International Journal of Humanities and Information Technology (IJHIT)
e-ISSN: 2456 –1142, Volume 05, Issue 2, (June 2023), ijhit.info

A Survey on Hybrid and Multi-Cloud Environments: Integration Strategies, Challenges, and Future Directions

Jaya Vardhani Mamidala[1], Avinash Attipalli[2],Sunil Jacob Enokkaren[3], Varun Bitkuri[4], Raghuvaran Kendyala[5], Jagan Kurma[6]
[1]University of Central Missouri, Department of Computer Science.
[2]University of Bridgeport, Department of Computer Science.
[3]ADP, Solution Architect.
[4]Stratford University, Software Engineer.
[5]University of Illinois at Springfield, Department of Computer Science.
[6]Christian Brothers University, Computer Information Systems.
Email ID: mvardhini29@gmail.com

DOI: 10.21590/ijhit.05.02.08

Abstract

The rapid evolution of cloud computing has led organizations to adopt hybrid and multi-cloud environments to meet increasing demands for scalability, flexibility, and resilience. While these environments provide significant benefits, they introduce unique challenges, including interoperability, data consistency, security, and vendor lock-in. This survey comprehensively reviews deployment architectures, integration strategies, middleware roles, and the challenges associated with multi-vendor cloud systems. The survey results reveal that middleware plays a critical role in enabling seamless communication, abstraction, orchestration, and maintainability across heterogeneous cloud platforms. Widely adopted integration strategies identified include API-driven integration, service-oriented architectures (SOA), containerization with orchestration, cloud brokers, and Middleware-as-a-Service (MWaaS). These strategies effectively mitigate heterogeneity, support workload portability, and enhance security, thereby enabling scalable and resilient multi-cloud deployments. Additionally, the survey highlights the operational complexities and open research challenges, emphasizing the need for standardized interfaces, unified governance frameworks, and automated management solutions. The findings provide a roadmap for enterprises to implement robust multi-cloud integration frameworks while addressing operational, security, and compliance requirements. This study contributes to a deeper understanding of hybrid and multi-cloud ecosystems, guiding future research toward adaptive middleware, AI-driven orchestration, and edge-cloud integration for enhanced performance, flexibility, and secure adoption.

Keywords*:* Multi-Cloud, Cloud Computing, Hybrid Environments, Integration Approach, Vendor Lock-In, API-Driven Strategies.

I. INTRODUCTION

The rapid digital transformation of businesses and organizations has led to a growing need for scalable, flexible and cost-effective solutions in computing. Conventional on-premise infrastructures do not tend to be dynamic, and with this requirement being dynamic, the adoption of cloud computing is widespread. Enterprises are currently shifting towards hybrid and multi-cloud settings to enhance performance, resilience, and independence of vendors. According to one definition, cloud computing is the provision of

software services, including applications, together with the supporting infrastructure, such as hardware and systems software, which are housed in data centers. Single-cloud, hybrid-cloud, and multi-cloud are popular forms of cloud architectures designed to meet different organizational needs (Oliveira et al., 2019). A single-cloud solution is simple and has centralized management, but it has a tendency to create a dependency on the vendor and a lack of flexibility. Unlike it, hybrid-cloud architectures are used in industries that require sensitive data as well as dynamic workloads and combine the resources between private and public accordingly to achieve security, scalability, and cost efficiency (Miyachi, 2018). Multi-cloud environments take this flexibility one step further and utilize services of a variety of providers to allow organizations to maximize performance, gain resilience, and prevent vendor lock-in.

The trend toward hybrid and multi-cloud has been a response to the necessity of optimization of performance, risk reduction, cost control, and independence of vendors. Compared to single-cloud adoption, multi-cloud adoption enables organizations to mix services of more than one vendor and, therefore, avoid vendor lock-in and gain business agility. Besides the transfer of goods and services, the market is placing increased emphasis on the flexibility of the process as well as the ability to respond to changes, which is the significance of agile enterprise design techniques. An example of this is Software Design as a Service, which has become one of the conceptual frameworks that combine cloud-native technologies and design thinking frameworks to accelerate innovation and competitiveness. The ease of entry of cloud-native models also gives more power to start-ups and enterprises to innovate rapidly and also bears more complexities in the field of operations (Vankayalapati, 2019).

There are solutions required within organizations so that they can address hybrid and multi-cloud ecosystems and be able to abstract platform heterogeneity and guarantee seamless communication and interoperability. In this regard, middleware has played a central role since it is the abstraction layer that creates an interface between applications and cloud services. It enhances significant attributes, such as interoperability, portability, transparency, flexibility, and maintainability, to simplify the development procedure of applications and enable them to operate in a broad variety of cloud vendors (Kritikos *et al.*, 2019).

However, the issue of multi-vendor, multi-cloud integration of middleware is a challenging one. Instances of interoperability inconsistency, inconsistent data formatting, compliance inconsistency, and the fear of lock-in that is common in vendors are an unusual occurrence in organizations and could impede the complete utilization of the multi-cloud advantages (Park et al., 2020). To resolve these issues, there is a need to have clear integration plans, which include the implementation of API-based architectures, container orchestration, service-based models, cloud brokers, and the global standardization initiative. (Gundu et al., 2020).

A. Structure of the Paper

The paper is structured in the following: Section II discusses cloud computing architecture, Section III elaborates on integration strategies, Section IV outlines the roles of middleware, Section V highlights the challenge of multi-vendor, Section VI is a review of related literature, and finally Section VII gives a conclusion on the findings and research directions.

II. CLOUD COMPUTING DEPLOYMENT ARCHITECTURES

The development of cloud computing has greatly changed how organizations handle, store and secure information. Even in contrast to traditional IT infrastructures, which utilize local servers, cloud computing can provide data storage, application hosting, and service delivery across distributed networks of servers. This movement has enabled customers to access their resources anywhere, anytime, using various gadgets and from any geographical location, without being limited by the ground infrastructure. Cloud computing has become a pillar of the modern digital ecosystem by decoupling users from physical resources, providing on-demand virtualized services. Its main strengths that add more value to it include flexibility, scalability, reliability, and cost-effectiveness, especially in mission-critical environments such as data recovery and disaster management. (Al-shammari and Alsaqre, 2012)

Cloud computing is basically the shift of data and applications model out of local infrastructure to remote models, that is, Internet-based models. In this paradigm, users are free to access, share and process information without any hassle, as shown in Figure 1. However, the openness of the Internet introduces inherent risks to privacy, security, and compliance, necessitating advanced mitigation techniques. The popular solutions to such problems are server clustering, distributed computing systems, wide-area network systems, and sophisticated encryption systems (Alshammari, 2017).

The necessity to work with the limitation of a single provider has been one of the major factors that have inspired the shift to multi-cloud and hybrid architectures of single-cloud deployments. While early cloud adoption focused on operational efficiency and cost savings, organizations soon realized that issues such as security vulnerabilities, regulatory compliance, and vendor lock-in could not always be effectively managed within a single-cloud environment (Mallareddy, 2014). This recognition has led to the adoption of more diverse deployment strategies, which are discussed in the following subsections.

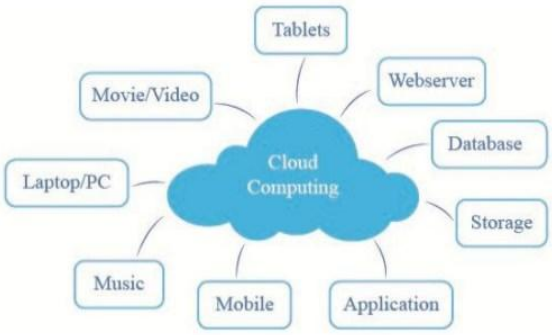

Fig. 1. Cloud Computing

A. Single-Cloud Architecture

A Single-Cloud architecture involves procuring services from a single cloud service provider, either through One central data center or several dispersed ones. As depicted in Figure 2, this model simplifies management and billing, as organizations deal with only one vendor. It is economical for smaller businesses and it is relatively simple to incorporate the service.

Fig. 2. Single-Cloud Architecture

However, being dependent on one vendor has its fair share of risks of dependency on a vendor, minimal likelihood of redundancy, and potential performance bottlenecks. Incidents or failures in the ecosystem of the selected provider have a direct effect on derailing organizational functions. Therefore, although Single-Cloud is still applicable to particular use scenarios, its shortcomings have hastened the transition to more flexible models.

B. Multi-Cloud Architecture

A multi-cloud system, as shown in Figure 3, allows organizations to use a combination of services provided by various cloud providers. This makes it more resilient because workloads are distributed to different environments, (Kushwaha, 2016) which helps mitigate the effect of failures or outages in the system of one provider.

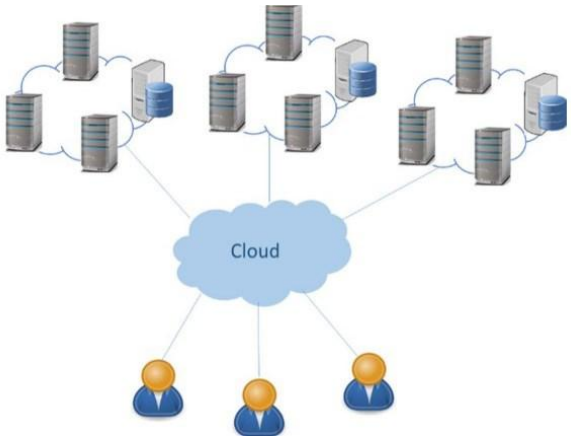

Fig. 3. Multi-Cloud Architecture

In addition to redundancy, multi-cloud strategies enable enterprises to enhance performance through the selection of specialized services offered by various vendors, including advanced analytics tools offered by one vendor and ML platforms by another one. Also, regulatory compliance requirements frequently tend to force the need to keep data in certain jurisdictions, and multi-cloud is a beneficial method to strike a balance between performance, cost, and legal limitations. However, the use of multi-clouds creates administrative complexity in controlling heterogeneous platforms. Interoperability, predictable security policies, and effective data migration among providers are some of the major challenges that require sophisticated integration procedures and middleware solutions.

C. Hybrid Cloud Models

A hybrid cloud combines a private and public cloud, allowing for the concentrate on each other's strengths. As Figure 4 demonstrates, Hybrid models offer the cost-effectiveness and scalability of the public clouds, as well as the security, control, and compliance advantages of the private clouds (Bhadani, 2020). This bilaterality makes hybrid architectures especially appealing to organizations with sensitive information that needs to be on-premises and at the same time needs to be able to scale the resources to meet the less critical workloads.

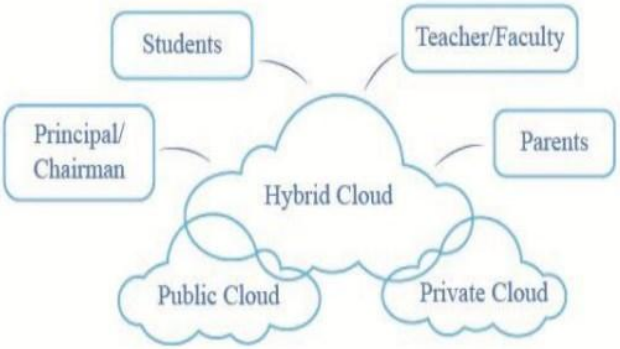

Fig. 4. Hybrid Cloud Models

The hybrid models also favor workload portability and dynamic provisioning, which allow organizations to develop resources on demand dynamically according to actual demand. By way of example, when a business is straining, it is possible to add capacity to the public cloud and maintain a secret infrastructure. However, there are no issues with Hybrid architectures. The joint association of the private and the public environment includes the powerful mechanism of orchestration, the sole instruments of management, and the interfaces. The safety of the different domains is also made complex and more advanced systems of control are demanded.

III. INTEGRATION STRATEGIES IN HYBRID AND MULTI-CLOUD ENVIRONMENTS

Heterogeneity dilemmas are part of balancing hybrid and multi-cloud configurations, interoperability, scalability and vendor lock-in and demand conscious efforts to overcome. These environments unlike the single-cloud ones need sophisticated systems to ensure that communication is smooth, the movement of workloads is easily achievable, and that the policy is implemented among providers. The following are the most prevalent approaches in the industry and research being summarized in Table I.

A. API-Driven Integration

Multi-cloud integration is based on the Application Programming Interfaces (APIs). They enable middleware to expose the standardized points of communication in such a way that the applications can communicate with the heterogeneous vendor platforms without using proprietary solutions (Bastião Silva, 2013). Among other things, simplicity and flexibility are recognized to be the two major attributes of RESTful APIs and GraphQL (Krutthika & Aswatha, 2021).

It is its strength because it is universal, and nearly all the providers accept APIs, yet differences in designs, authentication, and rate-limiting policies can complicate interoperability. Integration through API is typically considered as a floor strategy, which requires being supplemented by more sophisticated frameworks in order to become reliable and managed.

B. Service-Oriented Architecture (SOA) and Microservices

The integration of middleware has changed with the adoption of Service-Oriented Architecture (SOA) and microservices which have improved modular, reuse and deployable services separately. Such models offer organizations the ability to reduce the size of brake systems to individual functions unlike monolithic applications, which offer the opportunity to independently scale to the cloud.

- SOA also provides standardized protocols for defining and discovery services.
- Microservices are fault-tolerant, scalable with a larger granularity as compared to this model.
- Middleware is a load-balancing and cross-provider messaging, service-discovery agent.

Microservices may help to make the process more flexible, however, they complicate the process of integration, and complex orchestration and monitoring tools are required.

C. Containerization and Orchestration:

Containers and orchestration platforms have proven to be highly beneficial for cloud-agnostic integration. Containers are used to package and then deploy applications and middleware, and to scale, as well as to connect applications across environments using orchestrators, including Kubernetes (Reniers, 2016). This plan improves mobility among the two types of clouds, both the public and the private ones, and it supports functions such as multi-cloud load balancing and recovery in the event of a disaster (Geeta, 2019). To implement hybrid and multi-cloud, containerization and orchestration are indispensable to decouple the applications and vendor-specific infrastructure.

D. Cloud Brokers and Middleware Gateways:

In order to reduce the complexity of dealing with a multitude of providers, organizations tend to use cloud brokers and middleware gateways (Krutthika & Rajashekhara, 2019).

- Cloud brokers are middlemen who provide resources, track the load, and distribute the workload in the most efficient way.
- The middleware gateways can also offer extra interoperability through protocol translation, data format harmonisation, and uniform security policy.

These solutions are especially useful for businesses that lack in-house expertise. Nevertheless, they also pose risks of dependency, since organizations have to entrust the performance, cost and compliance management to the broker.

E. Standardization through Open APIs and Protocols:

Vendor lock-in remains one of the primary challenges associated with integrating multiple clouds and hybrid clouds. Open standards, such as OAuth 2 (security), OpenAPI (API documentation), RPC (remote procedure calls), and AMQP (messaging), provide a common ground for interoperability (Petcu, 2013). Standardisation promotes the following:

- Secure communication across heterogeneous platforms.
- Data portability and reduced integration overhead.
- Compatibility in compliance-heavy sectors such as healthcare and finance.

TABLE I. MIDDLEWARE INTEGRATION STRATEGIES IN HYBRID AND MULTI-CLOUD ENVIRONMENTS

Integration Strategy	**Purpose**	**Advantages**	**Challenges**	**Emerging Trends**
API-Driven Integration	Provides a baseline layer for interoperability across cloud providers	Universally supported, flexible, widely adopted	Inconsistent design, authentication, rate-limiting policies complicate integration	Standardized APIs, API gateways, automated API management
Service-Oriented Architecture (SOA) & Microservices	Promotes modular, reusable, and deployable services across clouds	Flexibility, scalability, fault tolerance, selective cloud deployment	Higher orchestration and monitoring complexity	Service mesh, microservice orchestration, serverless integration
Containerization & Orchestration	Enables cloud-agnostic deployment and operational consistency	Portability, multi-cloud load balancing, disaster recovery	Operational complexity, requires expertise in orchestration tools	Kubernetes federation, multi-cloud CI/CD pipelines, container security solutions
Cloud Brokers & Middleware Gateways	Simplifies multi-provider management and ensures interoperability	Simplified management, optimized workloads, enhanced interoperability	Dependency on third-party brokers, potential performance and compliance risks	AI-driven workload optimization, hybrid broker platforms
Standardization through Open APIs & Protocols	Reduces vendor lock-in and enables cross-cloud interoperability	Secure communication, reduced integration overhead, compliance-ready	Uneven global adoption, integration gaps remain	Wider adoption of open standards, universal API specification frameworks

Despite these advantages, uneven global adoption of standards limits their effectiveness, leaving integration gaps in cross-provider communication.

F. Middleware-as-a-Service (MWaaS):

An emerging approach is the delivery of middleware capabilities as a managed service. Middleware-as-a-Service (MWaaS) abstracts integration tasks such as identity management, messaging, and data synchronization into a cloud-native platform. This model offers enterprises as following:

- Reduced development overhead, as integration is handled by the provider.
- Scalable, on-demand middleware functions that adapt to dynamic workloads.
- Faster deployment cycles, enabling quicker adoption of multi-cloud strategies.

However, MWaaS can paradoxically reintroduce vendor lock-in, as businesses could grow reliant on the middleware architecture of a particular supplier

IV. MIDDLEWARE IN MULTI-CLOUD AND HYBRID CLOUD ENVIRONMENTS

Middleware is a critical enabler for applications to operate effectively in situations with many clouds and hybrid clouds. As more businesses utilize several cloud providers, middleware acts as an abstraction layer, hiding underlying heterogeneity and providing standardized interfaces and communication protocols (Farahzadi, 2018). It enhances interoperability, scalability, maintainability, and overall system reliability. Enabling technologies such as containerization, orchestration, Service-Oriented Architectures (SOA), and API-driven integration complement middleware by simplifying deployment, management, and monitoring across distributed cloud systems (Marpaung et al., 2013).

A. Multi-Cloud Middleware Capabilities

In multi-cloud setups, middleware assumes a very crucial role in enhancing smooth communication and integration of heterogeneous applications and services that are spread across several cloud providers. It generalizes underlying distinctions, scales interactions and provides interoperability, scalability and maintainability so that an organization is able to effectively manage complex infrastructures and minimize the challenges posed by multi-cloud deployment Its major features are as follows:

- **Flexibility:** Facilitates applications to scale and perform well in a wide range of cloud environments and configurations, with minimal modifications or redesigning.
- **Transparency:** Hides the complexities in the underlying system so that applications and services can communicate without the detailed knowledge of the architecture of each provider.
- **Interoperability:** Enables significant sharing of data and services among protocols, data formats and heterogeneous infrastructures and the seamless interoperability of multiple cloud providers.
- **Reusability:** Promotes the reuse of software and hardware systems through the decoupling of services and implementation to application resulting in a shorter time, cost and effort to develop new deployments.
- **Maintainability:** Supports robust fault isolation, rapid recovery mechanisms, and overall system resilience, ensuring high availability and reliability of multi-cloud applications over time.

B. Hybrid Cloud Middleware Capabilities

Middleware is the key enabler that makes hybrid cloud architectures practical. It serves as a link between public cloud services and on-premises systems, abstracts infrastructure differences, enables interoperability, and provides runtime services needed to deploy, manage, and secure applications across both environments (Kaur & Sachdeva, 2015). Middleware in hybrid clouds serves several high-level roles:

- **Abstraction & Interoperability:** Middleware provides applications and orchestration layers with stable APIs, SDKs, or model-driven artefacts by abstracting vendor-specific APIs and

infrastructure variations (Nitto *et al.*, 2012). Workloads moving between private and public clouds are simplified and vendor lock-in is avoided.

- **Orchestration, Portability & Runtime Management:** Middleware works with orchestration tools (container runtimes, schedulers, deployment managers) to deploy, scale, and heal applications across hybrid topologies. Middleware based on containerization and orchestration platforms like Kubernetes provides uniform execution environments and portability.
- **Policy, Security & Compliance Enforcement:** Middleware ensures identity federation, access control, encryption, and auditing across domains. These technologies safeguard service-to-service communication and enable private-public cloud compliance procedures. Middleware ensures data sovereignty and regulatory and operational compliance.

V. CHALLENGES IN MULTI-VENDOR MIDDLEWARE INTEGRATION

These challenges stem from dissimilarities across the architectures, service models, and compliance frameworks of cloud providers. If left unacknowledged, they can lead to interoperability issues, data inconsistencies, security vulnerabilities, or vendor lock-in. Identifying these challenges and their impacts is crucial to creating sensible integration strategies. The main challenges are:

- **Interoperability Challenges:** Multi-cloud environments require interoperability across different cloud providers. Differences in APIs, data formats, and service models can lead to inconsistent data structures and integration issues, complicating development, causing data discrepancies, and slowing business adaptation. Integration strategies such as API standardization, middleware abstraction, and service-oriented architectures help address these challenges (Dubey & Singh, 2020).
- **Data Consistency and Portability:** Ensuring consistent and transferable data across multiple cloud providers is critical. Variations in storage architectures, data switching mechanisms, and data management policies can create silos and inconsistencies, threatening data integrity, real-time analytics, and application mobility. Middleware-based data orchestration, cloud brokers, and distributed storage frameworks facilitate data consistency and portability across providers.
- **Security and Compliance Complexities:** The implementation of multi-cloud systems is problematic regarding imposing security and regulatory compliance. There are varying security policies, identity management systems and compliance requirements among cloud providers that can lead to breach of data, unauthorized access or breach of regulations. Identity management, encryption protocol, and zero-trust models are unified to provide security and compliance in different cloud platforms.
- **Vendor Lock-In Risks:** The problem of vendor lock-in appears when the organization is overly reliant on one cloud provider and can hardly be migrated. This may restrict the flexibility, value maximization and limit the organization's capacity to respond to dynamic business requirements. Vendor lock-in can be alleviated by using multi-cloud orchestration platforms, adopting open standards and using Middleware-as-a-Service (MWaaS).

VI. LITERATURE REVIEW

This section of the paper presents a thorough summary of the studies conducted on multi-vendor middleware integration strategies in hybrid and multi-cloud environments, together with a condensed summary in Table II.

Tomarchio, Calcaterra and Modica (2020) the cloud service providers and customers is continuously rising in number, which proves the effectiveness of the cloud computing paradigm. Nonetheless, such expansion comes with drawbacks: the providers have to effectively organize the resources to meet the demands of customers, whereas the customers have issues with choosing between a variety of similar services. Multi-cloud environment Cloud Resource Orchestration Frameworks (CROFs) are software frameworks that operate across providers to utilize heterogeneous resources in satisfying customer

requirements. This paper provides a systematic review and comparison of key CROFs and highlights open issues in multi-cloud computing that require further research (Tomarchio, 2020).

Karaja, Ennigrou and Said (2020) In a dynamic with a limited budget for a heterogeneous multi-cloud context, the Bag-of-Tasks scheduling technique is suggested. Experiments on artificial data sets are conducted to show the algorithm's performance in terms of making predictions. Because it enables the pay-per-use delivery of cloud computing, which provides on-demand services via the internet, has grown incredibly popular. However, A multi-cloud ecosystem, where clouds are coupled to satisfy consumer demands, has arisen as the number of cloud users rises (Karaja, 2020).

TABLE II. SUMMARY OF MULTI-VENDOR MIDDLEWARE INTEGRATION STRATEGIES

Reference	Focus Area	Approach Key	Key Findings	Challenges	Future Direction
Tomarchio, Calcaterra, and Modica (2020)	Multi-cloud resource orchestration	Cloud Resource Orchestration Frameworks (CROFs) to manage heterogeneous cloud resources	CROFs improve resource management and customer satisfaction across multiple cloud providers	Efficient orchestration for providers; selecting optimal resources for customers remains complex	Further research on adaptive, intelligent orchestration frameworks to handle dynamic multi-cloud environments
Karaja, Ennigrou & Said (2020)	Task Scheduling in Multi-Cloud	Dynamic Bag-of-Tasks scheduling technique with budget constraints	Improved makespan and efficiency on synthetic datasets	Scalability with real-world heterogeneous workloads	Extend to real-time large-scale cloud environments with diverse datasets
Haytamy & Omara (2020)	QoS-aware Service Composition	Modified Particle Swarm Optimization (PSO) for uncertain QoS attributes	Achieved high optimality with low time complexity	Handling dynamic and uncertain QoS parameters in real deployments	Develop adaptive QoS composition with real-time monitoring and prediction
Di Pietro et al. (2018)	Secure Storage in Multi-Cloud	Mobile secure storage framework "ARIANNA" for confidentiality & integrity	Demonstrated feasibility through Android app in real multi-cloud setup	Balancing performance with strong encryption mechanisms	Enhance usability, lightweight encryption, and integration with IoT devices
Colombo et al. (2019)	Data security in hybrid multi-cloud environments	Data Protection as a Service (DPaaS) framework with fine-grained access control and automated encryption	Provides flexibility, control, and visibility; works across private and public clouds; ensures automated data security	Integration with heterogeneous clouds and compliance across multiple platforms	Extend DPaaS with real-time monitoring, AI-driven access control, and edge-cloud integration
Girish & Nischita (2017)	Cloud Brokerage	Broker organizations between cloud providers & consumers	Brokers simplify management of multi-cloud consumption	Lack of standardized brokerage models & interoperability	Establish universal broker frameworks and cloud governance standards
Gupta, Kumar, and Jana (2016)	Workflow scheduling in heterogeneous multi-cloud	Two-phase priority-based workflow scheduling	Outperforms existing algorithms in makespan, speed-up, and resource utilization	Limited handling of dynamic workloads and failures	Adaptive scheduling with AI-based resource management

Haytamy and Omara (2020) modified Particle Swarm Optimization (PSO) has been utilized to give the best services based on the uncertainty of QoS attributes. A genuine QoS dataset has been used to implement the suggested method. The comparative findings demonstrate that the proposed approach has achieved a high degree of optimality with low time complexity when compared to the existing models. An enhanced QoS-based Service Composition Approach has been introduced in the multi-Cloud context to accurately determine which Cloud providers to hire to provide the required services in order to reduce the Cloud consumer cost function (Haytamy & Omara, 2020).

Di Pietro et al. (2018) provide that the primary goal of this mobile secure storage approach is to guarantee data confidentiality and integrity for smart devices that are a part of a multi-cloud environment. The Android app "ARIANNA" was shown and explored in this article. It integrates and enables the multi-cloud experimental framework, which has been detailed in the literature. Additionally, a number of tests were carried out to assess the concept by putting the mobile application into an authentic situation of a multi-cloud environment (Di Pietro et al., 2018).

Colombo et al. (2019) In contrast to A Data Protection as a Service (DPaaS) architecture is recommended for cloud users in place of the present Data Encryption as a Service (DEaaS) provided by firms like Amazon and Google, offering greater flexibility, control, and visibility. DPaaS goes beyond simple encryption by enabling data owners to create detailed access control policies. Data is automatically encrypted, and access is granted in accordance with these policies. It separates security from data management and provides a full cycle of data security automation. The prototype works across hybrid multi-cloud environments, including private clouds (OpenStack, CloudStack, VMWare) and public clouds (BT Cloud Compute, AWS), with experiments demonstrating its efficiency (Colombo et al., 2019).

Girish and Nischita (2017) present how a cloud broker company may act as providing cloud users with brokering services as a middleman between cloud providers and cloud consumer businesses. This article also provides a brief explanation of how conventional service organizations are investing in cloud-specific intellectual property and management frameworks in order to become cloud brokers. The number of clouds used by enterprises increases as the cloud industry develops. Under such circumstances, managing a multi-cloud system becomes more difficult for an enterprise (Girish & Nischita, 2017).

Gupta, Kumar and Jana (2016) incorporated a new priority scheme into a two-phase workflow scheduling system. When setting priorities in the first phase, it takes into account the task node's average communication cost divided by its average computation cost. The second step involves mapping prioritized tasks to appropriate virtual machines. Large-scale workflow scheduling in the proposed method enables a heterogeneous multi-cloud environment. Using a presumptive cloud model, the suggested algorithm is thoroughly simulated on typical scientific processes, and the outcomes of the simulation are contrasted with those of the current dependent task scheduling techniques. Significantly, the findings demonstrate that the suggested method outperforms the methods now in use for average cloud storage, speed-up, schedule length ratio, and make span (Gupta et al., 2016).

VII. CONCLUSION AND FUTURE WORK

Cloud computing has quickly progressed from single-cloud to multi-cloud and hybrid environments, allowing businesses to satisfy the increasing needs for resilience, scalability, and flexibility. These environments offer significant advantages but introduce unique challenges in interoperability, data consistency, security, and vendor lock-in. This survey highlights that middleware plays a central role in addressing these challenges by providing abstraction, orchestration, transparency, and maintainability across heterogeneous cloud platforms. According to the survey, the most used strategies of integration are API-driven integration, service-oriented architectures (SOA), containerization with orchestration, cloud brokers and Middleware-as-a-Service (MWaaS). Through the literature review, it is clear that the above-mentioned strategies are capable of alleviating heterogeneity, securing the seamless communication process, and facilitating secure, portable, and scalable multi-cloud deployments. Overall, the current research may be useful in understanding how organizations can pursue viable integration models to achieve effective and sustainable processes of hybrid and multi-cloud.

Future research should focus on dynamic middleware that is flexible to the heterogeneous environment in an attempt to alleviate the lock-in of vendors to facilitate seamless interoperability. APIs and protocols standardization is vital in this regard. The spheres with the potential to improve in resilience, governance, and secure multi-cloud adoption are lightweight encryption, real-time monitoring, AI-driven orchestration, and the adoption of IoT and edge computing on hybrid models.

REFERENCES

1. Oliveira, T., Martins, R., Sarker, S., Thomas, M., & Popovič, A. (2019). Understanding SaaS adoption: The moderating impact of the environment context. *International Journal of Information Management, 49*, 1–12. https://doi.org/10.1016/j.ijinfomgt.2019.02.009

2. Miyachi, C. (2018). What is 'Cloud'? It is time to update the NIST definition? *IEEE Cloud Computing, 5*(3), 6–11. https://doi.org/10.1109/MCC.2018.032591611

3. Vankayalapati, R. K., & Nampalli, R. C. R. (2019). Explainable analytics in multi-cloud environments: A framework for transparent decision-making. *Journal of Artificial Intelligence and Big Data, 1*(1), 1–12. https://doi.org/10.31586/jaibd.2019.1228

4. Kritikos, K., et al. (2019). Multi-cloud provisioning of business processes. *Journal of Cloud Computing*. https://doi.org/10.1186/s13677-019-0143-x

5. Park, J., Kim, U., Yun, D., & Yeom, K. (2020). Approach for selecting and integrating cloud services to construct hybrid cloud. *Journal of Grid Computing, 18*(3), 441–469. https://doi.org/10.1007/s10723-020-09519-x

6. Gundu, S. R., Panem, C. A., & Thimmapuram, A. (2020). Hybrid IT and multi-cloud: An emerging trend and improved performance in cloud computing. *SN Computer Science*. https://doi.org/10.1007/s42979-020-00277-x

7. Al-shammari, M. M., & Alsaqre, F. E. (2012). IT disaster recovery and business continuity for Kuwait Oil Company (KOC).

8. Alshammari, M. M., Alwan, A. A., Nordin, A., & Al-Shaikhli, I. F. (2017). Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. *2017 4th IEEE International Conference on Engineering Technology and Applied Science (ICETAS)*, 1–7. https://doi.org/10.1109/ICETAS.2017.8277868

9. Mallareddy, A., Bhargavi, V., & Rani, K. D. (2014). A single to multi-cloud security based on secret sharing algorithm. *International Journal of Research, 1*(7), 910–915.

10. Kushwaha, A., Pathak, P., & Gupta, S. (2016). Review of optimize load balancing algorithms in cloud. *International Journal of Distributed Cloud Computing, 4*(2), 1–9.

11. Bhadani, U. (2020). Hybrid cloud: The new generation of Indian education society. *International Research Journal of Engineering and Technology*, 2916–2922.

12. Bastião Silva, L. A., Costa, C., & Oliveira, J. L. (2013). A common API for delivering services over multi-vendor cloud resources. *Journal of Systems and Software, 86*(9), 2309–2317. https://doi.org/10.1016/j.jss.2013.04.037

13. Ré, R., Meloca, R. M., Roma, D. N., da C. Ismael, M. A., & Silva, G. C. (2018). An empirical study for evaluating the performance of multi-cloud APIs. *Future Generation Computer Systems, 79*, 726–738. https://doi.org/10.1016/j.future.2017.09.003

14. Reniers, V. (2016, December). The prospects for multi-cloud deployment of SaaS applications with container orchestration platforms. *Proceedings of the Doctoral Symposium of the 17th International Middleware Conference* (pp. 1–2). https://doi.org/10.1145/3009925.3009930

15. Geeta, Gupta, S., & Prakash, S. (2019). QoS and load balancing in cloud computing access for performance enhancement using agent-based software. *International Journal of Innovative Technology and Exploring Engineering, 8*(11S), 641–644.

16. Hentschel, R., & Strahringer, S. (2020, March). A broker-based framework for the recommendation of cloud services: A research proposal. In *Proceedings* (pp. 1–9). https://doi.org/10.1007/978-3-030-44999-5_34

17. Petcu, D. (2013). On the interoperability in multiple clouds. In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science (CLOSER 2013)* (pp. 581–590). https://doi.org/10.5220/0004503105810590

18. Farahzadi, A., Shams, P., Rezazadeh, J., & Farahbakhsh, R. (2018). Middleware technologies for cloud of things: A survey. *Digital Communications and Networks, 4*(3), 176–188. https://doi.org/10.1016/j.dcan.2017.04.005

19. Marpaung, J. A. P., Sain, M., & Lee, H. J. (2013). Survey on middleware systems in cloud computing integration. *International Conference on Advanced Communication Technology (ICACT)*, 709–712.

20. Kaur, P., & Sachdeva, M. (2015). A survey on cloud computing and its benefits. *International Journal of Computer Technology*, *15*(4), 6643–6648. https://doi.org/10.24297/ijct.v15i4.6905

21. Di Nitto, E., et al. (2012). MODAClouds: A model-driven approach for the design and execution of applications on multiple clouds. In *2012 ICSE Workshop on Modeling in Software Engineering (MISE 2012)* (pp. 50–56). https://doi.org/10.1109/MISE.2012.6226014

22. Dubey, M., & Singh, K. (2020). Multi-cloud management strategies. *International Journal*, 7(4), 4739–4746.

23. Tomarchio, O., Calcaterra, D., & Di Modica, G. (2020). Cloud resource orchestration in the multi-cloud landscape: A systematic review of existing frameworks. *Journal of Cloud Computing, 9*(1), 49. https://doi.org/10.1186/s13677-020-00194-7

24. Karaja, M., Ennigrou, M., & Ben Said, L. (2020, February). Budget-constrained dynamic bag-of-tasks scheduling algorithm for heterogeneous multi-cloud environment. In *2020 International Multi-Conference on "Organization of Knowledge and Advanced Technologies" (OCTA)* (pp. 1–6). IEEE. https://doi.org/10.1109/OCTA49274.2020.9151737

25. Haytamy, S., & Omara, F. (2020). Enhanced QoS-based service composition approach in multi-cloud environment. In *2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE)* (pp. 33–38). https://doi.org/10.1109/ITCE48509.2020.9047784

26. Di Pietro, R., Scarpa, M., Giacobbe, M., & Oriti, F. (2018). WiP: ARIANNA: A mobile secure storage approach in multi-cloud environment. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 273–275). https://doi.org/10.1109/SMARTCOMP.2018.00055

27. Colombo, M., Asal, R., Hieu, Q. H., El-Moussa, F. A., Sajjad, A., & Dimitrakos, T. (2019). Data protection as a service in the multi-cloud environment. In *2019 IEEE 12th International*

Conference on Cloud Computing (CLOUD) (pp. 81–85). https://doi.org/10.1109/CLOUD.2019.00025

28. Girish, G., & Nischita, N. J. (2017). Cloud broker and their role in a hybrid multi-cloud environment. In *2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon)* (pp. 1532–1535). https://doi.org/10.1109/SmartTechCon.2017.8358621
29. Nalluri, S. K., Parasaram, V. K. B., & Bathini, V. T. (2021). Autonomous Manufacturing Operations Using Intelligent MES and Cloud-Native Analytics. Journal of Multidisciplinary Knowledge, 1(1), 45–55. Retrieved from https://jmk.datatablets.com/index.php/j/article/view/127
30. Gupta, I., Kumar, M. S., & Jana, P. K. (2016). Compute-intensive workflow scheduling in multi-cloud environment. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 315–321). https://doi.org/10.1109/ICACCI.2016.7732066