

Examining Poly-Cloud in Enterprise Cloud Strategies: Differentiating Between Multi-Cloud and Hybrid Cloud Approaches

Antony Panteli

Head of CIO Advisory (UK/EU)

antony.panteli@ltimindtree.com

LTIMindtree, London, UK

Author Note

Antony Panteli 

<https://orcid.org/0009-0005-7672-9003>

Abstract

As cloud computing continues to evolve, enterprises are increasingly exploring strategies to optimise their use of cloud resources. This paper provides a detailed examination of the poly-cloud approach in an enterprise cloud strategy, contrasting it with multi-cloud and hybrid cloud strategies. The benefits and challenges of each approach are discussed, as well as their applications in various enterprise scenarios. The paper also delves deeper into the factors that influence the adoption of these strategies, such as cost considerations, security concerns, and compliance requirements.

Keywords: Cloud computing, cloud strategy, Poly-cloud, Multi-cloud, Hybrid-cloud, Enterprise cloud computing

The rapid growth of cloud computing has transformed how organisations manage and store their data, offering a flexible and cost-effective solution for leveraging multiple computing resources (Attaran, 2017). Among the various cloud strategies available, poly-cloud, multi-cloud, and hybrid-cloud have emerged as popular approaches for enterprises seeking to optimise their cloud resources (Gleb, 2021). While these strategies share some similarities, they differ in crucial ways, each presenting distinct benefits and challenges depending on the context in which they are applied. This paper aims to analyse these three strategies, focusing on their unique characteristics and applications in enterprise settings.

Poly-Cloud Strategy: Overview, Benefits, and Challenges

Poly-cloud is a strategy in which an organisation utilises multiple cloud providers, each specialising in a specific service or application (Atchison, 2021). This approach allows enterprises to leverage each provider's unique strengths and capabilities, ensuring they can access the most appropriate services.

Benefits of Poly-Cloud Strategy

Improved Performance and Reliability

By distributing applications and services across multiple providers, enterprises can reduce the risk of service outages and ensure that their systems remain operational even if

one provider experiences difficulties. While Poly-cloud is focused on vendor service differentiation and specialisms (Atchison, 2021), the ability to access services across multiple cloud providers systematically ensures that services can fail-over across zones, regions and provider clouds.

Increased Flexibility and Cost Savings

Poly-cloud enables organisations to choose the best provider for each service, mitigating vendor lock-in and allowing them to take advantage of the competitive pricing offered by different providers (Paloviita, 2022). Sophisticated implementations may well be able to take advantage of spot rates to maximise cost efficiency or identify optimal hosts in real-time based on service latency and geography.

Challenges of Poly-Cloud Strategy

Management Complexity

Implementing a poly-cloud strategy can increase the complexity of managing multiple providers (Gleb, 2021), requiring organisations to develop sophisticated management tools and processes. Poly cloud is a strategy for a mature organisational cloud function that requires a high level of digital empathy and culture.

Data Sovereignty and Compliance

Criticality and complexity increase when services are provided across multiple providers in product architectures that maintain synchronous, stateful workflows (Zhang et al., 2022). When using multiple providers, enterprises may face data sovereignty and compliance challenges, as different providers generally have variations in service agreements and policies across geo-political jurisdictions. Geographic compliance is itself a critical consideration.

Multi-Cloud Strategy: Overview, Benefits, and Challenges

Multi-cloud is a strategy in which an organisation utilises multiple cloud providers for the same service or application, often increasing redundancy and reducing the risk of vendor lock-in. This approach allows enterprises to distribute workloads across different providers, ensuring they can maintain operations even if one provider experiences issues (Vijayalakshmi & Hridya, 2022).

Benefits of Multi-Cloud Strategy

Redundancy and Resiliency

The primary benefit of a multi-cloud strategy is its ability to provide redundancy and improve the resiliency of an organisation's infrastructure. By distributing workloads across multiple providers, enterprises can reduce the risk of service disruptions and maintain high availability. Iqbal et al. described redundancy as the replication of applications and resources, noting that shared responsibility delegates physical redundancy to cloud providers. Therefore, multi-cloud redundancy can be considered a logical abstraction and orchestration of redundancy management services that implicitly introduce high resilience.

Avoidance of Vendor Lock-In

Multi-cloud can help organisations avoid vendor lock-in by allowing them to easily switch between providers (Pellegrini et al., 2017). This expects that workloads or services are created using an architecture that intermediates platform agnostic solutions techniques across the provider platforms. Typically cloud native technologies such as containers are used in this approach, but innovative approaches to microservices can also effectively provide a defensive façade for provider-native managed services. The multi-cloud approach stimulates the competitive landscape of the cloud market (Heilig et al., 2016), continuously driving providers to improve their services, features, and pricing. Ultimately, this translates to better performance, security, and cost efficiency.

Challenges of Multi-Cloud Strategy:

Management Complexity

Like poly-cloud, multi-cloud strategies can introduce management complexity as organisations must coordinate and oversee multiple providers (Imran et al., 2020). Service Mesh products assist in managing and monitoring the distribution and operation of containerised services (Li et al., 2019) but to provide a *single pane of glass* view across costs, resource usage, anomaly detection and operational observability with consideration of Infra/Software/Platform as a Service and their relative consumption models is fundamentally non-trivial (Achar & Tisuela, 2020).

Consistent Performance and Integration

Ensuring consistent performance and seamless integration between various providers can be challenging in a multi-cloud environment, as each provider may have unique configurations and standards (DAndria et al., 2012). There are no agreed standards on interoperability between cloud providers (Ramalingam & Mohan, 2021), notwithstanding the commonly accepted standards and patterns of resource consumption in implementation and solution architecture definitions.

Hybrid Cloud Strategy: Overview, Benefits, and Challenges

A hybrid cloud strategy refers to a combination of public and private cloud resources, with organisations using both types of clouds to meet their specific needs (Park et al., 2020). In this approach, enterprises can utilise the scalability and cost-effectiveness of public clouds for specific applications while maintaining the security and control of private clouds for more sensitive data and applications (Achar, 2021; Talaat et al., 2020).

Benefits of Hybrid Cloud Strategy

Balance Between Public and Private Clouds

The primary benefit of a hybrid cloud strategy is its ability to *balance* the advantages of public and private clouds (Géczy et al., 2013). Enterprises can take advantage of the cost savings and scalability offered by public clouds while maintaining the security and control provided by private clouds (Goyal, 2014).

Flexibility and Agility

A hybrid cloud allows organisations to quickly move workloads between public and private clouds as needed, enabling them to respond quickly to changing business requirements (Linthicum, 2016). Containerised applications have the potential for on-demand public cloud elasticity while scaling back cost-effectively to on-prem resources

when local capacity is sufficient for requirements in the immediate. Non-native apps can take advantage of hybrid cloud clustering to achieve point-to-point integration (Dash et al., 2021).

Challenges of Hybrid Cloud Strategy

Integration and Management

The process of integrating and managing public and private cloud resources can be quite challenging, particularly when multiple public cloud providers are involved in the hybrid environment. Hybrid cloud architectures are inherently complex, requiring careful balancing of services and workloads across the different components of the infrastructure and how these are maintained and managed with necessary tools and processes across the environments (Jackson & Goessling, 2018).

Observability and Monitoring

Observability and monitoring challenges arise from tracking events across multiple platforms. Unified logging and analytics toolsets are needed for comprehensive insight into the entire infrastructure. Hybrid cloud environments necessitate collecting, aggregating, and analysing unstructured and structured data between public and private environments (Ahola, 2022). The volume of monitoring data is typically high, and data egress costs across

environments can be considerable. Because of this, the complexity of observability architectures necessarily increases to ensure effective and timely insights.

Compliance

Hybrid cloud environments introduce compliance challenges with regulatory, industry-specific and geographic data protection regulations like PCI-DSS, GDPR and HIPAA across public and private boundaries (Agarwal et al., 2022). Ensuring that all parts of the hybrid cloud infrastructure meet these requirements is vital to avoid legal and financial consequences.

Security

Data security is vital in hybrid cloud systems, where data traverses on-premises, private, and public cloud platforms, increasing the number of threat vectors (Asadullah et al., 2020). Organisations must employ robust encryption measures, secure data transfer methods, and stringent access controls to safeguard data confidentiality, integrity, and availability across diverse environments. User and device identity and access management must be centrally orchestrated (Chewe, 2021), with an IAM system that consistently applies security policies across different environments.

Consideration must also be given to how responsibility models delineate accountability for specific security aspects in a hybrid environment (Lad, 2023). It is essential to have a clear understanding of the public cloud provider's fundamental shared responsibility model and the organisation's internal responsibilities for infrastructure and networking security to ensure comprehensive security coverage.

Comparison of Poly-Cloud, Multi-Cloud, and Hybrid Cloud Strategies

Resource Optimization

Each cloud paradigm has a distinct approach to enhancing the efficiency, resilience, and adaptability of IT infrastructures. Poly-cloud strategies involve the judicious selection of providers for individual services, thereby capitalising on each provider's unique strengths to optimise resource allocation. Multi-cloud strategies, on the other hand, underscore redundancy and workload distribution, utilising multiple providers to bolster fault tolerance, minimise vendor lock-in, and ensure optimal performance. Lastly, hybrid cloud strategies strive to balance the relative advantages of public and private cloud infrastructures, adeptly leveraging the scalability and cost-effectiveness of public clouds whilst maintaining the stringent security and customisability intrinsic to private clouds. Collectively, these strategies facilitate the creation of robust and versatile cloud ecosystems catering to diverse organisational requirements and objectives.

Risk Mitigation

All three paradigms have some variance in the priorities that must be addressed for risk mitigation:

Poly-cloud Priorities

- a) Vendor interoperability: Establish clear protocols and standards to ensure seamless integration of services across different providers.
- b) Data consistency: Implement robust data management and synchronisation mechanisms to maintain data integrity across multiple provider platforms.
- c) Governance and compliance: Develop a unified governance framework to ensure adherence to legal, regulatory, and organisational requirements.

Multi-cloud Priorities

- a) Complexity management: Utilise orchestration and management tools to simplify and streamline operations across multiple cloud environments.
- b) Cost optimisation: Regularly monitor and evaluate resource consumption to prevent cost overruns and inefficient resource allocation.
- c) Security: Implement consistent policies and controls across different providers to safeguard data and applications.

Hybrid-cloud Priorities

- a) Connectivity and latency: Employ reliable, high-performance network connections to ensure seamless communication between public and private cloud components.
- b) Data privacy and security: Establish clear data classification policies and apply corresponding security measures to protect sensitive information in both public and private clouds.
- c) Workload placement: Continuously assess the suitability of placing specific workloads in public or private clouds based on performance, cost, and security factors.

Vendor Lock-In

Poly-cloud

Enterprises inherently diversify their dependencies by selecting the most suitable provider for each service, mitigating the risk of vendor lock-in. This approach enables organisations to seamlessly transition to alternative providers for specific services without disrupting the entire infrastructure.

Multi-cloud strategies

Distributing workloads across multiple providers inherently avoids reliance on a single vendor. This strategy not only enhances redundancy and fault tolerance but also ensures greater flexibility in switching providers or redistributing workloads as needed.

Hybrid-cloud

Although not explicitly designed to circumvent vendor lock-in, hybrid cloud deployments can still confer some flexibility. By utilising a combination of public and private cloud resources, enterprises maintain control over their private infrastructure, thereby retaining the ability to reallocate workloads or switch public cloud providers as necessitated by evolving business requirements.

Cost Considerations

Poly-cloud, multi-cloud, and hybrid cloud strategies offer unique benefits and challenges for enterprises seeking to optimise their cloud resources. Poly-cloud and multi-cloud strategies can potentially lead to cost savings by allowing enterprises to take advantage of competitive pricing offered by different providers. Hybrid cloud strategies can also provide cost benefits by combining the cost-effectiveness of public clouds with the security and control of private clouds.

Conclusion

The ever-evolving landscape of cloud computing necessitates organisations remain vigilant and adaptable to fully harness the potential of cloud technologies. By understanding the nuances and distinctions between poly-cloud, multi-cloud, and hybrid-cloud strategies, enterprises can make well-informed decisions that align with their specific requirements regarding performance, reliability, cost-effectiveness, security, and compliance. Each approach presents its unique advantages and challenges, which should be carefully assessed and weighed against the organisation's goals and priorities.

As cloud computing continues to advance, enterprises must stay abreast of the latest developments and trends in cloud strategies, ensuring that their decisions remain informed and relevant. This proactive approach to cloud management will empower organisations to effectively navigate the complexities and challenges associated with these paradigms, optimising resource allocation and mitigating potential risks. Moreover, a comprehensive understanding of the diverse cloud strategies will enable organisations to balance cost savings, performance, and security. This is critical to unlocking the full potential of cloud computing.

Ultimately, embracing a forward-looking and adaptive approach to cloud computing will position organisations to capitalise on the numerous strategic benefits and opportunities presented by cloud technologies, enabling them to thrive in the modern, digitalised world.

References

- [1] Attaran M (2017) Cloud Computing Technology: Leveraging the Power of the Internet to Improve Business Performance. *Journal of International Technology and Information Management* 26: 112–137.
- [2] Gleb T (2021) Cloud Computing Primer, In: Gleb T (Ed.), *Systematic Cloud Migration: A Hands-On Guide to Architecture, Design, and Technical Implementation*, Berkeley, CA, Apress, 3–18.
- [3] Atchison L (2021) *What is polycloud?*, O'Reilly Media.
- [4] Paloviita O (2022) *Infrastructure as code for Managed Service Providers: A case study*.
- [5] Vijayalakshmi A, Hridya (2022) Functionalities and Approaches of Multi-cloud Environment, In: Nagarajan R, Raj P, Thirunavukarasu R (Eds.), *Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases*, Cham, Springer International Publishing, 257–268.

- [6] Pellegrini R, Rottmann P, Strieder G (2017) Preventing vendor lock-ins via an interoperable multi-cloud deployment approach, 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), ieeexplore.ieee.org, 382–387.
- [7] Heilig L, Lalla-Ruiz E, Voß S (2016) A cloud brokerage approach for solving the resource management problem in multi-cloud environments. *Comput Ind Eng* 95: 16–26.
- [8] Imran HA, Latif U, Ikram AA, et al. (2020) Multi-Cloud: A Comprehensive Review, 2020 IEEE 23rd International Multitopic Conference (INMIC), ieeexplore.ieee.org, 1–5.
- [9] Li W, Lemieux Y, Gao J, et al. (2019) Service Mesh: Challenges, State of the Art, and Future Research Opportunities, 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), ieeexplore.ieee.org, 122–1225.
- [10] Achar S, Tisuela NL (2020) A Review of Hosting Enterprise SaaS with IaC on Multi-cloud Platforms. *International Journal of Reciprocal Symmetry and Physical Sciences* 7: 14–23.

- [11] DAndria F, Bocconi S, Cruz JG, et al. (2012) Cloud4SOA: Multi-cloud Application Management Across PaaS Offerings, 2012 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, ieeexplore.ieee.org, 407–414.
- [12] Ramalingam C, Mohan P (2021) Addressing Semantics Standards for Cloud Portability and Interoperability in Multi Cloud Environment. *Symmetry* 13: 317.
- [13] Park J, Kim U, Yun D, et al. (2020) Approach for Selecting and Integrating Cloud Services to Construct Hybrid Cloud. *Int J Grid Util Comput* 18: 441–469.
- [14] Achar S (2021) An overview of environmental scalability and security in hybrid cloud infrastructure designs. *Asia Pac J Energy Environ* 8: 39–46.
- [15] Talaat M, Alsayyari AS, Alblawi A, et al. (2020) Hybrid-cloud-based data processing for power system monitoring in smart grids. *Sustainable Cities and Society* 55: 102049.
- [16] Géczy P, Izumi N, Hasida K (2013) Hybrid Cloud Management: Foundations and Strategies. *Review of Business & Finance*.

- [17] Goyal S (2014) Public vs private vs hybrid vs community - cloud computing: A critical review. *Int J Comput Netw Inf Secur* 6: 20–29.
- [18] Linthicum DS (2016) Emerging Hybrid Cloud Patterns. *IEEE Cloud Computing* 3: 88–91.
- [19] Dash MK, Devidutta S, Mohanta BK, et al. (2021) *Hybrid Cloud: The Next Generation of EAI, Internet of Things and Connected Technologies*, Springer International Publishing, 297–305.
- [20] Jackson KL, Goessling S (2018) *Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk*, Packt Publishing Ltd.
- [21] Ahola J (2022) *Cloud monitoring: cloud monitoring with dynatrace*.
- [22] Agarwal V, Butler C, Degenaro L, et al. (2022) Compliance-as-Code for Cybersecurity Automation in Hybrid Cloud, 2022 IEEE 15th International Conference on Cloud Computing (CLOUD), ieeexplore.ieee.org, 427–437.

- [23] Asadullah M, Yadav RK, Namdeo V (2020) A survey on security issues and challenges in cloud computing, 2020. Available from: <http://www.ijirtm.com/UploadContaint/finalPaper/IJIRTM-0404202007.pdf>.
- [24] Chewe M (2021) Hybrid cloud infrastructure security : Security automation approaches for hybrid IT.
- [25] Lad S (2023) Introduction: Dimensions of Cloud Security, In: Lad S (Ed.), Azure Security For Critical Workloads : Implementing Modern Security Controls for Authentication, Authorization and Auditing, Berkeley, CA, Apress, 1–23.