

Multi-Cloud Disaster Recovery Architecture

Sunny Kumar Ray, Ritik Kumar Jha

Department of Computer Science

and Engineering

Galgotias University

Greater Noida, India

sunnyroybagdulhan@gmail.com

jritik920@gmail.com

Abstract—Multi-Cloud Disaster Recovery Architecture Abstract Cloud computing is one of the most significant technologies that are currently utilized by companies to store information and implement applications. It provides companies with the benefit of scalability, resource flexibility and lower cost of physical infrastructure maintenance. Nevertheless, the complete dependence of a set of cloud service providers on one cloud service entity is dangerous to the overall system since cloud crashes may occur at any given moment. These failures can be the result of outage, cyberattacks, network errors, misconfiguration, service disruption or even natural disasters. This can result in significant downtimes and customer lost trust, loss of business and incurring of losses. A famous solution that assists in restoring data and applications in case of failures is Disaster Recovery (DR), so that services could be provided with the minimum number of delays. Multi-Cloud Disaster Recovery Architecture is a better way to improve the traditional DR by adopting more than a single cloud platform. Under this architecture, a single cloud serves as the main active environment and another cloud serves as a disaster recovery (DR) computer that contains replicated data and has resources available to recover. In case the main cloud goes offline, the traffic and workloads can be shifted to the second cloud in order to continue with operations within a very short period. The paper provides a human-readable and elaborate description of the multi-cloud disaster recovery architecture, the operating mechanism, significant components, recovery plan, and the most essential recovery metrics like Recovery Time Objective (RTO) and Recovery Point Objective (RPO). It also outlines such significant benefits as high availability, fault tolerance, and decreased dependency on the vendor as well as more practical obstacles as the expenses, complex administration, interoperability challenges, and security concerns between several cloud vendors. The paper concludes that multi-cloud disaster recovery is an efficient and realistic strategy to develop highly available

and reliable cloudbased solutions in current digital worlds.

Keywords: MultiCloud Disaster Recovery, Cloud Computing, High Availability, Fault Tolerance, Data Replication, Automated Failover, Business Continuity.

Index Terms—Multi-Cloud Disaster Recovery, Cloud Computing, High Availability, Fault Tolerance, Data Replication,

Automated Failover, Business Continuity

I. INTRODUCTION

Cloud computing has transformed the process by which companies develop and operate applications. Previously, businesses would have servers mounted within their campuses or their own personal data centres. That method was costly to start up, maintain and manpower. Many of these problems were addressed by cloud computing which offers its resources in form of services. Organizations are now able to rent storage, computing power and networking on demand. This elasticity aids in expansion of the businesses without the concern of infrastructure constraints. The cloud services according to cloud computing research and implementation serves various deployment requirements and enable enterprises to operate applications effectively at reduced complexity [4].

In the modern world, numerous applications that are important are fully operated in the cloud. As an example, internet shopping websites, internet payment systems, hospital management websites, student learning websites, and government websites are all cloud-based. There are numerous benefits accompanying this dependency and on the other hand it amplifies the effects of failures. In case even a few minutes a cloud service becomes unresponsive, the organization can experience several issues including client dissatisfaction, loss of income and postponement of the work.

Cloud failures may occur because of numerous causes. The issue may be technical sometimes such as a broken drive

or bugged software. In some cases it can be because of a human error, e.g. improper configuration or improper security rule. Failure may also occur as a result of cyberattacks such as Distributed Denial-of-Service (DDoS) attacks that flood the system rendering services inaccessible [16]. Security concerns have been among the largest concern in cloud computing since a security breach may result in unavailability or loss of sensitive information [2].

The fact that one cloud provider is easy to manage and has services that are fully bundled in a single platform has made many organizations continue to use a single cloud provider. This however results in dependence on that specific cloud company. In case the provider runs out of service or there is a failure in the region, the organization will lose full access. This vulnerability is more critical to companies that must operate at all times. Research on disaster recovery plans points out that companies need to take suitable recovery planning in order to ensure that services remain stable and are not affected out of failure [1]. The other issue of concern is the vendor lock-in where switching to a new cloud provider will be challenging because of the difference in service models and APIs.

The multi-cloud computing is a powerful solution to this issue. It entails the deployment of more than one cloud service provider. The multi-cloud computing is an area that is extensively researched because the technology enhances resilience, diminishes reliance on a specific vendor, and enables companies to select the most appropriate services among various platforms [7]. Nevertheless, other problems associated with the adoption of multi-cloud include complicated management and interoperability, since every provider has dissimilar tools and settings [12]. The most significant area that multi-cloud can bring significant value is Disaster Recovery (DR). MultiCloud Disaster Recovery Architecture can enable companies to back up their data and have recovery systems on various cloud services. When there is a failure in a cloud, the services of the cloud can be stored and be resumed by the cloud. This switching process is done more quickly and reliably through automated failover orchestration and does not require human intervention as much [14]. In this paper, multi-cloud disaster recovery architecture is presented in a humanized and understandable way. It addresses the key elements, recovery steps, disaster recovery strategies, and performance measures e.g. RTO and RPO. It also talks about the advantages and drawbacks of the implementation of multi-cloud disaster recovery into practice.

II. PROBLEM STATEMENT

Majority of organizations have one cloud service provider where they operate their critical applications and store

valuable business information. In the event of a failure that could be an outage, cyberattack, network or a disaster in the region, the system will not be available, leading to downtime and loss of information. Thus, multi-cloud disaster recovery architecture will be needed to provide high availability, fault tolerance, and business continuity.

III. OBJECTIVES

The primary goals of the study include:

- 1) To learn why disaster recovery is significant in cloud computing.
- 2) In order to examine the risks of single-cloud dependency.
- 3) To describe multi-cloud disaster recovery system architecture.
- 4) To talk about such critical disaster recovery indicators as RTO and RPO.
- 5) To characterize multi-cloud DR strategies and methodology of work.
- 6) To identify the advantages and limitations to multi-cloud DR implementation.

IV. LITERATURE REVIEW

The field of disaster recovery has also been examined when it comes to cloud computing since the issue of service failures has become a frequent problem to cloud-reliant organizations. According to a survey of disaster recovery strategies in cloud computing, disaster recovery is needed to lessen the downtime and safeguard business processes in the event of failures [1]. This survey demonstrates that organizations are not to wait until a disaster takes place, but rather they should prepare a recovery model.

Cloud security is another crucial subject that is related to disaster recovery. The challenges and problems of cloud computing security are data breach, insecure API, and unauthorized access. Such problems may decrease availability and cause severe threats to stored data [2]. Cloud reliability is also compromised by security threats such as denial of service attacks. In a full survey on DoS attacks in cloud computing, one of the ways in which DoS attacks can overload cloud servers, disorient services, and cause downtime is demonstrated [16]. Disaster recovery planning will then be required in these cases in order to recover in time.

Cloud disaster recovery planning consists of replication, recovery steps, and backups. Survey of cloud DR planning demonstrates that the most frequently employed technologies relate to the backup and restore technology due to its simplicity and affordability, but the recovery time is high [5]. Meanwhile, contemporary systems need quicker recovery and replication and standby models are now increasingly popular.

Resource provisioning is a second important factor. In the recovery process, the system requires access to the DR site in terms of compute resources, storage, and network access. A cloud resource provisioning survey describes the complexity of resource efficient allocation and underscores the impact of provisioning on performance and scalability [6]. The role of provisioning is paramount in the multi-cloud DR since the resources of DR should be made available in a short time to achieve RTO objectives.

The issue of multi-cloud computing was a significant theme in recent years. The systematic review on the topic of multicloud computing elaborates that multi-cloud solutions lessen the lock-in by vendors and enhance resilience as services are available across providers [7]. There is however no ease in managing multiple clouds. The survey on multi-cloud management and interoperability indicates the challenges of crossplatform monitoring, data portability, identity management and compatibility of services [12]. These problems have a direct impact on the success of multi-cloud DR.

There is also cloud architecture that is used in the design of reliable systems. As an example, the Google Cloud Architecture Framework gives best practices of reliability, system design, operations, and security [8]. These frameworks can be used to support DR preparation and develop recoveries that are scaleable.

The comparative analysis of disaster recovery models states that the strategies of disaster recovery should be chosen according to the recovery time and loss of data. Various strategies provide various trade-offs in terms of cost and speed of recovery [9]. The trends and future prospect regarding cloud disaster recovery reveals that the demand of DRs is on the rise due to the growing reliance of organizations on cloud-based technology [11]. Business continuity and DR of the cloud environment underscores the fact that without effective DR planning and constant testing business operations cannot be maintained [13].

The automation is a significant part of the contemporary recovery systems. Multi-cloud resilience Automated failover orchestration demonstrates that automation minimizes downtime and facilitates recovery time and reliability [14]. Recently, the issue of multi-cloud DR architecture has been emphasized in lightweight architecture where the role of high availability and constant functionality is highlighted, which demonstrates that multi-cloud DR is becoming more viable and operationalizable within organizations [15].

In general, the multi-cloud disaster recovery has a high support level in the literature as a successful solution of the current cloud systems. Nonetheless, security issues, management, interoperability, and resources provisioning

concerns continue to be significant improvement points [2], [6], [12], [16].

V. MULTI-CLOUD DR ARCHITECTURE

Multi-Cloud Disaster Recovery Architecture implies that two or more cloud providers are utilized in order to make sure that even in case of failure of one cloud provider, the services remain available. In this type of model, an organization develops the system such that when the primary cloud is down, a second cloud facility is immediately ready to carry on with the service with least disturbances.

In the majority of real systems the architecture involves a Primary Cloud and a Secondary Cloud (DR Cloud). The active application of production is operated on the primary cloud, and the backup and replicated data is stored on the secondary cloud and recovery resources are kept ready. The architecture makes it less reliant on a single provider and provides fault tolerance [7], [11].

A. Primary Cloud (Active Site): It is the primary cloudwhere the application is operating as it should. It harbors the live application servers, database systems and the storage services.

B. Secondary Cloud (Disaster Recovery Site): This is therecovering cloud setting. It keeps the duplicated copies of data and can also have the stand-by services according to the DR plan.

C. Data Backup: Backups are the periodical copies of datawhich are stored. They guard the organization against inadvertent deletion, corruption, malware or severe failures. Backupbased DR is easy yet slow as presented in DR planning research [5].

D. Data Replication: Replication refers to the process ofcontinuously/frequently copying data between the primary and secondary cloud. Replications minimizes loss of data, and accelerates recovery as opposed to just backups. Replication may be either asynchronous or synchronous based on RPO requirements.

E. Monitoring and Health Checks: Monitoring is requiredin order to identify failures at an early stage. Monitoring tools track the performance, availability, server health and database stability. Monitoring systems make alerts when failure occurs.

F. Automated Failover Orchestration: The reason behindautomation is that manual failover can be too long. The processes of failover orchestration are automatic and initiate services in the DR cloud and switch operations within a short time. Failover procedures should be highly automated to enhance the faster recovery [14].

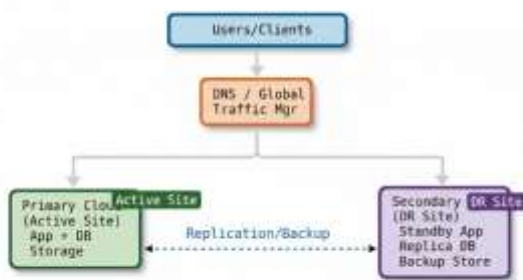
G. Traffic Management (DNS / Load Balancer): Trafficmanagement is used to direct users to the DR

location during the occurrence of failover. DNS routing can be used, for instance, to alter the destination of user requests to the secondary cloud. Traffic can also be distributed by load balancing.

Table 1: Multi-Cloud DR and DR Components

Component	Purpose	Example Function
Primary Cloud	Supports live production workload Serves user traffic.	
Primary Cloud	workload	Serves user traffic
Secondary Cloud	Hosted failover environment	Failover standby servers
Backup Storage	Stockpiling snapshots and	Rescue backups following loss
Data Replication	backups	
Data Replication	Maintains copy on DR site.	Constant synchronization of the DB.
Monitoring & Alerting	Monitors for failure early on	Health checks, alerts.
Automated Failover	Switches are run automatically	
Traffic Management	Switches are run automatically	Auto traffic switch.
Traffic Management	DR cloud redirection of users	DNS / Load Balancer

Fig. 1. Multi-Cloud Disaster Recovery Architecture



VI. DISASTER RECOVERY METRICS (RTO AND RPO)

In the effectiveness measurement of disaster recovery, RTO and RPO [9] are mostly employed.

A. Recovery Time Objective (RTO)

Recovery Time Objective (RTO) is the maximum period that can be allowed to restore services once they fail. In case of low RTO, the system should be started quickly and this usually requires standby environment and automatic failover [14].

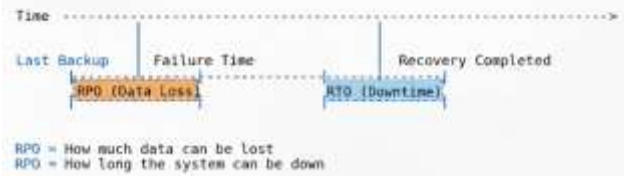
B. Recovery Point Objective (RPO)

RPO may be termed as the loss in the data that can be considered less. It tells about how far the recent information will be lost in case of disaster that the organization could face.

Replication and backup is common and reduces RPO [5], [9].

A good multi-cloud DR system will attempt to minimize the RTO and RPO depending on the business needs.

Fig. 2. RTO and RPO Representation



VII. WORKING METHODOLOGY

A typical multi-cloud DR workflow is:

- 1) Adopt application and database on the main cloud.
- 2) Inter-cloud replication between primary and secondary cloud is made possible.
- 3) My backup every now and then and ensure that they are stored in a secure location.
- 4) Track performance and availability through the assistance of monitoring tools.
- 5) It creates monitoring alerts in the event of failure and detects it.
- 6) Failover orchestration refers to the automatic start up of the services in the second cloud [14].
- 7) DNS or load balancer redirects the traffic to secondary cloud.
- 8) Services are continued to be operated on the secondary cloud.
- 9) It is able to carry out an after primary recovery fallback of requirement.

This workflow ensures the continuity and time to recuperate.

Fig. 3. Multi-Cloud DR Failover Workflow



VIII. MULTI-CLOUD DR STRATEGIES

Depending on the cost and recovery requirements, there are different DR plans that are implemented [9].

A. Backup and Restore

It is the least costly one. The data is archived and copied in another cloud. The system is reinstated when it comes to disaster. Recovery time is high

B. Pilot Light

The first example is one that operates on the DR cloud. More resources are instigated in case of failure.

C. Warm Standby

This is a miniature system which is on DR cloud. It is providing faster recovery and less downtime.

D. Active-Active

: Both clouds perform active services in parallel. This provides maximum availability and is expensive and requires high synchronization.

- **Security Enhancement:** Security threats are able to interfere with systems. The backup, replication, and recovery planning is also useful in the reduction of the impact of such attacks like DoS and breaches [2], [16].

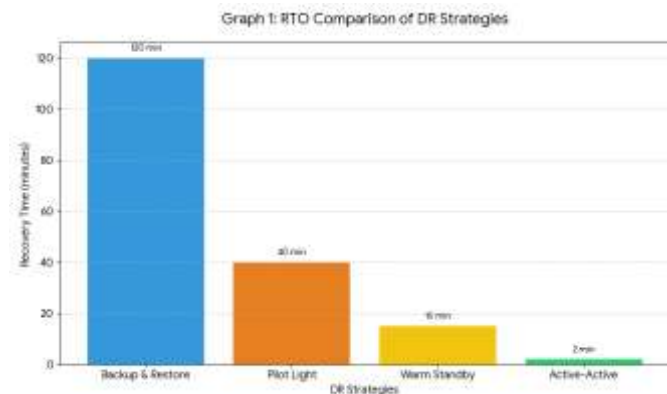


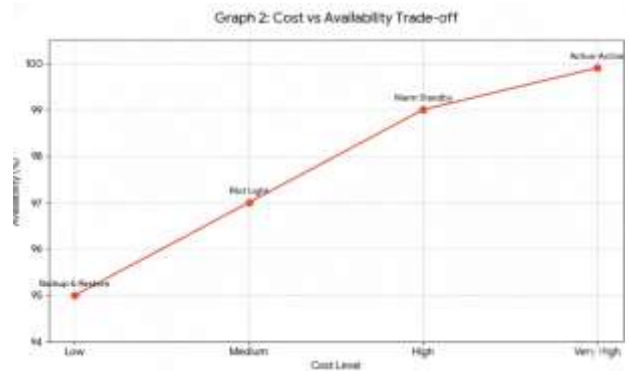
Table 2: Comparison of Disaster Recovery Strategies

DR Strategy	Cost	RTO (Recovery Time)	RPO (Data Loss)	Optimum Loss	Optimum to Use
Backup & Restore	Low	High / Medium	Low	Low	Moderate critical systems
Pilot Light	Low	High / Medium	Low	Low	Moderate critical systems
Warm Standby	Medium	Medium	Low	Moderate apps	Business-critical
Active-Active	Very High	Very Low	Low	Low	24/7 mission critical

IX. BENEFITS OF MULTI-CLOUD DISASTER RECOVERY

There are a number of benefits of multi-cloud DR:

- **High Availability:** Availability is the nature of the greatest advantage. Moving to another cloud reduces the downtime and helps to keep services [11], [15].
- **Better Fault Tolerance** Multi-cloud DR lacks single point of failure and it increases the reliability [7].
- **Business Continuity:** Prompt recovery and service availability are available to aid the business continuity in the event of failure [13].
- **Less Vendor Lock-In:** The system will become less attached and flexible to multiple cloud providers [7], [12].



X. CHALLENGES AND LIMITATIONS

Multi-cloud DR has problems as well:

- Increased Cost:** Standby Cost, and Multi-cloud maintenance Cost and Replication bandwidth is added.
- Complex Management:** The wide range of cloud providers is hard to deal with because they offer dissimilar services and APIs. The interoperability problems are one of the major issues [12].
- Security and Compliance:** In both clouds, there should be enforced security policies. Security problems are one of the usual problems with cloud systems [2], [16].
- Resource Provisioning:** DR site may have difficulties in terms of resources provisioning. The provisioning problems exist that affect the recovery rates [6].
- Data Replication Latency:** Inter-cloud replications are possible to generate the delay and performance impact due to network distance and bandwidth.

XI. USE CASE SCENARIO

Consider the case of online shopping platform that uses one cloud. The users can not use the site when the cloud area is down and no orders are made. Multi-cloud DR refers to the procedure by which the database will be replicated to the second cloud and the application environment will be sustained. Automated failover is configured to boot the secondary cloud on failure being detected and divert the traffic to allow the customers to shop as much as possible in the case of a failure [14], [15]. This creates uniformity and reduce wastage in terms of cost.

XII. CONCLUSION AND FUTURE SCOPE

The multi-cloud disaster recovery architecture is a sound and viable methodology of ensuring the high availability, fault tolerance, and the continuity of business in the modern cloud systems. It reduces the chances of being dependent on one cloud and allows replication and

recovery faster in case of failure with replication, monitoring, traffic control, and automated failover [7], [11], [14]. The cost and complexity of management remain issues, yet the multi-cloud DR may be of great benefit to the critical systems. The new changes may be oriented to better automation, successful provisioning, crosscloud security, and replication latency reduction [12], [15]. All in all, multi-cloud DR is an imperative method of developing reliable cloud programs during the current digital era.

REFERENCES

- [1] S. Grover, M. Bajaj, and A. Verma, "A survey on disaster recovery strategies in cloud computing," *International Journal of Computer Applications*, vol. 144, no. 9, pp. 1–6, 2016.
- [2] A. Ahmed and A. N. Khan, "Cloud computing security issues and challenges: A survey," *International Journal of Computer Networks and Communications Security*, vol. 4, no. 3, pp. 56–62, 2016.
- [3] Amazon Web Services, "Disaster Recovery of Workloads on AWS," AWS Whitepaper, 2017.
- [4] M. A. Vouk, "Cloud computing—Issues, research and implementations," *Journal of Computing and Information Technology*, vol. 24, no. 4, pp. 235–246, 2017.
- [5] R. A. Rashid and N. A. M. Isa, "Review on cloud disaster recovery planning and solutions," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 6, pp. 1–9, 2018.
- [6] S. Singh and I. Chana, "Cloud resource provisioning: Survey, status and future research directions," *Knowledge and Information Systems*, vol. 49, pp. 1005–1069, 2019.
- [7] A. A. Khan, M. Zakarya, and R. Ahmad, "Multi-cloud computing: A systematic review and future directions," *IEEE Access*, vol. 8, pp. 188687–188708, 2020.
- [8] Google Cloud, "Google Cloud Architecture Framework," Google Cloud Documentation, 2020.
- [9] A. K. Bairagi and R. K. Ray, "A comparative study of disaster recovery models in cloud computing," in *Proc. International Conference on Recent Trends in Computing*, pp. 210–215, 2021.
- [10] A. Saboor, M. H. Rehmani, and M. Reisslein, "Edge and cloud computing: A survey on architectures and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1054–1102, 2021.
- [11] V. Chang, R. J. Walters, and G. B. Wills, "Cloud computing and disaster recovery: Current trends and

future scope," *Journal of Cloud Computing*, vol. 10, no. 1, pp. 1–16, 2021.

- [12] A. Alharthi, "A survey on multi-cloud management and interoperability," *IEEE Access*, vol. 10, pp. 23421–23440, 2022.
- [13] N. Abid, M. A. Khan, and M. A. Khan, "Business continuity and disaster recovery in cloud environments: A review," *Procedia Computer Science*, vol. 201, pp. 1–8, 2022.
- [14] J. Zhang and Y. Li, "Automated failover orchestration for multi-cloud resilience," *IEEE Access*, vol. 11, pp. 100210–100223, 2023.
- [15] A. Rahman and S. Das, "Multi-cloud DR for high availability and business continuity: A lightweight architecture," in *Proc. International Conference on Computing and Communication Systems*, pp. 55–61, 2025.
- [16] M. Masdari and S. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Security and Communication Networks*, vol. 2019, pp. 1–18, 2019.
- [17] S. Singh and I. Chana, "Cloud resource provisioning: Survey, status and future research directions," *Knowledge and Information Systems*, vol. 49, pp. 1005–1069, 2019.