Disaster Recovery as a Cloud Service

Pooja A. Patil*, Manisha V. Dhaybar

Department of Computer Science, Dr. D. Y. Patil Arts, Commerce and Science College, Pimri-18, Pune, Maharashtra, India

***Corresponding Author**

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1413SP008

Received: 26 June 2025; Accepted: 30 June 2025; Published: 22 October 2025

Abstract: Within the modern advanced time, the danger of disasters—both normal and man-made—poses noteworthy dangers to organizational information judgment and operational progression. A novel concept called Catastrophe Recuperation as a Cloud Benefit (DRaaS) employments cloud computing to supply calamity recuperation arrangements that are reasonable and versatile. This consider analyzes the center thoughts of DRaaS, surveys the body of investigate and observational prove, and looks into the troubles and real-world employments of the innovation. The consider assesses the adequacy of DRaaS arrangements and looks at organizational appropriation patterns employing a mixed-method approach. Although it seems that DRaaS essentially reduces costs and speeds up recovery, problems with security, integration, and compliance persist. The primary focus areas of the proposals are future bearing research and the best practices for a successful DRaaS installation. The increasing dependence on digital infrastructure has heightened the need for efficient disaster recovery (DR) methods. Disaster Recovery as a Cloud Service (DRaaS) is researched here as an elastic, cost-saving substitute for conventional DR solutions. It is aimed at investigating how DRaaS can help industries reduce downtime and data loss, with a particular emphasis on small and medium-sized businesses (SMEs). The research utilizes a mixed-methods design, integrating comparative evaluation of cloud-based and on-premises DR models alongside case studies of organizations using DRaaS. Recovery time objective (RTO), recovery point objective (RPO), cost-effectiveness, and system robustness are measured through simulation and user-reported values. Outcomes show that DRaaS decreases RTO and RPO dramatically when compared to traditional systems, while providing increased flexibility and less capital investment. SMEs especially enjoy the pay-as-you-go approach and automated failover options. Concerns regarding data sovereignty and vendor lock-in are still significant challenges. Finally, DRaaS appears to be an efficient and feasible solution for disaster recovery in the contemporary era, particularly for companies requiring agility and cost savings. The publication recommends best practices for DRaaS implementation, including careful vendor scrutiny, compliance alignment, and hybrid deployment strategies.

Keywords: Disaster Recovery (DR), Cloud Computing, Disaster Recovery as a Service (DRaaS), Business Continuity, Recovery Time Objective (RTO), Recovery Point Objective (RPO), Data Backup, IT Resilience, Cloud Infrastructure, Cost Efficiency

I. Introduction

Background

The potential impact of disruptions—whether brought on by hardware failure, cyberattacks, human error, or natural disasters—has increased as businesses depend more and more on digital infrastructure to run their operations. Data loss and outages may lead to monetary losses, harm to one's reputation, and legal ramifications. Disaster Recovery (DR) that strives at restoring IT systems and services resulting from such incidents is a vital component of business continuity planning.

Maintaining backup facilities or duplicate data centers is a common component of traditional disaster recovery plans, which call for a large initial investment, continuous upkeep, and intricate administration. Since cloud computing has become more prevalent, organizations have adopted cloud-based disaster recovery solutions as they are more adaptable and economical as well.

Disaster Recovery as a Cloud Service (DRaaS)

Cloud-based services referred to as DRaaS allow organizations to failover to the cloud infrastructure in the case of a disaster by resembling and hosting physical or virtual servers. DRaaS delivers geographically distributed redundancy, automated recovery techniques, and on-demand access to backup resources, that, in contrast with conventional techniques, eliminates the need to maintain expensive physical infrastructure.

Statement of the Problem

Regardless of the potential benefits of DRaaS, many organizations are uncertain to fully adopt it. Cloud data security and privacy, challenges connecting with legacy systems, regulatory compliance, and the potential for vendor lock-in comprise some of the key challenges. The objective of this study is to analyze the adoption of DRaaS as it represents today, pinpoint it’s positive and negative aspects, and provide helpful guidance for effective deployment.

II. Literature Review

Disaster Recovery Fundamentals: Disaster recovery is a strategic framework designed to assist organizations acquire resume operations as normally after a disruption.

Off-site backups, tape storage, and redundant data centers that replicate the primary site are every component of the conventional disaster recovery model (Smith & Kumar, 2018). Even though these models are trustworthy, they frequently require significant upfront and ongoing costs.

Cloud Computing and Its Impact on Disaster Recovery

IT service delivery has been revolutionized by cloud computing, which is characterized by the on-demand availability of computer resources through the internet. Cloud platforms offer resources that are swiftly provisioned, scalable, elastic, and economical (Jones et al., 2020). DRaaS, which allows enterprises to automate failover procedures and replicate workloads in cloud environments, emerged as a result of the incorporation of cloud services into disaster recovery plans.

Benefits of DRaaS

Several benefits of DRaaS are outlined by research:

- Cost-effectiveness: Removes the need to spend money on redundant physical infrastructure.

- Scalability: Depending on demand, resources can be scaled up or down.

- Speed: Automation and cloud agility lead to reduced recovery times.

- Geographic Redundancy: To increase resilience, cloud providers provide data centers spread across several regions (Chen & Lee, 2019).

Challenges of DRaaS

Despite the advantages, there are obstacles to DRaaS adoption:

- Security Issues: Data preserved on cloud servers may be vulnerable to hacks or illegal access.

- Compliance Issues: Ensuring data sovereignty and compliance may be difficult in sectors with strict regulations, such as healthcare and finance (Patel & Singh, 2021).

- Complexity of Integration: Cloud DR platforms might not be entirely compatible with legacy systems.

- Vendor lock-in: Reliance on a single cloud provider may reduce negotiating leverage and flexibility (Patel & Singh, 2021).

Empirical Review

Recent empirical research sheds light on adoption patterns and results:

65% of large businesses either use or intend to implement DRaaS within the next two years, according to a Gartner survey from 2023.

According to case studies by Brown et al. (2022), companies that implemented DRaaS saw an approximate 50% decrease in their Recovery Time Objective (RTO).

DRaaS users saw an average 35% decrease in disaster recovery expenses, according to additional research by Jones et al. (2020).

Theoretical Framework: Technology Acceptance Model (TAM)

The theoretical foundation for this study is the Technology Acceptance Model (Davis, 1989). According to TAM, the main determinants of technology adoption are perceived utility (PU) and perceived ease of use (PEOU). Given the concerns about complexity and benefits, this framework can be beneficial for assessing an organization's willingness to adopt DRaaS.

III. Methodology

Research Design

To obtain thorough insights into the adoption and efficacy of DRaaS, a mixed-method research approach was selected:

- Quantitative Data: To gather information on DRaaS usage, perceived advantages, and difficulties, an online survey was sent to 100 IT managers from a variety of industries.

- Qualitative Data: To gather expert perspectives and practical knowledge, ten cloud service providers and disaster recovery professionals engaged in semi-structured interviews.

Data Collection

- Survey Instrument: Likert-scale items assessing adoption status, recovery performance metrics, perceived difficulties, and TAM variables (PU, PEOU) were included in the questionnaire.

• Interviews: Best practices, security plans, and integration methods were examined through open-ended questions.

Data Analysis

- To determine the factors influencing the adoption of DRaaS, quantitative data were analyzed using regression, correlation, and descriptive statistics.
- To identify recurring themes and suggestions, thematic analysis was applied to qualitative data.

IV. Result and Discussion

Adoption Status and Drivers

Seventy percent of those surveyed have implemented or intend to implement DRaaS. The main motivators are lower management complexity (60%) quicker recovery times (78%), and cost savings (85%).

Impact on Recovery Metrics

Organizations accomplished a normal 50% decrease in RTO and a 40% lessening in Recuperation Point Objective (RPO).

•Average cost savings were 35%, mostly because of reduced hardware and maintenance costs.

Challenges Identified

• Security and compliance concerns were reported by 65% of participants.

• Legacy on-premises systems integration is still a major stumbling block.

• Vendor lock-in and organize unwavering quality were highlighted as dangers.

Expert Insights

Interviews highlighted:

- The importance of hybrid DRaaS models combining on-premises backup with cloud failover.
- Repeated testing and DR plan validation to guarantee preparedness.
- Encryption and multi-factor verification as security basics.

Theoretical Implications

The relapse test vindicated TAM's appropriateness: seen ease of utilize was a capable indicator of selection, and seen convenience had a direct impact. This implies that organizations value quantifiable benefits but also demand feasible implementation procedures.

V. Conclusion and Recommendations

Conclusion

Disaster Recovery as a Cloud Advantage might be a change in misfortune recovery organizing that enables organizations to have versatile, sensible, and quick recovery highlights. Although the adoption of DRaaS is increasing because of its advantages, security, compliance, and integration issues remain to be addressed.

Recommendations

- **Adopt Hybrid DR Models:** Combine cloud and on-premises resources to balance control and flexibility.
- **Focus on Security:** Implement robust encryption, access controls, and compliance checks.
- **Regular Testing:** Conduct frequent disaster recovery drills to validate failover processes.
- **Vendor Evaluation:** Choose cloud providers with strong SLAs, transparent security policies, and multi-region redundancy.
- **Employee Training:** Enhance awareness of cloud DR processes and security protocols.

Future Research

Further studies should explore:

- DRaaS adoption in regulated industries such as healthcare and finance.
- The role of emerging technologies like AI and machine learning in automating disaster recovery.
- Longitudinal studies measuring the long-term impact of DRaaS on organizational resilience.

References

1. Brown, T., Lee, H., & Patel, R. (2022). Evaluating the Efficiency of Disaster Recovery as a Service. Journal of Cloud Computing, 11(3), 125-138.
2. Chen, J., & Lee, M. (2019). Cloud-based Disaster Recovery: Benefits and Challenges. International Journal of IT Management, 29(2), 65-79.
3. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.
4. Gartner. (2023). Enterprise Cloud Adoption Survey. Retrieved from https://www.gartner.com
5. Jones, S., Kumar, A., & Smith, R. (2020). Cloud Computing in Disaster Recovery: A Comprehensive Review. Computers & Security, 88, 101613.
6. Patel, V., & Singh, K. (2021). Security Issues in Cloud-Based Disaster Recovery. Cybersecurity Journal, 7(1), 45-58.
7. Smith, J., & Kumar, N. (2018). Traditional Disaster Recovery vs Cloud-Based Solutions. Information Systems Review, 34(4), 302-315.