IJMSERH

International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

Volume 10, Issue 1, January-March 2022

Impact Factor: 7.121

ijmserh@gmail.com

www.ijmserh.com

International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

Ensuring High Availability and Disaster Recovery in Hybrid IT Environments: A Systems Architecture Approach

Rajesh Adepu

Associate Principal and IT Architecture, GuideHouse LLC, USA

ABSTRACT: Hybrid IT environments, which integrate on-premises infrastructure with public and private cloud platforms, have become the foundation of modern enterprise systems. While this architectural model offers scalability, flexibility, and cost optimization, it also introduces significant challenges in ensuring high availability and robust disaster recovery. System failures, cyber threats, and infrastructure disruptions can lead to substantial operational and financial losses if not properly mitigated.

This paper presents a comprehensive systems architecture approach to achieving high availability and disaster recovery in hybrid IT environments. It explores the design principles, architectural patterns, and resilience strategies required to maintain continuous service delivery under failure conditions. Key aspects such as redundancy models, failover mechanisms, data replication strategies, and recovery time objectives (RTO) and recovery point objectives (RPO) are examined in detail.

Furthermore, the article discusses the integration of automation, monitoring, and orchestration tools to enhance system reliability and accelerate recovery processes. A layered architecture framework is proposed to align infrastructure, platform, and application-level resilience strategies. The study also highlights real-world implementation considerations, including cost-performance trade-offs, regulatory compliance, and operational complexity.

By synthesizing industry best practices and emerging trends, this paper provides a structured blueprint for designing resilient hybrid IT systems capable of sustaining business continuity in the face of evolving disruptions.

KEYWORDS: Hybrid IT Environments; High Availability; Disaster Recovery; Systems Architecture; Business Continuity; Failover Mechanisms; Data Replication; RTO (Recovery Time Objective); RPO (Recovery Point Objective); Cloud Computing; On-Premises Infrastructure; Resilience Engineering; Fault Tolerance; Infrastructure Redundancy; Automation and Orchestration

I. INTRODUCTION

The rapid evolution of enterprise IT landscapes has led to the widespread adoption of hybrid IT environments, where organizations integrate traditional on-premises infrastructure with public and private cloud platforms. This hybrid approach enables enterprises to leverage the scalability and elasticity of cloud computing while retaining control over critical workloads and sensitive data within on-premises systems. As digital transformation accelerates across industries, ensuring uninterrupted system availability and robust disaster recovery capabilities has become a fundamental requirement rather than an optional enhancement.

High availability (HA) refers to the ability of a system to remain operational and accessible with minimal downtime, even in the presence of component failures. Disaster recovery (DR), on the other hand, focuses on restoring systems and data following catastrophic events such as natural disasters, cyberattacks, or large-scale infrastructure failures. In hybrid IT environments, achieving both HA and DR is inherently complex due to the distributed nature of resources, heterogeneous technologies, and varying service-level agreements across platforms.

Modern enterprises face increasing risks from system outages, which can result in financial losses, reputational damage, and regulatory penalties. The growing dependence on real-time applications, data-driven decision-making, and global service delivery further amplifies the need for resilient architectures. Consequently, organizations must adopt a holistic systems architecture approach that incorporates redundancy, fault tolerance, and automated recovery mechanisms across all layers of the IT stack.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

This paper explores the architectural principles and design strategies required to ensure high availability and effective disaster recovery in hybrid IT environments. It emphasizes the importance of aligning infrastructure, platform, and application-level resilience measures to achieve end-to-end system reliability. Key considerations include replication strategies, failover configurations, load balancing, and the definition of recovery objectives such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Additionally, the introduction of advanced monitoring, automation, and orchestration tools has significantly improved the ability to detect failures and initiate rapid recovery processes. These technologies play a crucial role in minimizing downtime and ensuring business continuity. However, they also introduce challenges related to integration, governance, and operational complexity that must be carefully managed.

By adopting a structured systems architecture perspective, organizations can design hybrid IT environments that not only withstand failures but also adapt dynamically to changing conditions. This paper aims to provide a comprehensive foundation for understanding and implementing high availability and disaster recovery strategies that support resilient, scalable, and future-ready enterprise systems.

II. BACKGROUND AND RELATED WORK

The concepts of high availability (HA) and disaster recovery (DR) have evolved significantly with the transition from traditional data centers to cloud-enabled and hybrid IT environments. Historically, enterprise systems relied on vertically scaled, monolithic architectures hosted within single data centers, where redundancy was achieved through hardware duplication and manual failover processes. While effective to a certain extent, these approaches were often costly, inflexible, and limited in their ability to handle large-scale disruptions.

With the emergence of virtualization and cloud computing, architectural paradigms shifted toward distributed systems and service-oriented designs. Public cloud providers introduced built-in availability features such as multi-zone deployments, automated scaling, and managed backup services. At the same time, private data centers adopted virtualization technologies to improve resource utilization and enable faster recovery mechanisms. The hybrid IT model emerged as a convergence of these approaches, allowing organizations to balance control, performance, and scalability.
In this context, HA is typically achieved through redundancy and fault tolerance mechanisms, including active-active and active-passive configurations, load balancing, and clustering. These techniques ensure that system components can continue functioning even when individual elements fail. DR strategies, on the other hand, focus on data protection and system restoration through techniques such as synchronous and asynchronous replication, periodic backups, and geographically distributed failover sites.

A key aspect of modern HA and DR planning is the definition of Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO specifies the maximum acceptable downtime after a failure, while RPO defines the acceptable amount of data loss measured in time. These metrics guide architectural decisions and influence the selection of replication methods, storage solutions, and failover strategies.

Recent research and industry practices have emphasized the importance of adopting a layered resilience model. At the infrastructure layer, redundancy is implemented across compute, storage, and network components. At the platform layer, containerization and virtualization technologies enhance portability and scalability. At the application layer, microservices architectures and stateless design patterns improve fault isolation and recovery speed. This multi-layered approach ensures that resilience is embedded throughout the system rather than treated as an afterthought.

Several studies have also highlighted the role of automation and orchestration in improving HA and DR outcomes. Automated failover mechanisms, infrastructure-as-code (IaC), and policy-driven recovery workflows reduce human intervention and minimize recovery times. Monitoring and observability tools further enhance system reliability by providing real-time insights into performance, failures, and potential risks.

Despite these advancements, hybrid IT environments introduce unique challenges. These include network latency between on-premises and cloud systems, data consistency across distributed locations, security and compliance requirements, and the complexity of managing heterogeneous platforms. As a result, designing effective HA and DR strategies requires a comprehensive systems architecture approach that integrates multiple technologies and aligns with organizational objectives.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

III. ARCHITECTURE FOR HIGH AVAILABILITY IN HYBRID IT ENVIRONMENTS

Designing high availability (HA) in hybrid IT environments requires a structured architectural approach that ensures continuous service delivery despite failures across distributed components. Unlike traditional single-site deployments, hybrid architectures must account for failures occurring across on-premises infrastructure, cloud platforms, and the network connectivity between them. This necessitates a multi-layered design that integrates redundancy, fault tolerance, and intelligent traffic management.

3.1 Architectural Principles for High Availability

A robust HA architecture is guided by several key principles:

- **Elimination of Single Points of Failure (SPOF):** All critical components, including compute nodes, storage systems, and network paths, must have redundant counterparts.
- **Redundancy and Replication:** Systems should maintain duplicate resources across different availability zones or locations to ensure continuity.
- **Fault Isolation:** Failures in one component or region should not cascade across the entire system.
- **Scalability and Elasticity:** Dynamic scaling mechanisms help maintain performance during peak loads or partial failures.
- **Automated Failover:** Systems should detect failures and switch to backup resources without manual intervention.

These principles form the foundation for building resilient hybrid systems capable of maintaining uptime under varying failure scenarios.

3.2 Multi-Layered High Availability Architecture

High availability in hybrid environments is typically implemented across three architectural layers:

a) Infrastructure Layer

At this level, HA is achieved through:

- Redundant physical servers and virtual machines
- Multi-zone or multi-region deployments
- Network path redundancy (multiple ISPs, VPNs, or dedicated links)
- Distributed storage systems with replication

b) Platform Layer

This layer focuses on:

- Virtualization and container orchestration for workload mobility
- Load balancers to distribute traffic across instances
- Auto-scaling groups to handle demand fluctuations
- Middleware clustering for application services

c) Application Layer

Application-level HA includes:

- Stateless service design for easier failover
- Microservices architecture for fault isolation
- Graceful degradation and circuit breaker patterns
- Session replication or external session storage

3.3 High Availability Deployment Models

Hybrid IT environments commonly adopt the following HA deployment patterns:

Model	Description	Use Case
Active-Active	Multiple nodes serve traffic simultaneously across locations	Mission-critical, low-latency apps
Active-Passive	Primary system handles traffic; secondary remains on standby	Cost-sensitive environments
Pilot Light	Minimal resources run in secondary site, scaled up during failure	Disaster recovery readiness
Warm Standby	Partially active secondary environment ready for quick failover	Balanced cost and recovery time

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

Each model offers different trade-offs between cost, complexity, and recovery speed.

3.4 High Availability Architecture Diagram

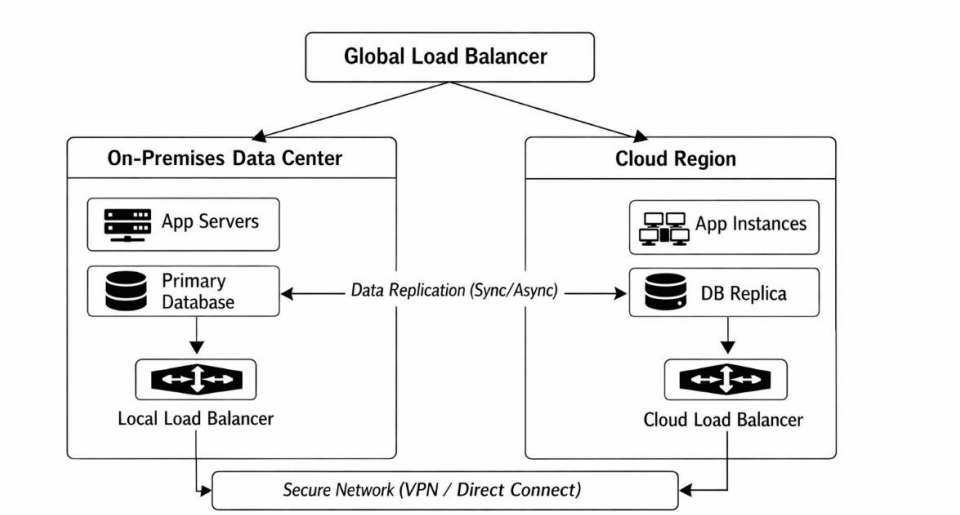

Figure 1: Hybrid IT High Availability Architecture

Figure 1: High Availability Architecture for Hybrid IT Environments

3.5 Key Considerations and Challenges

While implementing HA in hybrid environments, organizations must address several challenges:

- **Latency and Network Reliability:** Communication delays between on-premises and cloud systems can impact failover performance.
- **Data Consistency:** Ensuring consistency across distributed databases requires careful selection of replication strategies.
- **Cost Optimization:** Redundant resources increase operational costs and must be balanced with business requirements.
- **Operational Complexity:** Managing multiple environments demands advanced monitoring and automation capabilities.

IV. DISASTER RECOVERY STRATEGIES AND DESIGN CONSIDERATIONS

While high availability focuses on minimizing downtime during localized failures, disaster recovery (DR) addresses large-scale disruptions that can render entire systems or sites inoperable. In hybrid IT environments, disaster recovery becomes more complex due to the distributed nature of infrastructure across on-premises data centers and cloud platforms. A well-defined DR strategy ensures that critical services can be restored within acceptable timeframes and with minimal data loss.

4.1 Disaster Recovery Objectives

Effective DR planning begins with clearly defining recovery objectives:

- **Recovery Time Objective (RTO):** The maximum acceptable time required to restore services after a disruption.
- **Recovery Point Objective (RPO):** The maximum acceptable data loss measured in time before the failure event.

These metrics serve as key design parameters that influence replication strategies, backup frequency, and failover mechanisms. Applications with stringent RTO and RPO requirements typically require more sophisticated and cost-intensive solutions.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

4.2 Disaster Recovery Strategies in Hybrid Environments

Hybrid IT environments support multiple DR strategies, each offering different trade-offs between cost, complexity, and recovery speed:

a) Backup and Restore

- Periodic backups are stored in offsite or cloud storage
- Restoration occurs after failure
- **Pros:** Low cost, simple implementation
- **Cons:** High RTO and RPO

b) Pilot Light

- Minimal critical components run continuously in the cloud
- Full system is activated during disaster
- **Pros:** Faster recovery than backup approach
- **Cons:** Requires pre-configured infrastructure

c) Warm Standby

- Scaled-down but fully functional environment runs in parallel
- Can quickly scale up during failure
- **Pros:** Balanced cost and recovery time
- **Cons:** Moderate operational cost

d) Active-Active (Multi-Site DR)

- Full systems run simultaneously across locations
- Traffic is distributed across sites
- **Pros:** Near-zero downtime and minimal data loss
- **Cons:** High cost and architectural complexity

4.3 Data Replication Techniques

Data replication is a critical component of DR architecture. The choice of replication method directly impacts RPO and system performance:

- **Synchronous Replication:** Data is written simultaneously to primary and secondary sites ensures zero or near-zero data loss; higher latency and network dependency.
- **Asynchronous Replication:** Data is replicated with a time delay lower latency and better performance; acceptable data loss depending on delay.
- **Snapshot-Based Replication:** Periodic snapshots of system state useful for backup and archival purposes; may not meet strict RPO requirements.

4.4 Disaster Recovery Architecture Diagram

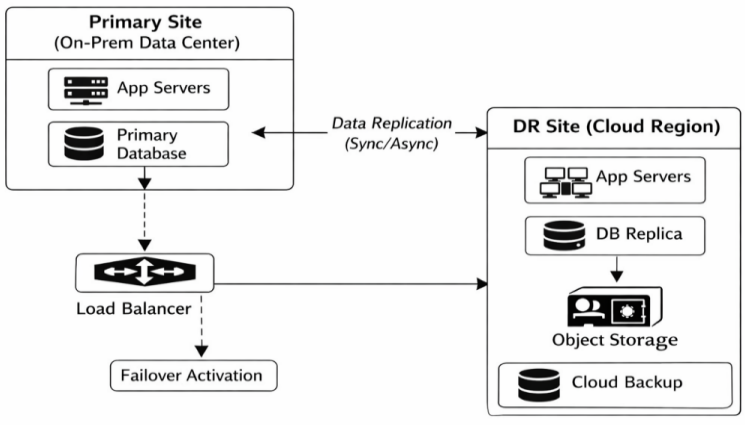

Figure 2: Disaster Recovery Architecture for Hybrid IT

Figure 2: Disaster Recovery Architecture for Hybrid IT

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

4.5 Automation and Orchestration in DR

Modern DR strategies rely heavily on automation to reduce recovery time and human error:

- **Automated Failover:** Detects failure and switches to DR site
- **Infrastructure as Code (IaC):** Enables rapid environment provisioning
- **Runbook Automation:** Predefined workflows for recovery steps
- **Monitoring Integration:** Triggers alerts and recovery actions

Automation ensures consistency, repeatability, and faster response during disaster scenarios.

4.6 Key Challenges in Disaster Recovery

Despite advancements, several challenges persist:

- **Data Consistency Across Sites:** Maintaining integrity during replication
- **Network Bandwidth Constraints:** Impacting replication speed
- **Testing and Validation:** Regular DR drills are required but often neglected
- **Cost Management:** Balancing resilience with budget constraints
- **Compliance Requirements:** Adhering to regulatory standards for data protection

V. INTEGRATED HA AND DR ARCHITECTURE FRAMEWORK

In hybrid IT environments, high availability (HA) and disaster recovery (DR) cannot be treated as isolated strategies. Instead, they must be integrated into a unified architectural framework that ensures both continuous operation during minor failures and rapid recovery from major disruptions. This section presents a comprehensive framework that aligns HA and DR mechanisms across multiple layers of the system.

5.1 Unified Resilience Architecture

An integrated HA-DR architecture combines real-time fault tolerance with strategic recovery planning. The goal is to create a system that not only withstands component-level failures but also recovers seamlessly from site-level outages. The unified framework operates across three primary dimensions:

- **Availability Layer:** Ensures continuous service through redundancy, clustering, and load balancing
- **Recovery Layer:** Focuses on backup, replication, and failover mechanisms
- **Management Layer:** Incorporates monitoring, automation, and orchestration

These layers work together to provide end-to-end resilience in hybrid deployments.

5.2 Layered Framework Design

The integrated architecture can be structured into the following layers:

a) Infrastructure Resilience

- Multi-region deployment (on-premises + cloud)
- Redundant compute, storage, and network resources
- Secure and redundant connectivity (VPN, dedicated links)

b) Data Resilience

- Real-time data replication (sync/async)
- Backup and archival strategies
- Data consistency and integrity mechanisms

c) Application Resilience

- Stateless service design
- Microservices-based fault isolation
- Automated failover and service discovery

d) Operations and Management

- Centralized monitoring and logging
- Automated alerting and incident response
- Policy-driven orchestration and recovery workflows

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

5.3 Comparative Analysis of HA and DR Integration

Aspect	High Availability (HA)	Disaster Recovery (DR)	Integrated Approach
Objective	Minimize downtime	Restore after failure	Ensure continuity + recovery
Scope	Component/system level	Site/region level	End-to-end system
Techniques	Load balancing, clustering	Backup, replication	Combined orchestration
Recovery Time	Near-zero	Minutes to hours	Optimized (based on RTO)
Data Loss	Minimal	Depends on RPO	Controlled and minimized
Cost	Moderate to high	Variable	Optimized trade-off

5.4 Performance vs Cost Trade-off Chart

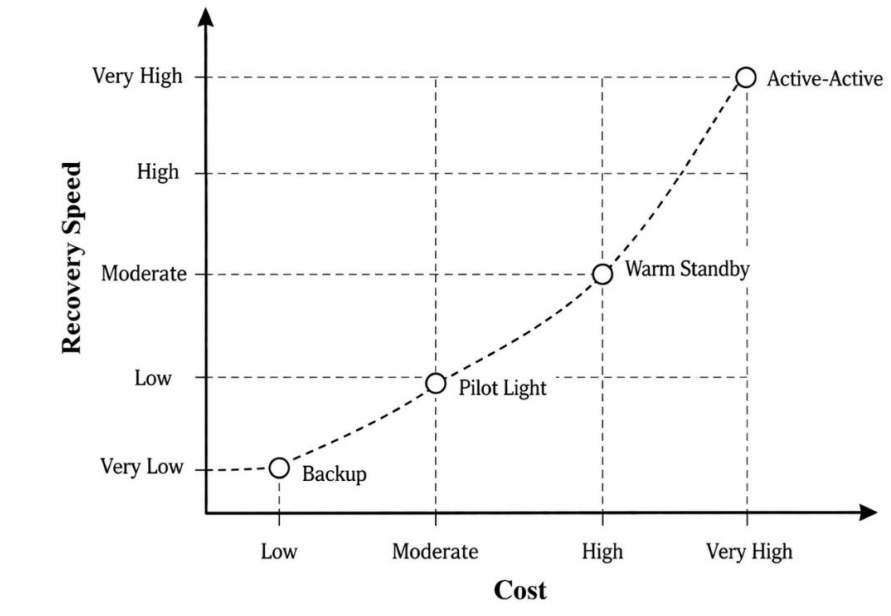

Figure 3: Cost vs Recovery Trade-off in HA/DR Models

5.5 Key Benefits of Integrated Framework

- **Improved System Resilience:** Combines proactive and reactive strategies
- **Reduced Downtime:** Faster detection and recovery through automation
- **Optimized Resource Utilization:** Balances cost with availability requirements
- **Enhanced Business Continuity:** Ensures uninterrupted service delivery
- **Scalability:** Supports dynamic workloads across hybrid environments

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

5.6 Implementation Considerations

Organizations adopting this framework should consider:

- Alignment with business continuity objectives
- Selection of appropriate HA/DR models based on workload criticality
- Regular testing through disaster recovery drills
- Integration with security and compliance frameworks
- Continuous monitoring and optimization

VI. IMPLEMENTATION STRATEGIES AND BEST PRACTICES

Implementing high availability (HA) and disaster recovery (DR) in hybrid IT environments requires a structured approach that aligns architectural design with operational execution. While the previous sections outlined theoretical models and frameworks, this section focuses on practical strategies and best practices for deploying resilient systems in real-world enterprise environments.

6.1 Workload Classification and Criticality Assessment

A successful HA/DR implementation begins with identifying and categorizing workloads based on their business impact:

- **Mission-Critical Applications:** Require near-zero downtime and minimal data loss (strict RTO/RPO)
- **Business-Critical Applications:** Allow minimal downtime with controlled recovery objectives
- **Non-Critical Workloads:** Can tolerate longer recovery times and higher data loss

This classification helps in selecting appropriate HA/DR strategies and optimizing resource allocation.

6.2 Designing for Redundancy and Fault Tolerance

Redundancy must be implemented across all layers of the architecture:

- **Compute Redundancy:** Deploy applications across multiple nodes and regions
- **Storage Redundancy:** Use replicated and distributed storage systems
- **Network Redundancy:** Ensure multiple communication paths and failover routes

Best practice is to adopt active-active architectures for critical systems and active-passive configurations for less critical workloads to balance cost and performance.

6.3 Data Protection and Backup Strategies

Data is the core of any enterprise system; hence, robust data protection mechanisms are essential:

- Implement multi-tier backup strategies (local + cloud)
- Use incremental and differential backups to reduce overhead
- Encrypt backups to ensure data security and compliance
- Regularly validate backup integrity through restoration tests

A combination of backup and replication ensures both short-term recovery and long-term data retention.

6.4 Automation and Infrastructure as Code (IaC)

Automation plays a crucial role in reducing recovery time and operational errors:

- Use Infrastructure as Code (IaC) to provision environments consistently
- Automate failover and failback processes
- Implement runbooks for standardized recovery procedures
- Integrate CI/CD pipelines to ensure deployment consistency

Automation enhances repeatability and ensures faster recovery during unexpected failures.

6.5 Monitoring, Observability, and Incident Response

Continuous monitoring is essential for proactive failure detection:

- Deploy centralized monitoring and logging systems
- Use real-time alerting mechanisms for anomaly detection
- Implement observability frameworks (metrics, logs, traces)
- Establish incident response protocols with defined roles and escalation paths

Proactive monitoring reduces downtime by identifying issues before they escalate into system-wide failures.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

6.6 Regular Testing and Disaster Recovery Drills

One of the most overlooked aspects of DR planning is testing:

- Conduct periodic failover and failback tests
- Simulate real-world disaster scenarios
- Validate RTO and RPO compliance
- Update recovery procedures based on test outcomes

Testing ensures that systems and teams are prepared to respond effectively during actual disasters.

6.7 Security and Compliance Considerations

HA and DR implementations must align with security and regulatory requirements:

- Ensure data encryption in transit and at rest
- Implement access controls and identity management
- Comply with industry standards and regulations
- Maintain audit logs for all recovery operations

Security must be integrated into every layer of the HA/DR architecture.

6.8 Cost Optimization Strategies

While resilience is critical, cost management remains a key concern:

- Use tiered storage and compute models
- Optimize resource utilization through auto-scaling
- Adopt pay-as-you-go cloud services
- Regularly review and optimize unused resources

Organizations should aim for a balance between availability requirements and budget constraints.

6.9 Summary of Best Practices

Category	Best Practice
Architecture	Eliminate single points of failure
Data Management	Combine backup and replication strategies
Automation	Use IaC and automated failover
Monitoring	Implement real-time observability
Testing	Conduct regular DR drills
Security	Integrate compliance and encryption
Cost Optimization	Balance performance with cost efficiency

This section provided actionable strategies and best practices for implementing high availability and disaster recovery in hybrid IT environments.

VII. CONCLUSION

Ensuring high availability (HA) and disaster recovery (DR) in hybrid IT environments has become a critical requirement for modern enterprises operating in increasingly digital and distributed ecosystems. As organizations continue to integrate on-premises infrastructure with cloud platforms, the complexity of maintaining system resilience grows significantly. This paper presented a comprehensive systems architecture approach to addressing these challenges by combining design principles, architectural frameworks, and practical implementation strategies.

The study highlighted that high availability and disaster recovery must be treated as complementary components of a unified resilience strategy rather than isolated solutions. While HA focuses on minimizing downtime through redundancy, failover mechanisms, and fault tolerance, DR ensures the restoration of services and data in the event of large-scale disruptions. The integration of these approaches enables organizations to achieve both continuous service delivery and rapid recovery.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 7.121||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 10, Issue 1, January-March 2022 ||

DOI: 10.15662/IJMSERH.2022.1001048

A layered architectural model was emphasized, incorporating infrastructure, platform, application, and management layers to ensure end-to-end resilience. Techniques such as active-active deployments, data replication, automated failover, and infrastructure as code (IaC) were identified as key enablers of robust hybrid systems. Additionally, the importance of defining Recovery Time Objective (RTO) and Recovery Point Objective (RPO) was underscored, as these metrics guide the design and implementation of HA/DR strategies.

The paper also addressed practical considerations, including workload classification, cost optimization, security compliance, and the need for continuous monitoring and testing. Automation and orchestration were shown to play a vital role in reducing recovery times and minimizing human error, while regular disaster recovery drills ensure preparedness for real-world scenarios.

In conclusion, achieving resilience in hybrid IT environments requires a holistic and well-orchestrated systems architecture approach. Organizations must carefully balance performance, cost, and risk while adopting modern technologies and best practices. By implementing integrated HA and DR strategies, enterprises can ensure business continuity, protect critical data, and maintain service reliability in the face of evolving operational and environmental challenges.

REFERENCES

[1] M. Villamizar, O. Garcés, H. Castro, et al., "Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud," IEEE Latin America Transactions, vol. 13, no. 10, pp. 3150–3157, 2019.
[2] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," Proceedings of the 2019 Workshop on Mobile Big Data, pp. 37–42, 2019.
[3] N. Grozev and R. Buyya, "Inter-cloud architectures and application brokering: Taxonomy and survey," Software: Practice and Experience, vol. 49, no. 2, pp. 1–25, 2019.
[4] A. Alhazmi and Y. Malaiya, "Evaluating disaster recovery strategies for cloud-based systems," Journal of Cloud Computing, vol. 9, no. 1, pp. 1–15, 2020.
[5] P. Costa, T. Pasin, and F. Bessani, "Towards dependable distributed systems: A survey on replication techniques," ACM Computing Surveys, vol. 53, no. 2, pp. 1–35, 2020.
[6] R. Jhawar, V. Piuri, and M. Santambrogio, "A comprehensive conceptual system-level approach to fault tolerance in cloud computing," IEEE Systems Journal, vol. 14, no. 2, pp. 1–12, 2020.
[7] Y. Jararweh, A. Doulat, and E. Alsmadi, "Scalable cloud architectures for disaster recovery and high availability," Cluster Computing, vol. 24, pp. 1–14, 2021.
[8] A. Marinos and G. Briscoe, "Community cloud computing and hybrid cloud models: A survey," IEEE Cloud Computing, vol. 8, no. 3, pp. 44–52, 2021.
[9] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques," Software: Practice and Experience, vol. 51, no. 1, pp. 1–20, 2021.
[10] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers," Computer Networks, vol. 210, pp. 1–20, 2022.

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

International Journal of Multidisciplinary and Scientific Emerging Research (IJMSERH)

Impact Factor: 7.121

ijmserh@gmail.com

www.ijmserh.com