Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

Analyzing the Limitations and Efficiency of Configuration Strategies in Hybrid Cloud Environments

Waddiat U Zahra[1], Muhammad Talha Amjad[1*], Anam Ahsan[2], and Gohar Mumtaz[1]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.
[2]Department of Computer Science, University of Lahore, Sargodha, 40100, Pakistan.
[*]Corresponding Author: Muhammad Talha Amjad. Email: talhaamjadmscs@gmail.com

Received: July 02, 2024 **Accepted:** August 21, 2024 **Published:** September 01, 2024

Abstract: The improvement in complexity and size of today's computing requirements has prompted the creation and widespread adoption of computing in the cloud as an accepted model for data processing and storage. The hybrid cloud architecture, which combines private as well as public cloud structures, is very appealing to organizations that want both the security benefits of private clouds and the scalability of public clouds. Numerous approaches of setting up and overseeing resources have been created in order to maximize the hybrid cloud environment. These tactics seek to strike a compromise between competing goals like security, performance optimization, cost effectiveness, and regulatory compliance. This observational research's aim was to obtain the effectiveness and drawbacks of various setup approaches in hybrid cloud settings. The results show that every strategy offers unique benefits. Policy-based resource management has several benefits, including increased resource efficiency and automated governance procedures, which reduces costs. Through intelligent traffic routing, cross-cloud load sharing improves performance and raises availability of services. By centralizing control, the Hybrid Cloud-Based Mesh makes cross-service connectivity secure and effective. One noteworthy aspect of Container orchestration across clouds is its capacity to streamline application migrations between various cloud environments. Log Management and Analytics enable real-time monitoring for prompt threat detection and regulatory compliance. On the other hand, policy-based resource management can be rigid and complicated. An additional expense associated with data transport across several cloud providers is a disadvantage of cross-cloud load sharing. Latency problems arise in Hybrid Cloud Service Mesh topologies when there are extra network hops. Cross-cloud Container Orchestration may put the system at risk for security issues if it is set improperly. Lastly, substantial storage and sophisticated analytical skills are needed for log management and analytics.

Keywords: Hybrid Cloud; Strategies; Resource Management; Cloud Computing; Limitations.

1. Introduction

The way computing resources are delivered, used, and distributed has been completely transformed by cloud computing. Under traditional approaches, businesses would have to shell out a lot of money for software licensing and physical hardware, which would result in high capital expenditure and continuous maintenance costs. Through the use of Internet technology and virtualization, resources can be provided as services, cloud computing modifies this paradigm [1], [2]. This implies that consumers can lease or hire these resources as needed, as opposed to owning actual servers or software. This strategy's immediate benefits include reduced upfront expenses, the capacity to dynamically increase resources in response to demand, and easier management and maintenance. Moreover, the centralized structure of cloud computing Figure 1 allows for high degrees of automation, which helps businesses save money and operate more efficiently.

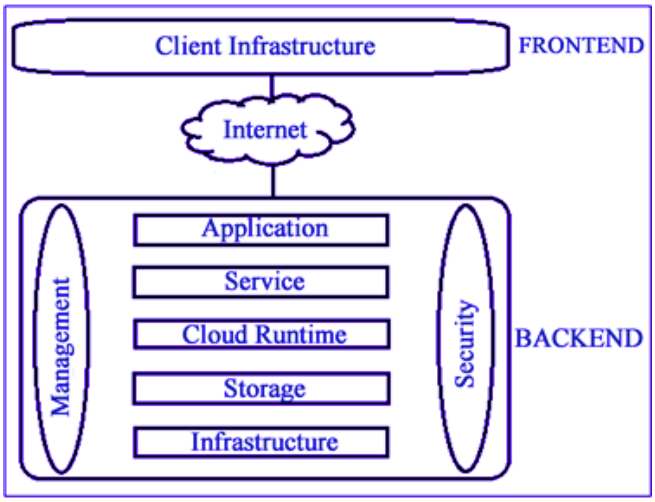

Figure 1. Cloud computing's general architecture

Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS) are the most often offered cloud computing model services [3]. Networks, storage, and virtual computers are all delivered via the Internet by IaaS. This eliminates the need for companies to purchase hardware by enabling them to run their own apps on rented servers. PaaS builds on this concept by providing an integrated platform where programmers can create, launch, and maintain apps without having concerns about the infrastructure that underlies them. By distributing software applications over the Internet, SaaS removes the need for end users to set up and operate software on their own computers [4]. These services are all typically provided on a pay-per-use or subscription basis, which makes them affordable for both individual users and businesses [5]. Table 1 is elaborating the characteristics of modern hybrid cloud environment.

Table 1. Characteristics of modern hybrid cloud computing

Characteristics	Explanation
Adaptability	Allows workload migration and makes it easier to integrate legacy infrastructure with public cloud services.
Management of costs:	Through environment selection, it enables the strategic deployment of capital and operating expenses.
Scalability and Agility:	Promotes resource deployment and provisioning; allows public cloud bursting to handle demand spikes.
Interoperability and Resiliency:	Facilitates component interoperability between private and public settings and offers task redundancy.
Compliance:	Ensures data location in line with legal requirements; allows for specific public cloud usage.1

The main method by which the user communicates with the system is via a 3rd Party API, which makes it possible to process their requests. The privately owned cloud, which is linked to a Kubernetes cluster and possesses integrated server abilities serves as the focal point for these interactions [6]. Together, these components facilitate the management and streamlining of user requests, resulting in an intuitive and effective overall experience. Furthermore, an architectural system for front-end clouds is defined. The more visible elements of the cloud environment are shown by this platform, such as a corporate interface that makes access to different apps easier. A firewall mechanism is in place to guarantee security and control access. Authorized users are able to connect and make use of the services offered by this firewall through interfaces with a variety of devices, including laptops and mobile phones [7].

2. Systematic Literature Review

The concept of cloud computing initially surfaced in the 1960s with the development of time-sharing, which allowed multiple users to utilize a single computer at simultaneously. However, the modern concept of cloud computing—which involves providing computer resources over the internet—was first introduced in the late 1990s. Computer scientist Ramnath Chellappa first used the term "cloud computing" in a 1997 paper to describe the novel approach of delivering computer services online. However, it wasn't until the middle of the 2000s, with the rise of virtualization and the expansion of online services that cloud computing became a popular commercial concept. Two more early cloud providers, Microsoft Azure and Google Cloud Platform (GCP), were both released in 2008. Since then, computing on the cloud has become widely accepted in society, providing access to a wide range of cloud providers and services for companies of all sizes. Without the requirement for direct user management, cloud computing is the on-demand provisioning of computer system resources, primarily processing power and data storage (cloud storage). Functions in big clouds are frequently dispersed among several sites, each of which is a data center. Cloud computing's "pay as you go" model may assist reduce capital expenses, but it may also result in unanticipated operating costs for users. Coherent operation of cloud computing requires resource sharing [8].

A cloud computing metaphor is shown in Figure 2. "The whole provider-managed suite of both software and hardware is capable of being thought of as an unstructured cloud; the group of networked components providing services does not have to be separately addressed or controlled by users [9]." Four main categories comprise cloud computing:

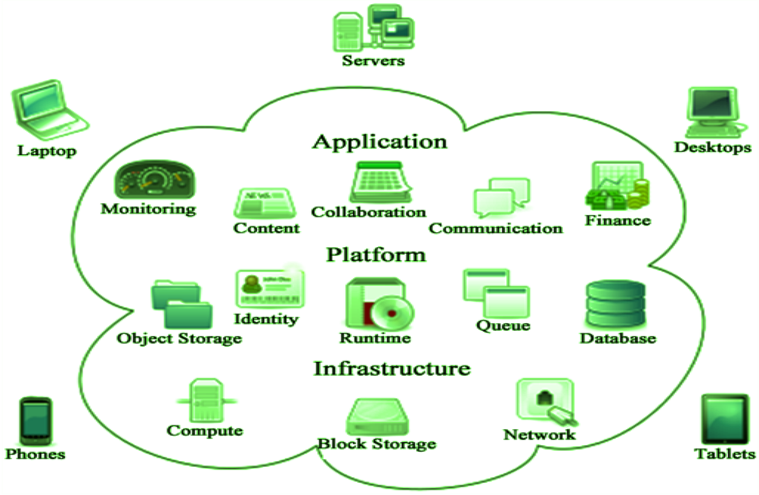

Figure 2. Basic architecture of cloud computing

2.1. Private Clouds

These are often employed by major enterprises or organizations that demand high levels of protection, management, and customization for their computer systems. They are devoted to a single firm or organization. Users in the organization have access to networking, storage, and servers that are virtualized. A cloud that is private can be housed on the company's property in its own data center or off-site by an outside provider.

2.2. Public Clouds

These environments are frequently constructed using IT infrastructure that is not end user owned. Alibaba Cloud, Google Cloud, IBM Cloud, Microsoft Azure, and Amazon Web Services (AWS) are some of the major suppliers of public cloud services.

2.3. Cloud Hybrids

This system seems to be integrated into a single, unified environment through the use of LANs, WANs, VPNs, and/or APIs. Hybrid clouds are intricate, with many moving parts and particular requirements [10].

2.4. Multi-Clouds

A multi-cloud architecture consists of several cloud services from various public or private cloud service providers. Even while not every multi cloud is a hybrid cloud, every hybrid cloud is a multi-cloud. When several clouds are coupled by management or equality, mixed clouds are produced. In addition, there are three main types of cloud computing services:

- IaaS stands for (infrastructure-as-a-service).
- PaaS stands for (Platforms-as-a-Service).
- SaaS stands for (software-as-a-service)

The cloud computing system is an innovative approach that has evolved recently for organizing and distributing services over the Internet. Business owners find the use of cloud computing appealing because it removes the need for customers to plan for deployment and allows firms to start tiny and grow only when demand for services increases [11]. Although the use of cloud computing has huge prospects for the IT sector, it is currently in its early stages and has numerous unresolved challenges. We present an overview of the cloud computing environment in this work, covering fundamental concepts, architectural principles, cutting-edge implementation, and unresolved research challenges. For example, with an imperfect cloud setup, the exact same performance target could cost up to 12 times more. If similar workloads are performed on an ongoing basis by recurring activities, effective cloud architecture can result in significant cost savings. Nevertheless, choosing the best cloud setup is necessary. For example, it is challenging to simultaneously achieve high accuracy, low costs, and adaptability for multiple applications, making it challenging to identify the fastest or most affordable solution [12].

3. Methodology

The two most popular deployment options are both public and private cloud. Under a public cloud strategy, a third-party provider's cloud service offers computational resources that are made available to the general public. These resources are usually provided over the Internet and are owned and managed overseen by the vendor of cloud services. Since resources are shared among several tenants, users of a public cloud can benefit from its cost-effectiveness and scalability [13]. Users have less control over the infrastructure, which can lead to worries about data security, compliance, and performance in a multi-tenancy setting.

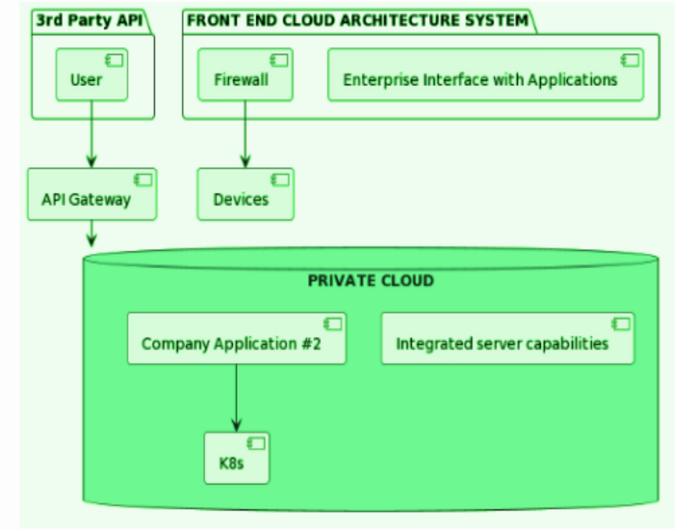
3rd Party API
FRONT END CLOUD ARCHITECTURE SYSTEM
User
Firewall
Enterprise Interface with Applications
API Gateway
Devices
PRIVATE CLOUD
Company Application #2
Integrated server capabilities
K8s

Figure 3. Frontend elements and user interaction in hybrid clouds

Because a single business uses all of the computing resources, the cloud model provides a more controlled environment. A cloud that is private may be remotely hosted by a different company or internally by an organization. The firm benefits from higher levels of security and compliance, increased customization options, and more control over its data in both scenarios. However, the Private Cloud approach typically entails greater expenses for both initial setup and continuing maintenance. Additionally, if the Private Cloud is housed on-premises, it could not have the same flexibility and scalability as a Public Cloud [14].

By offering a flexible computing environment, the hybrid cloud paradigm seeks to balance the advantages of private as well as public cloud installations as shown in Figure 3 and 4. An enterprise can employ its own cloud for highly specialized, sensitive tasks that demand a high level of control and safety, and a public cloud for activities that may profit from higher capacity and cost-efficiency, by implementing a hybrid cloud system. Crucially, in a hybrid cloud, the private and public cloud components stay separate but are linked by a variety of technologies that facilitate smooth data and application transfer. Organizations can allocate their workloads more strategically thanks to interoperability, selecting the best environment for each task [15].

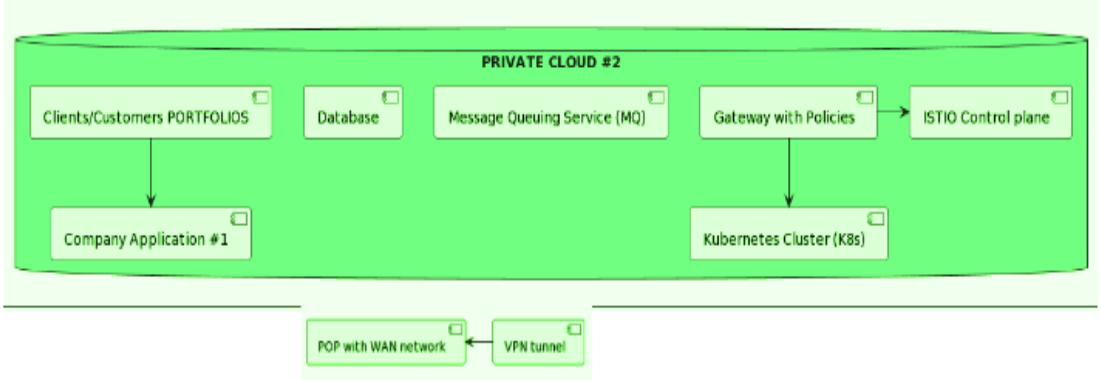

Figure 4. Data management and backend components of hybrid clouds

Implementing hybrid cloud solutions gives businesses a great deal of flexibility in how they allocate and manage their computer resources. Operating a private cloud on-site while utilizing services from a public cloud provider is a popular strategy used by enterprises. On the other hand, certain companies may choose to work with a provider who focuses in individual cloud solutions and is connected to a cloud service provider. The primary objective is to enable a company to tailor its internet computing environment to its own needs. For large-scale analysis of data, for instance, when the benefits of cost and scalability are most apparent, a company may decide to employ the public cloud. Sensitive client data is stored in a secure cloud where stricter security measures can be put in place in the interim.

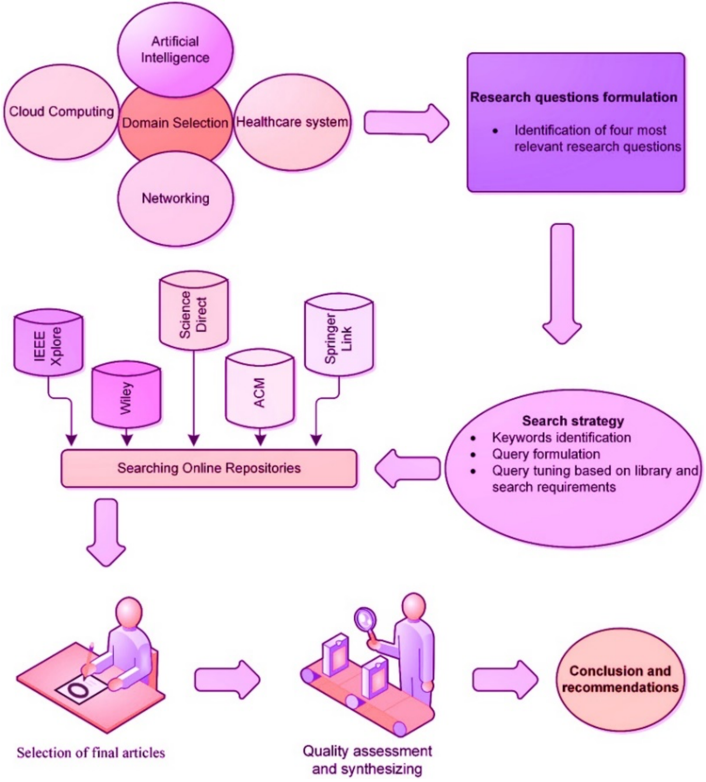
Artificial Intelligence
Cloud Computing
Domain Selection
Healthcare system
Networking
Research questions formulation
Identification of four most relevant research questions
IEEE Xplore
Wiley
Science Direct
ACM
Springer Link
Searching Online Repositories
Search strategy
Keywords identification
Query formulation
Query tuning based on library and search requirements
Selection of final articles
Quality assessment and synthesizing
Conclusion and recommendations

Figure 5. Research methodology suggestion

Operating requirements, strategic goals, and regulatory factors frequently come together to influence the choice to use a hybrid cloud. By distributing resources between public as well as private, settings in real-time in response to demand, operational efficiency can be enhanced. By doing this, businesses can minimize expenses without sacrificing security and performance requirements. Another important consideration is regulatory compliance; some data may be governed by laws requiring its processing and storage in a particular manner or inside a particular jurisdiction. A hybrid cloud gives you the freedom to abide by these rules while yet taking advantage of cloud computing's advantages. By fusing the more control and performance of private clouds with the scalable, economical features of public clouds, the framework of hybrid clouds seeks to provide enterprises with the ideal combination of both. Because of this, companies may easily incorporate cloud-based services into their current IT infrastructure without having to make significant changes. This is especially helpful for businesses that wish to leverage the benefits of computing in the cloud for specific company activities or workloads but have already invested a lot in on-premises systems. Hybrid clouds enable more flexible resource allocation, which can help businesses reduce expenses and boost productivity [16].

An extensive and comprehensive assessment of the proposed research was carried out on 5 digital libraries in order to gather data from different academics working in the area of developing sync software for cloud-based computing. The following online digital libraries were searched for pertinent research publications: IEEE Xplore, ScienceDirect, ACM Digital Library, Springer Link, and Wiley. Figure 5 shows the overall review procedure. The titles, the abstracts, and key words of researched papers such as articles from journals, papers for conferences, and textbook chapters were analyzed in order to complete the proposed study. Articles are obtained and searched from relevant libraries to avoid repetition.

4. Hybrid Cloud Management

Through the combination of cloud services and physical infrastructure, like services from several cloud providers, as well as both private and public clouds, hybrid cloud management offers a sophisticated method of managing computing resources. The goal is to provide an integrated platform that simplifies different organizational requirements [17]. IT resources can be easily created and scaled in both local and cloud-based systems thanks to resource provisioning. This is especially helpful for companies with varying workloads that need to allocate resources quickly. Management and monitoring capabilities enable the continuous observation of security indicators, system well-being, and resource performance across all organizational contexts. By lowering the possibility of human error and raising overall efficiency, automation features help to streamline routine processes and resource provisioning.

Tools for chargeback and show back are frequently included in the unified platform, offering a clear picture of resource usage and facilitating improved budgetary planning. Features related to security and compliance are essential to hybrid cloud management. Across a variety of situations, the platform may impose consistent security measures like encryption and access controls. This guarantees the uniform application of security regulations and compliance standards, such GDPR or HIPAA, irrespective of the location of data or the manner in which resources are employed [18].

Resource optimization, scalability, flexibility, and multi-cloud management are the main components of hybrid cloud management. Organizations may scale up or down their apps and services in response to demand thanks to scalability and flexibility. These characteristics also make it possible to select the best environment, on-site or in the cloud, for particular workloads. Resource optimization seeks to reduce waste through efficient resource allocation determined by performance measurements and real-time demand.

4.1. Policy-Based Resource Management

A systematic method called "policy-based resource management" applies pre-established guidelines or policies to the administration of different resources in a hybrid cloud environment. In this context, "resources" refers to the processing power, storage, bandwidth, and other elements required for cloud-based services and apps to operate. Policies can accomplish a variety of goals, such as restricting access, defining the distribution of computing resources, or complying with external legal and regulatory requirements, whereas Table 2 is describing the policy-based modules. Organizations can eliminate uncertainty and the possibility of misuse by defining explicit policies that set criteria for the distribution and utilization of resources [19].

Table 2. Advantages and Platforms for Policy-Based Resource Management

Modules	Discussion
Advantages:	**Automation of Tasks:** • Reduces human error. • Streamlines administrative procedures. • Distributes resources based on organizational guidelines. • Example: Automatically increasing server capacity during high online shopping periods.

	Access Control: • Limits access to sensitive information to authorized individuals. **Effective Policy Enforcement:** • Ensures compliance with legal and ethical obligations. • Adheres to data sovereignty laws and industry standards like PCI DSS and HIPAA. • Enhances organizational reputation and mitigates financial and legal risks. **Centralized Management:** • Provides a common dashboard for overseeing policies across various cloud services and environments. • Achieves a cohesive and effective management structure. **Optimized Resource Utilization:** • Defines parameters and criteria for resource allocation. • Example: Consolidating virtual machines onto fewer servers during low demand to save money and energy. • Maximizes resource value and minimizes waste. **Automated Governance:** • Facilitates compliance and security policy enforcement. • Reduces the need for manual monitoring and lowers the risk of human error. • Maintains consistent compliance across various cloud environments. **Cost Savings:** • Automatically distributes resources according to usage patterns. • Example: Relocating workloads to lower-performance storage during off-peak hours to save costs. • Minimizes wasteful spending by ensuring resources are only paid for as needed.
Platforms:	VMware vRealize Suite Microsoft Azure Policy **AWS Organizations** • These platforms help define, implement, and enforce policies. • Provide a centralized control for uniform policy application and execution.
Challenges:	**Complex Policy Creation:** • Requires specialized knowledge to address organizational needs and legal obligations. • Smaller businesses or departments may struggle due to a lack of technical expertise.

	Flexibility Issues: • Policies may be rigid and not adaptable to sporadic or extraordinary events. • Example: Difficulty in quickly distributing resources to meet sudden demand increases.

4.2. Cross-Cloud Load Sharing

A method of distributing incoming traffic from the network among many cloud environments, with the occasional extension to on-premises systems as well is called cross-cloud load balancing. By making sure that data flow and computational workloads are dispersed equally among the available resources, this strategy seeks to maximize application performance. By avoiding any one cloud environment or server from acting as a bottleneck, this strategy enhances user experience and application response times. Furthermore, because traffic can be routed to servers that are physically nearer to the end users or that are less busy due to cross-cloud load sharing, it allows for a more effective use of resources.

The load splitter device itself is specifically engineered to be globally operational, computer-based, and platform-neutral. Known as multi-cloud or hybrid cloud settings, this load balancer controls traffic between several cloud deployments. The elements of a cloud-based hybrid system are one or more on-premise data centers and public clouds, whilst a multi-cloud environment may consist of several public cloud providers. Traffic is routed to servers situated in these various environments via the load balancer. The servers within distinct clouds or data centers manage incoming traffic in accordance with the load balancer's instructions. Regardless of where the servers are situated, server farms or cloud environments, load balancers, and the DevOps team work together to ensure that traffic is dispersed effectively [20].

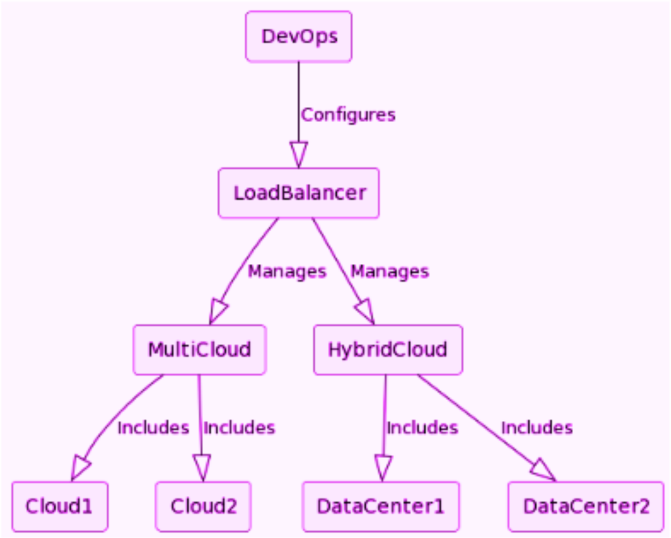

Figure 6. Multi-cloud and hybrid load balancing

Cross-cloud load balancing enhances high availability by distributing traffic across multiple environments Figure 6, reducing the risk of service disruption from a single provider's failure. The load balancer minimizes downtime and ensures continuous application operation by automatically rerouting traffic to other environments in the event of an outage in one of the compromised environments.

Additionally, cross-cloud load balancing uses advanced algorithms to route traffic based on server health, load, and latency. This intelligent routing optimizes performance and resource utilization, adapting flexibly to fluctuating demand and improving overall application efficiency. By distributing network traffic across multiple cloud environments, cross-cloud load balancing reduces only one point of failure's influence. Should a cloud provider experience outages or other problems, traffic can be quickly redirected to operational services, ensuring continuous availability and meeting high availability standards crucial for business continuity. The system also adapts to changing application demands, such as seasonal traffic spikes, by scaling resources across different cloud providers. Algorithms direct traffic to the nearest or most effective servers, reducing latency and enhancing user experience. This approach optimizes resource usage by balancing workloads and preventing overloading in any single environment [21].

Handling several cloud providers can introduce an additional degree of operational complexity that can be difficult to manage because each has its own set of tools, APIs, and pricing plans. Because of this complexity, maintaining coherency across several cloud systems may need for additional management tools and specialized knowledge. The benefits of increased performance and availability may be somewhat negated by the expenses associated with data transfer, which can be substantial. Concerning possible discrepancy is another issue. It can be difficult to maintain uniform setups, security methods, and policies across several providers, which raises the possibility of configuration errors or security flaws. Thus, even though cross-cloud load sharing has many benefits, these drawbacks must exercise caution taken into account before implementing.

4.3. Hybrid Cloud Service Mesh

Services meshes are advantageous in hybrid cloud structures for modern enterprises with distributed, complicated systems. Serving as a control plane for communication, a service mesh oversees data flow, policies, and inter-service communication between different clouds and on-site hardware. Developers and IT teams can concentrate on creating applications rather than networking problems by using it to streamline operations like distributing loads, traffic routing, and resource discovery. Furthermore, by offering integrated features like identity-based authorization, the use of encryption, and common TLS authentication, a hybrid cloud service mesh improves security. This imposes a zero-trust security approach and guarantees safe data transfer across several platforms. In order to preserve application resilience, it also enables sophisticated traffic management, such as intricate routing rules, canary's experience deployments, and split testing, availability while quickly rerouting traffic in the event of a service failure [22].

In distributed architectures, tracking dynamic service endpoints is challenging due to frequent scaling and migration. A service mesh addresses this by maintaining an up-to-date register of services and their locations, ensuring efficient and timely communication. When services are dispersed across several platforms in hybrid cloud environments, this constantly changing service discovery is especially helpful. Adopting a hybrid cloud service mesh enhances operational flexibility and efficiency by simplifying communication control across diverse environments. It standardizes practices, reducing errors and discrepancies, while it’s centralized monitoring and logging offer valuable insights for troubleshooting and decision-making. The service mesh enables comprehensive performance monitoring and analytics, streamlining data collection and improving overall operational excellence.

Service meshes offer essential built-in functionalities like identity-based access controls and robust encryption, ensuring secure communication between microservices across various cloud environments and on-premises systems. They establish a zero-trust model, enforcing strict access controls and compliance with industry regulations. Moreover, a service mesh facilitates seamless communication across diverse technologies and infrastructures by standardizing interactions between services developed in different languages or hosted on various platforms. This abstraction allows services to interact without needing to understand the specifics of their platforms [23]. However, adding a service mesh can introduce latency due to additional network hops required for routing and security checks, which can be problematic in real-time or high-throughput systems. There is also the risk of vendor lock-in, as some service meshes are optimized for specific platforms, limiting future flexibility. Additionally, configuring and maintaining a service mesh requires specialized knowledge, making it crucial for organizations to invest in skilled engineers to avoid potential service disruptions or security issues.

4.4. Cross-cloud Container Orchestration

The main objective of cross-cloud orchestration of containers is the automated setup, collaboration, and administration of packaged software programs across multiple cloud-based systems and physical data centers. A centralized orchestration engine, usually run by orchestration software like Kubernetes, is at the center of this orchestration Figure 7. This engine initiates operations like load balancing, scaling, and container deployment by interacting with the API of each cloud provider. It converts higher-level instructions into cloud provider-specific API calls, enabling uniform application deployment and maintenance across heterogeneous infrastructures.

The management engine determines the placement of each container based on a set of established guidelines and the system's present metrics. It considers factors including CPU and RAM availability, network latency, and data proximity while making these decisions. Once the optimal location has been determined, the scheduling engine will launch the container's instance and dynamically adjust resources as needed. Containers can be scaled vertically, altering the allocation of CPU and memory, or horizontally, based on predefined rules and real-time demand. When a service is terminated or new instances are deployed, the automation engine maintains a central register. This registry helps to better route incoming requests to the appropriate instances. Load balancers distribute receiving network or application data among multiple servers, preventing any one server from experiencing overloading. In order to guarantee optimal network traffic distribution, the management engine may utilize load balancing techniques and dynamically update the load balancer [24].

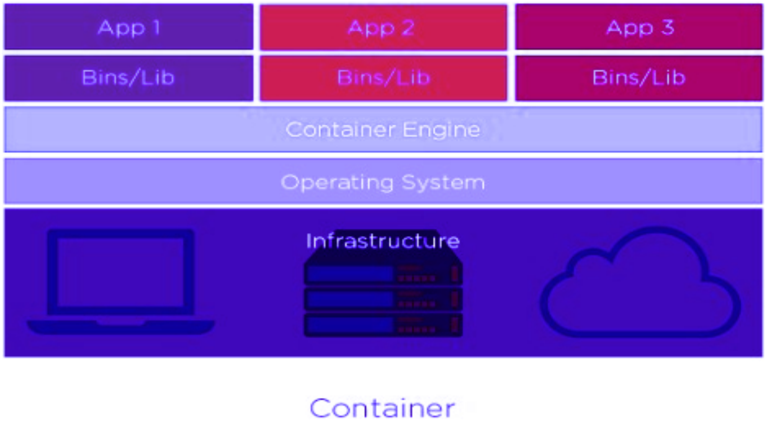

Figure 7. Cross-cloud container orchestration

Frameworks for cross-cloud container orchestration also include monitoring and logging features. These technologies gather logs, performance metrics, and other important data from every instance of a container, no matter where it is located. The combined data is utilized for performance optimization, debugging, and real-time monitoring. Infrastructure that heals itself can be enhanced by using monitoring tools that are set up to generate alerts or start automatic processes like scaling activities in response to particular circumstances. Organizations can swiftly launch and scale apps using cross-cloud container orchestration, meeting real-time computing demands and market demands. Time-to-market for new products and services is accelerated and manual intervention is much reduced because to the centralized orchestration engine's automation of container distribution and scaling. The transfer of apps across cloud providers or between cloud and physical systems is made easier by this orchestration technique. Applications can be moved with ease since containers encapsulate all the dependencies needed for a program to function. When combined containerization combined with a cross-cloud management engine enables companies to take advantage of best-of-breed services from several cloud providers without being locked into a single vendor [25].

The orchestration engine makes sure that all cloud platforms and physical data centers follow the same policies, monitoring procedures, and management practices. Because firms can establish regulations or make adjustments in one location and be sure that the changes will be reflected in other contexts, this consistent approach streamlines governance and compliance. It can be difficult to manage several managements, or even just one management with varied configurations for various cloud providers. The complexity of networking configurations, policy definitions, and configuration files can lead to a high learning curve and continuous administration overhead. Even though the orchestration engine has several security features, including encryption and role-based access controls, an incorrectly configured engine might put the system at danger. In a multi-cloud setting, security needs to be strictly upheld on all fronts, necessitating a thorough comprehension of the unique security capabilities offered by each cloud provider. Concern over resource consumption is also present. The processing capacity and memory needed for the orchestration services itself could result in the need for further infrastructure expenditures [26].

4.5. Analytics and Log Management

In a hybrid cloud platform, Analytics and log management involve several integrated processes to provide a comprehensive opinion on the structure. The process begins with collecting logs from diverse sources such as virtual machines, databases, and networking hardware. Depending on the infrastructure of the business, these logs are collected via brokers or collectors and kept in a single database that may be either directly or in the cloud [27]. After being gathered, logs are normalized to a standard format for consistent analysis. This involves extracting relevant data and mapping it into defined fields. Enrichment follows, adding contextual information like threat intelligence, which enhances the effectiveness of analytics. Statistical models and machine learning techniques are then used to detect patterns, anomalies, and potential security threats, generating alerts for administrators or initiating automated responses.

Log management systems must address challenges related to cloud diversity, including data privacy regulations, latency, and network costs. Some systems offer features to ensure compliance with regulations such as HIPAA and GDPR, and secure log transfer through encryption. Furthermore, container orchestration uses an array of control planes and nodes to automate setting up, growing, and administration of container-based apps across different cloud environments. This is especially true with platforms like Kubernetes. Worker computers executing containers are referred to as nodes in Kubernetes, whereas the control plane oversees the cluster's general state. Declarative configuration is used by Kubernetes, where configuration files define the ideal state of the system, and the platform implements it. This model standardizes resource allocation for CPU, memory, and network bandwidth, allowing consistent management of containerized applications across private, public, or hybrid clouds through a unified API and abstractions like volumes, services, and pods [28].

Real-time monitoring tools continuously analyze incoming information data to identify patterns or occurrences that check predefined criteria. Alerts are generated for administrators to address or trigger automated responses. In hybrid cloud environments, where resources are highly dynamic, real-time monitoring is crucial for maintaining a consistent security posture and ensuring continuous service [29]. Robust log management is essential for compliance with regulations such as HIPAA and GDPR, which mandate secure log management and retention. Centralized log data simplifies audits, creating traceable audit trails and supporting accountability and regulatory compliance.

Log analytics offers valuable insights into various system aspects, including user behavior, performance, and bottlenecks. Modern log management tools feature data visualization and dashboards for both historical and real-time analysis, helping organizations identify trends and anomalies. This insight is crucial for addressing security threats, enhancing user experience, and optimizing performance. Storage is a key consideration in log management, especially given the vast amounts of data generated by hybrid cloud environments. Logs must be managed with guidelines on data lifecycle and retention, utilizing high-capacity storage solutions or cloud services with encryption and redundancy. The two biggest obstacles to data management and analytics are complexity and noise. As systems grow more intricate, specialized analytics tools are needed to process large datasets efficiently. Additionally, "noise"—irrelevant data that can obscure significant patterns—requires ongoing filtering through machine learning and rule-based methods to highlight important events [30].

5. Conclusions

Hybrid cloud combines architecture for both public as well as private clouds to offer businesses an adaptable architecture for compute requirements, software deployment, and storage of information. It provides benefits like increased security, cost savings, and scalability. For security purposes, important data can be stored in a private cloud, whereas fewer critical tasks can be performed by the more affordable public cloud. This setup allows for efficient workload distribution and rapid infrastructure adjustments to meet evolving business demands. Effective management of hybrid clouds involves regulatory compliance, performance monitoring, and resource allocation. By aligning management strategies with organizational goals, IT departments can minimize risks, optimize resources, and ensure compliance. Policy-based resource management enhances efficiency by standardizing tasks such as compliance and access control, and by automating governance to reduce human error. However, this approach can introduce complexity and reduce flexibility, as policies may need regular updates and can be rigid in handling unusual events.

Cross-cloud load sharing distributes network communication across multiple clouds and physical systems, enhancing fault tolerance and performance. It dynamically adjusts to demand but introduces complexities in managing various providers and costs related to data transfers and maintaining consistency. A hybrid cloud service mesh enables secure, seamless communication across diverse environments, offering centralized control and enhanced security. Challenges include the need for specialized setup and maintenance, potential latency, and risk of vendor lock-in. Cross-cloud container orchestration manages containers across multiple clouds and on-premises, providing flexibility and portability. However, it can be complex to handle, requires significant knowledge, and may incur additional costs and security risks. Hybrid cloud log management involves collecting and analyzing log data from various sources, enabling real-time monitoring and compliance. Challenges include managing large data volumes, needing substantial storage, specialized analysis skills, and filtering out irrelevant information.

References

1. Boss, G., Malladi, P., Quan, D., Legregni, L., & Hall, H. (2007). Cloud computing. IBM White Paper, 321, 224–231.
2. Voorsluys, W., Broberg, J., & Buyya, R. (2011). Introduction to cloud computing. In Cloud Computing: Principles.
3. Kim, W. (2009). Cloud computing: Today and tomorrow. Journal of Object Technology, 8(1), 65.
4. Hayes, B. (2008). Cloud computing. Communications of the ACM, 51(7), 9–11.
5. Wang, L., von Laszewski, G., Kunze, M., Tao, J., Foster, I., McCusker, J., & Cao, J. (2010). Cloud Computing: A Perspective Study. New Generation Computing, 28(2), 137–146.
6. Vaishnnave, M., Devi, K. S., & Srinivasan, P. (2019). A survey on cloud computing and hybrid cloud. International Journal of Engineering Research and Applications.
7. Lackermair, G. (2011). Hybrid cloud architectures for the online commerce. Procedia Computer Science, 3, 550–555.
8. Weinman, J. (2016). Hybrid Cloud Economics. IEEE Cloud Computing, 3(1), 18–22.
9. Luo, F., Dong, Z. Y., Chen, Y., Xu, Y., & Meng, K. (2012). Hybrid cloud computing platform: The next generation IT backbone for smart grid. In 2012 IEEE Power and Energy Society General Meeting.
10. Raju, R., Amudhavel, J., & Kannan, N. (2014). A bio-inspired Energy-Aware Multi-Objective Chiropteran Algorithm (EAMOCA) for hybrid cloud computing environment. In Green Computing Conference.
11. Dubey, A., Shrivastava, G., & Sahu, S. (2013). Security in hybrid cloud. Global Journal of Computer Science.
12. Wang, J. K., & Jia, X. (2012). Data security and authentication in hybrid cloud computing model. In 2012 IEEE Global High Tech Congress on Electronics.
13. Tariq, M. I. (2019). Agent-based information security framework for hybrid cloud computing. KSII Transactions on Internet & Information Systems.
14. Lu, P., Sun, Q., Wu, K., & Zhu, Z. (2015). Distributed online hybrid cloud management for profit-driven multimedia cloud computing. IEEE Transactions on Multimedia, 17(8), 1297–1308.
15. Khmelevsky, Y., & Voytenko, V. (2015). Hybrid cloud computing infrastructure in academia. In WCCCE 2015 - The 20th Western Canadian Conference on Computing Education (pp. 8–9).
16. Tariq, M. I. (2018). Analysis of the effectiveness of cloud control matrix for hybrid cloud computing. International Journal of Future Generation Communication and Networking, 11(4), 1–10.
17. Rao, T. V. N., Naveena, K., & David, R. (2015). A new computing environment using hybrid cloud. In Computing Conference.
18. Goyal, S. (2014). Public vs private vs hybrid vs community - Cloud computing: A critical review. International Journal of Computer Networks & Communications, 6(3), 20–29.
19. Balasubramanian, R., & Aramudhan, M. (2012). Security issues: Public vs private vs hybrid cloud computing. International Journal of Computer Applications.
20. Mateescu, G., Gentzsch, W., & Ribbens, C. J. (2011). Hybrid Computing—Where HPC meets grid and Cloud Computing. Future Generation Computer Systems, 27(5), 440–453.
21. Zou, C., Deng, H., & Qiu, Q. (2013). Design and implementation of hybrid cloud computing architecture based on cloud bus. In Mobile Ad-hoc and Sensor Networks Conference.
22. Gordon, A. (2016). The hybrid cloud security professional. IEEE Cloud Computing, 3(1), 82–86.
23. Linthicum, D. S. (2016). Emerging hybrid cloud patterns. IEEE Cloud Computing, 3(1), 88–91.
24. Beaty, K. A., Kumaraswamy, S., Nelson, S. R., & Liu, Y. (2016). Managing sensitive applications in the public cloud. IBM Journal of Research and Development, 60(2-3), 4:1-4:13.
25. Thaler, J., Shin, W., Roberts, S., & Rogers, J. H. (2020). Hybrid approach to HPC cluster telemetry and hardware log analytics. In 2020 IEEE High Performance Extreme Computing Conference.
26. Birje, M. N., & Bulla, C. (2019). Cloud monitoring system: Basics, phases and challenges. International Journal of Recent Technology and Engineering, 8(3), 4732–4746.
27. Wikipedia. (2022). Cloud computing. In Wikimedia Foundation. Retrieved from https://en.m.wikipedia.org/wiki/Cloud_computing
28. Red Hat. (2022). Types of cloud computing. We Make Open-Source Technologies for the Enterprise. Retrieved from https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud
29. Cloud Computing: Literature Review. (2022). Retrieved from https://mars.gmu.edu/bitstream/handle/1920/11608/hassan_cloud.pdf?sequence=1
30. Home. (2022). Architecture of cloud computing. Retrieved from https://www.geeksforgeeks.org/architecture-of-cloud-computing/amp/