuring compliance with the data protection principles as recommended by AU (2020).

5.2 International Considerations

According to (UN, 2013), Cloud computing services do not present unique issues in data protection, but they do add to the complexity of existing issues, especially in relation to cross-border data transfers. To date, few jurisdictions have attempted to draft regulations expressly designed to regulate the provision of cloud computing services. This probably reflects both the broad range of services that fall within the concept of cloud computing, as well as the flexibility of scope within existing regulatory concepts. In this context, we proposed that, the government of Mozambique should:

- **Regulate international data transfers:** States and businesses often have a legitimate need to share data across national borders for economic and logistical purposes. This must be balanced with the protection of privacy and data security of the data of their citizens. It is important for frameworks to consider how to institute accountability mechanisms to ensure that those processing and using the data are accountable (UNDP, 2023). Thus, Data protection law must expressly regulate international data transfers, allowing it if the requirements set forth by law for such purpose is met. Requirements vary, essentially according to the purpose of the data transfer; and to the country where data is exported. GA Solanki (Solanki, 2012) also stated that the traditional rules of private international law, the jurisdiction of a nation only extend to individuals who are within the country or to the transactions and events that occur within the natural borders of the nation. However, this traditional rule pertaining to jurisdiction has become less effective with the advancement of commerce and technology. In cases of cloud transactions, it may happen that a company which is resident of one country may stored data on a cloud which is located in altogether different country and such cloud may belong to a vendor who is located in a third country. In such cases there are ample chances that the laws of third jurisdictions are applicable. Therefore, various factors would need to be considered while determining an appropriate jurisdiction along with the harmonization of domestic laws of each applicable country to avoid conflict of laws. We also propose the Government of Mozambique to keep cloud data compliant with global regulations (GDPR, CCPA, HIPAA, PCI DSS and FISMA) and internal policies as stated by (Sentra, 2024).

6. Conclusion

Despite the fact that cloud computing provides several services to individuals and organizations alike, there are also many problems that need to be addressed and one of them is related to the way how information is managed. As discussed in Section 4 data security and privacy protection is the main concern in cloud computing environment. This is due to the characteristics of the cloud infrastructure because cloud computing services are often owned by a third party. Moreover, without knowledge of the physical location of the servers by users, user's data in the cloud computing environment are easier to manipulated leading to the loss of control. In this paper, we have examined the challenges of data protection and privacy in cloud computing. The study was based from the following sources, UA, NIST, UN, ITU and UNDP, just to enumerate a few. The findings from this study show that despite some efforts, data protection and privacy, especial in cloud computing is still a challenging process in Mozambique. To date, there are no data protection authority and specific legislation on data protection or privacy. Therefore, the paper made some recommendations for the government of Mozambique in order to change the current situations as described on section 5. However, we believe that more efforts should be done by the Mozambican government to provide trusted, safe and protected cloud computing environment to its citizens and the society in general.

References

Ambrosio, Vumo and Josef, Spillner. (2019). A Data Security Framework for Cloud Computing Adoption: Mozambican Government Cloud Computing. *18th European Conference on Cyber Warfare and Security*, ACPI, pp. 720.

AU, (2020) "African Union Convention on Cyber Security and Personal Data Protection", [online], African Union, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Siani, Pearson and Azzedine, Benameur. (2011). "Privacy, Security and Trust Issues Arising from Cloud Computing", *International Conference on Cloud Computing Technology and Science*, IEEE.

Dla Pipel, (2024) "Data Protection Laws of the World: Mozambique", [online], Dla Piper, https://www.dlapiperdataprotection.com/.

Dlodlo, N. (2011). "Legal, privacy, Security, Access and Regulatory Issues in Cloud Computing", *Interntional Conference on Information Management and Evaluation*.

ITU, (2014) "Information technology - Cloud computing - Overview and vocabulary", [online] https://www.itu.int/rec/T-REC-Y.3500201408-I

ITU. (2012). *Demystifying Relation in the Cloud: Opportunities and Challenges for Cloud Computing.*

ITU. (2024), "Global Cybersecurity Index 2020", [online], ITU, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Joao, Luis Traca and Lidia, Neves. (2016). "Data Protection in Mozambique: Inception Phase. *African Data Privacy Laws, Law, Governance and Technology"*, Spring International Publishing, pp. 363-367.

Lisandro, Frene and Juan, Cardinal (2019). *Data Protection and CyberSecurity.* Chambers: Global Practice Guide.

Michael, E. Whiteman and Herbert, J. Mattord. (2012). *Principles of Information Security.* Course Technology, Ed. 4, Boston.

Debabrada, Nayak. (2012), "Understanding the Security, Privacy and Trust Challenges of Cloud Computing". *Journal of Cyber Security and Mobility*, Vol.1, pp. 277-288.

Nelson, Fonseca and Raouf, Boutaba. (2015). "*Cloud Service, Networking, and Management*", New Jersy: John Wiley & Sons.

NIST. (2019). "*The NIST definition of Cloud Computing" [online]*, NIST, https://www.nist.gov/publications/nist-definition-cloud-computing.

Sentra. (2024) "Cloud Data Security: Challenges and Best Practices" [online], Sentra, https://www.sentra.io/cloud-data-security.

SG. (2019). *"*Data Privacy is one of the most Important Components*"* [online], SG, https://sg.inflibnet.ac.in/bitstream/10603/98806/14/14_chapter7.pdf.

Solanki, G. (2012). "Welcome to the Future of Computing: Cloud Computing and Legal Issues". *InternationalJournal of Scientific and Technology Research*, Vol. 1, pp. 30-33.

UN. (2013). *Information Economy Report 2013: The Economy and Developing Countries.*

UNDP. (2023), "Legal identity and data protection in modern societies", [online], UNDP, https://www.undp.org/blog/legal-identity-and-data-protection-modern-societies

Varnika, V. (2018). "Cloud Computing Advantages and Challenges for Developing Nations". *Interntional Journal of Scientific Research in Computer Science and Engineering*, ISE, Vol.6, pp. 51-55.