Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2021, 8(12):227-232**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Best Practices for Data Governance and Security in a Multi-Cloud Environment

Chandrakanth Lekkala

Email id: Chan.lekkala@gmail.com

Abstract Multi-cloud computing is one of the technologies that has received rapid adoption over the years as many organizations seek to leverage its benefits. From cost reduction to offering scalability, cloud computing has many benefits to offer to the businesses that integrate it into their operations. That said, the effective use of this technology calls for users to apply the best practices when it comes to data governance and security. This paper will explore the said best practices.

Keywords: Multi-cloud computing

Introduction

Over the past decades, many organizations have integrated cloud computing technologies into their operations [1]. That said, cloud computing is of many forms, but many of the adopters of this technology have favored a multi-cloud approach. This form of cloud computing offers organizations many benefits, including reduced costs of running the business and scalability of the services [2]. With such benefits, it means that any organization that wants to remain competitive must adopt cloud computing in its operations; otherwise, it faces the risk of failing to keep up with the pace and growth of its competitors, a scenario that is likely to end up driving the given organization out of business. That said, the use of a multi-cloud computing approach is not all smooth. It introduces data governance and security concerns, which must be addressed using the available best practices.

Best Practices

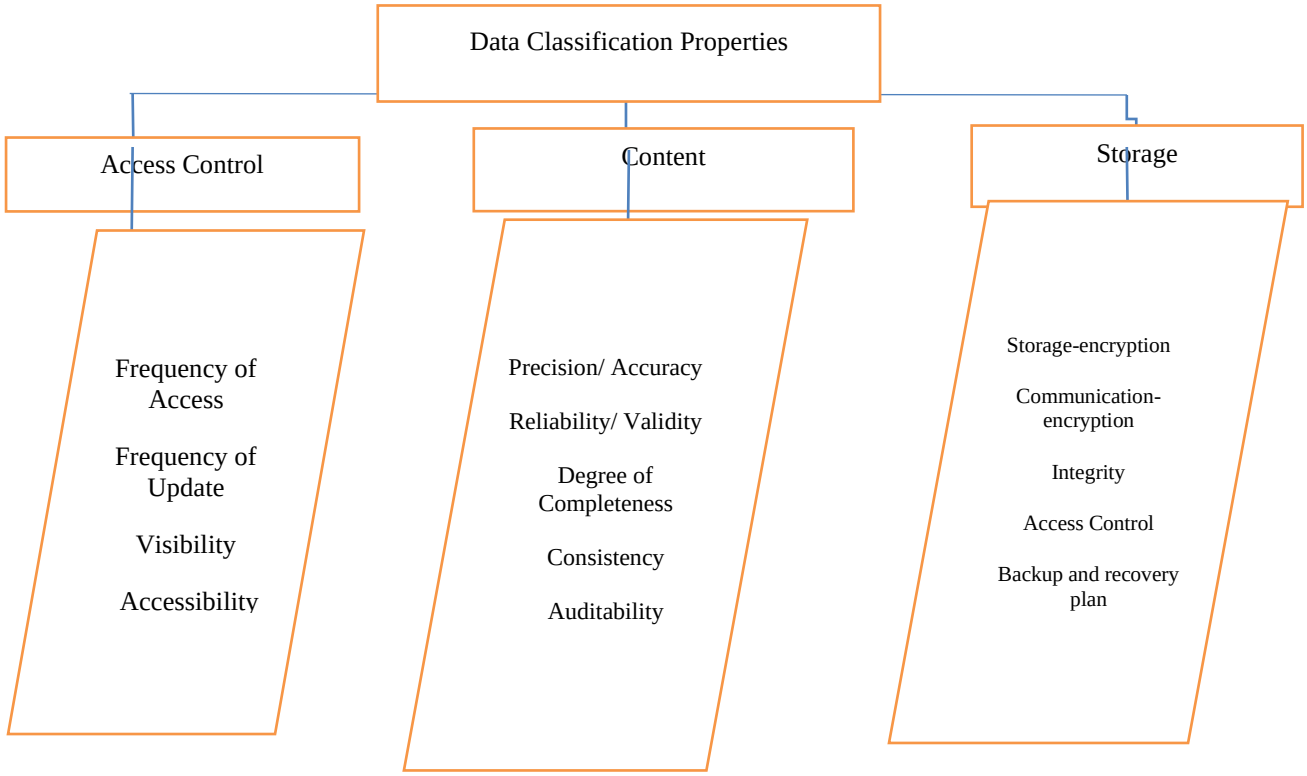
A. Data Governance Framework

Establish a Comprehensive Data Governance Framework

For organizations using multiple cloud platforms, a strong data governance framework is essential [3]. The general role of this framework is to provide the fundamental set of rules and procedures that should be used in managing data across all the cloud environments utilized by an organization. For instance, the set policies and procedures should define the classification of data and access control. Notably, given that the organization is using cloud services from more than one provider, it is crucial for the organization to ensure that the set policies are consistently applied across all cloud platforms utilized [3]. While creating data governance policies might seem straightforward, implementing them effectively is another story, and for that reason, it is important for an organization to have a dedicated data governance team to oversee the whole process.

Among the crucial roles that the dedicated team should establish in order to facilitate effective data governance and security is the classification of data and labeling. While there is no doubt that every type of data should be protected, it is important to remember that the value of data in relation to the use it has to the organization varies, and this is an aspect that should be considered while defining a data governance framework. The process of identifying data elements with respect to their value in the business is what is termed classification. The identification of the value of data elements should be guided by a number of key factors, which include their

usage and access control restrictions. The figure below illustrates three types of characteristics that define the category on which data element should be placed during classification, and security considerations follow each category.



The classification of data, as illustrated above, serves the crucial role of guiding the data governance team in deciding the criticality of the different data elements and, consequently, the type of regulatory requirements that each data element demands.

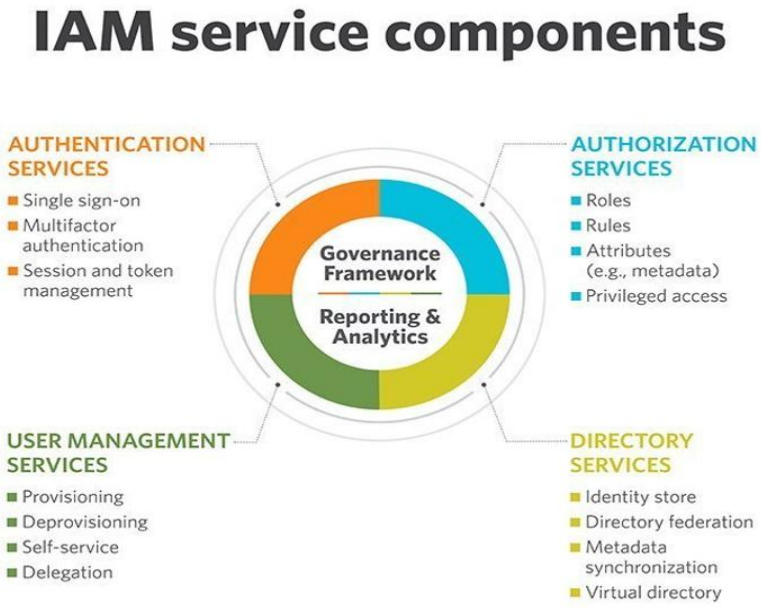
B. Identity and Access Management

Implement Robust Identity and Access Management (IAM)

An effective IAM strategy is essential for managing and safeguarding data. Implementing the IAM is characterized by the introduction of many security features, one of the most effective and obvious one being multi-factor authentication (MFA). Through the adoption of MFA, the login process requires additional information beyond passwords, thereby enhancing security measures to access data. In addition to MFA, organizations using cloud platforms are supposed to enforce the principle of least privilege. The principle ensures that users and applications are granted the minimum necessary permissions to perform their duties [5]. This helps to limit the potential damage that could result from compromised credentials or insider threats. In line with the need to have an IAM strategy in place, the organization should also ensure that there is regular reviewing and auditing of the user access rights in order to ensure that they are evolving as the organizational needs evolve, hence meeting the changing security needs.

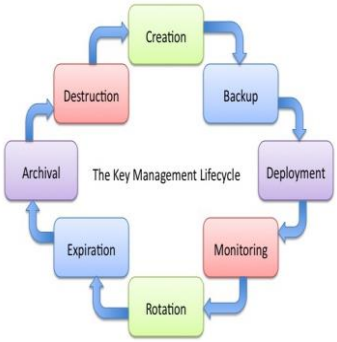
For instance, employees can leave the organization, which is common in the organizational landscape. The leaving of the employees can be a consequence of many issues. However, regardless of the reasons that lead to an employee leaving an organization, it is important for the data governance and security team to remember that those employees leaving the organization had access rights to the organizational data, and by virtue of the leaving, they should no longer have access to any type of the organizational data in any of the cloud platform utilized by the organization. Their access, therefore, should be removed with immediate effect upon their

leaving the company; otherwise, the data is at risk of unauthorized access. That is, periodically auditing user permissions and appropriately adjusting access is indispensable in data governance and security. In light of this discussion, the figure below represents what IAM encompasses.



Data Encryption and Key Management

Providing data safety in a multi-cloud environment also necessitates employing data encryption strategies alongside robust key management plans. The modern standards of data security require data security to be guaranteed all the time. To that end, an organization using cloud services is responsible for ensuring that data is safe both at rest and in transit by encrypting the data regardless of its state. Encryption is done using algorithms such as AES and RSA, guaranteeing that at no point is data exposed to unauthorized access, even if underlying cloud infrastructure is compromised. To further ensure the betterment of the encryption approach in safeguarding data, it is advisable for the encryption keys to be managed centrally using various methods, including, using tools such as a key management system (KMS), which ensures that not only does the primary goal of centralization of keys achieved but additional features such automated key rotations are introduced [8]. Generally, key management is a lifecycle of eight major components as shown in the diagram below.



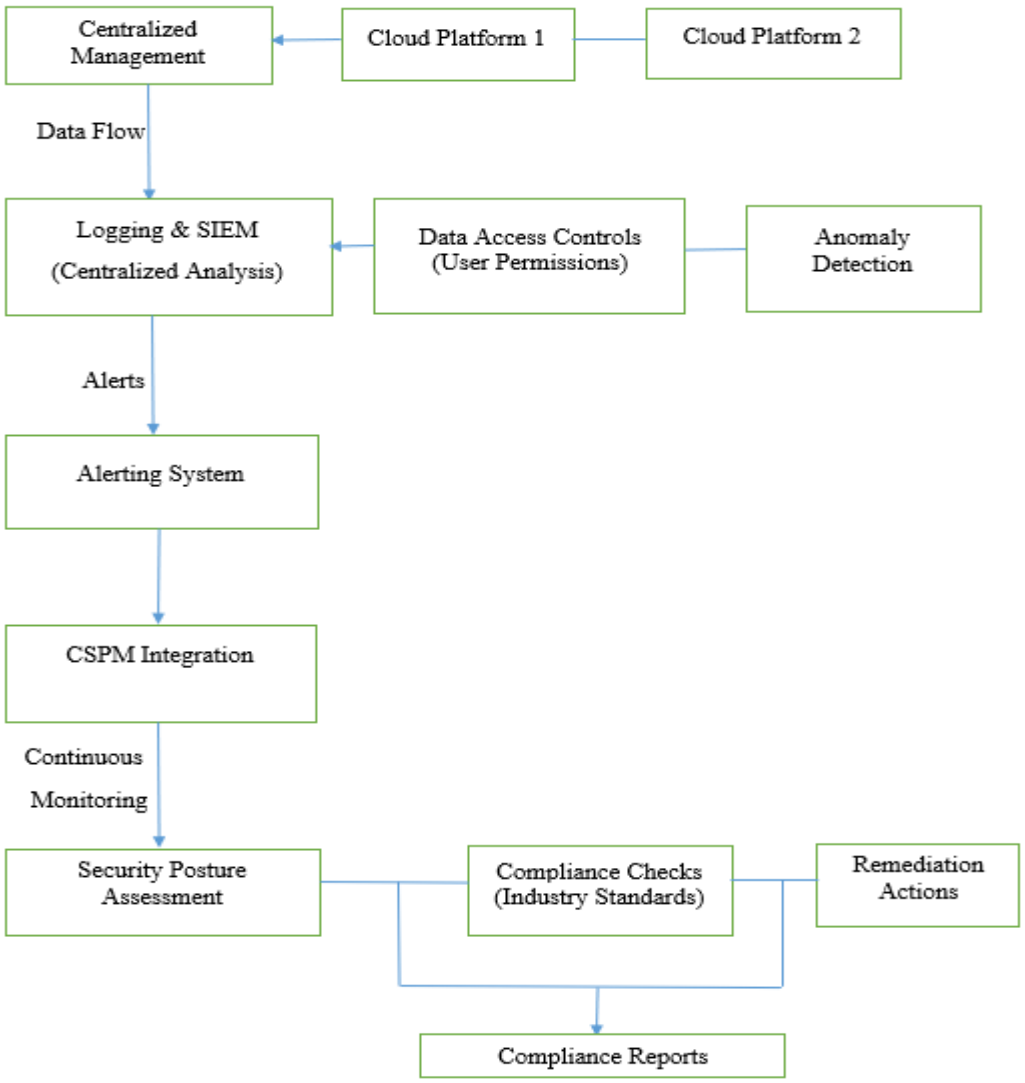
Data Visibility and Monitoring

Another best practice with regard to managing and securing data when using multi-cloud computing is enforcing data visibility and monitoring. This strategy calls for all the activities that involve data to be centralized, hence making it possible to track data access and usage patterns. Tracking access, as well as the usage of data, ensures that any case of anomaly is detected on time [4]. In other words, the centralization of these key security aspects provides the security team with a holistic view of activities in all the cloud platforms utilized by the

organization, hence making it possible to take the right action at the right time in case of anything, say, unauthorized access attempts.

Continuous Monitoring and Compliance Automation

As this discussion has already demonstrated, a multi-cloud environment, while it comes with many benefits, comes with its inherent complexities. Hence, it is possible to put all the above-discussed measures with regard to data security and governance and still, sometimes, fail to catch some anomalies, especially, when the monitoring process is not automated. It is for that reason that it is crucial for organizations to automate continuous monitoring of the security posture across all the cloud platforms they are utilizing. This can be done through cloud security posture management (CSPM) tools. CSPM tools provide organizations with real-time visibility of the data in the cloud platforms, facilitating timely detection of any anomaly and making it possible to remediate security risks before they materialize into real security problems. CSPM tools can be designed in many ways that are in line with the automation of security posture monitoring. For instance, they can assess cloud resources against industry-recognized security standards and certifications, such as CIS Benchmarks or the NIST Cybersecurity Framework, and generate compliance reports. This helps organizations maintain a consistent security posture across their multi-cloud infrastructure. The figure below is a presentation of how data visibility and monitoring architecture can be achieved.



Backup and Disaster Recovery

Another best practice for data governance and security in a multi-cloud environment involves having a reliable backup and disaster recovery strategy in place [12, 19]. Every organization that utilizes multiple cloud computing platforms should invest in having a robust backup and recovery plan that addresses data on all the platforms. The organization, therefore, should have consistent backup policies in place as well as appropriate backup frequencies [10]. Notably, it is not uncommon for even the most robust technology to fail at times; hence, it is important for an organization to have regular testing of the backup and recovery processes to ensure that the working of the processes is assured all the time, avoiding cases of failure, which can occur even in times when the backup resources are needed the most. That said, it is advisable for an organization to consider enhancing its resilience by leveraging cloud-based disaster recovery services [11]. These services often provide advanced features, such as automatic failover and real-time data replication, which are key in ensuring that an organization is able to recover in case of any unexpected event.

Cloud Provider Security Assurance

Data governance and security also require organizations to explore the security posture of cloud service providers. The posture of these service providers indicates how secure the data is within their cloud platform and how effectively users of the platform can manage their data. For this reason, organizations utilizing a multi-cloud computing approach must seek security assurance from their service providers [13], [20]. Ensuring that all providers they engage with possess compliance certifications is crucial, as these certificates indicate adherence to required security and regulatory standards. That said, it is important for organizations to remember that the regulatory standards are always evolving as the technology advances. Therefore, the evaluation process is not a one-time process; it should be ongoing, ensuring that the service providers' compliance with the management and security practices is regularly reviewed. Additionally, it is important for the organization to have clear service-level agreements (SLAs) that address data protection and incident response [14].

Employee Training and Awareness

Employees play a crucial role in data governance and security [15]. The recognition of this truth, therefore, requires the organization to ensure that its workforce is well-trained and security-aware, hence fit to promote effective data governance and security. All organizations using multi-cloud services should provide comprehensive training to all employees on relevant data governance and security practices [16]. That said, some security issues, regardless of how well the organization and its providers have addressed governance and security issues, are set to inevitably happen; therefore, employees should also be trained on timely incident reporting procedures. The organization should ensure that employees at all levels understand the importance of safeguarding sensitive information and their role in maintaining the overall security posture of the multi-cloud infrastructure [17].

Conclusion

In conclusion, a multi-cloud environment is one of the impactful technologies in the business world when it comes to computing. Many organizations are aware of all the benefits that come with this new technology, and over the years, cloud computing has experienced rapid growth and adoption as many organizations shift to it. That said, cloud computing, and particularly multi-cloud computing, comes with a number of governance and security challenges that must be addressed. This paper has discussed many of the best practices that organizations can adopt in managing and securing their data in a multi-cloud environment. Having these practices in place is meant to ensure that organizations are able to leverage all the benefits that come with multi-cloud computing while keeping governance and security issues in check.

Reference

[1]. S. Bowman, "Best Practices for Governance of IT Systems, Applications, and Operations in the Cloud," Sep-Dec. 2016.

https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/21961/Bowman2016.pdf?sequence=1&isAllowed=y

[2]. H. Witti, C. Ghedira-Guegan, E. Disson, and K. Boukadi, "Security Governance in Multi-cloud Environment: A Systematic Mapping Study," IEEE Xplore, Jun. 01, 2016. https://ieeexplore.ieee.org/abstract/document/7557398

[3]. M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Data Governance Taxonomy: Cloud versus Non-Cloud," Sustainability, vol. 10, no. 2, p. 95, Jan. 2018, doi: https://doi.org/10.3390/su10010095.

[4]. M. Al-Ruithe and E. Benkhelifa, "Analysis and Classification of Barriers and Critical Success Factors for Implementing a Cloud Data Governance Strategy," Procedia Computer Science, vol. 113, pp. 223–232, Sep. 2017, doi: https://doi.org/10.1016/j.procs.2017.08.352.

[5]. D. Walkowski, "What Is the Principle of Least Privilege and Why is it Important?," F5 Labs, Dec. 21, 2020. https://www.f5.com/labs/learning-center/what-is-the-principle-of-least-privilege-and-why-is-it-important

[6]. I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," Engineering Science and Technology, an International Journal, vol. 21, no. 4, pp. 574–588, May. 2018, doi: https://doi.org/10.1016/j.jestch.2018.05.010.

[7]. Z. Ch. Oleiwi, W. A. Alawsi, Wisam. Ch. Alisawi, A. S. Alfoudi, and L. H. Alfarhani, "Overview and Performance Analysis of Encryption Algorithms," Journal of Physics: Conference Series, vol. 1664, no. 1, p. 012051, Nov. 2020, doi: https://doi.org/10.1088/1742-6596/1664/1/012051.

[8]. J. Liu, X. Tong, Z. Wang, M. Zhang, and J. Ma, "A Centralized Key Management Scheme Based on McEliece PKC for Space Network," IEEE access, vol. 8, pp. 42708–42719, Jan. 2020, doi: https://doi.org/10.1109/access.2020.2976753.

[9]. M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance," Personal and Ubiquitous Computing, vol. 23, Jan. 2018, doi: https://doi.org/10.1007/s00779-017-1104-3.

[10]. R. Chandramouli and D. Pinhas, "Security Guidelines for Storage Infrastructure," NIST Special Publication 800-209, Oct. 2020, doi: https://doi.org/10.6028/nist.sp.800-209.

[11]. I. Kumar, "Cloud Computing-based Disaster Recovery," Turkish Journal of Computer and Mathematics Education, vol. 11, no. 1, pp. 815–820, Apr. 2020, doi: https://doi.org/10.17762/turcomat.v11i1.13562.

[12]. P. Chandra Srivastava, "Enhancing Cloud Security: The Crucial Role of Third-Party Auditors (TPAs)," April. 2016, doi: https://www.jetir.org/papers/JETIR1701B08.pdf.

[13]. V. Casola, A. De Benedictis, M. Rak, and U. Villano, "A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach," Journal of Systems and Software, vol. 163, p. 110537, May 2020, doi: https://doi.org/10.1016/j.jss.2020.110537.

[14]. J. J. Stephens, “Data governance importance and effectiveness: health system employee perception,” Feb. 2018, doi: https://www.proquest.com/openview/a80278e979fd9c9cc0f99805241401ea/1?pq-origsite=gscholar&cbl=18750.

[15]. S. M. Faizi and S. Rahman, "Securing Cloud Computing Through IT Governance," Jan. 2019, doi: https://dx.doi.org/10.2139/ssrn.3360869.

[16]. K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organizations: a systematic literature review," Computers & Security, vol. 106, no. 1, p. 102267, April. 2021, doi: https://doi.org/10.1016/j.cose.2021.102267.

[17]. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," IEEE Access, vol. 9, no. 1, pp. 1–1, April. 2021, doi: https://doi.org/10.1109/access.2021.3073203.

[18]. A. Bicaku, M. Tauber, and J. Delsing, “Security standard compliance and continuous verification for Industrial Internet of Things,” International Journal of Distributed Sensor Networks, vol. 16, no. 6, p. 155014772092273, Jun. 2020, doi: https://doi.org/10.1177/1550147720922731.