Turkish Journal of Computer and Mathematics Education *Vol.11 No.01 (2020), 815-820*
DOI: https://doi.org/10.17762/turcomat.v11i1.13562
Research Article

Cloud Computing-based Disaster Recovery

Indrajeet Kumar
Department of Computer Science & Information Technology,
Graphic Era Hill University, Dehradun Uttarakhand India 248002

Abstract. Cloud-based disaster recovery (DR) solutions help organisations recover from natural disasters and cyberattacks quickly and affordably. Cloud-based disaster recovery solutions improve recovery times, capital costs, scalability, and security. Yet, data security and DR strategy are still barriers to adoption. Only two issues. Besides these challenges, cloud-based catastrophe recovery looks promising. Cloud-based disaster recovery solutions will continue to grow as cloud technology improves. Hybrid cloud disaster recovery solutions, which integrate public and private cloud environments, will continue to grow in popularity, as will DRaaS, a cost-effective and flexible disaster recovery solution. As cloud-based disaster recovery solutions grow more prevalent, organisations must understand their disaster recovery needs, carefully analyse their cloud service providers' security and compliance procedures, and regularly test and update their disaster recovery plans and solutions. If organisations follow these measures, they may maximise the benefits of cloud-based disaster recovery solutions to safeguard their critical data and apps and ensure business continuity in a disaster.
Keywords. Cloud, Disaster recovery, environment, analysis, scalability.

I. Introduction

It is impossible to overestimate the significance of ensuring the continuity of corporate operations and safeguarding vital information and systems from disruptions in this day and age of widespread digitization [1]. The growing dependence that corporate operations have on technology has led to a rise in the likelihood that such activities would be disrupted as a result of natural catastrophes, cyberattacks, or other unanticipated occurrences [2]. In the event that this occurs, planning for disaster recovery (DR) has evolved into an essential component of managing the continuity of corporate operations. Traditional methods of disaster recovery carried out on-site can, however, be expensive, difficult to install, and time-consuming to maintain. Disaster recovery (DR) strategies that make use of cloud computing come into play at this point.

Using the available resources provided by cloud service providers, cloud computing-based disaster recovery (DR) is a solution that is both extremely effective and efficient for the purpose of backing up and restoring essential data and systems [3]. The concept of cloud-based disaster recovery refers to the practise of storing data and applications in a distant cloud environment that is situated in a location that is distinct from the original data centre. In the event that there is a disruption, this makes it possible to quickly restore data and maintain business continuity [4].

The use of cloud-based disaster recovery offers a variety of advantages, some of which include cost efficiency, scalability, flexibility, dependability, and geographic diversity [5]. Cloud-based disaster recovery gives businesses the opportunity to scale their DR capabilities up or down fast and easily in response to shifting business requirements. This may be done without the need to make expensive investments in infrastructure. In addition, cloud-based disaster recovery provides greater flexibility in terms of recovery alternatives, enabling businesses and other organisations to select the sort of DR that is most suited to meet their individual requirements [6].

II. Benefits of Cloud Computing-based Disaster Recovery

Organizations may profit from cloud computing-based disaster recovery in a variety of ways [7][8], including:

a. Cost-effectiveness: Cloud-based DR reduces the need for enterprises to invest in infrastructure, such as servers and storage, as well as in-house DR specialists, which saves money. Organizations using cloud-based DR simply pay for the services they use, allowing them to control expenses and scale their DR capabilities up or down based on changing business demands.

b. Scalability: Cloud-based DR enables enterprises to swiftly and inexpensively extend their DR capabilities without the need to acquire new infrastructure or recruit extra people. Cloud-based disaster recovery services may be established and deployed in minutes, allowing enterprises to swiftly extend their DR capabilities as needed.
c. Flexibility: Cloud-based DR provides enterprises with broader recovery alternatives. Organizations can select between cold, warm, or hot standby conditions depending on the type of DR required. Moreover, cloud-based DR may be tailored to individual business requirements, ensuring that enterprises have the appropriate amount of DR protection for their specific needs.
d. Reliability: Cloud service providers often provide greater levels of uptime and dependability than on-premises infrastructure, lowering the risk of data loss and downtime in the event of a disaster. Cloud-based disaster recovery companies often have numerous geographically different data centres, which adds redundancy and protection against regional calamities.
e. Geographic diversity: Cloud-based disaster recovery allows enterprises to store their data and applications in numerous geographically different locations, guaranteeing that vital business processes may be swiftly and effectively restored in the case of a regional or local disaster.

III. The Challenges of Disaster Recovery Using Cloud Computing

While cloud computing-based disaster recovery [9][10] has numerous advantages, it also has certain drawbacks, including:
a. Security and Data Privacy: When enterprises use cloud-based DR, they are handing their essential data and systems to a third-party supplier. This necessitates enterprises carefully evaluating their cloud DR provider's security and data privacy policies and procedures, as well as implementing suitable safeguards to assure data protection.
b. Compliance: Companies in highly regulated sectors may experience difficulties in meeting regulatory standards when utilising cloud-based DR. Organizations must verify that their cloud DR provider complies with all relevant legislation and has adequate controls in place.
c. Latency: Latency might be a problem for enterprises that need to duplicate significant volumes of data to the cloud DR provider. This can have an influence on recovery timeframes, especially if the business requires significant volumes of data to be recovered fast.
d. Network Dependence: Cloud-based disaster recovery is significantly reliant on network connection. Businesses must verify that their network architecture is capable of enabling cloud-based DR and that adequate backup connections are in place to assure network connectivity dependability and availability.
e. Testing: Testing is an essential component of any disaster recovery plan, including cloud-based DR. Companies must ensure that proper testing techniques are in place to assess the efficacy and dependability of their cloud-based disaster recovery strategy.

IV. Cloud-based DR Strategies

Cloud-based disaster recovery (DR) methods refer to the many techniques that businesses may use to duplicate their data and apps to the cloud in order to maintain business continuity in the case of a disaster. Cold, warm, and hot standby are the three basic types of cloud-based DR techniques [11][12]. Each solution provides varying levels of security, recovery time goals (RTOs), and prices.

a. Cold Reserve

A cold standby DR method involves storing data and apps in the cloud but not replicating them in real time. Instead, data and applications are duplicated on a regular basis, such as daily or weekly, thus some data and application loss is to be expected in the case of a disaster. Because it requires the least amount of equipment and resources, cold standby is the most cost-effective DR solution. Nevertheless, the RTO for this technique is longer since the business must restore the most recent backup of data and apps before operations can restart.

b. Cold Standby

A warm standby DR approach involves a business replicating its data and applications to the cloud in real time, but the cloud infrastructure is not completely operational. Instead, the company leverages the cloud environment to pre-stage its apps and data so that they are ready to launch. In the case of a disaster, the business may swiftly restore operations by spinning up its pre-staged cloud environment. Since it demands more resources than cold standby but is less expensive than hot standby, this method strikes a compromise between cost and recovery time.

c. Active Standby

A hot standby DR approach involves an enterprise replicating its data and applications to the cloud in real time, and the cloud infrastructure is fully operational and ready to go. In the case of a disaster, the business may effortlessly transition to the cloud environment with no data loss or delay. This technique provides the most security and the quickest RTO, but it is also the most expensive because it requires a fully running cloud infrastructure at all times.

Organizations must examine issues such as recovery time targets, cost, and the criticality of their data and applications when selecting a cloud-based DR plan. It is also critical to test the chosen approach on a regular basis to ensure that it fits the DR requirements of the company and that the recovery process works as planned. Moreover, enterprises should collaborate closely with their cloud DR provider to develop the optimal solution for their specific requirements and to ensure that the provider is achieving their service level agreements.

V. Current State of Cloud-based DR Adoption

Cloud-based disaster recovery (DR) solutions are gaining popularity among businesses of all sizes and sectors. According to MarketsandMarkets, the worldwide cloud-based DR market is predicted to rise at a compound yearly growth rate (CAGR) of 23.3% from USD 5.1 billion in 2020 to USD 14.5 billion by 2025. Factors such as the necessity for business continuity, the increasing prevalence of cloud computing, and the increased frequency of natural catastrophes and cyber-attacks are driving this expansion [13].

Numerous sectors are pioneering the use of cloud-based disaster recovery systems. Because of the importance of patient data and the requirement for continuous access to electronic health records, the healthcare industry, for example, has been fast to adopt cloud-based DR solutions (EHRs). Given the sector's requirement for high availability and data protection, the financial services industry was an early user of cloud-based DR solutions[14].

Small and medium-sized enterprises (SMBs) are also rapidly embracing cloud-based disaster recovery (DR) solutions. Cloud-based disaster recovery solutions provide SMEs with a low-cost approach to secure their data and applications without the need for large capital investments or professional IT expertise [15]. Moreover, cloud-based DR solutions allow SMEs to scale up or down as their company needs evolve.

Notwithstanding the benefits of cloud-based disaster recovery systems, there are certain barriers to adoption. One of the most difficult difficulties is guaranteeing data security and privacy in the cloud. Businesses must carefully analyse the security standards of their cloud service providers to guarantee that their data is always secure. Another problem is the complexities of disaster recovery planning and implementation [16]. Companies must understand their DR requirements and create a complete DR plan that includes testing and frequent upgrades.

Finally, as firms seek cost-effective and efficient ways to assure business continuity in the face of disasters and cyber-attacks, cloud-based disaster recovery solutions are gaining traction. While there are significant barriers to adoption, the benefits of cloud-based disaster recovery solutions make them an appealing alternative for enterprises of all sizes and sectors.

VI. Best practices for cloud-based DR implementation

Best Practice	Description
Conduct a Business Impact Analysis (BIA)	A BIA helps organizations identify critical applications and data and prioritize their recovery in the event of a disaster. This information is crucial for developing a comprehensive DR plan.
Develop a	A DR plan should include procedures for backing up data and applications, testing the

Comprehensive DR Plan	DR environment, and restoring operations in the event of a disaster. The plan should also be regularly updated to ensure its effectiveness.
Choose a Reliable Cloud Service Provider	Organizations should choose a cloud service provider that offers robust security measures, data redundancy, and a proven track record of uptime and availability.
Implement Data Encryption	Data encryption is critical to protect data from unauthorized access or theft. Organizations should encrypt data both in transit and at rest in the cloud.
Conduct Regular Testing and Maintenance	Organizations should test their DR plan regularly to ensure its effectiveness and make any necessary adjustments. Additionally, organizations should regularly maintain their cloud infrastructure to ensure that it is up-to-date and functioning correctly.
Implement Access Controls	Organizations should implement access controls to restrict access to sensitive data and applications in the cloud. This includes implementing role-based access controls and multi-factor authentication.
Monitor and Audit Activity	Organizations should monitor and audit activity in the cloud environment to detect and respond to any potential security incidents. This includes logging and reviewing access logs, network activity, and application usage.
Develop an Incident Response Plan	An incident response plan outlines the steps that organizations should take in the event of a security incident. This plan should include procedures for containing the incident, notifying stakeholders, and restoring operations.
Provide Employee Training and Awareness	Employees play a critical role in maintaining the security of cloud-based DR solutions. Organizations should provide regular training and awareness programs to ensure that employees are aware of security best practices and how to respond to security incidents.

Table.1 Best practices for cloud-based DR implementation

VII. Future of Cloud-based DR

Factor	**Future Outlook**
Market Growth	The cloud-based DR market is expected to continue growing rapidly due to the increasing adoption of cloud computing, the need for business continuity, and the rising frequency of disasters and cyber-attacks.
Technology Advancements	Advances in cloud technology, such as serverless computing, edge computing, and artificial intelligence, will continue to enhance the capabilities of cloud-based DR solutions.
Hybrid Cloud DR	More organizations will adopt hybrid cloud DR solutions that combine public cloud and private cloud environments to ensure high availability and cost-effectiveness.
Security and Compliance	Cloud service providers will continue to enhance their security and compliance measures to address concerns about data privacy and security.
Disaster Recovery as a Service (DRaaS)	DRaaS will become increasingly popular as organizations look for cost-effective and flexible ways to implement DR solutions.
Importance of Testing	The importance of testing and validating DR plans and solutions will continue to be emphasized to ensure successful disaster recovery.

Table.2 Future of Cloud-based DR

VIII. Conclusion

Cloud-based disaster recovery (DR) solutions provide businesses with a method that is both efficient and cost-effective for ensuring the continuation of their company operations in the face of natural catastrophes and cyberattacks. Improved recovery times, decreased capital expenditures, higher scalability, and enhanced security are

some of the benefits that come with using cloud-based disaster recovery systems. Nevertheless, there are still certain obstacles to adoption, such as protecting the privacy and security of data and building a complete DR strategy. These are only two of the problems.

In spite of these obstacles, cloud-based disaster recovery appears to have a bright future. It is anticipated that the market for cloud-based disaster recovery solutions will continue its rapid expansion, and developments in cloud technology will further improve the capabilities of cloud-based disaster recovery solutions. Hybrid cloud disaster recovery solutions, which combine public cloud and private cloud environments, will continue to gain popularity, and Disaster Recovery as a Service, also known as DRaaS, will continue to gain traction as a method that is both cost-effective and flexible for implementing disaster recovery solutions.

It is essential to ensure that organisations have a clear understanding of their disaster recovery requirements, carefully evaluate the security and compliance measures implemented by their cloud service providers, and routinely test and update their disaster recovery plans and solutions as cloud-based disaster recovery solutions become increasingly popular among businesses. If enterprises follow these steps, they will be able to maximise the benefits of cloud-based disaster recovery solutions, which will allow them to secure their essential data and applications and maintain business continuity in the case of a catastrophe.

References

[1] Barsallo, J., & García, F. (2017). Disaster Recovery Strategies in Cloud Computing. International Journal of Computer Networks and Communications Security, 5(6), 148-155.

[2] Chen, M., Mao, S., & Liu, Y. (2014). Big Data: A Survey. Mobile Networks and Applications, 19(2), 171-209.

[3] Sivakumar, R., & Samy, D. (2018). Cloud Computing Based Disaster Recovery: An Overview. International Journal of Advanced Research in Computer Science and Software Engineering, 8(4), 355-359.

[4] Wu, L., & Buyya, R. (2015). Cloud-Hosted vs. On-Premise Disaster Recovery: A Performance Cost Analysis. IEEE Transactions on Cloud Computing, 3(2), 133-146.

[5] Zabrowski, E., & Bezborodova, O. (2017). Cloud-Based Disaster Recovery: Benefits and Challenges. Journal of Telecommunications and Information Technology, 3, 24-31.

[6] Li, L., Zhang, Y. and Li, Y., 2018. An efficient disaster recovery solution based on cloud computing. Future Generation Computer Systems, 87, pp.590-602.

[7] B. Mathew and K. W. K. Lui, "A review of disaster recovery mechanisms for cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2229-2253, 2013.

[8] Y. Chen, S. Xu, J. Ren, and Y. Zhang, "A novel disaster recovery framework for cloud data center," in Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2015, pp. 743-748.

[9] S. S. V. S. N. Reddy, K. Varma, and V. K. Mago, "Disaster recovery in cloud computing environments: A survey," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 23-37, 2013.

[10] K. Li, C. Wang, and Y. Zhang, "A survey of cloud-based disaster recovery technologies," in Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), 2016, pp. 234-238.

[11] S. Sharma and S. R. Jindal, "Disaster recovery for cloud computing: A review," in Proceedings of the IEEE International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 485-490.

[12] A. H. Al-Mamun, S. R. Chowdhury, and M. A. Razzaque, "A review of disaster recovery techniques for cloud computing," Journal of Cloud Computing, vol. 4, no. 1, 2015.

[13] D. K. Dey and P. Kumar, "A review on disaster recovery solutions in cloud computing," in Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2016, pp. 1-6.

[14] N. Nasser, N. Alzeidi, and M. Alazab, "A review of disaster recovery challenges and solutions in cloud computing," Journal of Cloud Computing, vol. 7, no. 1, 2018.

[15] J. Zhu, J. Shao, and J. Han, "Research on disaster recovery in cloud computing environment," in Proceedings of the IEEE International Conference on Computer Science and Network Technology (ICCSNT), 2013, pp. 743-748.

[16] S. M. A. Mollah and C. C. Dutta, "Disaster recovery in cloud computing: A systematic review," in Proceedings of the IEEE International Conference on Advanced Computing Technologies (ICACT), 2017, pp. 1-6.
[17] N. Nasser, N. Alzeidi, and M. Alazab, "Towards a comprehensive disaster recovery solution for cloud computing," Future Generation Computer Systems, vol. 95, pp. 782-795, 2019.
[18] S. S. V. S. N. Reddy, V. K. Mago, and K. Varma, "Disaster recovery planning in cloud computing environments: A review," Journal of Parallel and Distributed Computing, vol. 73, no. 12, pp. 1719-1731, 2013.
[19] B. Wang, X. Yu, and L. Zhang, "A novel disaster recovery system for cloud computing," Journal of Network and Computer Applications, vol. 36, no. 2, pp. 771-778, 2013.