IST-Africa 2024 Conference Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
IST-Africa Institute and IIMC, 2024
ISBN: 978-1-905824-72-4

South Africa's Cloud and Data Storage Readiness - A Policy Review

Phumelela MJOLI[1], J.H.P ELOFF[1], M.T. DLAMINI[2]
[1]*Department of Computer Science, University of Pretoria, Hatfield, 0002, South Africa*
Tel: +27 012 420 4111, Email: Phumi.Mjoli@tuks.co.za
[2]*Council for Scientific and Industrial Research (CSIR), Defense & Security, Information and Cyber Security Centre, Pretoria, South Africa*

Abstract: The South African government continuously strives to work on the development of legislations that protect the confidentiality, integrity, and availability of its citizen's information in the digital space. The contagion of the Coronavirus (COVID-19) led to a global lockdown that put governments in emergency mode. Post-COVID-19, the benefits of digitization became more noticeable. During the lockdown era cloud computing proved its effectiveness and efficiency in helping employees continue working even outside of their workstations. The objective of this paper is to scrutinize the current state of cloud data protection in the public sector within South Africa. The emphasis is placed on the draft National policy for cloud and data storage. This paper also makes recommendations to further strengthen and improve the current state of South Africa's cloud and data storage. It goes further to review existing legislations such as POPI, ECT, and cyber law acts and their relevance to the draft National Data and Cloud Policy. A proposal for a model that incorporates the cloud-shared responsibility model is presented and briefly discussed.

Keywords: Cloud Computing, POPI Act, ECT Act, Data Protection, Draft National Policy

1. Introduction – Why cloud computing?

Cloud computing is defined as a model that enables ubiquitous, convenient, and on-demand access to a set of shared and virtualized computing resources, e.g., networks, servers, storage, applications, and services, which can be quickly provisioned without great management effort, with minimum complexity, and at a low cost [1]. This is the most widely accepted definition of cloud computing in literature [2] [3] [4] & [5]. Therefore, this paper also adopts it. As defined in the NIST publication, cloud computing offers three foundational services. These include software as a service (Saas), platform as a service (Paas), and infrastructure as a service (Iaas) [1]. Saas pertains to hosting applications and making them accessible through internet use. Paas is concerned with the hosted platform for developing, running, maintaining, and managing applications. Iaas refers to virtualized infrastructure such as virtual machines, virtual storage and virtual networks that are provisioned as a service for customers on a pay-as-you go. It must be noted though, that there are now more cloud services such as serverless computing, and data analytics as a service, which is a model that is also referred to as function as a server (Faas) [6]. No matter what form they may come, these cloud services are all provisioned in a manner that allows scalability, high availability, and improved resilience. These are some of the features that make cloud computing services attractive to organizations.

An interesting point to note in the context of South Africa, unlike other countries is that the adoption of cloud computing services is currently higher within the private sector than it is in the public sector [7]. Even post-COVID-19, the South African public sector is still

reliant on on-premises information system infrastructure to process public workloads and store state information that it processes for the citizens. Despite the lockdowns of the pandemic playing a vital role in forcing most organizations to re-think their working models, it somehow did not resonate with the public sector in South Africa. The lockdowns forced organizations to find strategies that would enable their employees to effectively work even when they were not at their workstations. Cloud computing was one of the strategies employed by most organizations in the private sector as a coping mechanism. It became a good tool to help employees efficiently accomplish their tasks from anywhere besides their normal workstation [8].

This new model has proven to work effectively in most organizations in the private sector. As much as most organizations in the private sector have moved their workloads into the cloud space, the security thereof remained a critical concern. Most organization in the private sector currently relies on internal controls to assess and determine if their cloud-hosted workloads and data are secure within the cloud space. The authors of the current paper argue that, this is neither a credible nor sustainable way to prove that cloud-hosted workloads and data are secure in the cloud. Therefore, there is a need to add extra security assurance for cloud-hosted workloads. This may start from a legal and regulatory compliance perspective. For example, section 2 of the POPI Act regulates and legislates on cross-border information flows. This section mandates that no public data can be transferred to foreign countries where there are no security measures and protections in place [9]. This is a tough requirement to achieve in the cloud where workloads may be spread across multiple jurisdictions at a time. This may be the reason why the South African public sector still relies strongly on its government's policies, regulations, and legislation to not put its data in the cloud [10].

2. Objectives

This study aims to provide a critical literature review of the latest advancements in South Africa concerning policies and regulations that are meant to protect data in the cloud space. Therefore, this paper seeks to:

- Study the current state of cloud computing policies and regulations in South Africa.
- Investigate how existing legislations like the Protection of Personal Information (POPI) Act, Cybercrime Act together with the Electronic Communication Transfer (ECT) Act can aid in the protection of data in the cloud environment.
- Review the appropriateness of the Draft National Policy on Cloud and Data Protection to mandate and ensure safe and secure cloud services.

3. The Current State of Cloud Computing

When looking at the current state of securing cloud-hosted workloads in South Africa, it is vital that we holistically review current policies that are in place for data protection in South Africa. Raaf et al. [11] studied the alignment of South Africa's cloud policy and the POPI Act looks at issues such as availability, regulation, legislation, security, localization, and confidentiality of data in the cloud. Interestingly, Raaf et al. [11] compare the POPI Act to the Draft policy for cloud computing. The Draft Policy seeks to create an environment that enables the provisioning of data cloud services intending to move towards a data-driven South Africa for all while ensuring social and economic development [12]. The National Draft Policy on Data and Cloud Computing was released by the government on the 1st of April 2021 for public commentary and review [13]

3.1 Understanding The Draft National Policy on Cloud and Data Protection, POPI Act, and ECT Act for Cloud Computing Readiness in SA

In the same breath of data protection, on the 26th of November 2013, the Protection of Personal Information (POPI) Act originated [14] and came into force on the 1st of July 2021. The POPI Act together with the ECT Act [15] have played a very vital role in protecting and placing measures that reassure South Africans that the new technology adoption can be a safe environment. The POPI Act together with the ECT Act has been adopted not only by the government but also by the private sector and South Africa's citizens have taken an interest in understanding these acts and abiding by them.

Furthermore, any person who violates these acts will be prosecuted and dealt with accordingly. However, more innovations are being implemented in the technology space, new applications are being developed, and more and more people are using the applications. As cloud computing has become the new era of innovation a digital government in SA has also begun, there is now a need to revisit the existing laws of communication, data storage, and security. Currently, no law in South Africa speaks to data security in the cloud. However, On the 1st of April 2021, the South African government published the 'National Data and Cloud Policy' in terms of the ECT Act for comment [11].

The purpose of the National Data and Cloud Policy is the "alignment of existing policies, legislation and regulations" and to "enable South Africans to realize the socio-economic value of data" [11]. The objectives of the Policy are to:

- Promote connectivity and access to data and cloud services.
- Remove regulatory barriers and enable competition.
- Ensure implementation of effective cybersecurity, privacy, and data and cloud infrastructure
- Protection measures
- Provide institutional mechanisms for the governance of data and cloud services.
- Support the development of small, medium, and micro enterprises (SMMEs); and
- Provide for research, innovation, and human capital development.

In addition, the Draft National Data and Cloud Policy also seeks to align the proposed South African developments with the Fourth Industrial Revolution (4IR) and global trends.

As introduced above, the ECT act is one of South Africa's legislation that is used as a foundation for policies, especially for policies that are being drafted such as the South African Draft policy for Data and Cloud. However, many researchers still argue that there is no policy to guide localized data acquisitions, ownership, use, storage, and analytics. The above-mentioned laws (POPI act and ECT policy) show no reciprocity to support the drive to develop a digital economy in the Republic of South Africa with measures that will preserve the citizen's data privacy and ensure security in the cloud space.

More concerns rise as it has been projected that by 2025, the global data sphere will grow to 164 Zettabytes from 40 zettabytes in 2019 [16]. This, therefore conveys the need for a scalable, reliable, and secure solution to store cloud-hosed data. Currently, data that is owned and generated by the government is stored mostly in privately owned companies and third-party providers with no policy to guide its use or acquisition [2]. Thus, developed regions like the European Union and the Russian Federation, have fully migrated to the digital economy and designed developed policies and regulations that protect their citizen's data from cyber threats and attacks, especially in the cloud or those that are held beyond borders in different jurisdictions. Typically, the European General Data Protection Regulation's (GDPR's) ultimate objective is to provide Europeans within the private and public sectors with access to safe and secure data storage, and sustainable and interoperable cloud infrastructure wherever they are in the world.

In addition, the GDPR sets a good benchmark for the development and implementation of the POPI ACT [17]. Therefore, this research aims to explore the legislation, regulations,

and/or policies that SA currently has or planning to put in place for managing cloud-bound data or workloads and the security thereof. Furthermore, it critically analyzes the draft national data and cloud policy and conducts a comparison of the cloud data and computing policies that have been designed in other countries.

3.2 Current Development for Cloud Computing Readiness in SA's Public Sector

Shibambu [2] conducted research that investigated the public sector's willingness to entrust its records to the cloud infrastructure. Shibambu's study highlights the government's sentiments and concerns when migrating its records and other data to the cloud. The apprehensions are attacks on physical hosts, jurisdiction, and sovereignty. In conjunction with the latter, a report published by the Center for Africa-China [18] critically analyzed the merits and limitations of South Africa's data sovereignty regulations. This study makes use of the POPI act as legislation that regulates the record and data movement and its storage in the country and across borders, revealing that there is a need for a more robust data protection law as the POPI act is limited on this aspect and does not cover how the data is destroyed after use, be it in the country or cross border.

Moreover, without neglecting the vital role that has been played by the POPI Act [19] in covering most aspects of data and record transfer in the country, a study by [3] suggests that the POPI Act alone is not sufficient when it comes to cloud computing. However, it is granted the act provisions for cross-border data transfer. The act becomes inadequate when it comes to cloud computing and needs readjustments as Jangara and Bezuidenhout [2] [20] mention that the data location, security, privacy, legal compliance, and cloud service providers are remaining concerns raised by cloud computing amid the POPI act. An even greater concern is raised, especially because cloud computing is now evolving towards multi-cloud environments which have their datacentres across various countries with various legal systems that may not be in harmony. The emerging multi-cloud environment adds further complexity to the already complex difficulty of harmonization of national, regional, and international cloud computing regulations, legislations, standards, and frameworks. Though the emerging complex issue of multi-cloud environments is important and relevant, this study just highlights it and its importance. However, it does not delve deep to unpack it. The next section discusses the methodology of this current research.

4. Methodology

This paper conducts a rigorous and critical analysis of literature studies that cover the following:

- Cloud Security
- Data storage policy
- Laws and regulations (POPI and ECT acts)
- The draft national data and cloud policy

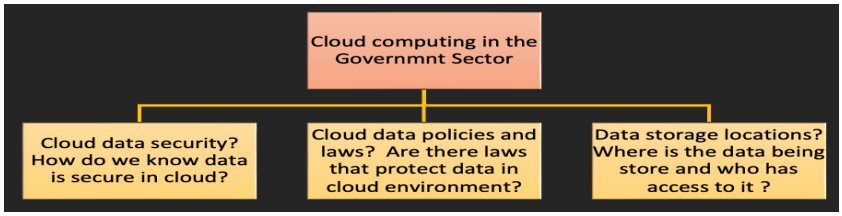

Figure 1:Research Methodology

Figure 1 highlights and summarises the method of how this research was conducted. The study starts by exploring cloud computing in the context of the public sector. It then goes into formulating several research questions that in answering will help the authors

understand how the public sector approaches cloud computing. The questions have been used as a benchmark to gather all the necessary information that pertains to cloud security in the public sector.

The literature review involves previously published research works between 2012 and 2023. This is due to the significant progress that has already been achieved by several government departments that have embraced and migrated some of their workflows and data into cloud computing. This migration from on-premises data centers to cloud computing over the past decade has been necessitated by several reasons, but mainly the remote-working push from the pandemic of 2020 where lockdowns were enforced.

This paper has selected some topics that include the following:

- Cloud computing and its protection
- Cloud infrastructure, application, and data security
- Governance, risk management, and compliance (GRC) policies that have already been documented or implemented to protect data in cloud environments.
- Suggestions from authors on how to strengthen protection and safety measures for data stored in the cloud, and lastly
- Through these reviews of related work, this paper identifies and explores existing research gaps and tries to predict the future research direction for cloud computing in the context of the public sector.

From the selected related work, the authors hope to design a suitable framework that addresses the existing research gaps and protects cloud-bound data and the cloud infrastructure. The framework will be designed using the existing Draft National Data and Cloud Policy of South Africa as a main pillar of the foundation. This draft policy remains relevant to an extent. However, in this research, the authors of this paper aim to extend it by incorporating the security aspects to try and improve data protection in the cloud.

Moreover, this research paper acknowledges and is aware of various shared responsibility models together with the well-architected frameworks available from Google Cloud [21], Microsoft Azure [22], and Amazon Web services [23] and a snapshot of all these cloud platform models has been summarized and also used as a basis of this study.

5. Discussion

It is palpable that cloud computing has had an impact on South Africa's existing regulatory frameworks. As discussed in the sections above, the POPI and ECT Act have been incorporated in the compilation of the Draft National Data and Cloud Policy, which is quite important. This is because the safety and security of citizens' sensitive data such as personally identifiable information (PII) remains a major concern. These concerns are raised regardless of whether the data is being stored on the cloud or an on-premises data center. It is also important to note how the cyberlaw lays a firm foundation for any innovations made in data protection. However, after a critical analysis of the Draft National Data and Cloud Policy, the authors of the study strongly believe that it is also very vital that the existing cloud-shared responsibility models are used by the government to ensure the effectiveness of the National Draft policy for cloud and data storage.

The question then arises, what is a 'cloud security shared responsibility model'? The shared responsibility model for the cloud speaks to how the cloud service provider protects the client's data, workloads, and infrastructure. This also considers the security roles and responsibilities of the cloud consumers for their data or workloads that are hosted in the cloud.

With the South African government making use of a model, critical security measures such as identity and access management, data encryption, and endpoint security

configurations fully are covered by law, and it is a regulation and compliance that assure stakeholders whether they are ready for cloud adoption. This is depicted in Figure 2 below.

In conjunction with the related studies discussed in the research paper which have revealed the usefulness of the POPI and ECT Acts in aiding to protect data in the cloud, this study has further unpacked its involvement and inclusiveness of acts together with the cyber law in the Draft National policy on data and cloud. This study identified the gaps in the existing policy and proposed a shared responsibility framework together with the well-architected framework for cloud computing as a tool to be used to strategically strengthen the Draft policy while other studies analyze and criticize the policy, this study proposed a solution.

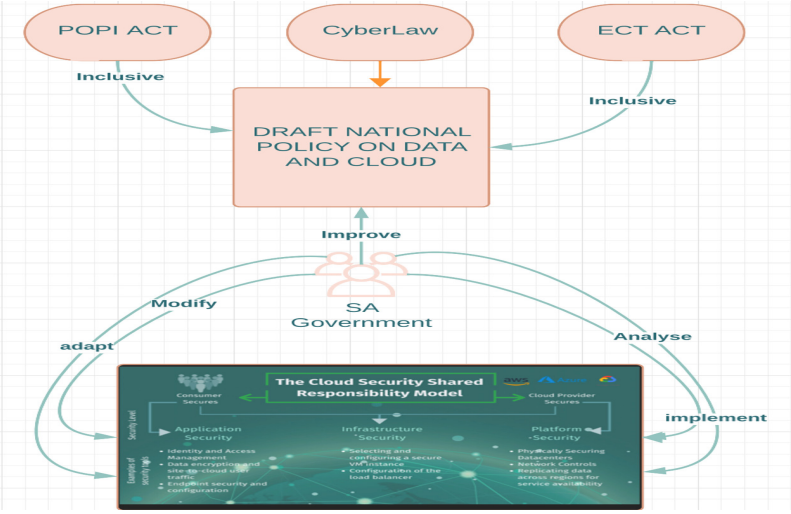

Figure 2: Proposed Model

6. Conclusion

The work has reviewed the latest advancements in South Africa about the policies and laws that have been implemented with the aim being the protection of data in the cloud space, from the articles reviewed, it is quite clear that SA is maneuvering towards a digital era and one that is secure. So far, there have been enhancements and new developments being done over the past 11 years. For instance, the POPI Act has been adopted by many organizations including the private sector. The very same POPI act is included in the emerging draft national policy for data and cloud security.

Moreover, the Draft Policy relates to the POPI Act, as it includes the availability, confidentiality, data regulation, data localization, and digital security of data. This is very important as the latter is more of what stakeholders focus on when storing data on physical servers, so having the same principles applied in the cloud confirms reassurance for their data security. Therefore, this study has revealed that the draft is heading in the right direction but restructuring and advancements that include the adoption of the models that are currently in place for cloud computing such as the 'cloud security shared responsibility model' depicted in Figure 2 above. This Adoption will thus enable the benefits and responsibilities associated with cloud computing to be known and understood.

Thus, future works of this study are to help the South African government strengthen the security of data stored cloud by compiling and implementing a compliance model that can used by the SA government to detect the readiness to migrate data to the cloud. The authors of this study also propose that the compliance model is treated as a strict mandatory step for anyone wanting to migrate data or any workloads to the cloud. This proposed solution will work in conjunction with the model proposed in Figure 2.

References

[1] P. Mell, “The NIST Definition of Cloud Computing,” NIST, 2011.

[2] A. Shibambu, “Migration of government records from on-premises to cloud computing storage in South Africa,” SA Jnl Libs & Info Sci, vol. 88, no. 1, 2022.

[3] N. Mohlameane and M. Ruxwana, “Exploring the impact of cloud computing on existing South African regulatory frameworks,” South African Journal of Information Management, vol. 22, no. 1, p. 1132, 2020.

[4] A. Fargana, “Cyber resilience and cyber security issues of intelligent cloud computing systems,” Results in Control and Optimization, vol. 12, no. 1, 2023.

[5] V. Moonasar and V. Naicker, “Cloud Adoption: A Conceptual Model to Assess the Maturity of South African Large Enterprises,” in ICEME: International Conference on E-business, Management and Economics, 2018.

[6] Google, “What are the different types of cloud computing?,” Google, 2022. [Online]. Available: https://cloud.google.com/discover/types-of-cloud-computing#:~:text=The%20main%20three%20types%20of,SaaS)%2C%20and%20serverless%20computing..

[7] T. Toader, V. Dinu, D. Manea and M. Mihai, “he effects of private sector companies’ research and development investments on the adoption of cloud computing services in the European Union,” E&M Economics and Management, vol. 26, no. 2, pp. 189-202, 2023.

[8] Z. Alashhab, M. Anbar, M. Singh, L. YB and Al-Sai, “Impact of coronavirus pandemic crisis on technologies and cloud computing applications,” Journal of Electronic Science and Technology., vol. 19, 2021.

[9] U. E. M. a. E. Terem, “South Africas Data Soveriegnty Regulations”.

[10] V. Naicker and V. Moonasar, “Cloud capability maturity model: A study of South African large enterprises,” in South African Journal of Information, Cape Town, 2020.

[11] E. Raaff, N. Wynne and A. Rothwell, “Aligning South African Data and Cloud Policy with the PoPI Act,” in Proceedings of the 17th International Conference on Information Warfare and Security, Johanessburg, 2022.

[12] D. Cooper, D. Mkhize and M. Govender, “Global Policy Watch Key Public Policy Developments Around the World,” AFRICA, ARTIFICIAL INTELLIGENCE (AI), BLOCKCHAIN, COMPLIANCE ISSUES, FINTECH, INTERNET OF THINGS (IOT), POLICY AND LEGISLATION, PRIVACY, 5 November 2021. [Online]. Available: https://www.globalpolicywatch.com/2021/11/overview-of-south-africas-draft-national-data-and-cloud-policy/.

[13] “Draft National Policy on Data and Cloud,” GOVERNMENT GAZETTE, Cape Town, 2021.

[14] G. Government, “Protection of personal Information Act, 2013,” Republic of South Africa, Cape Town, 2013.

[15] G. Government, “No. 25 of 2002: Electronic Communications and Transactions Act, 2002.,” REPUBLIC OF SOUTH AFRICA, Cape Town, 2002.

[16] D. Reinsel, “The Digitization of the World From Edge to Core,” 2020.

[17] V. BRONSTEIN, “Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the Protection of Personal Information Act.,” Potchefstroom Electronic Law Journal, vol. 25, pp. 1727-3781, 2023.

[18] T. Matambo and U. Edmund, “South Africa's Data and Sovereignty Regulations: merits and possible limitations,” UNIVERSITY OF JOHANNESBURG ✲ CENTRE FOR AFRICA-CHINA STUDIES, Johannesburg, 2022.

[19] “Government Gazette,” South African Government Gazette, cape town, 2013.

[20] T. Bezuidenhout, “Addressing emerging risks in transborder cloud computing and the protection of personal information,” The role of internal auditors’, Southern African Journal of Accountability and Auditing Research, vol. 17, no. 1, pp. 11-24, 2015.