International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V6I2P104
Eureka Vision Publication | Volume 6, Issue 2, 30-37, 2025

Original Article

Testing in Multi-Cloud Environments Ensuring Consistency Across Distributed Systems

Daniel Raj Jeevaguntala
State of NY, Dept. of Health.

Received On: 18/02/2025 ***Revised On: 03/03/2025*** ***Accepted On: 28/03/2025*** ***Published On: 19/04/2025***

Abstract *- Multi-cloud architectures integrate multiple cloud service providers to manage data, applications, and computing resources, delivering advantages such as enhanced flexibility, redundancy, and cost-effectiveness. However, these environments encounter challenges related to resource fragmentation, inconsistent governance structures, and interoperability limitations, which impact overall performance during high workloads, system failures, and sudden demand fluctuations. This study presents a systematic evaluation framework to assess multi-cloud strategies using critical performance indicators, including response time, fault recovery, scalability, and data consistency. A scenario-based testing methodology is employed to analyze the performance of four multi-cloud architectures: Hybrid Multi-Cloud, Multi-Cloud Balancing, Cloud Bursting, and Distributed Multi-Cloud. Additionally, SWOT and PESTLE analyses are incorporated to examine strategic, technical, and regulatory factors influencing multi-cloud deployment. The findings demonstrate that Distributed Multi-Cloud Architecture achieves the highest reliability (94%) and the fastest failure recovery time (15s), ensuring superior fault tolerance. Meanwhile, Cloud Bursting offers the lowest response time (220ms) and the highest scalability rating (5), making it ideal for dynamic workload management. This study provides data-driven insights to support organizations in optimizing multi-cloud performance, improving governance models, and enhancing interoperability.*

Keywords *- Multi cloud strategies, Distributed systems, SWOT analysis, PESTLE analysis, Scenario analysis and Interoperability.*

1. Introduction

Multi cloud storage is an architectural framework that uses multiple cloud storage services from different providers to manage data, application and resources shown in Fig.1. The rapid adoption of cloud computing has leads to the emergence of multi cloud environments where the organizations utilize the services to predict performance, scalability and reliability. Computing systems are interconnected with various cloud storage providers. The data files are stored at devices situated at various cloud storage provider's locations. Computers of cloud user employ these storage devices through cloud access interface functionalities offered by each cloud provider [1].

The complexity of managing resources across different cloud platforms offers results in performance discrepancies, resource fragmentation and difficulties in ensuring fault tolerance. Multi cloud environments provides several advantages including flexibility, redundancy and cost optimization. The management of multi cloud environments is filled with complexities that can impact the performance of the metrics. Variations in performance across different cloud platforms specifically during high load or failure scenarios that can damage the overall efficacy of the system [2]. The increased risk of resource fragmentation and the difficulty in implementing consistent governance and security policies across cloud providers contribute to operational inefficiencies. The lack of unified governance framework across multi-cloud environments intensifies these problems. These highlight the need for a structured approach for testing and evaluating multi cloud strategies.

To examine the performance of multi cloud strategies, it is essential to focus on several key performance metrics such as response time, scalability, throughput and system reliability. These metrics offer information into how well a system can handle increased workloads, how quickly it can recover from failures and how efficiently it manages resources across different cloud platforms. Examining the cost efficiency of multi cloud environments ensures that organizations can obtain optimal performance without excessive operational costs [3]. This study takes a comprehensive approach to evaluate the performance of multi cloud strategies. Through scenario analysis the study simulates high load conditions, system failure and sudden demand changes to evaluate strategy performance in real world situations. By analyzing the scenarios, the study provides valuable information into how different strategies can maintain consistent performance even in the face of adversity. In addition, the study employs SWOT and PESTLE analyses [4]. They help in understanding both the internal and external factors that impact the adoption and implementation of multi cloud strategies. The findings from the study provides information for organizations looking to implement multi cloud systems, ensuring that they can maintain uniform performance over their distributed infrastructure. The study also contributes to the academic understanding of multi-cloud environments by providing a detailed examination of how different strategies measure up under real-world conditions. The key contributions of the study are:

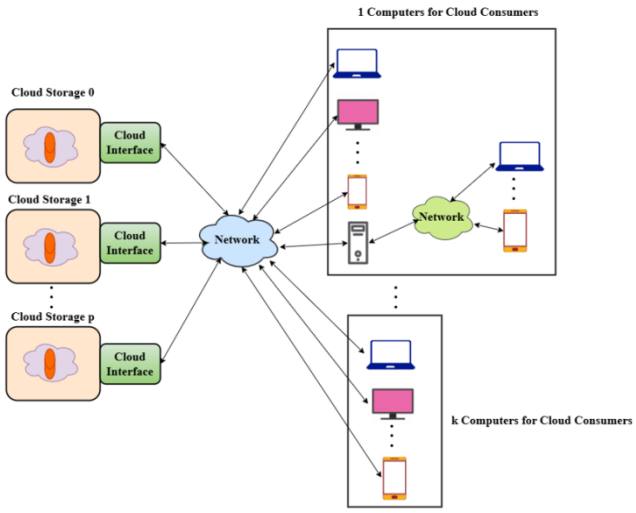

Figure 1. Multi cloud storage system

- To assess multi-cloud strategies under different operational conditions by analyzing response time, fault recovery, data consistency, and scalability
- To perform scenario-based consistency testing across Hybrid Multi-Cloud, Multi-Cloud Balancing, Cloud Bursting, and Distributed Multi-Cloud architectures.
- To provide strategic insights through SWOT and PESTLE analyses for optimizing multi-cloud governance, interoperability, and fault tolerance.

The structure of this paper is as follows: Section 2 provides a comprehensive review of related research on multi-cloud strategies and consistency testing, highlighting existing challenges and research gaps. Section 3 describes the methodological approach for scenario-based consistency testing. Section 4 presents the findings and analysis, covering consistency evaluation, SWOT and PESTLE assessments, and performance. Finally, Section 5 outlines the key conclusions drawn from the study, along with recommendations and future research directions.

2. Related Works

Yeboah-Ofori et al. (2024) [5] aimed to address security and governance problems in multi cloud setups by looking at the vulnerabilities, attack routes and operational inefficiencies. The study evaluated three multi-cloud management tools such as Azure Arc, Google Anthos and AWS elastic Kubernetes Service (EKS). They conducted simulated attacks on multi cloud platforms to determine weaknesses and offers security enhancements. Findings illustrated the efficiency of these methodologies in securing multi-cloud environments and highlighted the significance of governance mechanisms, whereas resource optimization and interoperability remains as a challenge. Zhang et al. (2023) [6] aimed to improve the security detection in multi cloud systems by examining the file processing over its full life cycle. They combined control flow and performance analysis using event logs from various cloud services to determine the security threats such as insider attacks that are frequently overlooked by typical intrusion detection systems. The study demonstrated the efficacy of mining process in offering more information into file security.

Alyas et al. (2022) [7] developed a multi cloud security approach utilizeng honeypot technology to enhance security by diverting the attackers and offering time to analyze and reduce intrusions. The study comprised of two-phase experiment such as the attacks were analyzed without honey pot module and at the second phase the honey pot module was engaged resulting improvement in detection accuracy. Ouchaou et al. (2022) [8] developed an innovative cloud federation architecture for resolving the complexities of service management in multi cloud environments focusing interoperability, users' needs and service administration. The study utilized trust principles, semantic web ontologies, clustering methods and graph theory to develop a service management system and a service publication algorithm for automating operations, optimizing storage and enhancing user experience. Results indicated that federated environments outperformed single cloud setting, whereas the virtual views remained a significant limitation for the proposed system.

Viswanath and Krishna (2021) [9] designed a hybrid encryption method to protect massive data in multi-cloud environments towards theft and illegal access. They provided a secure framework for data uploading, slicing, indexing and encryption and decryption, in order to protect data from insider and DoS attacks. The authors determined that their AES-Feistel network method surpassed benchmark algorithms in encryption speed and security using a medical dataset. The study did not address scalability difficulties in large scale multi cloud setups. Lahmar and Mezni (2021) [10] developed a security aware multi cloud service composition strategy utilizing fuzzy formal concept analysis (fuzzy FCA) and rough set theory (RS) to enhance precision and decrease search complexity in choosing secure cloud services. They employed fuzzy relations to analyze cloud security policies and approximate user demands to optimize service composition. This leads to improved performance and reduced search space for trusted cloud services. The study

could not verify whether cloud security policies were effectively implemented.

Anwarbasha et al. (2021) [11] proposed a Dynamic Level Based Integrity Checking Protocol (DAICP) for securing data accuracy and security in multi-cloud systems without requiring data downloads. The method employed provable data possession (PDP) with public key cryptography and EfficientPDP (EPDP) encryption to obtain 96.78% accuracy. Results revealed that the method supports dynamic operations like block modification, deletion and append. Pachala and Sumalatha (2021) [12] presented a hybrid method to improve the data security and privacy in multi cloud environments combining the three modules such as Byzantine protocol, DepSky architecture and shamir secrets sharing method. The study evaluated the performance of the hybrid approach in terms of encryption/decryption time, memory use and authentication time. Findings revealed an enhancement in encryption time, decryption time, memory use and average precision with hybrid approach surpassing conventional methods.

Ramamurthy et al. (2020) [13] examined security, cost and manageability when selecting cloud service providers (CSP)s for hosting web applications in a multi cloud background. They proposed a holistic method employing multiple criteria decision making (MCDM) to examine CSP combinations and an optimization model to select the best CSPs based on budget and ranking. They employed numerical experiments to determine how data residency laws and latency constraints affect CSP selection. The study did not address the scalability approach for large enterprises. Chimakurthi (2020) [14] studied the zero-trust security model's implementation and principles in Multi cloud background to secure the users, devices and resources over public and hybrid cloud architectures. The study addressed the shift from static network perimeters to dynamic authentication and authorization process. Findings highlighted the growing adoption of zero trust principles by leading tech organizations while the integration of this model into numerous corporate structures was difficult.

While significant advancements made in addressing security, governance and service optimization in multi cloud environments, there exist a gap in ensuring consistency across distributed systems during testing. The difficulties of optimizing resources and interoperability continue to pose barriers to seamless multi cloud integration [5]. It highlighted the limitation of a typical intrusion detection systems in identifying insider attacks [6]. Virtual views in cloud federation and service management can make multi cloud operations inconsistent and unreliable [8]. Scalability challenges [9], inconsistent security policy implementation [10] and difficulties in zero trust model integration [14] can hinder uniform service validation, policy enforcement and consistent testing across multi cloud environments. While the existing studies addressed several aspects, but there is still a lack of thorough frameworks and methodologies designed for ensuring consistency during testing in distributed multi cloud systems.

3. Methodology

This study utilized a combined approach thereby integrating the qualitative and quantitative analytical methods to examine the multi-cloud strategies and ensuring consistency across the distributed systems. The methodology addresses the complexity of the multi cloud environments by examining the cost efficiency, performance, reliability and security. At its core the methodology is centered on the evaluation of the multi-cloud strategies by measuring its performance metrics such as processing speed, resource utilization and response time, predicting a clear picture of how different strategies perform in real world scenarios. Techniques such as SWOT and PESTLE were employed to understand the broad strategy and contextual elements influencing the implementation of multi cloud systems.

3.1 Analysis of Multi-Cloud Strategies

3.1.1 Key Testing Challenges in Multi-Cloud Systems

Maintaining consistency in multi-cloud environments poses significant challenges, particularly in data synchronization, latency fluctuations, interoperability, and failure recovery. Variations in replication mechanisms among cloud providers can lead to inconsistencies in distributed datasets, while differences in network routing contribute to variable response times. The absence of standardized APIs across platforms complicates system integration and cross-cloud communication. Additionally, fault tolerance and disaster recovery mechanisms must be rigorously assessed to minimize service disruptions. A systematic testing framework is essential for evaluating resilience, consi

3.1.2 SWOT and PESTLE Analyses

SWOT analysis is employed to examine the strategic positioning of various multi-cloud methods. The analysis help organizations to understand the internal dynamics of each strategy by identifying internal strengths like improved reliability and weakness that includes the integration challenges. External opportunities such as advancements in cloud interoperability and threats like regulatory changes are examined to offer a thorough understanding of the strategic environment. Complementing the SWOT analysis is the PESTLE analysis which moves deeper into the external factors that influence multi-cloud adoption. For instance, political factors include regulations governing cross border data transfer, economic factors, technological factors explore innovations, while legal and environmental considerations evaluate compliance with standards and the ecological impact of data center operations.

3.1.3 Scenario-Based Testing Evaluation

Scenario-based testing assesses multi-cloud strategies by simulating various operational environments to evaluate their performance. This testing approach examines response time deviations, data integrity across cloud providers, fault recovery efficiency, and system scalability. The study systematically analyzes Hybrid Multi-Cloud, Multi-Cloud Balancing, Cloud Bursting, and Distributed Multi-Cloud Architectures, determining which framework

ensures optimal reliability and fault tolerance. By replicating high-traffic scenarios, infrastructure failures, and dynamic workload surges, this evaluation identifies the most robust testing methodologies for maintaining cross-cloud consistency and resilience.

4. Results And Discussion

4.1 Consistency Testing Results and Insights

To effectively communicate the data collected throughout the study a range of graphs, tables and figures were employed. These representations not only highlight important findings but also provide a clear overview, improving its ability to interpret and understand the results in depth.

Table I presents a detailed comparative analysis of consistency testing results for four multi-cloud strategies, evaluating key metrics such as consistency rate, response time, failure recovery, and scalability. The analysis provides insights into how these strategies perform under real-world operational conditions within distributed cloud environments. Fig. 2 to 5 illustrate how each strategy performs under different operational conditions in a distributed cloud environment

Table 1: Consistency Testing Results And Insights

Type of strategy	Consistency (%)	Response Time (ms)	Failure Recovery (s)	Scalability (1-5)
Hybrid multi-cloud strategy	92%	250	20	4
Multi-cloud balancing	89%	280	25	3
Cloud bursting	85%	220	18	5
Distributed multi-cloud architecture	94%	260	15	4

The hybrid multi-cloud strategy achieves a 92% consistency rate, demonstrating strong data integrity and synchronization capabilities across multiple cloud platforms. With a response time of 250ms, it ensures relatively fast resource access, though it falls slightly behind the cloud bursting strategy in this aspect. The failure recovery time of 20 seconds indicates moderate fault resilience, making it capable of handling system disruptions with minimal downtime. A scalability score of 4 suggests that this approach can effectively manage workload fluctuations, making it an ideal choice for organizations that prioritize a balance between redundancy and performance efficiency. The multi-cloud balancing strategy maintains an 89% consistency rate, which is slightly lower than that of the hybrid multi-cloud approach. This variation results from dynamic workload distribution, which may introduce data inconsistencies across cloud providers. With a response time of 280ms, it is the slowest strategy among the four, primarily due to network overhead associated with continuous traffic reallocation. Its failure recovery time of 25 seconds is the highest, indicating that restoring operational stability after failures takes longer in comparison to other strategies. Despite this, a scalability rating of 3 implies that while this approach can support growing demands, it may encounter performance bottlenecks during peak loads.

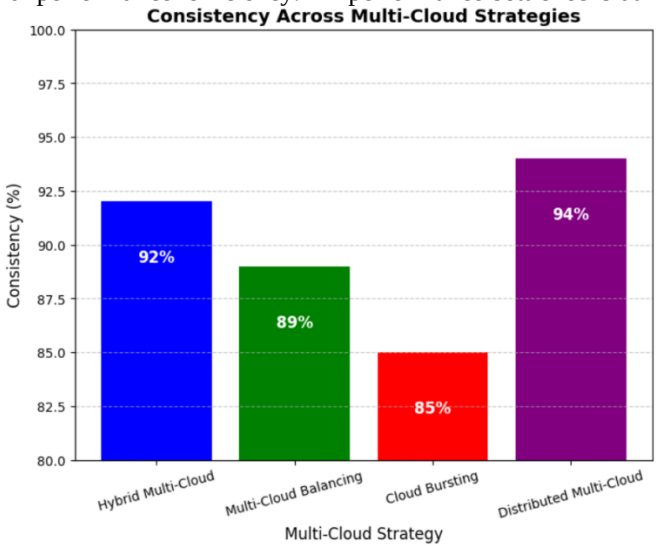

Figure 2. Consistency across multi-cloud strategies

The cloud bursting strategy, designed for dynamic resource scaling, records an 85% consistency rate, the lowest among all strategies. This is likely due to frequent transitions between private and public cloud infrastructures, which introduce synchronization challenges. However, it boasts the fastest response time of 220ms, making it well-suited for handling sudden workload spikes with minimal latency. Its failure recovery time of 18 seconds ranks second best, ensuring swift adaptation to service disruptions. The highest scalability rating of 5 confirms that this strategy excels in elastic resource management, though it comes at the expense of data consistency challenges across different cloud platforms. The distributed multi-cloud architecture emerges as the most resilient and consistent approach, achieving the highest consistency rate of 94%, ensuring robust synchronization across cloud environments. With a response time of 260ms, it outperforms multi-cloud balancing while being slightly slower than cloud bursting. The failure

recovery time of 15 seconds is the fastest among all strategies, emphasizing its superior fault tolerance and autonomous recovery mechanisms. A scalability score of 4 indicates effective workload distribution and resource utilization, minimizing downtime while maintaining high system availability

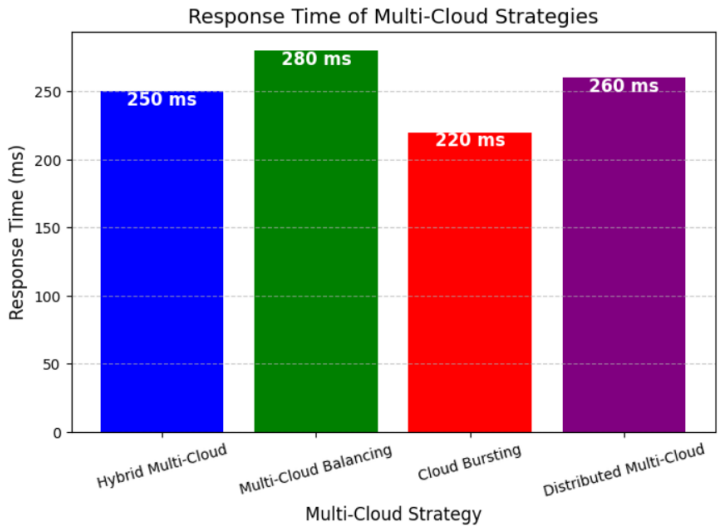

Figure 3. Response time of multi-cloud strategies

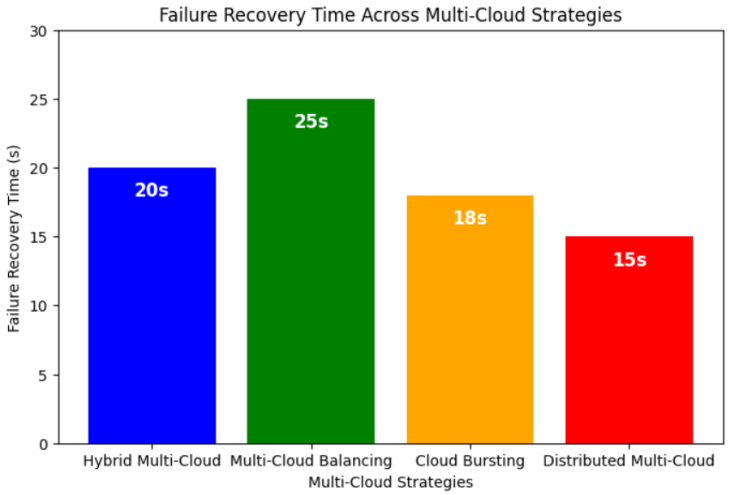

Figure 4. Failure recovery time across multi cloud strategies

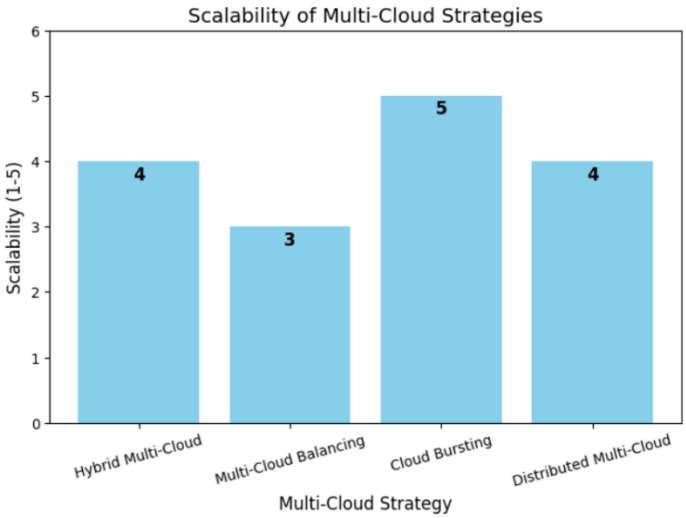

Figure 5. Scalability of multi cloud strategies

4.2 SWOT Analysis for Multi Cloud Strategies

SWOT analysis was performed to examine the effectiveness of numerous multi cloud strategies. This analysis determines the strength, weakness and threats related with each approach. By summarizing the key factors of each strategy, this evaluation provides information into their practical application that helps the organizations to make decisions when selecting a multi-cloud approach. Table II presents the findings related to SWOT analysis.

Table 2: Swot Analysis

Strategy Type	Strengths	Weaknesses	Threats
Hybrid multi-cloud strategy	Provides flexibility by using both private and public clouds	Complex integration and security challenges across different cloud environments	Risk of vendor lock-in and security vulnerabilities from multi cloud complexity.
Multi cloud balancing	Optimizes resource and increases availability by balancing workloads	Requires advanced monitoring tools and operational complexity	Potential performance issues and network bottlenecks to inter cloud information
Cloud Bursting	Enables scalability during peak demand and savings using public clouds	Security concerns when sensitive data moves to the public cloud	High cost during burst usage and risks from sudden bursts to service disruptions.
Distributed multi cloud architecture	Enhances availability and fault tolerance by distributing workloads	High complexity in architecture management and inter cloud communication	Risk of outages in one cloud provider affecting the entire system.

4.3 PESTLE Analysis for Multi Cloud Strategies

The PESTLE method was utilized to examine the external factors influencing the adoption and implementation of multi cloud strategies. This thorough analysis examines the political, economic, social, technological, legal and environmental elements that effect the multi cloud adoption. Table III shows the results for each factor.

Table 3: Pestle Analysis

Factor	Analysis
Political	Policies supporting data sovereignty and cross border regulations influence cloud provider section.
Economic	Cost variability due to fluctuating cloud service pricing frameworks and exchange rate volatility.
Social	Increased demand for data-driven services enhances the adoption of multi-cloud strategies.
Technological	Advancements in tools and workload management simplify multi cloud operations
Legal	Compliance with regulations like GDPR and HIPAA poses constrains on cross-cloud data handling.
Environmental	Growing concerns over the carbon foot print of data centers push organizations toward energy efficient solutions.

4.4 Scenario Analysis for Multi Cloud Strategies

In multi-cloud environments, choosing an optimal strategy is essential to maintaining consistency, fault tolerance, and scalability across distributed systems. Table IV outlines a scenario-based evaluation of consistency testing, assessing four multi-cloud strategies under critical operational conditions such as high workload stress, system recovery efficiency, data synchronization accuracy, and scalability adaptability. Each strategy is evaluated based on response latency under heavy load, recovery duration post-failure, data consistency across cloud platforms, and scalability effectiveness. These findings offer a systematic, data-driven assessment for determining the most robust and resilient multi-cloud approach to ensure stability in dynamic computing environments.

Table 4: Scenario Analysis Multicloud Strategies

Scenario	Metric	Hybrid Multi-Cloud	Multi-Cloud Balancing	Cloud Bursting	Distributed Multi-Cloud
High Load Conditions	Response Time (ms)	250	280	220	260
Failure Recovery	Recovery Time (s)	20	25	18	15
Data Synchronization	Consistency (%)	92	89	85	94
Scalability Test	Scalability Score (1-5)	4	3	5	4

Fig. 6 presents the scenario-based consistency testing results for four distinct multi-cloud strategies: Hybrid Multi-Cloud, Multi-Cloud Balancing, Cloud Bursting, and Distributed Multi-Cloud. It analyzes four critical performance metrics: Response Time (ms), Failure Recovery Time (s), Consistency (%), and Scalability Score (1-5). Among these strategies, Cloud Bursting exhibits the lowest response time (220ms), demonstrating its effectiveness in managing sudden surges in workload, whereas Multi-Cloud Balancing records the highest response time (280ms) due to increased network overhead caused by dynamic traffic allocation. In terms of system recovery, Distributed Multi-Cloud Architecture achieves the shortest recovery time (15s), indicating superior fault tolerance, while Multi-Cloud Balancing requires the longest recovery duration (25s). Regarding data consistency, Distributed Multi-Cloud ensures the highest level of

reliability (94%), while Cloud Bursting scores the lowest (85%) due to frequent transitions between cloud providers. Lastly, Cloud Bursting leads in scalability (5), making it ideal for elastic workloads, whereas Multi-Cloud Balancing has the lowest scalability rating (3).

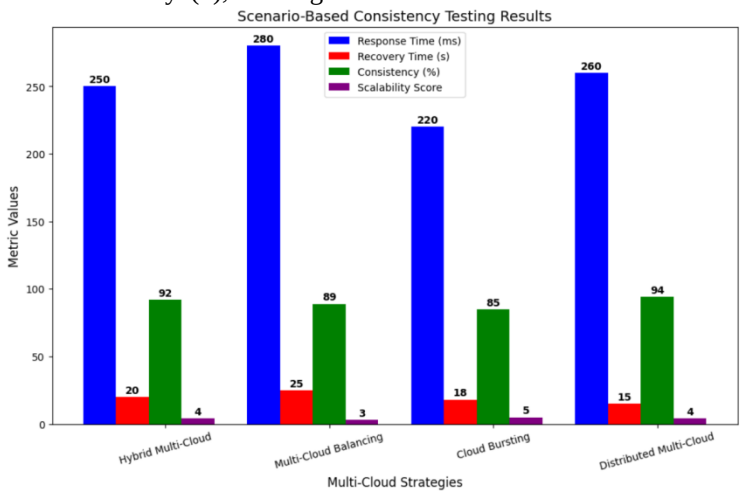

Figure 6. Scenario based consistency testing results

5. Conclusion

This study introduces a structured evaluation framework for analysing multi-cloud strategies through scenario-based consistency testing. By assessing key performance metrics such as response time, failure recovery, data consistency, and scalability, the study provides a comparative analysis of Hybrid Multi-Cloud, Multi-Cloud Balancing, Cloud Bursting, and Distributed Multi-Cloud Architecture. The findings indicate that Distributed Multi-Cloud Architecture offers the highest reliability (94%) and the fastest recovery time (15s), making it the most resilient and fault-tolerant approach. Conversely, Cloud Bursting demonstrates the lowest response time (220ms) and the highest scalability (5/5), making it well-suited for handling dynamic workloads while presenting data synchronization challenges. Meanwhile, Hybrid Multi-Cloud and Multi-Cloud Balancing provide a middle ground, offering trade-offs between resource redundancy, workload distribution, and cost-effectiveness. Additionally, the SWOT and PESTLE analyses identify internal and external influences affecting multi-cloud adoption, addressing critical concerns such as interoperability limitations, security regulations, and governance complexities. These evaluations offer strategic recommendations for organizations to optimize multi-cloud deployment and management. Future research should focus on AI-driven cloud orchestration, autonomous workload optimization, and advanced security frameworks to enhance multi-cloud system reliability, adaptability, and governance enforcement.

References

[1] Mhaisen, N., & Malluhi, Q. M. (2020). Data consistency in multi-cloud storage systems with passive servers and non-communicating clients. *IEEE Access*, *8*, 164977-164986.

[2] McAuley, D. (2023). Hybrid and multi-cloud strategies: balancing flexibility and complexity. *MZ Computing Journal*, *4*(2).

[3] Sivakumar, S. Performance Engineering for Hybrid Multi-Cloud Architectures.

[4] Ahmadi, M. R., Maleki, D., & Ahmadi, A. (2019). SMC-SPMV: A new strategic management model for cloud computing based on SWOT/PESTEL multi view. *African journal of engineering research*, *7*(1), 17-32.

[5] Yeboah-Ofori, A., Jafar, A., Abisogun, T., Hilton, I., Oseni, W., & Musa, A. (2024, August). Data Security and Governance in Multi-Cloud Computing Environment. In 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 215-222). IEEE.

[6] Zhang, X., Cui, L., Shen, W., Zeng, J., Du, L., He, H., & Cheng, L. (2023). File processing security detection in multi-cloud environments: a process mining approach. *Journal of Cloud Computing*, *12*(1), 100.

[7] Alyas, T., Alissa, K., Alqahtani, M., Faiz, T., Alsaif, S. A., Tabassum, N., & Naqvi, H. H. (2022). Multi-Cloud Integration Security Framework Using Honeypots. *Mobile Information Systems*, *2022*(1), 2600712.

[8] Ouchaou, L., Nacer, H., & Labba, C. (2022). Towards a distributed SaaS management system in a multi-cloud environment. *Cluster Computing*, *25*(6), 4051-4071.

[9] Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary Intelligence*, *14*(2), 691-698.

[10] Lahmar, F., & Mezni, H. (2021). Security-aware multi-cloud service composition by exploiting rough sets and fuzzy FCA. *Soft Computing*, *25*(7), 5173-5197.

[11] Anwarbasha, H., Sasi Kumar, S., & Dhanasekaran, D. (2021). An efficient and secure protocol for checking remote data integrity in multi-cloud environment. *Scientific reports*, *11*(1), 13755.

[12] Pachala, S., Rupa, C., & Sumalatha, L. (2021). An improved security and privacy management system for

data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, 14, 1117-1133.

[13] Ramamurthy, A., Saurabh, S., Gharote, M., & Lodha, S. (2020, November). Selection of cloud service providers for hosting web applications in a multi-cloud environment. In *2020 IEEE international conference on services computing (SCC)* (pp. 202-209). IEEE.

[14] Chimakurthi, V. N. S. S. (2020). The challenge of achieving zero trust remote access in multi-cloud environment. *ABC Journal of Advanced Research*, *9*(2), 89-102.