



DATA GOVERNANCE CHALLENGES IN CLOUD-NATIVE AND HYBRID DATA ARCHITECTURES

Danish Ali Syed

PhD (MIS), Girne American University

consultant.danishsyed@gmail.com

ABSTRACT

The growing use of cloud-native and hybrid data architectures has changed the enterprise data ecosystems providing agility and scalability, as well as cost optimization. These environments however raise complicated data governance issues that jeopardize data security and compliance, quality, ownership and financial control. This paper discusses cloud-native and hybrid-specific issues in governance and breaks them into seven dimensions, namely security and privacy, compliance, data quality, ownership and accountability, monitoring, scalability, and cost governance.

The paper presents a comparison of the governance issues in both cloud-native and hybrid settings using an exploratory conceptual approach grounded in secondary data and identify the differences. Results indicate that cloud-native systems have challenges with decentralization, short-lived workloads, and scaling quickly, and systems based on hybrid systems are challenged by their heterogeneity, conflicts between regulations, and cross-border data sovereignty. In its paper, the author suggests a single governance framework with the help of metadata-based solutions, automated compliance, well-defined stewardship patterns, end-to-end observability, FinOps, and adaptive governance facilitated by AI and blockchain. The recommendations are designed to change governance into a compliance-related necessity to the strategic facilitator of trust, accountability, and innovation. These frameworks should be empirically proved by future studies by means of case studies and industry applications.

Keywords

Cloud-native architecture; Hybrid data architecture; Data governance; Compliance; Metadata; Observability; FinOps; Adaptive governance

1. INTRODUCTION

The use of cloud-native and hybrid data structures has been embraced swiftly and it has altered the way organizations design, manage and scale their digital ecosystems. A cloud-native system, which is developed using the concepts of microservices, containerization, Kubernetes orchestration, and serverless computing, allows agility, scalability, and expedited time to market (Dragoni et al., 2017). Concurrently, hybrid data architectures combine on-premises infrastructure with either a single or a mixture of multiple public or private clouds, which offers organizations with the liberty to stabilize security, compliance, and performance requirements (Marston et al., 2011; Hashizume et al., 2013).

There are undeniable benefits associated with these architectures, but these architectures also come with major challenges associated with data governance. The term data governance is used to refer to those policies, processes, and standards that provide the guarantee of the quality,



security, compliance, ownership, and accountability of the data (Alhassan, Sammon, and Daly, 2016). Governance in distributed, multi-cloud, and hybrid environments is complicated by such problems as fragmentation of data flows, the presence of multiple stakeholders, and dissimilar regulatory requirements (Zhang et al., 2022). Security and privacy is one of the key challenges. As information is distributed in hybrid and cloud-native systems, organizations have a wide attacker surface, higher chances of malconfigs, and challenges in providing end-to-end encryption and access control (Hashizume et al., 2013; Fernandes et al., 2014). The other concern touches on the compliance and regulations, particularly where organizations have multi jurisdictions that have different regulations on data protection, sovereignty, and retention (Pearson and Benameur, 2010). As an example, the migration of data between on-premises systems and moving to a number of cloud vendors complicates compliance with GDPR or HIPAA.

No less important are the issues of data quality and consistency. Structured, semi-structured, and unstructured data of various platforms are frequently mixed in hybrid environments, which contributes to the challenges of metadata management, schema development, and real-time synchronization maintenance (Batini and Scannapieco, 2016). Equally, the problem of ownership and accountability of data arises due to the fact that under the shared responsibility model, ownership, as well as the responsibility of governance, is divided between organizations and cloud providers (Goyal, 2014). However, in spite of the realization of these problems, the current governance frameworks do not generally offer complete solutions to cloud-native and hybrid ecosystems. The issues raised by research include inability to be interoperable, vendor lock-in, and ineffective governance of the non-functional requirements (security, availability, auditing) in multi-cloud environments (Vega et al., 2018; Zhang et al., 2022). Furthermore, the challenge of cost governance has not been studied extensively, and companies find it difficult to trace the financial consequences of governance implementation (data storage, transfers, and monitoring), in hybrid infrastructures (Gaw and Wolski, 2019). The paper will seek to fill these gaps by critically analyzing the problem of data governance in cloud-native and hybrid data architecture. Specifically, it seeks to:

1. Identify and categorize the governance challenges unique to cloud-native and hybrid environments.
2. Compare how these challenges differ across pure cloud-native, hybrid, and multi-cloud setups.
3. Propose recommendations or a governance framework to guide organizations in managing these challenges effectively.

The rest of the paper is organized as follows: Section 2 is a review of the existing literature on the topic of cloud-native and hybrid architecture and data governance models. Section 3 indicates the methodology used in the research. Section 4 gives the analysis of major governance issues. In section 5, the findings and recommendations are discussed. Lastly, Section 6 ends with conclusions and future research recommendations.

REVIEW OF LITERATURE

The emerging notion of data governance has received more and more interest as organizations shift to distributed digital ecosystems. Khatri and Brown (2010) have explained that data



governance is the general framework that outlines roles, duties, and procedures of proper management of the data assets. In the contemporary world, this governance should be reexamined to meet the needs of the fast proliferation of cloud-native and hybrid infrastructures.

Cloud-Native Architectures and Governance

Cloud-native systems are based on the principles of containerization, orchestration and DevOps, which focus on scalability, resilience and continuous integration/deployment. Although these paradigms are fast in transforming new inventions, they tend to decentralize data. According to Kalske, Mäkitalo, and Mikkonen (2017), microservice-based systems are flexible systems that make it difficult to trace ownership of data and its traceability because data storage is fragmented.

In a similar manner, Soldani, Tamburri, and Van den Heuvel (2018) emphasize that control of cloud-native architecture demands dynamic (instead of static) monitoring tools that are able to control distributed and volatile resources. It has also been proposed through research that automation is a two-sided sword in cloud-native data governance. Though automated orchestration provides agility, it also has the propensity to spread policy wrongs to a variety of services (Villamizar et al., 2016). Thus, the control in this kind of setting should not be limited to the elements of static controls, but dynamic compliance and observability should also be involved in the governance.

Hybrid Data Architectures and Governance

Hybrid data environments are resources based on on-premises and clouds with the goal to maximize both control and flexibility. Nonetheless, according to Chang et al. (2016), hybrid models make things more complex since information flows through a heterogeneous platform with different compliance and operation standards. This complexity has some consequences in relation to maintaining a consistent governance in different environments. The research on the adoption of hybrid clouds highlights the problem of data sovereignty.

As an example, Géczy, Izumi, and Hasida (2012) note that cross-border data flow represents conflicting regulatory demands, especially in those areas where privacy laws are highly developed, like the EU, the APAC. Similarly, Wu, Garg, and Buyya (2011) highlight that it becomes challenging to build trust and accountability relationships between enterprises and cloud providers in case there is fragmentation in governance roles.

Governance Dimensions in Distributed Environments

Literature has observed that there are various aspects of governance of distributed data architecture. According to Otto (2011), governance maturity models, which emphasize data quality, metadata, and stewardship are important constituents. Expanding on the same view, Tallon, Ramirez, and Short (2013) believe that the governance in the cloud era should be highly aligned with the business strategy particularly on risk management and compliance. New studies position big data governance as an element of hybrid environments.

Lee, Madnick, Wang, and Zhang (2015) state that the speed and diversity of data in the hybrid system makes the issue of governance more significant, especially the data provenance and



lineage. Hildebrandt and Kolb (2015) also highlight that it is necessary to have metadata-based governance in terms of interoperability and auditability on different platforms.

Gaps in Current Literature

Although there is ample research on either cloud-native or hybrid governance, and on all, there is a paucity of studies that can combine these two viewpoints in a complete framework. The current studies have concentrated on security and compliance only, thus other aspects of governance, including cost governance, observability in real-time, and automated governance powered by AI, are under-researched.

Moreover, according to the authors, Schempp, Krcmar, and Wortmann (2018) observe that the systematic approaches are required to be dynamic enough to adapt the governance policies whenever organizations transfer workloads between hybrid and multi-cloud environments.

Research Methodology

The study will rely on a qualitative and conceptual approach to examine the issue of data governance in cloud-native and hybrid data architectures.

The methodology would be systematic in identifying, categorizing and analyzing the governance issues both in the technological as well as organizational perspectives.

Research Design

The research design adopted is exploratory research design because the aim of the research is to develop a better understanding of the issue of governance as opposed to testing a particular hypothesis.

The exploratory design allows flexibility in the analysis of different aspects of governance including security, compliance, data quality, accountability and cost management.

Data Collection

Secondary data collection is the main foundation of the paper and it was composed of extensive review of academic journals, conference proceedings, industry reports and white papers.

These can be technology standards, documentation by cloud provider or reports by international organizations. There is the assurance of the possibility of capturing both the theoretical perspectives and practical practices.

Analytical Framework

The analysis involves three key stages:

1. **Identification of Challenges** – Data governance challenges are identified by synthesizing insights from literature and industry sources related to cloud-native and hybrid architectures.
2. **Categorization** – Challenges are grouped into major dimensions such as security, compliance, data quality, ownership, auditing, and cost governance.
3. **Comparative Analysis** – The identified challenges are analyzed to understand how they differ across cloud-native, hybrid, and multi-cloud environments.

Scope and Delimitations

The research problem addressed in the study is the issue of governance at both infrastructure and data management tiers of cloud-native and hybrid systems. It does not have detailed technical implementations of particular governance tools and vendor specifications. It is meant



to be a conceptual framework and practical suggestions to organizations, as opposed to an empirical statistical analysis.

Ethical Considerations

As the research relies solely on secondary sources, no direct ethical risks such as human subject involvement arise. However, care has been taken to ensure that all sources are credible, accurate, and relevant to the research objectives.

KEY DATA GOVERNANCE CHALLENGES IN CLOUD-NATIVE AND HYBRID DATA ARCHITECTURES

1. Security and Privacy

Security is the hottest issue of governance in distributed architectures. Cloud-native systems are based on microservices and containerized workloads, both of which can demonstrate a certain vulnerability unless properly configured. The issue is also exacerbated in a hybrid environment since data moves both inside on-premises and cloud providers and increases the attack surface. Weak access policies, misconfigurations and the lack of encryption pose the threat of unauthorized access and breaches. Furthermore, the compliance complexity may be further complicated by privacy requirements, which are imposed by regulations like GDPR and CCPA (Subashini and Kavitha, 2011; Takabi, Joshi, and Ahn, 2010).

2. Compliance and Regulatory Requirements

Multi-region organizations are required to meet different regulatory requirements such as data residency, data sovereignty, and others. This is made complicated with hybrid architectures since sensitive data can cross international borders, as workloads are dynamically moved between cloud and on-premises systems. The implementation of a standardized compliance on a disparate platform is a big gap. As an example, it becomes hard to guarantee the auditability and demonstrate compliance to authorities as long as the data is stored on a set of environments simultaneously (Dutta, Peng, and Choudhary, 2013; Shih and Lin, 2019).

3. Data Quality and Consistency

In cloud-native systems, independent data stores are common in the decentralized micro services hence it is not easy to impose any standards of data quality. The hybrid system is yet another complexity, which would require structured data in the traditional relational databases to live with unstructured or semi-structured data delivered by the cloud-based analytics systems. This produces governance loopholes in accuracy, completeness, and timeliness of information. It is also worsened by the absence of a common metadata strategy, leading to further inconsistency and data assets duplication (Abadi, 2009; Fan and Geerts, 2012).

4. Data Ownership and Accountability

The data ownership and data accountability in the shared responsibility model of cloud providers is blurred. Though cloud vendors take care of physical infrastructure, business organizations are left with the responsibility of safeguarding their data. A hybrid architecture does not have a single service provider with control over this and internal teams, and this ambiguity on stewardship does not aid in establishing a single team in charge. This ambiguity complicates the process of holding individuals responsible in case of failures in governance,



particularly when there is a security breach or data loss (Rimal, Jukan, Katsaros, and Goeleven, 2011; Youssef, 2012).

5. Monitoring and Auditing

Constant monitoring and audit are important aspects of data governance. In cloud-native and hybrid environments, however, companies are facing the challenge of poor visibility across a multiplicity of environments. The traditional audit logs can be spread among vendors which makes it hard to have end-to-end traceability. There are also automated observability tools, which are seldom interoperable across providers, and which introduce a blind spot in the governance oversight (Ko et al., 2011; Aceto, Botta, De Donato, & Pescape, 2013).

6. Scalability and Performance Governance

Cloud-native systems are created with the ability to scale elastically, but the governance structures tend to lag in the implementation of dynamic scaling. Consider the case wherein the policy that applies to a static on-premise setting might fail to adapt to the large-scale workloads in the cloud. Hybrid systems also make the performance governance a little more complicated as there is latency, and resource distribution involves the processes operating either locally or in cloud environments. It is also important to make sure that the governance controls do not hinder the scalability (Zhang, Cheng, and Boutaba, 2010; Jennings and Stadler, 2015).

7. Cost Governance

Although one of the main reasons of cloud adoption is cost optimization, data-related costs governance is still underdeveloped. Hidden costs in data egress, replication and compliance auditing are the common effects of hybrid deployments. Organizations can not manage soaring costs incurred in the implementation of governance policies in the environments without effective monitoring frameworks. Cost governance is thus a highly important yet underresearched subject of academic and industrial literature (Lehrig, Eikerling, and Becker, 2015; Mazrekaj, Rrustemi, and Ajdari, 2016).

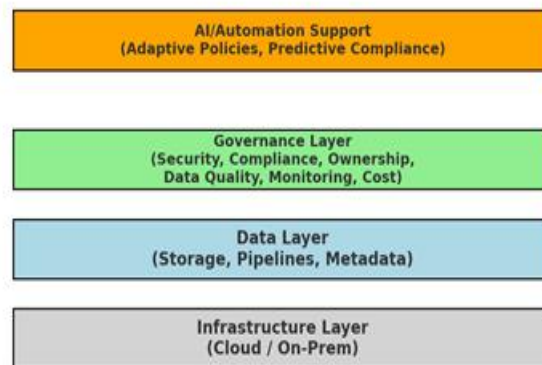
Table 1: Comparison of Governance Challenges in Cloud-Native and Hybrid Architectures

Governance Dimension	Cloud-Native	Hybrid	Impact Level
Security & Privacy	Container misconfigurations, API vulnerabilities	Cross-border data transfer risks	High
Compliance	Dynamic workloads hard to regulate	Conflicting jurisdictional laws	High
Data Quality	Microservices with fragmented stores	Heterogeneous on-prem + cloud systems	Medium
Ownership	Shared responsibility with cloud vendors	Ambiguity across multiple providers	High
Monitoring	Difficult in ephemeral workloads	Fragmented audit trails across platforms	High



Cost Governance	Unpredictable elastic scaling	Hidden egress & integration costs	Medium
------------------------	-------------------------------	-----------------------------------	--------

Figure 1: Conceptual Framework for Data Governance in Cloud-Native and Hybrid Architectures



DISCUSSION AND RECOMMENDATIONS

Discussion

The comparison of governance issues of the cloud-native and hybrid data architectures has shown that both paradigms have similar problems however, the type and level of these problems are different.

The problems of governance in cloud-native systems are mostly connected with the concepts of decentralization and scalability. Microservices and containerized workloads are flexible and cause data fragmented ownership and monitoring problems. The dynamism in cloud-native workloads also makes the traditional ways of the governance mechanism difficult, since policies need to evolve dynamically on a real-time basis.

Hybrid data architectures, however, create the complexities of governance because they are heterogeneous and decentralized on-premises and in the cloud. In the context of hybrid environments, regulatory compliance and data sovereignty are especially challenging since information tends to cross-organizational and geographical borders. In addition, there is a consistency issue of quality, metadata and lineage that has not been addressed in hybrid platforms.

The other area of differentiation is in cost governance. Elastic scaling can impose unpredictable costs on cloud-native systems, whereas hybrid systems have hidden costs, including integration, data migration and compliance audits of multi-platform compliance. Therefore, whereas cloud-native issues are dynamic and operational, hybrid ones tend to be structural and regulatory.

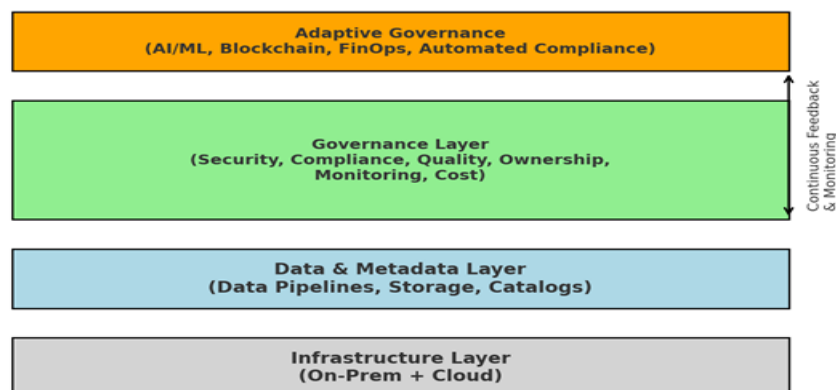
Lastly, the two models emphasize the inefficiency of current systems of governance. The existing practice commonly takes security and compliance dimensions and implies that the other equally relevant dimensions like real time observability, clarity of ownership and accountability are overlooked. This implies that there is a necessity to have more holistic and adaptive governance structures.



Table 2: Existing vs. Proposed Governance Approaches

Governance Dimension	Existing Approaches	Proposed Approaches (This Study)
Security & Privacy	Vendor-provided security controls; manual access policies	Unified policy enforcement across platforms; AI-driven anomaly detection
Compliance	Periodic/manual audits; region-specific compliance checks	Automated compliance monitoring; dynamic regulatory mapping
Data Quality	Ad-hoc data cleaning; decentralized quality controls	Centralized metadata-driven governance; enterprise-wide data catalogs
Ownership & Accountability	Shared responsibility model, often unclear	Clearly defined stewardship roles; governance charters and SLAs
Monitoring & Auditing	Fragmented logs across multiple platforms	End-to-end observability dashboards; blockchain-based audit trails
Cost Governance	Reactive cost tracking; limited financial oversight	Proactive FinOps practices; predictive cost governance models
Adaptability	Static policies; slow to respond to changes	Adaptive governance models powered by AI/ML

Figure 2: Proposed Unified Governance Model for Cloud-Native and Hybrid Architectures



Recommendations

To address these gaps, the following recommendations are proposed:



1. Unified Governance Framework

Organizations are to strategize to use a cohesive governance model across cloud based and hybrid infrastructure. This model must combine data quality, security, ownership, and compliance policies into one level of governance. Platform-agnostic or cloud-agnostic orchestration technologies (such as: Kubernetes with policy engines such as OPA - Open Policy Engine) may be used to enforce them uniformly across environments.

2. Metadata-Driven Governance

Metadata is to be regarded as the first-class citizen in terms of governance strategies. The use of centralized metadata repositories and data catalogs can improve enterprises in their visibility of data lineage and provenance and compliance status. Metadata-based solutions are also useful to provide automated auditing as well as to ease interoperability across platforms.

3. Automated Compliance and Policy Enforcement

The cloud-native and hybrid systems cannot be checked out in terms of compliance manually. The organizations need to take advantage of automation and AI-driven software to perform constant checks of compliance. Such tools have the ability to dynamically issue access policies, monitor the violation in real time and automatically report compliance to regulators.

4. Clear Data Ownership and Stewardship Models

Enterprises need to clarify the role of data stewardship by defining it clearly. The governance charters must determine who is responsible in security, quality, and compliance under varying teams and vendors. It is also important to make service-level agreements with cloud providers that explicitly define the role of governance.

5. Observability and Auditing Enhancements

End-to-end observability platforms investment can be used to address blind spots in hybrid and multi-cloud deployments. Integrated dashboards with logs, metrics, and traces between environments help to offer more oversight to auditors and governance teams. Audit trails are a new system of blockchain that can provide unchangeable and verifiable governance records.

6. Cost Governance Mechanisms

To manage the cost associated with governance, enterprises must adopt FinOps practices which is an art that involves integrating financial management and DevOps. It is necessary to monitor the costs of data storage, transfer, and compliance on a regular basis. Predictive models and cost dashboards may be utilized to predict the presence of financial risks in terms of scaling workloads or implementing governance policies.

7. Adaptive Governance Models

Lastly, the governance structures must be flexible and responsive, and be able to keep pace with technology. The use of AI/ML in detecting anomalies, predicting compliance, and automatic adjustment to policies can contribute to the organization responding appropriately to the dynamic environment of cloud-native and hybrid architecture.

Implications

When they adopt these suggestions, organizations will be in a position to change governance as a compliance-based function to a strategic facilitator. By operating on unified frameworks, metadata-driven visibility, and automated compliance, enterprises can make sure that data is



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

both trustworthy, secure and cost-efficient, whether it is in cloud-native systems, in a hybrid infrastructure or even in a multi-cloud environment.

CONCLUSION

The growing trend in the use of cloud-native and hybrid data architectures has radically transformed how organizations store, operate and use data. Although such paradigms provide scalability and agility, as well as cost optimization, they also introduce the significant issue of data governance. As it has been pointed out in this paper, these issues are multifaceted in nature and can be characterized through security and privacy threats, complexities in compliance, inconsistencies in data quality, ambiguity in ownership, gaps in monitoring, performance governance, as well as the cost management issues.

The comparative analysis reveals that the major issues facing cloud-native architectures are those of decentralization, dynamic scaling, and the fleeting workloads whereas the additional challenges facing the hybrid architectures are those of heterogeneity, regulatory compliance, and data sovereignty. Regardless of those distinctions, the two models have demonstrated that existing governance practices are fragmented as they tend to be strictly focused on security and compliance without considering other aspects of observability, cost governance, and adaptive policies.

The suggestions made in this document come up with a holistic and integrated mode of governance. Through metadata-based governance, automated compliance management, well-defined stewardship frameworks, end-to-end observability, and cost governance systems, organizations can cease to govern through a compliance-based approach and adopt a more strategic and value-creating model of governance. Additionally, AI/ML-driven adaptive governance can be used to make sure that governance policies change in accordance with the technological progress and the needs of the organization.

Limitations

The research is grounded on a conceptual and a secondary data review, which implies that the results are restricted to the literature and industry reports. In that regard, it lacks empirical evidence based on primary data, including organizational case studies, survey, and experiments. This restricts the possibility of generalizing results to industries or regions.

Future Research Directions

Future research should focus on:

1. Empirical validation of governance frameworks through case studies in industries such as healthcare, banking, and government.
2. Quantitative models for cost governance in hybrid systems, including predictive analytics for compliance-related expenditures.
3. Technology-specific governance models, for example, frameworks tailored for Kubernetes, serverless platforms, or edge-cloud hybrids.
4. Cross-border governance strategies, particularly in contexts involving conflicting data protection and sovereignty laws.
5. Exploration of AI-driven governance systems that can dynamically adapt policies and automate compliance with minimal human intervention.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

Following such directions, researchers and practitioners may work on building stronger frameworks, which will not only eliminate threats but also turn governance into a source of trust, innovation, and competitive edge in cloud-native and hybrid ecosystems.

REFERENCES

- Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: An analysis of the literature. *Journal of Decision Systems*, 25(1), 64–75.
- Batini, C., & Scannapieco, M. (2016). *Data and information quality: Dimensions, principles and techniques*. Springer.
- Dragoni, N., et al. (2017). Microservices: Yesterday, today, and tomorrow. *Present and Ulterior Software Engineering*, 195–216.
- Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, 13(2), 113–170.
- Gaw, N., & Wolski, R. (2019). Cloudsweeper: Enabling cost-effective data governance in the cloud. *Proceedings of the ACM Symposium on Cloud Computing*, 1–13.
- Goyal, S. (2014). Public vs. private vs. hybrid vs. community—Cloud computing: A critical review. *International Journal of Computer Network and Information Security*, 6(3), 20–29.
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 5.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176–189.
- Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702.
- Vega, R., De la Torre, D., & Moctezuma, L. (2018). Challenges and opportunities of multi-cloud governance. *International Conference on Cloud Computing and Services Science*, 77–87.
- Zhang, Y., Chen, L., Wang, Y., & Li, Y. (2022). A survey of multi-cloud management: Taxonomy, challenges, and opportunities. *Journal of Cloud Computing*, 11(1), 1–21.
- Chang, V., Walters, R. J., & Wills, G. B. (2016). Organisational sustainability modelling—An emerging service and analytics model for evaluating Cloud Computing adoption with two case studies. *International Journal of Information Management*, 36(1), 167–179.
- Géczy, P., Izumi, N., & Hasida, K. (2012). Hybrid cloud management: Foundations and strategies. *IEEE Internet Computing*, 16(6), 22–32.
- Hildebrandt, T., & Kolb, S. (2015). Big data governance: A framework for data-driven decision-making. *Proceedings of the International Conference on Big Data Analytics*, 39–50.
- Kalske, M., Mäkitalo, N., & Mikkonen, T. (2017). Challenges when moving from monolith to microservices. *Proceedings of the International Conference on Cloud Computing and Services Science*, 153–160.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

- Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, 53(1), 148–152.
- Lee, Y. W., Madnick, S., Wang, R. Y., & Zhang, H. (2015). A cubic framework for big data governance. *Proceedings of the International Conference on Information Quality*, 1–13.
- Otto, B. (2011). A morphology of the organisation of data governance. *Proceedings of the International Conference on Information Systems*, 1–20.
- Schempp, T., Krcmar, H., & Wortmann, F. (2018). Cloud governance: Balancing control and flexibility in cloud service consumption. *Journal of Cloud Computing: Advances, Systems and Applications*, 7(1), 1–17.
- Soldani, J., Tamburri, D. A., & Van den Heuvel, W. J. (2018). The pains and gains of microservices: A systematic grey literature review. *Journal of Systems and Software*, 146, 215–232.
- Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, 30(3), 141–178.
- Villamizar, M., et al. (2016). Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud. *Proceedings of the IEEE 8th International Conference on Cloud Computing*, 593–600.
- Wu, L., Garg, S. K., & Buyya, R. (2011). SLA-based resource allocation for software as a service provider (SaaS) in cloud computing environments. *Proceedings of the International Conference on Cloud and Service Computing*, 195–202.
- Abadi, D. J. (2009). Data management in the cloud: Limitations and opportunities. *IEEE Data Engineering Bulletin*, 32(1), 3–12.
- Aceto, G., Botta, A., De Donato, W., & Pescapé, A. (2013). Cloud monitoring: A survey. *Computer Networks*, 57(9), 2093–2115.
- Dutta, A., Peng, G. C., & Choudhary, A. (2013). Risks in enterprise cloud computing: The perspective of IT experts. *Journal of Computer Information Systems*, 53(4), 39–48.
- Fan, W., & Geerts, F. (2012). *Foundations of data quality management*. Morgan & Claypool.
- Jennings, B., & Stadler, R. (2015). Resource management in clouds: Survey and research challenges. *Journal of Network and Systems Management*, 23(3), 567–619.
- Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. *Proceedings of the IEEE World Congress on Services*, 584–588.
- Lehrig, S., Eikerling, H., & Becker, S. (2015). Scalability, elasticity, and efficiency in cloud computing: A systematic literature review of definitions and metrics. *Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures*, 83–92.
- Mazrekaj, A., Rrustemi, V., & Ajdari, J. (2016). Cost governance challenges in cloud computing: A business model perspective. *International Journal of Computer Applications*, 150(4), 30–36.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

- Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y. (2011). Architectural requirements for cloud computing systems: An enterprise cloud approach. *Journal of Grid Computing*, 9(1), 3–26.
- Shih, D. H., & Lin, B. (2019). A governance framework for hybrid cloud service management. *Information Systems Management*, 36(3), 206–220.
- 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.
- 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.
- Youssef, A. E. (2012). Exploring cloud computing services and applications. *Journal of Emerging Trends in Computing and Information Sciences*, 3(6), 838–847.
- Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18.