ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

JOURNAL OF APPLIED LINGUISTICS AND TESOL (JALT)

Vol.8.No.1 2025

DATA EXPOSURE RISKS IN HYBRID VS. MULTI-CLOUD MIGRATIONS: A COMPARATIVE ANALYSIS

Abubakar Sadique[1], Hijab Sehar[2], Suhaib Nasim[1], Fawad Nasim[1]
[1]Department of Computer Science, The Superior University, Lahore, 54000, Pakistan.
[2]Riphah School of Computing and Innovation, Lahore

Abstract

Hybrid and multi-cloud have increasingly emerged as a dominant trend of adopting better flexibility, scalability and control for data among organizations. A hybrid cloud is a combination of on-premise hardware or software with the more flexible and open public and/or private clouds, covering a range of options for workloads based on data sensitivity, regulatory constraints, and case of operation. While multi-cloud architectures split resources among multiple Providers, multi-cloud in turn restricts businesses from vendor lock-in, offering flexible services to different workloads. Nevertheless, all methodologies present a different level of data exposure which may compromise the integrity, privacy, and security of data.

This research takes a look at the challenges associated with migrating into hybrid and later multi-cloud, comparing the self-evident risks to data exposure that arise from each approach. Data transfer between on-premises and cloud environments is a common problem for hybrid cloud models, which combined with misconfigurations and uneven access policies, increases the risk of breaches. On the other hand, security policy management for multi-cloud setups becomes too cumbersome to handle on a single environment and often lead to security gaps and more compliance issues. Risking these factors are very important as firms shape migration to the cloud strategies. In this paper, we are interested in understanding the best security practices and mitigation approaches so that we can provide practical insights to companies looking at how to protect sensitive data and how to make an educated choice on a cloud migration strategy.

Keywords
Data Exposure risks, Hybrid-cloud security, Multi-cloud security, Cloud migration strategies, Security challenges in cloud

1. Introduction:

Over the recent decade, cloud computing has drastically altered how businesses manage and extend their IT infrastructure, turning away from the usual on-premises models and against the better judgment, moved to more flexible, cloud-based solutions. The main driver for this transition has been to increase scalability, cost efficiency, and agility (Malallah et al., 2023). With enterprises becoming increasingly dependent on data-driven decision-making cloud solutions offer the right infrastructure to handle tremendous amounts of data while being able to scale resources up and down based on demand. But for many enterprises, a single cloud provider or even fully public clouds will not create enough good fit to accommodate all of their operational, regulatory, and security requirements; hybrid and multi-cloud solutions are the norm. When it comes to a hybrid cloud approach, businesses can combine their on-premise infrastructure with one or more public and private clouds. The availability of this strategy means that businesses can enjoy the same scalability and cost benefits of the cloud, without exposing sensitive data, or even certain applications, to the cloud environment for regulatory reasons or legacy system dependency. In contrast, methods for multi-cloud providers (multi-cloud) imply the use of various cloud providers as a means to reduce dependence on a single vendor and take advantage of cloud utilization based on the requirements or costs of an application workload (Tummalachervu & Kanth Tummalachervu, 2023).

The motivation behind using these mixed models is indirect. Companies that use hybrid cloud gain more control over data location and regulatory compliance, most importantly in industries such as banks, healthcare, and government where data sovereignty is vital. With multi-cloud, they can choose between several providers based on its capability and balance performance pricing and redundancy. Also, this method is resistant as it distributes the workloads throughout several clouds, making it unlikely that downtime is due to the failure of a single provider. Both models enjoy several benefits but also have considerably different security data security risks to consider for each paradigm, necessitating a careful analysis and mitigation of data security exposure issues with each paradigm. On any shift to cloud, whether any of it to cloud, to hybrid, to multi-cloud, the responsibility for the security of your data becomes a top responsibility. After any cloud migration, there’s the chance to continue transferring data from one place to another, expanding the options for potential exposure. Data moves all over the place in hybrid and multi-cloud environments where data is constantly flowing across so many platforms, obviously complicating things when it comes to secure data flow, consistent access, rules, and compliance. Failure to take proper care of these data exposure risks can incur tremendous consequences, like data breaches, regulatory sanctions, bad publicity and fiscal loss (Patil & Desai, n.d.).

Ensuring the life of your confidential data from storage to its transmission to its access is one of the most difficult pieces of cloud migration. There are sensitive data especially which is personally identifiable information (PII), financial records and intellectual property which have to be defended from unwanted access as well as even leakage. At the same time, hybrid and multi-cloud architectures are composed of providers with diverse security standards and varying compliance requirements to which different groups apply, thus leaving data protection holes if not handled carefully (Oluwafemi Clement Adeusi et al., 2024). The increased sophistication of cyber threats targeting cloud infrastructure, that attack the cloud infrastructure, in turn adversely impacts data exposure risks in the cloud;

1) Attacks against cloud infrastructure exposing configuration problems
2) Attacks based on identity and access management (IAM) weaknesses
3) Attacks based on unsecured application programming interfaces (APIs)

If all clouds have different vulnerabilities, then each cloud environment would need its own security layer tailored to migration model. Responding to all the horizontal risks pertaining to unauthorized data access is critical, not only to stop, avoid unauthorized data access, but also to keep consumer confidence high, legal compliance, and the organization’s reputation. In this context, any organization whose decision or process of cloud migration includes consideration of data exposure risks needs to take a targeted approach to evaluate, manage, and reduce the risk of data exposure.

Hybrid cloud migration:

A hybrid cloud modeling approach incorporates traditional on-premises IT infrastructure with cloud based resources, in which an organization accesses a mix of both private and public cloud services to meet its specific operating necessities. The combination of a private cloud or a specialized private environment together with one or more public cloud services such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud comprise this system. With this combination, businesses can host sensitive data domestically, while taking advantage of the low cost scalability public cloud environments provide, for the remainder of their applications(Hosseini Shirvani et al., 2022). It may be able to immediately shift the workload to the public cloud if the workload exceeds the available resources. Cloud bursting is also called an add-on technology that can extend scalability of services on the demand. This will free the storage, computing, and other capacity will be nearly limitless and can be handled with the public cloud(© *2024 Zhongbo Zhu*, 2024).

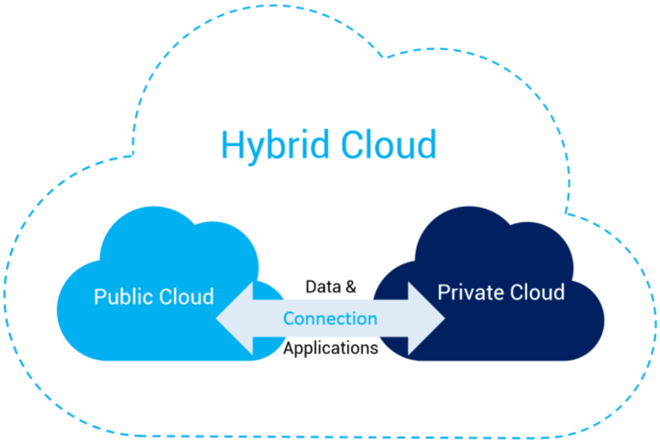

Fig 1. Connection between private and public cloud

There are two main methods to connect public cloud and private cloud: VPN along with Express Connect (point to point dedicated connection). This is where the major benefit of a hybrid cloud approach comes in — Enterprises have the ability to manage exactly where and how their data is located and how secure it is. By having sensitive or regulated data in a private environment (e.g. organization owns the security parameters), security is monitored directly on the organization's side. It’s especially useful when dealing with areas of strict data protection rules, like banking, healthcare, and government among other places, because any data breach can result in severe legal and reputation backlashes(El-Attar et al., 2021).

Multi cloud migration:

Multi cloud is the combination of services from different cloud provider to achieve better performance, greater flexibility, lower the risk of being on one vendor. This method helps companies to choose the best services according to their requirements, public, private and hybrid cloud solutions(Clearlake & Engineering, 2021). Where many suppliers are used, businesses can improve operational efficiency, save on competitive pricing and prevent vendor locked in to costly production. The multi cloud architecture is used to increase dependability and disaster recovery. If anyone provider goes down they can assure business continuity by distributing workloads across many of the cloud environments.

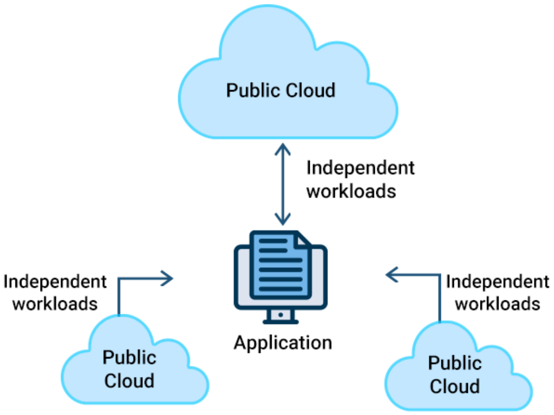

Fig 2. Distribution of workloads

While hybrid and multi cloud systems have many advantages, these come with unique data exposure problems. Data exposure in cloud systems is caused by misconfiguration, security rule inconsistency, unwanted access and weak data transmission methods(Imran et al., 2020).

There are complexities inherent in managing data across potentially disparate environments (hybrid models) or vendors (multi cloud models) which make it difficult to provide consistent, comprehensive security. Data transfer risks in hybrid cloud environments arise when network vulnerabilities, insufficient encryption or configuration issues allow data exposure when data is transferred between on premises infrastructure to the cloud. Yet, the multi cloud solutions are challenged to implement consistent security rules to various platforms leading to the vulnerability or exposing the data to risk as there are differences in the same security requirements and the gaps in the same cross cloud data management.

2.1 Objectives:

The objectives of this comparative analysis on data exposure risks in hybrid and multi-cloud migrations are to:

1. Examine the unique data exposure risks of hybrid and multi cloud strategies and identify.
2. Understanding the security challenges associated with each model, that is, data transfer, access control, etc.
3. Evaluate the effectiveness of existing mitigation techniques in an area along these cloud migration approaches.

2.2 Research questions:

1. For hybrid and multi cloud migration strategies what are the concrete data exposure concerns?
2. What happens to security controls and compliance requirements when we are moving to hybrid to multi-cloud?
3. What are the key weaknesses in how data flows and to integrate between on premises and cloud infrastructures?

2. Literature review:

Initiative use of cloud computing has been on the rise, and their dependence on hybrid and multi-cloud solutions to optimize infrastructure, get more flexibility and avoid vendor lock-in continues to grow. However, these mobility choices come with unique hurdles, in particular regarding the hazards of data exposure.

Hybrid architecture’s public and private cloud components must interoperate and collaborate well. Thus, organizations must support equipment with dependable and secure network connectivity; low latency and high bandwidth to support smooth data interchange while supporting application performance in hybrid environment(Gawande, 2024).

This might involve developing powerful data synchronization methods, constraining data accessibility and having a coherent outlook of data resources across public and private cloud parts. For the operational and managerial challenges of hybrid cloud data, there is the need for good data management solution both in structures and software’s(Gawande & Gorde, 2024).

There could be various situations when enterprises require utilizing cloud environments as an extension of enterprise-owned or legacy structures. Cloud hybrid integration utilizes technologies including Virtual Private Networks; direct connect facilities and cloud integration software to smoothly transfer data and resource from on-premise and cloud environments(Gawande, 2024).

Multi-cloud environments refer to consolidation of various services from different clouds from different providers. It is aiming at minimization of the risks associated with the creation of vendor lock-in, duplicity in systems and exploitation of performance benefits provided by the array of cloud services. Multi-cloud systems be highly effective due to their flexibility and redundancy, however, these systems create significant management and orchestration challenges (Sekar, 2024).

In this multi tenancy the users have no control on infrastructure and this can cause fear of data security, compliance and performance. Hybrid cloud architecture creates a dynamic environment for cloud computing intended to balance the advantages of private and public installations. In a hybrid cloud setup, a company uses a private cloud for very specialized, very sensitive functions that require a very high level of security, and control, and a public cloud for things that work better with scalability and cost effectiveness. In a hybrid cloud, the private and public cloud parts keep working separately but are joined by a health of technologies for smooth hops between data and application (Seth et al., 2024).

Simply while the idea of comprehensive data flow with centralized control between on-premises and the cloud may sound great in principle, in practice hybrid clouds focus on unified workflows and security rules between on-premises and the cloud. Diversifying their cloud resources, multi-cloud setups, enable enterprises on the one hand to rely on different cloud resources without a lot of integration, while having each cloud providing capabilities with respect to specific applications and following its own security and the administration rules. Different architecture presents unique advantages and challenges in data management, scalability and security, which specifically influence the corporate cloud migration plans according to the specific operational demands and risk profile.

3.1 Data Exposure Risks in Hybrid Cloud Migrations

While flexible and scalable, hybrid cloud migrations bring great data exposure owing to the complexity of connecting on-premises and cloud systems Fig 3. Data transfers between private, on premises, systems and public cloud services is one of the main things that people are concerned with. If these transfers are not protected, they can be hijacked and potentially cause data breaches. In simple terms, the most common vulnerability to expose your sensitive data in transit is unsecure APIs, lack of adequate encryption mechanisms, and poor network segmentation(Geczy et al., 2013). These risks are only further exacerbated by misconfigurations, like restricting access for important systems to parties that don't have the authority to access them.

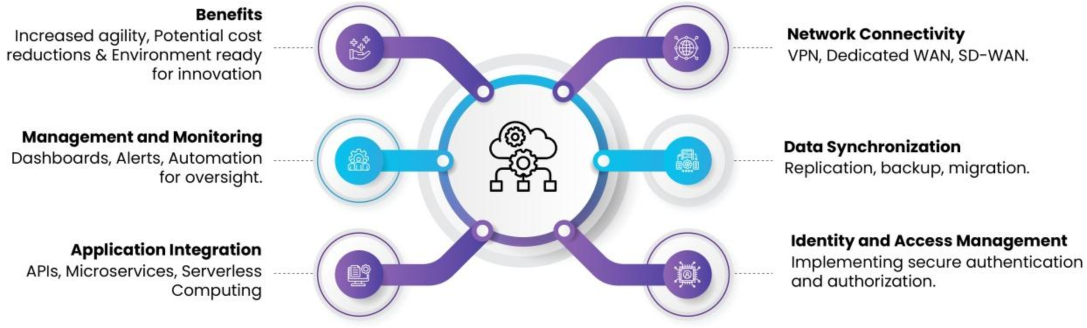
Benefits
Increased agility, Potential cost reductions & Environment ready for innovation
Management and Monitoring
Dashboards, Alerts, Automation for oversight.
Application Integration
APIs, Microservices, Serverless Computing
Network Connectivity
VPN, Dedicated WAN, SD-WAN.
Data Synchronization
Replication, backup, migration.
Identity and Access Management
Implementing secure authentication and authorization.

Fig 3 On-premises and cloud resources

Finally, insider attacks and poor monitoring are big risks to hybrid cloud migrations. The system is used in hybrid way in that it can be accessed by various stakeholders such as internal teams, external partners, as well as cloud service providers. And without strict identity and access management (IAM) controls privileged misuse or unintentional data leakage is possible. Along with that, the lack of visibility across hybrid systems hinders users to observe anomalous activities or intrusion. Businesses that lack strong monitoring and alarm methods are at risk of not identifying and controlling hazards in time which could put them at risk for chronic assaults and massive data exposure. To address these threats, we need broad methods including safe data transfer, rigorous policy enforcement and continuing monitoring, among others(Alotaibi et al., 2021).

3.2 Data Exposure Risks in Multi Cloud Migrations

With many benefits such as avoiding vendor lock in and being able to utilize more specialized services, enterprises often combine multi cloud migration with increased redundancy between clouds. The problem, however, is that administering many platforms is difficult and breeds new data exposure vulnerabilities. The one of the most difficult difficulties are your consistent security rules across multiple providers that could have different access control, encryption standards, and the way they handle data. This disparity increases the risk of setup fail with access to sensitive data once exploited by person likely unauthorized. Using different Application Programming Interfaces (APIs) that allow data exchange between platforms provides an attack surface for the malicious actor(Nadia Tabassum et al., 2023).

One example where there are many benefits for enterprises adopting ‘Multi cloud’ migrations is avoiding vendor lock in, using specialized services and redundancy. But administering many platforms is difficult and this method introduces new data exposure vulnerabilities. However, one of the most difficult for me is attempting to keep consistency in security rules among several providers, since each provider may have its own unique access controls, encryption standards, and data handling ways. Since the data is exchanged via various Application Programming Interfaces (APIs), they serve as attack surfaces towards malicious actors. But multi cloud setups are all the more jeopardized because they rely on third party providers for the integration and administration. Third party solutions for monitoring, analytics and security must be uniform given utilization of different suppliers. Unfortunately, these technologies can be hacked or misconfigured which can expose a ton of data across many platforms. But there is little centralized control and that hinders users from being able to figure out and react to security breaches quickly. However, to successfully mitigate these risks, adopting a multi-cloud approach, businesses must have rigorous governance framework, must use end to end encryption and must have robust identity and access management (IAM)(Reece et al., 2023).

3. Research methodology

To further identify the unique data exposure concerns in hybrid and multi-cloud migrations, a comparative analysis research method will be employed. This method will thoroughly investigate both models to find their specific security problems. By analyzing the two approaches, the research hopes to highlight the merits and drawbacks of each, eventually giving significant insights for businesses looking to reduce risks and enhance their security posture.

4.1 Complexity of data flow and management

However, data exposure risks are different for hybrid and multi cloud migrations, which sometimes present different levels of complexity in data flow and management. Part of what makes these distinctions come out is in the way data gets transferred from one system to another, how you keep it across these environments, and how you maintain it based on what security rule you guys have in place. Data flows between on premise systems and public or private cloud infrastructures for hybrid clouds which lead to complicated integrations of each of the legacy systems with cloud services. This enables firms to keep vital data in private places and to repatriate the less important processes to public cloud resources. Integrating on premises and cloud system though, raises a problem of synching data securely and frequently. Data integration misconfigurations can render data open to incidental access or leakage particularly if integration protocols or restrictions in access are not properly configured. Since we are obligated to monitor and manage these interfaces, control and visibility issues become apparent and it becomes difficult to swiftly identify and resolve security events in a rapid security event 'signature' fashion across environments. On the other hand, multi cloud setups are many cloud providers that employ different architecture, APIs, and security requirements. One of the advantages of this strategy lies in the fact it provides the flexibility to partner with many suppliers specialized in many areas rather than being dependent upon a single vendor for a single service. Multi cloud deployments make data flow difficult because data often moves across clouds that use different security protocols and encryption standards. This comparison may be described using the terms data management, moving, storage, and protection. Below is a thorough table that details the difficulties in each model.

Table 1. Difficulties in Hybrid and Multiple cloud models

Aspect	**Hybrid-cloud**	**Multi-cloud**
Data Handling	Centralized administration of on-premises and cloud data; integration allows consistent control across environments.	Decentralized administration, with separate policies for each cloud provider; frequently lacks uniform monitoring.
Data Movement	Frequent migration between on-premises and cloud settings need safe and fast transfer techniques.	Limited inter-cloud data mobility; transfers are frequently manual or via third-party technologies, raising security issues.
Data Storage	Sensitive data is often housed on-premises or in private clouds, with public clouds utilized for less important applications.	Data saved across several clouds according to the capabilities of each provider
Protection Measures	Centralized access control and end-to-end encryption provide unified security.	Different providers have different security requirements; access controls and encryption must be put in place in accordance with the provider's guidelines.
Configuration Challenges	Misconfigurations at on-premises and cloud system integration points are highly likely to occur.	Cloud setups could be inconsistent because of provider-specific tools and APIs.
Scalability and Flexibility	Efficient scaling in hybrid settings, but constrained by the capacity of the on-premises infrastructure.	Incredibly scalable since many providers can manage workloads separately, although at the expense of greater complexity.
Data Visibility	Because of integration, there is considerable visibility and control throughout data flow; integrated monitoring tools are frequently used.	Fragmented visibility and the need for various monitoring technologies make it more difficult to consistently identify and address threats.
Compliance	Centralized oversight over sensitive data makes regulatory compliance easier to maintain.	Enforcing compliance varies throughout suppliers, making it difficult to manage regional rules.
Attack Surface	Fewer external cloud connections, which reduces the attack surface; possible vulnerabilities at integration points	Increased exposure risks because of a wider attack surface brought up by several providers, APIs, and third-party technologies.

4.2 Security Policy Consistency and Enforcement Challenges

That is due to the necessity to combine on-premises systems and cloud platforms to function as a single integrated whole, which creates significant management problems for continuous security rule compliance in hybrids. A hybrid architecture common in organizations proves challenging in defining rules across various infrastructures, for instance, modern cloud situations and traditional structures. In this case, data can be exposed to breaches together with problems such as holes in audit trails, restricted access and waived encryption standards. Also, it may be unfeasible to ensure that policies apply during data transfers like in normal cloud and on-premise systems' synchronization. Centralized policy management tools often require a good deal of tweaking and integration mistakes may make sensitive information easily accessible.

However, as also due to various drivers, different cloud providers have disparate security perceived frameworks, APIs, and compliance, etc., thus multi-cloud systems present even more challenges. Those platforms could be encrypted with different standards or IAM procedures, and monitoring could be implemented in a different way, which also imposes the need for the same security policies to be implemented across the organization. The absence of normal technologies that function across a number of providers increases this and often tends to make enterprises utilize third-party solutions, which could be risky. This is partly because of the confusing nature of multi-cloud architecture, with many policies often violated through cross-cloud transfers and interconnections. There remains a problem of excessive variability in tools and governance with no single orchestration to provide similar patterns in different environments.

4.3 Vendor Dependency and Lock-In Risks

Many businesses are even in a hybrid cloud arrangement where they retain ownership of their local IT infrastructure, yet largely rely on a single cloud solutions vendor. Such dependence may lead to vendor lock-in where businesses become reliant on the vendor's tools, frameworks, and APIs. While on it, this dependence increases gradually which limits flexibility to explore other platforms and conversions is costly. Many vendors may also change the prices they charge or may even withdraw some of the services they offer which is financially and operationally dangerous for businesses. While on-premises resources are one of the advantages of the hybrid model, it may provide limited scalability and innovation due to the involvement of vendors in that model(Opara-Martins et al., 2016).

It is done intentionally in organizations with a multi-cloud system because it helps minimize the risk of becoming locked into a particular provider. It also improves vendor dependence and negotiating ability because it minimizes dependence on a single supplier. However, interoperability becomes hard to achieve as well as uniform security standards and procedures for the whole team, all of which become harder to maintain when dealing with multiple service providers. Some applications that are built specifically for vendors may require multiple modifications, which can easily cause misconfiguration, or increased management overhead. Additionally, due to the absence of a unified multi-cloud model, exposure expands with the outcomes of divided governance. Paradoxically, multi-cloud reduces the risks of lock-in but it does so at the cost of requiring a good management approach in order not to become more and more dependent on external tools for management and integration(Waldhofer, 2024).

4.4 Analysis of how dependency on single vs. multiple vendors affects exposure risks

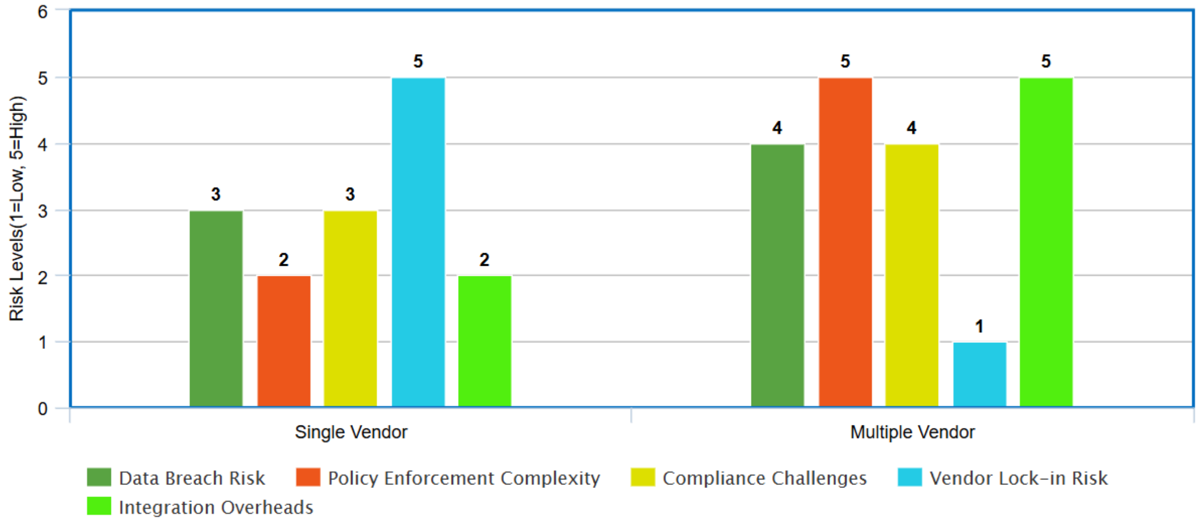

Fig 4. Dependency on single vs multiple vendors: Exposure risks

The chart compares risks associated with dependency on single versus multiple vendors across five categories: Some of the threats involved are Data Breach Risk, complexity of enforcing policies, compliance issues; risks associated with vendor lock-ins and integration overheads. For single vendor risks of data breach and non-compliance are moderate, the risk of integration overheads is medium but the risk of vendor lock-in is very high because of low flexibility. In this case, policy enforcement complexity is low. In the same respect, multiple vendors support various dangers in terms of data breaches, policy enforcement issues, compliance, and integration costs, while strongly decreasing the risk of vendor lock-in at the same time. As shown in this analysis, there is a tension between flexibility of operations and potential exposure to higher security and management risks.

4.5 Comparative Analysis of Security Recommendations for Hybrid Cloud and Multi-Cloud Setups

Table 2. Analysis of security recommendations

Strategies	Hybrid-cloud	Multi-cloud
Data Management	Emphasizes the on-premises storage of sensitive data.	Focuses on making sure data is consistent between clouds
Policy enforcement	Centralized regulations designed for hybrid settings.	Needs tools for cross-platform standardization.
Monitoring and Governance	Simplified by using a single set of monitoring tools.	complex, requiring CSPM and cloud-agnostic tools
Encryption	Concentrate on securing on-premises-to-cloud communications.	End-to-end encryption over several clouds.
Operational Complexity	There are fewer integration points, hence the complexity is moderate.	High complexity owing to various sources.
Cost	Lower, as there are fewer vendors involved.	Higher, because of the many tools and platforms.

In a broad sense, the insights stress that, although the hybrid cloud deployments are more unified in management and most probably less costly than the multi-cloud deployments, the latter give more freedom and potential to scale up flexible and accommodate different security elements and management practices.

4. Results

The comparison of a hybrid cloud model of operation and that of a multi-cloud platform shows different security factors and risks at play. Each of them poses challenges and opportunities with regards to data flow, integration, and management and these imply different kinds of data exposure dangers, at the same time, both models have their own strengths, and weaknesses.

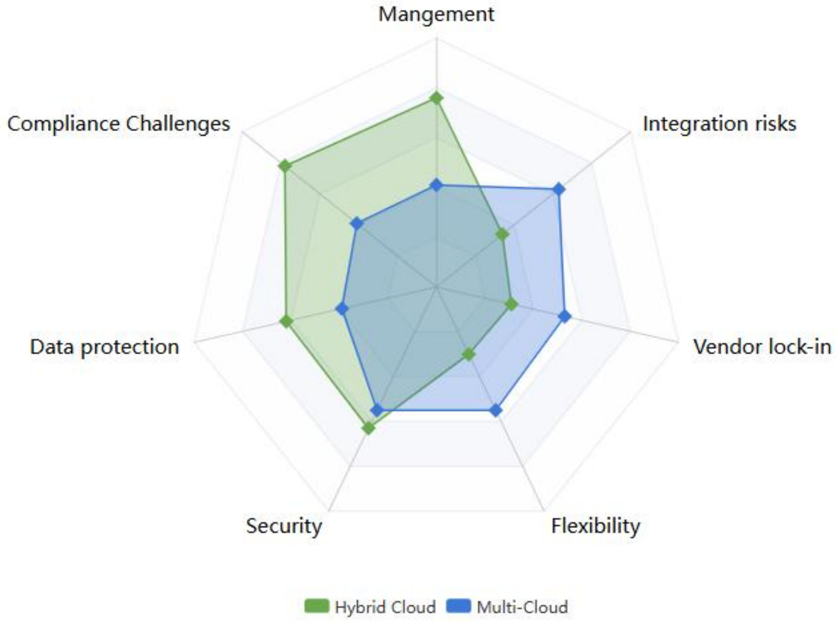

Fig 5 Performance comparison between Hybrid and Multi cloud models

The radar chart compares the performance of Hybrid Cloud and Multi-Cloud models across seven dimensions: Evaluation Criteria: Management, Integration Risk, Vendor Lock-In, Flexibility, Security/ Data Protection/ Compliance Issues. Multi-cloud does better than Hybrid Cloud in Management, Security, &Compliance Challenges; however, the centralized structure of management is the major selling point of Hybrid Clouds compared to Multi-Clouds. But it lacks Vendor Lock-In and it is not flexible as compared to Multi-Cloud. On the other hand, Multi-Cloud does well in Flexibility and also has lower risks of Vendor Lock-In hence offering info sec an opportunity to engage multiple providers. However, the issue most concerning to Nerds are Security, Data Protection, and Compliance because by its very architecture, it is difficult to address these issues. Through the comparison of the Hybrid Cloud model with the Multi-Cloud model pushed forward by Amazon and other vendors, the reader sees that the former allows one to gain more control and simplify the management of the infrastructure at the expense of flexibility and freedom from specific vendors.

The findings captured show the tension between hybrid and multi-cloud solutions. Although management of the hybrid cloud is easier whereby there is centralized management, policies and procedures can also be easily enforced the risks in integration and vendor lock-in are often high Multi-cloud advantages include flexibility coupled with relatively low vendor lock-in and yet security management compliance and data protection challenges can be extremely demanding. Hence it calls for business to analyze their unique needs and their tolerance to risks before choosing the CCRM model that will suit them most out of the two while ensuring adequate measures, controls and monitoring systems have been put in place to counter data exposure risks adequately.

6. Future Research Directions:

1. As for the further studies, the idea worth investigation is how new technologies such as AI and machine learning can be applied to improve security in the environments characterized by the utilization of both, hybrid and multi-cloud models.
2. One such research area could be in establishing real-time automatic means to set and implement security policies in all the providers of tangential clouds.
3. An area of further study could be the idea of building the security solutions that would be inherent to the multi-cloud model.
4. So, the following trends for future research can be identified: what consequences will quantum computing have on cloud security and how it will affect hybrid and multi-clouds?

7. Conclusion

This paper focuses on various data exposure threats that are unique to the organization after the shift to hybrid and multi-cloud mechanisms. Hybrid cloud also has centralized control, governance and compliance benefits that make it easier to be managed from a single point or location as well as being easier to be governed as they are already centrally located Even though that is the case, hybrid cloud has some issues such as like misconfiguration and vendor lock in which makes it have restricted flexibility and scalability. In contrast, multi-cloud set-ups reduce risks associated with vendor lock-in and offer more flexibility as well; however, it evolves the challenge to implement consistent security policies, follow compliance requirements or even, protect data securely across multiple cloud vendors.

From comparative analysis it emerged that the hybrid cloud is more appropriate for organizations that value data sovereignty decision and operational efficiency while multi-cloud is appropriate where there is need for redundancy and unique services from different providers. Yet, both models require effective governance controls, secure transmission and storage mechanisms of data, as well as sophisticated risk management instrumentation.

Organizations need to necessarily assess their operational needs, legal compliance, and risk appetite before arriving at a migration strategy. AI and machine learning technology, in particular, will continue to evolve and create opportunities for strengthening security, improving consistency and compliance with the requirements in hybrid and multi-cloud environments; these requests are the domains for further investigations.

8. Reference

1. *© 2024 Zhongbo Zhu*. (2024).
2. Alotaibi, S., Alharbi, K., Abaalkhail, B., & Ibrahim, D. M. (2021). Sensitive Data Exposure: Data Forwarding and Storage on Cloud Environment. *International Journal of Online and Biomedical Engineering*, *17*(14), 4–18. https://doi.org/10.3991/IJOE.V17I14.27365
3. Clearlake, H., & Engineering, S. (2021). *Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain Hemanth Gadde*. *01*(02).
4. El-Attar, N. E., El-Morshedy, D. S., & Awad, W. A. (2021). A New Hybrid Automated Security Framework to Cloud Storage System. *Cryptography*, *5*(4), 37. https://doi.org/10.3390/cryptography5040037
5. Gawande, S. (2024). *Orchestrating The Cloud Multiverse : Strategies For Seamless Integration And Unified Management ORCHESTRATING THE CLOUD MULTIVERSE : STRATEGIES FOR*. *October*, 12–15. https://doi.org/10.56726/IRJMETS63079
6. Gawande, S., & Gorde, S. (2024). Hybrid Cloud Architectures: Balancing the Benefits of Public and Private Clouds. *ISAR-International Journal of Research in Engineering Technology*, *9*(October), 2024. www.IJORET.com
7. Geczy, P., Izumi, N., & Hasida, K. (2013). Hybrid cloud management: Foundations

and strategies. *Review of Business and Finance Studies*, *4*(1), 37–51.

8. Hosseini Shirvani, M., Amin, G. R., & Babaeikiadehi, S. (2022). A decision framework for cloud migration: A hybrid approach. *IET Software*, *16*(6), 603–629. https://doi.org/10.1049/sfw2.12072
9. Imran, H. A., Latif, U., Ikram, A. A., Ehsan, M., Ikram, A. J., Khan, W. A., & Wazir, S. (2020). Multi-Cloud: A Comprehensive Review. *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*. https://doi.org/10.1109/INMIC50486.2020.9318176
10. Malallah, H. S., Qashi, R., Abdulrahman, L. M., Omer, M. A., & Yazdeen, A. A. (2023). Performance Analysis of Enterprise Cloud Computing: A Review. *Journal of Applied Science and Technology Trends*, *4*(01), 01–12. https://doi.org/10.38094/jastt401139
11. Nadia Tabassum, Humaria Naeem, & Asma Batool. (2023). The Data Security and multi-cloud Privacy concerns. *International Journal for Electronic Crime Investigation*, *7*(1), 49–58. https://doi.org/10.54692/ijeci.2023.0701128
12. Oluwafemi Clement Adeusi, Yusuf Olalekan Adebayo, Praise Ayomide Ayodele, Tajudeen Tunde Onikoyi, Kayode Blessing Adebayo, & Ibrahim Oyeyemi Adenekan. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. *World Journal of Advanced Research and Reviews*, *22*(3), 2050–2057. https://doi.org/10.30574/wjarr.2024.22.3.1982
13. Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing*, *5*(1). https://doi.org/10.1186/s13677-016-0054-z
14. Patil, K., & Desai, B. (n.d.). *MZ Journals AI-Driven Adaptive Network Capacity Planning for Hybrid Cloud Architecture*. *4*(2), 1–12.
15. Reece, M., Lander, T. E., Stoffolano, M., Sampson, A., Dykstra, J., Mittal, S., & Rastogi, N. (2023). *Systemic Risk and Vulnerability Analysis of Multi-cloud Environments*. http://arxiv.org/abs/2306.01862
16. Sekar, J. (2024). *MULTI-CLOUD STRATEGIES FOR DISTRIBUTED AI WORKFLOWS AND*. *August*.
17. Seth, D., Nerella, H., Najana, M., & Tabbassum, A. (2024). Navigating the Multi-Cloud Maze: Benefits, Challenges, and Future Trends. *International Journal of Global Innovations and Solutions (IJGIS), June*. https://doi.org/10.21428/e90189c8.8c704fe4
18. Tummalachervu, C. K., & Kanth Tummalachervu, C. (2023). EFFICIENT STRATEGIES FOR SEAMLESS CLOUD MIGRATIONS USING ADVANCED DEPLOYMENT AUTOMATIONS Chaitanya Kanth Tummalachervu et.al Introduction. *Journal of Science Technology and Research*, *1*(4), 61–70.
19. Waldhofer, F. (2024). *Cloud Vendor Lock - In : Identify , Strategies and Mitig ate Aashish Kumar*.