Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2024, 11(4):372-379**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Optimizing Performance, Cost-Efficiency, and Flexibility through Hybrid Multi-Cloud Architectures

Nikhil Bhagat

Sr. Technical Account Manager – Network Specialist
Independent Scholar, Network Engineering
nikhil.bhagat90@gmail.com

Abstract Cloud Computing is the foundation of every modern company that is scalable, adaptable and economical. Hybrid multi-cloud environments, which combine private clouds, public clouds, and multiple cloud providers, represent the next generation for scaling cloud infrastructures. Hybrid cloud architecture lets organizations reap the security and control benefits of a private cloud while also taking advantage of the scalability and cost efficiency of a public cloud. Meanwhile, multi-cloud models avoid vendor lock-in, provide risk mitigation, and enable organizations to choose the best options from multiple providers. Hybrid and multi-cloud solutions together offer an integrated cloud architecture that maximizes usage, performance, and resilience. The paper delves into the advantages of hybrid and multi-cloud environments, including agility, cost efficiency and increased security. The paper also touches on organizational design considerations such as workload assignment, interoperability, security, and vendor selection. The paper provides guidelines for implementing hybrid multi-cloud environments where orchestration tools and automation play a vital role to facilitate the operations. Even though Hybrid multi-cloud architectures provide greater flexibility, they must be strategically designed, implemented and managed. By modernizing these environments, businesses can enhance performance, profitability, and agility, better preparing them to thrive in today's competitive market.

Keywords Hybrid Cloud Architectures, Multi-Cloud Architectures, Design Considerations, Cost Optimization, Best Practices.

1. Introduction

Cloud computing has radically transformed business models, with the power of unparalleled flexibility, scalability, and efficiency. Enterprises across the globe are moving to the cloud for optimal IT operations, operational efficiencies and digital transformation [1]. However, as cloud maturity has increased, most companies are witnessing more complex solutions that involve multiple providers and environments for cloud. This is reflected in the emergence of hybrid and multi-cloud environments, which allow for a more sophisticated cloud infrastructure management.

A hybrid cloud combines private and public clouds, enabling enterprises to balance the power and security of private clouds with the flexibility and capacity of public clouds [2]. It allows organizations to store confidential data and workloads in private clouds and reap the on-demand capacity and cost advantages of public clouds. The model is particularly favorable for enterprises with highly regulated industries with varying workloads.

Meanwhile, multi-cloud architectures, where organizations deploy multiple public cloud providers, are also gaining popularity. The advantage of a multi-cloud solution is that companies can reduce vendor lock-in, achieve the best performance from each provider, and maintain resilience through redundancy [3]. By distributing workloads among different cloud platforms, companies can customize their clouds according to their performance, compliance, and budget requirements.

In order to manage cloud deployment more effectively, hybrid multi-cloud solutions have become the perfect blend of hybrid and multi-cloud approaches. This paper reviews the components, advantages, and design considerations of hybrid multi-cloud systems to help organizations understand how to maximize performance, efficiency, and agility in the fast-moving digital world.

2. Hybrid Cloud Architectures

Hybrid cloud solutions integrate both the private and public clouds, allowing organizations to take advantage of each while tailoring solutions to specific operational needs [4]. A hybrid cloud environment enables companies to hold back sensitive data and mission-critical workloads in a private cloud and harness the agility, scalability and affordability of public cloud for less sensitive or fluctuating workloads.

A. Key Components of Hybrid Cloud Architectures

• **Private Cloud:** A private cloud is generally held on-premise or with an off-site provider. This is a landscape where businesses have full ownership of their infrastructure in terms of security, compliance, and customization [5]. A private cloud typically hosts sensitive data, highly controllable workloads, or applications with tighter specifications, allowing enterprises to maintain closer control.

• **Public Cloud:** Public clouds providers like Amazon Web Services (AWS), Microsoft Azure or Google Cloud provide organizations on-demand computing capacity to grow according to a varying demand [6]. Public clouds offer high availability, elasticity, and cost savings, making them ideal for workloads with high usage or significant computing requirements.

• **Orchestration and Integration Layer:** In hybrid clouds, the orchestration layer is important for communication and management between the private and public clouds. Workload management, data integration and automation capabilities are offered on this layer so that enterprises can move data and applications from one cloud to another as needed [7]. It also enables governance, security policies, and monitoring to ensure high-level performance and compliance across both environments.

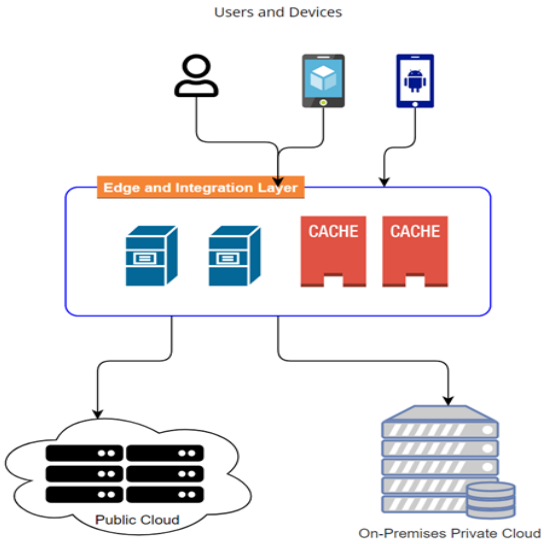

Fig. 1 *Hybrid Cloud Architectures*

B. Hybrid Cloud Use Cases

Hybrid cloud solutions are particularly helpful in the scenarios where organizations seek to get a balance between performance, cost and compliance [8]. Some of the use cases are:

• **Data Sovereignty:** Many industries, including healthcare and finance, have regulated policies requiring that certain data reside on-premises or within a specific geographic area [5]. These compliance requirements can be accommodated by hybrid clouds, where organizations can keep sensitive data on the private cloud while still utilizing the scalability of the public cloud for other workloads.

• **Disaster Recovery and Business Continuity:** Hybrid clouds provide better disaster recovery solutions. In Hybrid cloud environments, key infrastructure could be left on a private cloud while backup or non-critical

systems could be replicated on a public cloud [9]. In an event of failure or downtime in the main environment, the public cloud could take over the traffic for business continuity.

• **Workload Optimization:** Enterprises can optimize workloads by splitting it between public and private clouds, depending on performance, cost and sensitivity [6]. Hence, high-performance applications (such as those that use large amounts of data) can be executed in the private cloud to reduce latency, while massive data processing can be performed on the public cloud due to its elasticity.

C. Challenges in Hybrid Cloud Architectures

While their benefits are great, hybrid clouds also present challenges, primarily in terms of security, interoperability, and complexity. For seamless deployment of private and public clouds, it needs sophisticated orchestration tools and governance models [4]. Furthermore, businesses must ensure that their security policy is consistent on both cloud platforms to avoid any misconfigurations.

Overall, hybrid clouds enable companies to tailor their environments in order to manage the workloads, secure the data, and reduce costs. Using both private and public cloud systems, companies can establish a cloud solution that is tailored to the business's specific operations while preparing for the future of expansion and innovation.

3. Benefits of Using Hybrid Cloud Architectures

A. Flexible and Scalable

A hybrid cloud offers more flexibility to enterprises as it can scale out or scale in depending on the demand [10]. Organizations can take advantage of the elasticity of public clouds in peak periods while keeping business-critical applications in private clouds.

B. Security and Compliance

The more sensitive workloads that do not require advanced security/compliance are allowed to stay in the private cloud, and the less sensitive workloads can run on the public clouds. This way businesses can comply with industry specific regulations and still stay competitive.

C. Cost Efficiency

By bundling private and public cloud resources, organizations can reduce costs. Public clouds eliminate overprovisioning, and private clouds minimize ongoing cloud services costs for static workloads [11]. With this mixed structure, an organization can budget more efficiently.

D. Disaster Recovery and Resilience

Hybrid clouds enhance business continuity and disaster recovery. When systems fail, businesses can failover to the public cloud and continue providing services.

E. Improved Performance

Hybrid architectures allow optimization of workload. Organizations can run expensive workloads in public clouds to consume their cutting-edge infrastructure, while keeping high-throughput, low-latency applications in private clouds, closer to the customer [12].

4. Multi-Cloud Architectures

Multi-cloud architectures involve two or more cloud platforms from multiple providers to share workloads, applications, and services. Multi-cloud, unlike hybrid cloud which includes a combination of private and public clouds, is limited to deploying multiple public clouds (Amazon Web Services (AWS), Microsoft Azure, Google Cloud, etc.) for specific business requirements [13]. This model enables enterprises to leverage each of the cloud providers' individual features, services, and pricing in order to achieve optimal performance, cost, and agility.

A. Key building blocks of Multi-Cloud Architectures

• **Multiple Cloud Service Providers:** With multi-cloud deployment, companies choose the cloud service provider based on their individual offerings. One can opt for AWS for infrastructure-as-a-service (IaaS) features, Azure for integration with Microsoft products, and Google Cloud for machine learning and data analytics [14]. This enables companies to select the best provider for any workload or use case, enhancing overall performance and efficiency.

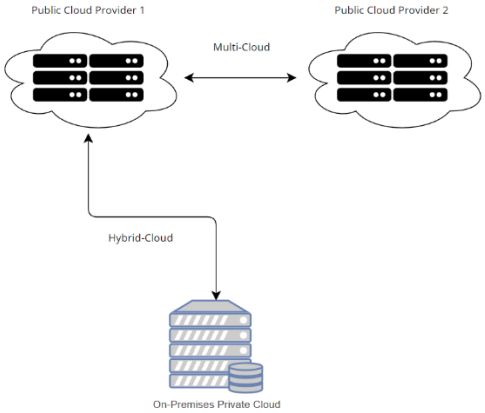

Fig. 2 *Hybrid and Multi-Cloud Architectures*

• **Workload Distribution:** Workloads are distributed to various cloud environments based on performance, geography, compliance, and cost-effectiveness [15]. Stacking services from multiple vendors can give organizations optimal resource utilization, avoiding reliance on a single public cloud provider.

• **Interoperability and Integration:** To administer a multi-cloud environment, cloud providers must be interoperable. Cloud providers will typically provide their own tools and APIs but companies will need to add middleware, cloud management system or orchestration tools that will help integrate and communicate between the environments [16]. Interoperability is essential for ensuring consistent performance and governance across multiple clouds.

B. Use Cases for Multi-Cloud Architectures

• **Avoiding Vendor Lock-In:** Vendor lock-in prevention is one of the main motivators of multi-cloud. As workloads are distributed across different cloud providers, enterprises maintain freedom and negotiation leverage, avoiding dependence on a single provider's pricing, technology, or service levels [17].

• **Performance Optimization:** Cloud providers provide various functionality, features, and services. Through a multi-cloud model, businesses can leverage the best of both platforms and make their services run at their peak [18]. For instance, latency sensitive workloads can be hosted on a provider that has data centers close to end-users and compute-intensive applications can be hosted on a provider that has the most powerful CPUs.

• **Effective Cost Utilization:** There are multiple cloud providers and they provide different plans and discounts. Multi-cloud allows organizations to select the lowest cost platform for any workload resulting in savings and optimal usage of resources [19].

• **Risk Mitigation and High Availability:** Multi-cloud architectures increase resilience by minimizing downtime. During an outage or service interruption on one provider, workloads that are business-critical can automatically be migrated to a different cloud environment to ensure business continuity [20].

C. Challenges in Multi-Cloud Architectures

Although multi-cloud architectures are beneficial, they’re complex. Multi-cloud operation demands well-defined governance architectures, complex security policies, and orchestration capabilities [3]. As Data interoperability, compliance, and seamless provider-to-provider integration can be tricky, it may require dedicated resources and technical expertise to manage multi-cloud environments.

Monitoring and cost optimization for several providers can become tricky without proper cloud management tools [21]. In addition, enterprises have to consider the potential differences in SLAs, data residency and performance metrics between different cloud environments that might make managing services more difficult.

5. Advantages of Using a Multi-Cloud Environment

A. Avoiding Vendor Lock-In

Multi-cloud deployment enables businesses to operate independently of a single cloud vendor [22]. This not only provides leverage during contract negotiations but also helps avoid dependence on a vendor's ecosystem for essential services.

B. Better Performance

By leveraging multiple cloud vendors based on their capabilities, businesses can optimize application speed, reliability, and user experience to ensure the right applications align with their workloads. Workloads can be distributed across providers by geography, latency, or SLAs.

C. Cost Optimization

Price models are quite different from one cloud provider to the next and a multi-cloud strategy allows organizations to choose the lowest priced solution for any use case [23]. This optimization ensures that organizations don't pay for similar services that are available elsewhere at lower costs.

D. Risk Mitigation

By sharing workloads across multiple cloud providers, an organization can prevent vendor-dependent disruption or outages. Critical workloads can also continue to operate on another platform if one provider fails [24].

E. Regulatory Compliance

A multi-cloud approach allows companies to meet geographic data residency requirements by using vendors with data centers in specific locations, ensuring compliance with regulations such as the General Data Protection Regulation (GDPR).

F. Flexibility and Innovation

As cloud providers continue to launch new services, multi-cloud environments allow enterprises to leverage powerful tools from multiple vendors, fostering innovation and creating a more agile IT culture [25].

Lastly, Multi-cloud environments help enterprises to benefit from cloud computing leveraging the strengths of several providers. This strategy provides more performance, agility, savings and resilience and is the right choice for businesses looking to mix up their cloud investments and stay relevant in a changing digital environment.

6. Building Hybrid Multi-Cloud Environments

The deployment of hybrid multi-cloud must be planned well before implementation. A hybrid multi-cloud infrastructure integrates private clouds, public clouds, and various cloud providers into a single, orchestrated ecosystem. Organizations must address several factors, including integration, security, governance to achieve optimal performance, cost and flexibility.

A. Cloud Strategy and Implementation

It is important to have a strategic well planned strategy that is relevant to business objectives. Enterprises need to identify workloads appropriate for each scenario (public, private, or multi-cloud), assess compliance, and model usage to make the best use of available cloud resources [26].

B. Interoperability and Orchestration

While designing a hybrid multi-cloud infrastructure, the organization needs to carefully consider cloud vendor and service interoperability. Companies need to deploy orchestration tools that support end-to-end communication and data movement. Solutions such as Kubernetes, container orchestration tools, and cloud management tools offer automation and administration tools to bridge multiple cloud ecosystems [27].

C. Security and Compliance

Security is one of the key areas an organization should focus while designing Hybrid multi-cloud architectures. Businesses must provide robust IAM, encryption, and network security across every environment. Security policies have to be identical across private and public clouds, and regulations have to be followed when it comes to sensitive data.

D. Data Management and Integration

A hybrid multi-cloud architecture requires advanced data management. Businesses must determine how to integrate, replicate, and back up data across clouds with low latency and consistency. APIs and middleware can help to facilitate data flow between private and public clouds.

E. Monitoring

Continuous monitoring of resource utilization, application performance and costs is vital in a hybrid multi-cloud [3]. Businesses must define Key Performance Indicators (KPIs) to monitor the effectiveness of cloud services and leverage tools that provide live analytics for optimization.

F. Delivery of SLAs

Each cloud provider may have a unique SLA, and managing multiple providers in a hybrid multi-cloud environment requires configuring SLAs to align with business needs. Monitoring the service contracts and terms of each vendor is crucial for preventing service outages or performance degradation [28].

7. Design Considerations for Organizations Adopting Hybrid Multi-Cloud Environments

Organizations seeking to deploy hybrid multi-cloud architectures must address several design considerations to achieve optimal results.

A. Workload Distribution

Organizations will need to evaluate each application workload thoroughly to understand which workload should be deployed on private, public or multi-cloud. Companies should decide on the workloads that need scaling based on performance, data integrity and other requirements [29].

B. Cloud Service Provider Selection

It's important to choose the right cloud providers depending on business requirements, use cases, location, and features [30]. Organizations should be taking providers' capabilities into consideration along with their cost, security and compliance metrics.

C. Cloud-Native Architecture

Leveraging cloud-native solutions such as containers, microservices and serverless computing can increase portability and flexibility across different cloud environments. Cloud-native solution reduces dependency on specific platforms, allowing for more efficient private/public cloud migrations.

D. Security, Compliance and Governance

Data protection, access control, and compliance must be supported by an effective governance and security solution. Security policies should be enforced consistently across all cloud environments, preventing vulnerabilities to arise from misconfigurations or inconsistencies [31].

E. Cost Optimization

In terms of costs, a multi-cloud model can be challenging to manage and may result in a loss of revenue if not effectively implemented. Companies should adopt cloud financial management platforms that provide visibility into spending across providers [32]. Companies should use cloud-native solutions that can automatically right-size resources during scaling process to optimize cost utilization.

F. Orchestration and Automation Tools

Hybrid multi-cloud environments require automation to effectively manage resources and services across multiple cloud environments [33]. Orchestration tools are capable of automating provisioning, scaling, and deployments. Providing Infrastructure as Code (IaC) solutions makes infrastructure manageable through code, minimizing human error and increasing consistency [34].

8. Conclusion

Hybrid multi-cloud architectures offer a compelling solution for businesses that want to maximize their IT infrastructure performance, cost, and agility. By combining the advantages of private clouds such as enhanced security and management, and the scalability and affordability of public clouds, hybrid solutions enable companies to support a wide variety of rapidly changing business needs. Adding a multi-cloud solution complements the model by allowing businesses to bypass vendor lock in, spread workloads across different cloud providers and leverage the features of each platform.

While designing Hybrid Multi-Cloud environments, organizations needs to strategically plan before implementation. Companies need to identify the workload requirements, the correct mixture of cloud providers, and cross-vendor interoperability. Security and governance strategies must be robust and consistent across the private and public clouds to reduce risk of data breaches. Companies should also consider cost control and monitoring tools to optimize resource utilization and avoid platform duplication. Automation and orchestration services also play a key role in the enablement of cloud service operations and scaling.

Finally, hybrid multi-cloud architectures provides organizations with a highly adaptable, scalable, and affordable model to meet varying business requirements. These environments bring tremendous benefits, such as enhanced performance, disaster recovery and the power to innovate faster. As cloud technologies continue to

evolve, hybrid multi-cloud services will be essential for helping organizations remain relevant in a rapidly changing business environment.

References

[1]. C. T. S. Xue and F. T. W. Xin, "Benefits and challenges of the adoption of cloud computing in business," Int. J. Cloud Comput. Serv. Archit., vol. 6, no. 6, pp. 1-15, Dec. 2016. [Online]. Available: https://doi.org/10.5121/ijccsa.2016.6601

[2]. G. Aryotejo, D. Y. Kristiyanto, and M. Mufadhol, "Hybrid cloud: bridging of private and public cloud computing," IOP Conf. Ser. Mater. Sci. Eng., vol. 1025, no. 1, May 2018. [Online]. Available: https://doi.org/10.1088/1742-6596/1025/1/012091

[3]. D. Petcu, E. D. Nitto, D. Ardagna, A. Solberg, and G. Casale, "Towards multi-clouds engineering," in Proc. IEEE INFOCOM Wkshps, Apr. 2014. [Online]. Available: https://doi.org/10.1109/infcomw.2014.6849159

[4]. A. Viloria et al., "Hybrid cloud computing architecture based on open source technology," Adv. Comput. Eng., Springer, Jan. 2019, pp. 191-200. [Online]. Available: https://doi.org/10.1007/978-981-15-1304-6_16

[5]. P. Raj and A. Raman, "The hybrid cloud: The journey toward hybrid IT," Cloud Computing, Springer, Jan. 2018, pp. 91-110. [Online]. Available: https://doi.org/10.1007/978-3-319-78637-7_5

[6]. R. Simões and C. Kamienski, "Elasticity management in private and hybrid clouds," in Proc. IEEE CLOUD, Jun. 2014. [Online]. Available: https://doi.org/10.1109/cloud.2014.110

[7]. K. Bakshi, "Secure hybrid cloud computing: Approaches and use cases," in Proc. IEEE Aerosp. Conf., Mar. 2014, pp. 1-8. [Online]. Available: https://doi.org/10.1109/aero.2014.6836198

[8]. E. Sturrus and O. V. Kulikova, "Orchestrating hybrid cloud deployment: An overview," IEEE Comput., vol. 47, no. 6, pp. 85-87, Jun. 2014. [Online]. Available: https://doi.org/10.1109/mc.2014.159

[9]. L. Wang, H. V. Ramasamy, R. E. Harper, M. Viswanathan, and E. Plattier, "Experiences with building disaster recovery for enterprise-class clouds," in Proc. DSN, Jun. 2015. [Online]. Available: https://doi.org/10.1109/dsn.2015.53

[10]. G. Breiter and V. K. Naik, "A framework for controlling and managing hybrid cloud service integration," in Proc. IEEE Int. Conf. Cloud Eng., Mar. 2013, pp. 217-224. [Online]. Available: https://doi.org/10.1109/ic2e.2013.48

[11]. J. Kozhipurath, "Cloud service costing challenges," in Proc. IEEE Int. Conf. Cloud Comput. Eng. Manag., Oct. 2012, pp. 1-6. [Online]. Available: https://doi.org/10.1109/ccem.2012.6354604

[12]. B. Zhou, F. Zhang, J. Wu, and X. Li, "Cost reduction in hybrid clouds for enterprise computing," in Proc. IEEE ICDCSW, Jun. 2017. [Online]. Available: https://doi.org/10.1109/icdcsw.2017.13

[13]. D. Petcu, "Multi-cloud: Expectations and current approaches," in Proc. ACM SAC, Jun. 2009. [Online]. Available: https://doi.org/10.1145/1543834.1544004

[14]. P. H. B. Patel and P. N. Kansara, "Cloud computing deployment models: A comparative study," Int. J. Res. Comput. Sci. Technol., vol. 9, no. 2, pp. 45-50, Mar. 2021. [Online]. Available: https://doi.org/10.21276/ijircst.2021.9.2.8

[15]. S. Venkateswaran and S. Sarkar, "Architectural partitioning and deployment modeling on hybrid clouds," Softw. Pract. Exp., vol. 48, no. 2, pp. 345-365, Mar. 2017. [Online]. Available: https://doi.org/10.1002/spe.2496

[16]. D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the Intercloud - Protocols and formats for cloud computing interoperability," in Proc. IEEE ICIW, Jan. 2009. [Online]. Available: https://doi.org/10.1109/iciw.2009.55

[17]. R. Pellegrini, P. Rottmann, and G. Strieder, "Preventing vendor lock-ins via an interoperable multi-cloud deployment approach," in Proc. IEEE Int. Conf. Inf. Technol. Secur. Trans., Dec. 2017. [Online]. Available: https://doi.org/10.23919/icitst.2017.8356428

[18]. V. V. Rajendran and S. Swamynathan, "Parameters for comparing cloud service providers: A comprehensive analysis," in Proc. IEEE CESYS, Oct. 2016, pp. 1-5. [Online]. Available: https://doi.org/10.1109/cesys.2016.7889826

[19]. G. Pandey, V. N. Rao, A. Srivastava, U. Banerjee, and E. Narasimhan, "Current cloud scenario review and cost optimization by efficient resource provisioning," in Proc. ACM Symp. Appl. Comput., Mar. 2011, pp. 1-4. [Online]. Available: https://doi.org/10.1145/1980422.1980440

[20]. P. T. Endo et al., "High availability in clouds: Systematic review and research challenges," J. Cloud Comput., vol. 5, no. 1, pp. 1-20, Oct. 2016. [Online]. Available: https://doi.org/10.1186/s13677-016-0066-8

[21]. E. Nogueira, A. Moreira, D. Lucrédio, V. C. Garcia, and R. P. D. M. Fortes, "Issues on developing interoperable cloud applications: Definitions, concepts, approaches, requirements, characteristics and evaluation models," J. Cloud Comput., vol. 4, no. 1, pp. 1-19, Dec. 2016. [Online]. Available: https://doi.org/10.1186/s40411-016-0033-6

[22]. J. Opara-Martins, R. Sahandi, and F. Tian, "Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective," J. Cloud Comput., vol. 5, no. 1, pp. 1-18, Apr. 2016. [Online]. Available: https://doi.org/10.1186/s13677-016-0054-z

[23]. Y. Shen, H. Chen, S. Lingxuan, M. Cheng, and X. Pu, "Cost-optimized resource provision for cloud applications," in Proc. IEEE HPCC, Aug. 2014, pp. 1060-1067. [Online]. Available: https://doi.org/10.1109/hpcc.2014.179

[24]. M. F. Zhani and R. Boutaba, "Survivability and fault tolerance in the cloud," Cloud Computing, Wiley, Apr. 2015, pp. 295-308. [Online]. Available: https://doi.org/10.1002/9781119042655.ch12

[25]. F. Pfarr, T. Buckel, and A. Winkelmann, "Cloud computing data protection: A literature review and analysis," in Proc. IEEE HICSS, Jan. 2014, pp. 1-10. [Online]. Available: https://doi.org/10.1109/hicss.2014.616

[26]. M. L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "Cloud computing synopsis and recommendations," NIST Special Publication, Jan. 2012. [Online]. Available: https://doi.org/10.6028/nist.sp.800-146

[27]. J. M. Wrabetz and E. Weaver, "Leveraging hybrid cloud workflows in media and entertainment," J. Media Inf., vol. 127, no. 4, pp. 16-20, Apr. 2018. [Online]. Available: https://doi.org/10.5594/jmi.2018.2811343

[28]. M. Alhamad, T. S. Dillon, and E. Chang, "Conceptual SLA framework for cloud computing," in Proc. DEST, Apr. 2010. [Online]. Available: https://doi.org/10.1109/dest.2010.5610586

[29]. A. M. Caulfield et al., "A cloud-scale acceleration architecture," IEEE Micro, vol. 36, no. 5, pp. 1-16, Oct. 2016. [Online]. Available: https://doi.org/10.1109/micro.2016.7783710

[30]. W. Zeng, Y. Zhao, and J. Zeng, "Cloud service and service selection algorithm research," in Proc. ACM SAC, Jun. 2009. [Online]. Available: https://doi.org/10.1145/1543834.1544004

[31]. H. Takabi, J. Joshi, and G. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," in Proc. COMPSAC Workshops, Jul. 2010, pp. 393-398. [Online]. Available: https://doi.org/10.1109/compsacw.2010.74

[32]. L. Lee and R. D. Mautz, "Using cloud computing to manage costs," J. Corp. Acct. Finance, vol. 23, no. 3, pp. 11-15, Feb. 2012. [Online]. Available: https://doi.org/10.1002/jcaf.21748

[33]. F. Huang, H. Li, Z. Yuan, and X. Li, "An application deployment approach based on hybrid cloud," in Proc. IEEE BigDataSecurity, May 2017, pp. 1-7. [Online]. Available: https://doi.org/10.1109/bigdatasecurity.2017.54

[34]. J. C. Patni, S. Banerjee, and D. Tiwari, "Infrastructure as a code (IaC) to software defined infrastructure using azure resource manager (ARM)," in Proc. IEEE COMPE, Jul. 2020, pp. 575-578. [Online]. Available: https://doi.org/10.1109/compe49325.2020.9200030