Cloud-Based Disaster Recovery and Business Continuity

Author Name - Chandan Kumar , Anumesh Rao

Arya College of Engineering and Information Technology

Jaipur (Rajasthan), India

ck1516017@gmail.com , anumeshrao638@gmail.com

Abstract - Cloud disaster recovery (DR) has become a necessary strategy to ensure a continuous business operation while protecting data in a world of unexpected interruptions and disasters. The article on this topic summarizes the importance of preparing and executing a cloud DR plan for critical data and application security. The abstract discusses significant factors in establishing an effective cloud DR plan, including risk assessment, data backup (and replication), failover, and recovery time objectives (RTOs), and recovery point objectives (RPOs). Advantages for using cloud services in DR programs are discussed, including cost savings, scalability, and geographic redundancy. Some challenges and considerations related to cloud DR, including data security and compliance, are mentioned. Ultimately, this article investigates a complete overview of best practices for cloud disaster recovery in order to provide organizations a good reference for establishing business continuity plans that are robust and resilient.

Index Terms - Cloud Disaster Recovery, Business Continuity, Data Protection, Risk Assessment, Data Backup, Replication, Failover, Recovery Time Objective (RTO), Recovery Point Objective (RPO), Cloud Services, Data Security, Compliance.

1.INTRODUCTION

Cloud disaster recovery and business continuity are the technologies, policies and procedures of an organization that are used to ensure that the organization IT systems and data can be protected in the event of disaster, such as natural disaster, cyberattack or hardware failure. The aim of a disaster recovery and business continuity strategy is to reduce the impact of a disaster on the organization's operations and to return to normality with the recovery of business critical systems and data. As cloud computing becomes more prevalent, cloud disaster recovery and business continuity strategies has become vital parts of the IT operations of many organizations. By using the cloud with its different flexibility and scalability, organizations, can develop a disaster recovery and business continuity in a cloud that meets their needs at a lower price. In a cloud-based disaster recovery and business continuity solution, the critical IT systems and data have been replicated in the cloud, and can be quickly restored in the event of a disaster. A cloud-based disaster recovery and business continuity solution can minimize the length of downtime and maximize the assurance that IT operations can continue even if the primary on-premise IT infrastructure is down.

2. LITERATURE REVIEW

A cloud platform for disaster recovery and business continuity is one of the main factors influencing how organizations handle unforeseen events and subsequently return to normal organizational functions. The following review of the literature brings together all significant sources and findings related to cloud-based disaster recovery and business continuity.

2.1 Limited Role of Cloud Service Providers in Disaster Recovery Management

Disaster recovery planning has been shown to be important, and some studies have shown that cloud service providers are a vital part to the overall disaster recovery plan and efforts. To summarize, according to what was previously stated, Li et al. (2018) state that disaster recovery services such as data hosting, backup, cloud storage, and disaster readiness have moved cloud service providers to be a vital part of organizations looking for disaster recovery, leveraging a SaaS delivery model and faster recovery efforts. The study continues to reinforce the importance that there should be an ongoing dialog and these partners should work

together to updating and maintaining
the recovery plans

2.2 Backup and recovery are the facets to ensure disaster resistance and resilience in cloud services.

On-demand backup and recovery systems are categorized as a dependable system that allows you to maintain the business operations through the occurrence of a disaster. One thing Zhou and others (2018) stated is that cloud backup and recovery solutions can give companies flexibility and enable business to grow that may not happen with traditional backups and recovery solutions. In addition to this information, the paper explains the important consideration of selecting the cloud service provider that has a strong recovery system and robust backup infrastructure.

2.3 Evaluating and Monitoring Disaster Recovery in the Cloud Computing.

The resiliency of cloud-based disaster recovery models depends on effective evaluating and monitoring plans that are carried out simultaneously. Previous research supports the premise for on-going monitoring and evaluation of a cloud-based disaster recovery solution by businesses, detecting potential issues before affecting business operations (Chen et. al., 2020). Importantly, this research demonstrates the importance of selecting an appropriate method for both evaluating and monitoring with the intent to provide a high level of confidence that each of the aspects related to the disaster recovery protocols, are monitored and evaluated appropriately.

2.4 The Advantages Related to Cloud Disaster Recovery and Business Continuity is Impressive and While Certainly Not Free, is Worth Implementing in Any Organization.

The extensive surveying done has indicated the value of cloud-based disaster recovery and business continuity for organizational effectiveness. Lai and Wu (2020) note that cloud-based disaster recovery services increase responsiveness and flexibility, reduces downtime, and improves business resiliency. In addition, they mention the potential cost-savings of networked recovery technologies. Moreover, the current review of the literature on cloud disaster recovery and business continuity illustrates the real importance of cloud for operational capability when continuity of business is challenged by an unforeseen disruption. Notably, the literature indicates that cloud service providers are a critical factor in planning for disaster recovery, implementing and testing backups and recovery procedures in the cloud, monitoring security and disaster recovery procedures, and responsiveness to business continuity. In sum, the literature highlights the tremendous improvements and value of cloud disaster recovery/services when responding to a disturbance and maintaining business continuity.

3. METHODOLOGY

3.1 Business Continuity

Disaster recovery describes the various systems, policies and technology elements that can be put in place to ensure that the core function and systems of an organization can be maintained in the case that a disaster occurs (whether that's a natural disaster, cyber-attack, or hardware failure). The primary function of business recovery planning is to take the necessary steps to mitigate the possible aftermath of a disaster on a business' operations, as well as ensure timed business systems and necessary data, can be restored in a timely manner. Business continuity planning is mainly concerned with the planning of a detailed plan of what a company needs, what risks are possible, and what actions and technology needs to be applied when a disaster occurs. The plan includes regular testing as a measure of the plan's effectiveness, and to produce something applicable to the real-time working environment. Given the complicated processes involved in considering business interruption, these areas address disaster recovery, risk management, and crisis management. Disaster recovery is focused on restoration of operational data and systems after the failure has taken place, while risk management identifies risks or potential threats to organizational functions. Crisis management is concerned with how to manage a disaster and ensure that both people and resources are appropriately positioned to respond to it in a timely manner. A business continuity plan (BCP) is defined as a document that outlines the key emergency preparedness actions of an organization during and post a significant disruption to its normal business operations. BCPS primarily focus on minimizing the impact to the business during a disruption, whether the disruption is caused by a natural disaster, cyber-attack, pandemic or any other situation that may disrupt business operations.

BCP's usually contain a risk assessment, which includes identifying the risks that could negatively impact the organization and their respective impact and likelihood of occurrence.

Figure 1: Business Continuity model

3.2 Disaster Recovery

Disaster recovery (DR) is the act of resuming the normal business practices after a disruptive event such as a natural disaster, cyberattack or pandemic. Disaster recovery is part of a business continuity plan and relates to the speediest and most effective means of recovering the organizations critical systems and data. Disaster recovery planning is a continual process that also involves ongoing testing, monitoring, and review to keep disaster recovery capabilities current and effective. Disaster recovery is to minimize the impact of a disruption so that a business can return to its normal/expected operations as soon as possible. An organization that has an established, tested disaster recovery plan can minimize financial loss, protect company reputation, and ultimately, support the company's long-term viability. A disaster recovery plan (DRP) is a documented plan that outlines the actions to be taken by an organization when it experiences any kind of disruptive event such as a cyclone or cyberattack, which is more disruptive to the organization than a typical disaster. The primary aim of a disaster recovery plan is to lessen the effects of a disaster on an organization, along with its ability to carry out its mission-critical functions in a short and timely manner. A disaster recovery plan is very important for the continuity of its business. In essence, cloud computing offers organizations flexible, scalable, and economical options for the provision of continuous service, especially in the event of a disaster. Leveraging the latest trends in cloud reputation of your organization, after a disruptive event.

Figure 2: Disaster Recovery

3.3 Business Continuity and Disaster Recovery in Cloud Computing (BCDR)

Cloud computing can significantly enhance business continuity and disaster recovery by offering organizations an economical, flexible, and scalable infrastructure for the protection of their core systems and data.

Scalable: Organizations can utilize cloud computing for its scalability by quickly and easily scaling up and down their IT infrastructure as needed for any process, allowing the organization to respond quickly to changing business needs and difficulties (from disasters to crises).

Flexible: Through cloud computing solutions, organizations now can store their essential systems in the cloud, which means that organizations can access those systems from wherever they have an Internet connection. This simplifies the rescue and safeguarding of essential systems entirely. Cost-effective: Clouds offer organizations a few cost-effective solutions like disaster recovery and business continuity, thus, decreasing the cost of storage and infrastructure by pooling them with other organizations.

Automated backups: In a cloud computing environment, automated synchronization of critical data and systems can easily be achieved to ensure that it is kept updated and in sync in the event of a disaster.

Geo-redundancy: Cloud computing allows critical data and systems to be maintained in different locations, removing the risk of a disaster affecting your data due to a regional emergency and greatly increasing your organizational security.

Improved disaster recovery times: While unplanned downtime occurs occasionally, cloud computing reduces the number of hours required to recover business functions because critical systems and critically important data can be brought back from disaster from the cloud.

Easy testing: The cloud computing environment enables organizations to test disaster recovery by backing up its customer's critical data and applications to an easy to access secure cloud-based data center. Testing and validating: The DRaaS vendor periodically tests the DR capacity for the customer's computing DRaaS service, permitting another opportunity to assure that the customer's critical systems and data are secure.

3.4. Strategies for disaster recovery and Business Continuity strategies must include (BCDR) cloud services

3.4.1. Infrastructure as a Service (IaaS): Infrastructure as a Service (IaaS) is an extremely powerful disaster recovery service that allows organizations to maintain their IT infrastructures in an effective and timely manner in the event of an incident. IaaS uses a model whereby an organization replicates its management of IT infrastructure to a cloud-service provider such that the cloud-service provider has the capacity to give computing resources, storage, and network resources as needed. Disaster recovery resiliency and traditional replication models using IaaS as the underlying service provide a lot more flexibility than existing subsystems yet are also scalable to adapt to changes in an environment. Relevant organizations can remain on standby with the appropriate supplementary resources required for the job quickly but need not really procure any additional hardware/infrastructure. This feature provides disaster recovery environment in a miniature time span and lowers setup costs. So, like IaaS can enhance flexibility for the disaster recovery process, IaaS can also heighten organization’s control over their disaster recovery environment. Organizations can customize separate shapes of their architecture to meet their needs and can easily simulate and amend their action plans over time. To really distill this down, IaaS is important because it can afford organizations an elevated layer of security and data protection.

Ultimately, we cannot deny that media plays the role to shape perceptions to define the election. Assuming from industry practices, cloud service operators use highly sophisticated security methods to protect their infrastructure and database, including encryption, multi-factor identification, and intrusion detection and prevention systems. This will provide a level of assurance that if the incident occurs, the essential data and programs are protected.

3.4.2. Disaster Recovery as a Service (DRaaS):

Disaster Recovery as a Service (DRaaS) is a core cloud-based service that provides an effective and affordable way for organizations to recover important computer networks and data in the event of a disaster. DRaaS is designed to help organizations reach their declared DR operation objectives by introducing cloud-based infrastructure, data storage, and recovery recovery services undefined.

1. Data security: A DRaaS provider continues to safeguard the customer's important data and applications to a secure, cloud-based data centre.

2. Testing and ensuring service levels: A DRaaS supplier periodically conducts disaster recovery tests of the customer’s disaster recovery environment to ensure correct functionality of the environment as well as recoverability of the customer’s data in an incident

3. Restoration: The DRaaS supplier would then prioritize their customers and restore the critical systems and storage in a seemingly uninterrupted manner. More and more organizations are turning to DRaaS solution to enhance their disaster recovery while reducing the risk associated with revenue loss and reputational damage after experiencing disruptions. However, the decision-making for about which DRaaS solution to implement, must be done with suitable due diligence about a provider's reputation, security practices and service level agreement (SLAs). When organizations consider a trusted DRaaS provider, they will have a truly assured and effective failover plan in place for their disaster recovery.

3.4.3. Backup as a Service (BaaS):

Backup as a Service (BaaS) is a cloud backup solution that securely stores an organization's critical data in a note-safe remote service. The backup process is managed by a third-party provider who makes sure customer data is available for access depending on the scheduled time, when tested, and the security mechanism.

If disaster strikes, and the customer, say lost or corrupted their data, the provider still can potentially bring it back, meaning the customer does not necessarily have to be interrupted from their normal cadence.

The main advantage of BaaS is that it takes the burden off of the organizations of provisioning and managing their own backup infrastructure. They are generally able to lower their costs associated with backing up and recovering data, as well as reduce the risk of data loss in the case of hardware failures and other disasters that can occur onsite in an organization's premises. In addition, most BaaS providers use highly secure transfer protocols so that customers can trust their data will be securely transferred to those providers with every backup and recovery. The BaaS offering is suitable for all industries and sizes of organizations, including but not limited to, healthcare, tech, retail, and finance. However, considering the reputation of the provider, their security measures, and service level agreements (SLAs) should all be part of the consideration, when reviewing the BaaS offering. If an organization combines its internal IT resources with the services of a trusted BaaS provider, they can prevent the loss of information, should a disaster happen to occur.

4. RESULTS AND DISCUSSION

According to an IDG report, 72% of organizations have a disaster recovery plan in place to some extent, while 46% of organizations use a cloud-based solution, which is a considerable number. In their report, the Disaster Recovery Planning Council stated that 20 percent of organizations have dealt with a disaster for the past five years, and 80 percent of those organizations have always experienced downtime or data loss. Research by the Institute has shown that, on average, organizations which experience downtime spend $5,600 per minute. According to a survey by the Disaster Recovery Journal, 38% of organizations find a cloud-based disaster recovery solution to be the easiest way to recover from disaster. The world witnesses that the cloud technology, which is anticipated is aimed not just at stimulating growth in the disaster recovery market, but also at enhancing it. The value of the disaster recovery market, which was $12 billion in 2020, is expected to reach $60 billion in 2030. Statistics and estimates indicate that by 2025, we will see an 82 billion increase in enterprise size, anticipating a 29% compound annual growth rate (CAGR), according to Market.

According to the Disaster Recovery Journal, which surveyed organizations, a 46% majority said that they plan to increase their spending on cloud-based disaster recovery solutions in the next year. A Gartner survey found that 72 percent of organizations using cloud disaster recovery are satisfied with the solution. The data presented in these studies plainly demonstrate that nearly every organization that maintains data in the cloud has suffered some sort of breach, and/or lost a significant amount of revenue due to hacks. Unquestionably, the immense value cloud disaster recovery solutions are realizing will increase in popularity and create more firm's awareness of their appeal in protecting data and ensuring significantly less downtime in a disaster.

5. CONCLUSION

Cloud disaster recovery has become a crucial and changing approach for maintaining business continuity and protecting data in unexpected disruptions or disasters. Cloud-based disaster recovery solutions have significant benefits when adopted, providing organizations with cost savings, scalability, redundancy in different locations, and greater availability of data. Organizations may develop prevention plans for threats and vulnerabilities by creating comprehensive risk assessments and utilizing data backup and replication methods and processes, while ensuring availability and redundancy of key data is established. Failover processes provide business continuity by enabling organizations to move or failover seamlessly and with speed to secondary sites during a disruption, ultimately minimizing downtime and impact to business operations.

The extent of disaster recovery in the cloud to offer unmatched scalability enables organizations in all recovery scenarios to alter their resources as needed to gain optimized use of resources. Geographical redundancy across multiple centers of data ensures data protection and data loss risk mitigation, increasing the overall robustness and resilience of disaster recovery processes. Disaster recovery plans that are routinely tested and validated can provide a level of assurance regarding the.

organizations abilities to respond to harrowing disaster scenarios in a speedy and effective way. Cloud-based disaster recovery solutions can adequately test disaster recovery strategies without disrupting the production systems, ensuring speed and readiness of the disaster recovery measures. Nevertheless, adopting cloud disaster recovery solutions also poses challenges that must be considered and overcome. Data security and compliance is a major concern when trusting sensitive data to a third-party cloud provider. Organizations need to conduct their due diligence in assessing the organizations cloud service provider policies regarding security measures, data encryption mechanisms, and regulatory compliance.

It is important to address planning around potential internet connectivity challenges in recovery plans to facilitate a seamless and effective recovery. This may include redundancies and contingency plans for maintaining network connectivity during critical operational periods. Hybrid cloud disaster recovery strategies provide organizations with the flexibility of using some on-premises resources and some cloud-based solutions, thus allowing for optimized disaster recovery strategies for an organization's needs or workloads. Hybrid strategies are practical and balanced approach to business continuity planning.

In a nutshell, cloud disaster recovery is a vital aspect of modern organizations' business continuity planning, offering resilient, scalable, and robust solutions for safeguarding essential data and operations. As organizations are more reliant on data and digital services, the need for cloud disaster recovery will be vital for organizations that want to not just survive but truly flourish in an evolving, increasingly interconnected business context. Cloud disaster recovery solutions also provide organizations the means to successfully cope with potential difficulties and disruptions, after an incident occurs, to safeguard essential assets while continuing operational and business continuity. Organizations can focus on enhancing resilience, providing assurance of recovery capability, and to ultimately prosper in a dynamic, uncertain, and competitive environment. A converted attitude to cloud disaster recovery will allow organizations to address possible difficulties and disruptions with confidence, ultimately ensuring business continuity and trust in the integrity of data in a digital world.

6. REFERENCES

[1] REFERENCES M. M. Al–shammari and A. A. Alwan, "Disaster Recovery and Business Continuity for Database Services in Multi-Cloud," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2018, pp. 1-8, doi: 10.1109/CAIS.2018.8442005.

[2] Alhazmi, H.; Malaiya, K. Evaluating disaster recovery plans using the cloud. In Proceedings of the 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, USA, 28–31 January 2013.

[3] Gaire, R. et al. (2020). Internet of Things (IoT) and Cloud Computing Enabled Disaster Management. In: Ranjan, R., Mitra, K., Prakash Jayaraman, P., Wang, L., Zomaya, A.Y. (eds) Handbook of Integration of Cloud Computing, Cyber Physical Systems and Internet of Things. Scalable Computing and Communications. Springer, Cham. https://doi.org/10.1007/978-3-030-437954_12.

[4] H.E. Miller, K.J. Engemann, R.R. Yager, Disaster planning and management. Commun. IIMA 6(2), 25–36 (2006).

[5] P. Pareek, Cloud Computing Security from Single to Multi-clouds using Secret Sharing Algorithm, vol. 2, no. 12, pp. 12-15, 2013.

[6] S.Sengupta and K. M. Annervaz, "Multi-site data distribution for disaster recovery-A planning framework", Futur. Gener. Comput. Syst., vol. 41, pp. 53-64, 2014.

[7] Y.Gu, D. Wang and C. Liu, "DR-Cloud: Multi-cloud based disaster recovery service", Tsinghua Sci. Technol., vol. 19, no. 1, pp. 13-23, 2014.

[8] V. Javaraiah, "Backup for cloud and disaster recovery for consumers and SM Bs", Int. Symp. Adv. Networks Telecommun. Syst. ANTS, 2011.

[9] S. Prakash, S. Mody, A. Wahab and S. Swaminathan Ramani, Disaster Recovery Services in the Cloud for SMEs Waves Of Cnange, pp. 139-144, 2012.

[10] A. Prazeres and E. Lopes, "Disaster Recovery - A Project Planning Case Study in Portugal", Procedia Technol., vol. 9, pp. 795-805, 2013.

[11] https://www.aws.amazon.com/what-is/disaster-recovery/

[12] https://cloudian.com/guides/disaster-recovery/disaster-recovery-and-business-continuity-plans/

[13] Muraidhara, P. (2013). Security issues in cloud computing and its countermeasures. International Journal of Scientific & Engineering Research, 4(10).

[14] Sriram, I., & Khajeh-Hosseini, A. (2010). Research agenda in cloud technologies. arXiv preprint arXiv:1001.3259.

[15] Muralidhara, P. (2017). THE EVOLUTION OF CLOUD COMPUTING SECURITY: ADDRESSING EMERGING THREATS. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, 1(4), 1-33.

[16] Muralidhara, P. (2017). IoT applications in cloud computing for smart devices. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, 1(1), 1-41.

[17] Serrano, N., Gallardo, G., & Hernantes, J. (2015). Infrastructure as a service and cloud technologies. IEEE Software, 32(2), 30-36.

[18] Muralidhara, P. (2019). Load balancing in cloud computing: A literature review of different cloud computing platforms.

[19] Elmurzaevich, M. A. (2022, February). Use of cloud technologies in education. In Conference Zone (pp. 191-192).