International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Compliance and Regulatory Challenges in Public Sector Cloud Adoption

Pavan Nutalapati

Email: *pnutalapati97[at]gmail.com*

Abstract: ***This research explores the regulatory and compliance challenges faced by public sector organizations in the period of cloud adaptation. Since the government is rapidly shifting towards cloud computing to increase service delivery and cost-efficiency, they are facing complex legal frameworks, data privacy concerns, and sovereignty issues. Hence, this research aims to investigate the complete and regulatory challenges faced by the public or governmental organizations in cloud adoption.***

Keywords: Cloud adaptation, “Envisioned evidence regulation”, “CLOUD act”

1. Introduction

Project Specification

In recent times, cloud adoption in the public sector has significantly transformed how governmental services get initially delivered, providing cost-efficiency, and scalability and improving the entire accessibility. Moreover, the shift towards cloud computing has provided notable compliance and regulatory challenges [1]. Hence, public sector organizations had to navigate a complex legal framework, composite regulatory requirements, and data privacy concerns. Properly understanding those challenges is vital for adopting better cloud adoption in the public sector which can effectively adapt to the advanced cloud technologies while effectively maintaining international and national regulations. Hence, this research aims to investigate the complete and regulatory challenges faced by the public sector.

2. Aims and Objectives

2.1 Aims

The research aims to investigate the complete and regulatory challenges faced by the public or governmental organizations in cloud adoption.

2.2 Objective

- To assess the significant regularity frameworks influencing cloud adoption in the public sector
- To scrutinize the particular compliance issue that arises during the implementation
- To evaluate how the arising challenges impact the entire adoption process
- To provide recommendations for overcoming those barriers in cloud adoption.

2.3 Research Questions

R1: What are regularity frameworks influencing cloud adoption in the public sector?
R2: What is the particular compliance issue that arises during the implementation of cloud adoption?
R3: What are the raised challenges that impact the entire adoption process in the public sector?
R4: What are the recommendations for overcoming those barriers in cloud adoption?

2.4 Research Rationale

The implementation of cloud computing in the public sector is critical for modernizing the government service [2]. However, it presents notable regulatory and compliance challenges which can hamper its evaluation. This research is vital as it addresses the vital requirements for the public sector organization to properly understand and adapt the composite legal landscape related to cloud adoption. Through a proper investigation of those challenges, this present study would provide an in-depth analysis of regulatory and compliance issues which would help to make strategies. This strategy would assist in optimizing the benefits, decreasing risks and handling compliance significantly. Overall, this would help to provide several benefits regarding cloud technologies in the public service delivery.

3. Literature Review

3.1 Research background

Cloud computing has become an important strategic tool for public sector modernization. It effectively increases service efficiency and delivery. Moreover, the shift to a cloud environment presents significant compliance and regulatory challenges [3]. These challenges mainly involve specifically concerning privacy, data security and adherence to the legal framework which makes it vital for this study.

3.2 Critical assessment

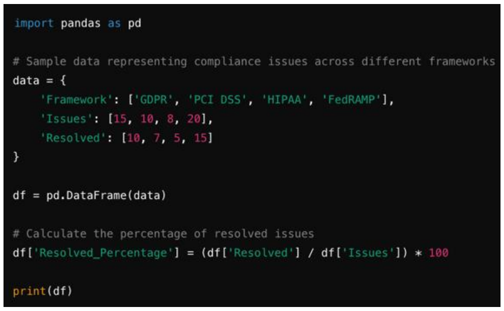
The existing literature on public sector cloud adoption shows both the complexities of regulatory compliance and the transformative potential of cloud technologies. As per the view

DOI: https://dx.doi.org/10.21275/SR24903075206

of [4], there is a growing concern for compliance with data protection laws, risk of vendor lock-in, and jurisdiction challenges. Hence, [5] stated that cloud adoption in the financial organization provides significant challenges for implementation. Financial organizations should follow specific laws such as "Payment card industry data security standards", and the "Gramm-Leach-Bliley Act" in finance as data protection and consumer trust are the second most vital factors. Hence, the financial system must protect their customer information and transactions besides mobile payments in finance.

Figure 1: Importance of compliance in cloud environment [5]

However, [6] stated that, when it comes to the challenges across cloud adoption, a few areas are unmanageable as compliance and security. This is specifically true within the U.S. public sector, in which there are many effective time-consuming requirements and compliance frameworks. The public sector has been significantly struggling with the different compliance requirements with various types of frameworks such as FedRAMP, NIST, PCI DSS, and HIPAA [7]. On the far side of these existing compliance frameworks, the new requirements and frameworks have been continuing to change. However, the government service provider's reliance on third-party cloud providers raises questions regarding data sovereignty besides the ability to maintain control of overall sensitive information.



```
import pandas as pd

# Sample data representing compliance issues across different frameworks
data = {
    'Framework': ['GDPR', 'PCI DSS', 'HIPAA', 'FedRAMP'],
    'Issues': [15, 10, 8, 20],
    'Resolved': [10, 7, 5, 15]
}

df = pd.DataFrame(data)

# Calculate the percentage of resolved issues
df['Resolved_Percentage'] = (df['Resolved'] / df['Issues']) * 100

print(df)
```

Linking with aim

The aim of this research is to fill the gap between compliance challenges and adoption benefits in the public sector by analyzing the regulatory landscape. This paper further aims to investigate the compliance and regulatory challenges that the public sector faces. However, the existing literature also shows the different kinds of challenges and issues that arise during the implementation of cloud computation in the government sector. Hence, it can be stated that the research effectively met its aims.

Encapsulation of applications

The overall research findings would be applied to improve the entire cloud adoption strategies within the public sector by providing a clear understanding of regularity challenges. The obtained insights would help the policymakers and IT leaders for developing a complete framework. It would further help to ensure a secure cloud implementation that would satisfy the regulatory and legal standards throughout different jurisdictions.

Theoretical framework

This research is restrained in the theory of technology compliance and acceptance, which shows how organizations adopt new technologies while fostering regulatory requirements. This framework has significantly helped to explore cloud intersections technology adoption, and compliance with the governmental sector by focusing on operational, ethical and legal aspects.

4. Literature Gap

This research paper provided an in-depth insight into the challenges and benefits of cloud adoption within the public sector. In this section, there is a noticeable gap within the studies which particularly address the refined regulatory and compliance challenges throughout different jurisdictions. The majority of this research focused on widely in cloud technology without examining the practical complexities of the government sector's compliance requirements. On the other hand, there is limited guidance on developing the standardized compline framework developed for the unique requirements of public sector organizations.

5. Methodology

5.1 Research Philosophy

Research Philosophy is a specific belief in the way any data or information is gathered and properly analyzed [8]. A well-suited philosophy would provide a critical analysis of the information's source, nature, and development of any information. Moreover, In this research, the interpretivism research philosophy was implemented. This philosophy is mainly chosen as it assists in interpreting the elements of a study. Interpretivism research philosophy can generate high research validity which aims to obtain significant meanings.

5.2 Research approach

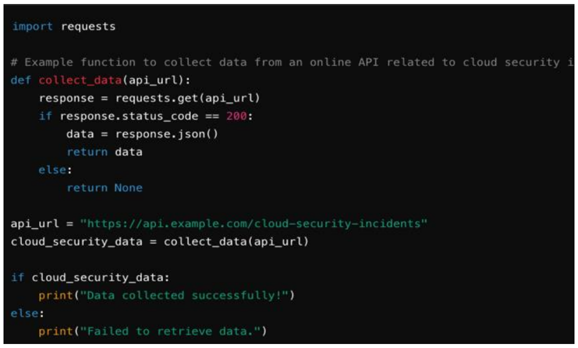
A well-structured research approach is primarily defined as a specific process and strategy that notably decides the entire methods that would be evaluated in a paper [9]. This paper notably includes assessing the challenges that arise in the public sector during the implementation of cloud computation. In this regard, this paper implements the inductive research approach as it aids in evaluating research findings for the extent of the significant and frequent themes. Furthermore, this approach would assist in giving an in-depth analysis of different challenges.

5.3 Research design

A well-structured research design is a certain framework regarding the entire research methods and other strategies for choosing a better method to conduct the whole paper. There are three types of research design which involve explanatory, exploratory, and descriptive research design. In this concern, this paper implemented the descriptive research design. This research design is better for this research, it would assist in enabling a comprehensive analysis of challenges that occur during cloud computation in the public sector. Through describing the present method and a systematic data collection. This overall design would aid in identifying the patterns, trends, and gaps in the domain.

5.4 Data collection method

There are two types of data collection methods which involve primary or quantitative data collection and secondary or qualitative data collection methods. In this regard, this paper implemented the secondary data. The existing secondary data was invaluable for this study since it provided proper access to existing studies on different challenges for implementing cloud computation in the public sector.



```
import requests

# Example function to collect data from an online API related to cloud security i
def collect_data(api_url):
    response = requests.get(api_url)
    if response.status_code == 200:
        data = response.json()
        return data
    else:
        return None

api_url = "https://api.example.com/cloud-security-incidents"
cloud_security_data = collect_data(api_url)

if cloud_security_data:
    print("Data collected successfully!")
else:
    print("Failed to retrieve data.")
```

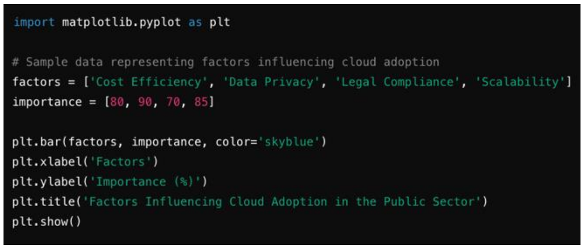
Ethical consideration

During the period of the data collection process, this study significantly maintained a few codes of conduct and ethics. Additionally, this paper collected all the data from reliable and authoritative sources. The information was collected by genuine and peer-reviewed journals. Any sort of biased presentation of secondary sources and misleading data had been avoided as well.

6. Results

6.1 Critical analysis

The research would significantly highlight several key findings regarding the challenges in the public sector for cloud computation implementations. Different kinds of vital factors such as elements influencing the adoption of cloud computation in the public sector, competencies issues in government service and legal reflection in cloud computing have been properly analyzed.



```
import matplotlib.pyplot as plt

# Sample data representing factors influencing cloud adoption
factors = ['Cost Efficiency', 'Data Privacy', 'Legal Compliance', 'Scalability']
importance = [80, 90, 70, 85]

plt.bar(factors, importance, color='skyblue')
plt.xlabel('Factors')
plt.ylabel('Importance (%)')
plt.title('Factors Influencing Cloud Adoption in the Public Sector')
plt.show()
```

7. Findings and Discussion

Theme 1: Factors influencing the adoption of cloud computation in the public sector

Government sectors throughout the world have been struggling to provide more effective and efficient public services to meet the rapid expectations and demands of citizens. The sector also struggling to handle with primary problem of reduced financing and public resources at the same time [10]. In the previous time, it was broadly accepted that an "Electronic government" was much more complex compared to any earlier efforts of IT which had brought several changes to the public sector. After that, the integration of advanced and new technologies within the e-government domain poses significant challenges activity due to numerous numbers of factors [11]. These factors mainly involve the influence of bureaucratic politics, slow rate of adoption, flexibility of its target stakeholder and interoperability of systems and applications. The rapid emergence of cloud computing technology has opened up new possibilities for several governments. In this present time, cloud computing is one of the most advanced IT innovation phenomena which has arisen through the concepts of standardizing, consolidating and idea of sharing within a centralized facility and infrastructure.

Theme 2: Compliance Issues in Government Cloud Service

In the governmental sector, utilizing cloud computing significantly enhances privacy risks as governmental data is accessible to the public [12]. There is a lack of proper framework or guidance designed for supporting privacy in cloud computing. This lack of regulatory frameworks shows the necessity of creating privacy protection conditions in cloud computing to the requirements of privacy protection and effective data protection. Data sovereignty challenges had been a significant political factor that had arisen in the proper analyses of cloud service, jurisdiction factors, and notable data preferences. Governments or the public sector worldwide are facing significant issues related to data safety which helps through the " foreign cloud providers and governments" [13]. In this regard, it is vital to develop a sovereignty policy, particularly to those protecting the public sector's cyber security data and system. On the other hand, protecting data sovereignty has become much more difficult through taking the marginal law nature such as "Envisioned evidence regulation" through the EU and the "CLOUD act" from the USA. These specific regulations effectively develop the law enforcement process concerning the cloud-stored public sector data. In the present time, the government experiences numerous regulation and governance issues while entering a development environment. The rapid pace of advancement and growth in technology required synchronized and swift policies for safety, adaptability and efficiency.

Theme 3: Legal and compliance reflection in cloud computing

The security employment and data privacy of cloud computing face jurisdictional problems and legal difficulties. The exposure of privacy compliance and data transfer became a significant concern after the "European Union" evaluated the "General Data Protection Regulation" [14]. This had been further worsened through the cloud service developing a strong base regarding their GDPR compliance on the study. In this concern, public organizations should follow norms such as GDPR, or their reputation will be damaged. It effectively showed the significance of states by following international standards and regulations.

Evaluation

The research effectively recognized and analyzed the key regulatory and compliance issues faced by public sector organizations in the period of cloud adoption. It shows the complexities included in the handling of legal adoption, sovereignty and data privacy. The above data findings show the requirements for a better compliance framework to ensure efficient and secure cloud implementation in government services.

8. Conclusion

This study showed that cloud computing provides significant benefits to the public sector, yet its adoption is challenging due to compliance and regulatory issues. The issues are mainly associated with the legal framework, sovereignty and data privacy. This effectively highlights the requirements for public sector organizations to create a better strategy to handle compliance more effectively. By effectively addressing these issues, governments can better adapt cloud technologies to increase service delivery and reduce costs. On the other hand, the public sector can satisfy the growing demands of citizens while assuring adherence to national and international regulations.

9. Research Recommendation

In order to mitigate the regulatory and compliance challenges within the public sector cloud computation, it is significantly recommended that government organizations implement and develop a standardized compliance framework adapted to the unique requirements [15]. This framework should address jurisdictional, sovereignty and data privacy which would assure a proper alignment of different international standards such as the GDPR. In addition, adopting a proper collaboration among the cloud service providers, IT leaders and policymakers is vital for developing a secure and better cloud environment. Besides, continuous training and awareness programs for public sector employees must also be established to ensure that they understand the complexities of cloud compliance and can effectively manage risks.

10. Future Work

Future research could explore the overall development of automatic tools based on the advanced cloud computation system for real-time compliance and monitoring in the public sector. In addition, comparative studies throughout the various regions might provide in-depth insights into the effectiveness of different regulatory frameworks.

References

[1] Hashmi, A., Ranjan, A., & Anand, A. (2018). Security and compliance management in cloud computing. *International Journal of Advanced Studies in Computer Science and Engineering*, *7*(1), 47-54. [Online]. Available: https://www.academia.edu/download/58213942/Security-as-a-Service.pdf

[2] Nanos, I., Manthou, V., & Androutsou, E. (2017). Cloud computing adoption decision in E-government. In *Operational Research in the Digital Era–ICT Challenges: 6th International Symposium and 28th National Conference on Operational Research, Thessaloniki, Greece, June 2017, pp. 125-145*. Springer International Publishing. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-95666-4_9

[3] Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. *International Journal of Advanced Computer Science and Applications*, *8*(10). [Online]. Available: https://www.researchgate.net/profile/Muhammad-Mushtaq-20/publication/320802850_Cloud_Computing_Environment_and_Security_Challenges_A_Review/links/59fc20da458515d07062864c/Cloud-Computing-Environment-and-Security-Challenges-A-Review.pdf

[4] Opara-Martins, J. (2018). Taxonomy of cloud lock-in challenges. In *Mobile Computing-Technology and Applications*. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=73eQDwAAQBAJ&oi=fnd&pg=PA3&dq=Opara-Martins,+J.+(2018).+Taxonomy+of+cloud+lock-in+challenges.+Mobile+computing-technology+and+applications.&ots=7n8dle4Juw&sig=E01ZjeW6PUYdBYTucBCfi6VyEwo

[5] Yoo, S. K., & Kim, B. Y. (2019). The effective factors of cloud computing adoption success in organization. *Journal of Asian Finance, Economics and Business*, *6*(1), 217-229. doi: 10.13106/jafeb.2019.vol6.no1.217

[6] Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: Technical review. *Future Internet*, *14*(1), 11. doi: 10.3390/fi14010011

[7] Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017). Cloud standards in comparison: Are new security frameworks improving cloud security?. In *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, June 2017, pp. 50-57. doi: 10.1109/CLOUD.2017.16

[8] Abu-Alhaija, A. S. (2019). From epistemology to Structural Equation Modeling: An essential guide in understanding the principles of research philosophy in Selecting the Appropriate Methodology. *Australian Journal of Basic and Applied Sciences, 13*(9), 122-128. doi: 10.22587/ajbas.2019.13.9.12

[9] Sovacool, B. K., Axsen, J., & Sorrell, S. (2018). Promoting novelty, rigor, and style in energy social science: Towards codes of practice for appropriate methods and research design. *Energy Research & Social Science, 45*, 12-42. doi: 10.1016/j.erss.2018.07.007

[10] Hodgkinson, I. R., Hannibal, C., Keating, B. W., Buxton, R. C., & Bateman, N. (2017). Toward a public service management: past, present, and future directions. *Journal of Service Management, 28*(5), 998-1023. doi: 10.1108/JOSM-01-2017-0020

[11] Obodo, N. A., & Anigbata, D. O. (2018). Challenges of implementing electronic governance in public sector organizations in Nigeria. *International Journal of Applied Economics, Finance and Accounting, 2*(1), 30-35. doi: 10.33094/8.2017.2018.21.30.35

[12] Mohammed, F., Ibrahim, O., Nilashi, M., & Alzurqa, E. (2017). Cloud computing adoption model for e-government implementation. *Information Development, 33*(3), 303-323. doi: 10.1177/0266666916656033

[13] Mergel, I. (2021). Open innovation in the public sector: Drivers and barriers for the adoption of Challenge.gov. In *Digital Government and Public Management*. Routledge, pp. 94-113. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003258742-6/open-innovation-public-sector-drivers-barriers-adoption-challenge-gov-ines-mergel

[14] Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *ecancermedicalscience, 11*. doi: 10.3332%2Fecancer.2017.709

[15] Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IoT standardisation: Challenges, perspectives and solution. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, June 2018, pp. 1-9. doi: 10.1145/3231053.3231103

[16] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[17] Rimal, B. P., Choi, E., & Lumb, I. (2011). A taxonomy and survey of cloud computing systems. *In Proceedings of the 2010 Fifth International Joint Conference on INC, IMS and IDC (pp. 44-51)*. IEEE. doi: 10.1109/NCM.2010.58

[18] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583-592. doi: 10.1016/j.future.2010.12.006

[19] Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *IEEE Internet Computing, 14*(5), 14-22. doi: 10.1109/MIC.2010.84

[20] Ardagna, C. A., Asal, R., Damiani, E., & Vu, Q. H. (2015). From security to assurance in the cloud: A survey. *ACM Computing Surveys, 48*(1), 1-50. doi: 10.1145/2767005

[21] Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing, 16*(1), 69-73. doi: 10.1109/MIC.2012.14

[22] Voorsluys, W., Broberg, J., & Buyya, R. (2011). Introduction to cloud computing. In *Cloud Computing: Principles and Paradigms* (pp. 1-41). John Wiley & Sons, Inc. doi: 10.1002/9780470940105.ch1

[23] Wang, S., Yan, K., & Wang, H. (2010). A model-driven approach to developing cloud applications. *In Proceedings of the 5th International Conference on Software and Data Technologies (ICSOFT), vol. 1, pp. 86-91*. SciTePress. doi: 10.5220/0002937800860091

[24] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11. doi: 10.1016/j.jnca.2010.07.006

[25] Siani, P. (2010). Cloud computing security: The scientific challenge, and a survey of solutions. *Computer Security and Applications Conference, ACSAC 2010*. doi: 10.1109/ACSAC.2010.43

[26] Gellman, R. (2009). Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. *World Privacy Forum*. [Online]. Available: https://www.worldprivacyforum.org/wp-content/uploads/2009/02/WPF_Cloud_Privacy_Report.pdf

[27] Gens, F. (2011). IT cloud services user survey, pt. 2: Top benefits & challenges. *IDC eXchange*. [Online]. Available: https://blogs.idc.com/itcloud-services-user-survey-pt-2-top-benefits-challenges/

[28] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. *IEEE Transactions on Services Computing, 5*(2), 220-232. doi: 10.1109/TSC.2011.24

[29] Berman, S. J., Kesterson-Townes, L., Marshall, A., & Srivathsa, R. (2012). How cloud computing enables process and business model innovation. *Strategy & Leadership, 40*(4), 27-35. doi: 10.1108/10878571211242920

[30] Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy, 8*(6), 24-31. doi: 10.1109/MSP.2010.186