© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 10 Issue: 03 | July - September 2019
Paper is available at www.jrps.in | Email : info@jrps.in

Disaster Recovery in Cloud Environments: Strategies for Business Continuity

Hitesh Premshankar Rai
Independent Researcher, USA.

Pavan Ogeti
Independent Researcher, USA.

Narendra Sharad Fadnavis
Independent Researcher, USA.

Gireesh Bhaulal Patil
Independent Researcher, USA.

Uday Krishna Padyana
Independent Researcher, USA.

DOI: https://doi.org/10.36676/jrps.v10.i3.1460

Abstract

The most important components of a firm are business continuity and disaster recovery planning, although they are often disregarded. Even before a crisis strikes, businesses need to have a well-organized strategy and documentation for business continuity and recovery after a disaster. A single cloud is characterised as a collection of servers housed in one or more data centres that are provided by a single supplier. Nonetheless, there are several reasons why switching from a single cloud to multiple clouds is sensible and crucial. For example, single cloud providers are still vulnerable to outages, which impacts the database's availability. Furthermore, the single cloud may experience partial or whole data loss in the event of a catastrophe. Due to the significant risks of database accessibility failure and the potential for malevolent insiders inside the single cloud, it is anticipated that consumers would become less fond of single clouds. Cloud-based Disaster Recovery (DR) enables the coordinated use of resources from many cloud services offered by the DR Service provider. Thus, it is essential to create a workable multi-cloud-based Disaster Recovery (DR) architecture that minimises backup costs in relation to Recovery Time Objective (RTO) and Recovery Point Objective (RPO). By achieving high data dependability, cheap backup costs, quick recovery, and business continuity before to, during, and after the catastrophic incidence, the framework should preserve accessibility to data. This study suggests a multi-cloud architecture that ensures high data availability before to, during, and after the catastrophe. Additionally, it guarantees that database services will continue both before and after the financial crisis.

Keywords: - Disaster Recovery, Single Cloud, (RTO) and (RPO), Business Continuity, Multi-Cloud, Database, Backup Cost.

I. INTRODUCTION

With digital data and services at the centre of today's dynamic corporate landscape, unplanned interruptions have the potential to have a massive impact [1]. Organisations confront several hazards that might impair operations and damage data, ranging from the continual problem of cyberattacks to the potential of hardware failures and natural catastrophes. These disruptions may have expensive repercussions, such as idle labour, missed profits, and disastrous financial losses [1, 2]. Disaster

Recovery (DR) techniques are crucial since the world is becoming more and more data-dependent and linked.

In the past, disaster recovery often included the upkeep of specialised on-premises infrastructure, which might be a challenging and costly option to administer. However, in recent years, cloud disaster recovery has altered the landscape. It is a crucial tactic in the current business environment because it gives organisations a more scalable and effective way to guarantee data security and business continuity [1]. The significance of organising and putting into practice cloud-based solutions for disaster recovery is examined in detail in this study. By using cloud service capabilities, organisations may access flexible and affordable infrastructures. This architecture lowers the risk of interruptions and loss of data by greatly enhancing the effectiveness and efficiency of disaster recovery operations.

The term "Business Continuity" (BC) refers to the capacity of an organisation to go on operating even in the face of interruptions. Business continuity is described as "the organization's ability to continue providing products or services at adequate predetermined levels following disrupting incident" (International Organisation for Standardisation, publication 22301:2012) [2, 3]. It seems to imply a comprehensive strategy to maintain the company solution even in the event of an upsetting situation [3]. On the other hand, disaster recovery (DR) is more technically focused and focuses on maintaining a BC solution's technical features to enable company continuity and recovery in the event of a catastrophe [4].

As a result, DR gives BC a new dimension since, whereas BC may be used to any kind of disruptive occurrence, disasters are only related to those that fall under certain categories. Thus, unless otherwise indicated, BC, Business Continuity Management (BCM), and other related activities are exclusively covered in the context of DR in this thesis. DR is thus a component of BC, but they combine (BC/DR) in order to distinguish between the unique characteristics of the solutions [2, 4]. This research focuses on Information Technology (IT)-based solutions, but it may also be applicable to most non-IT-based systems, including a power grid and other essential infrastructure technologies. Any IT-based solution used by any organisation is considered business in this sense, and going forward, business will be viewed as such.

A business needs a variety of resources, including personnel, equipment, and infrastructure. The majority of organisations focus only on technology and believe that it is essential to success [4]. Even while technology is unquestionably one of the most important factors in success, there are several situations that may quickly destroy an organisation. Both big and small businesses nowadays depend on the internet, and any disruption to it will cause the business's main functioning regions and activities to cease [4, 5]. Organisations must thus be prepared for any disruptions in technology that may arise from unforeseen circumstances; the 9/11 attacks serve as the prime example. An organisation might deal with such unforeseen catastrophes more effectively if it had a solid and well-organized business continuity and disaster recovery strategy [5].

The majority of organisations still do not have a plan; in fact, many do not even try to create one, despite the fact that some are prepared to assist them in dire circumstances thanks to a solid contingency plan. It is astonishing to learn how few organisations do not have robust data backup strategies in place [5]. While a disaster recovery plan or any other kind of contingency plan won't help a corporation make money, it will undoubtedly assist avoid losses—major losses. A firm has to be ready for any kind of crisis since they may happen at any moment [5]. "A corporation must develop an ideal strategy to minimise the impact of catastrophe and continue the essential business tasks, depending on the type of the organisation, its size, and several other factors.” A perfect strategy will take into account a variety of variables, such as the extent and impact of the crisis, financial limitations, RTO, RPO, and MTO [5, 6].

The link between the Disaster Recovery Plan (DRP) and the Business Continuity Plan (BCP) is shown in the image since both plans oversee the implementation of a BC/DR solution. Although it is evident from the figure that DRP is a component of BCP, [6, 7], DRP does not appear to be linked to the actual technical fix. The technological solution is significant because it may display specifics and interdependencies among its technical components, all of which are necessary for a BC/DR solution. Additionally, [8] a technological solution consists of several parts that may be handled by various providers.

Furthermore, the complexity of today's IT systems suggests that there may be close connection between different IT solutions, meaning that all of them should be included in BC/DR. In a similar vein, a single business process may potentially be connected to many different systems, in which case all supporting IT solutions would also need to be included in the BC/DR scope. It seems that in order to address the gaps, a high degree of granularity must be reached, which calls for delving into the specifics of an IT solution [8, 9]. By doing this, it would be feasible to assist in bridging the gaps that are highlighted in this chapter, including defining the function of a provider and emphasising dependencies.

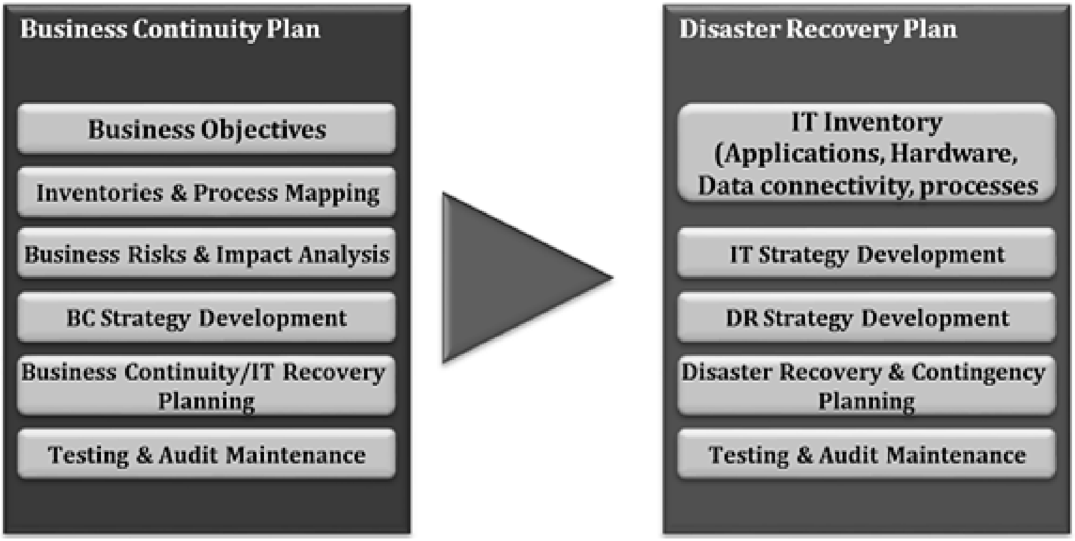
Business Continuity Plan
Business Objectives
Inventories & Process Mapping
Business Risks & Impact Analysis
BC Strategy Development
Business Continuity/IT Recovery Planning
Testing & Audit Maintenance
Disaster Recovery Plan
IT Inventory (Applications, Hardware, Data connectivity, processes
IT Strategy Development
DR Strategy Development
Disaster Recovery & Contingency Planning
Testing & Audit Maintenance

Fig. 1 Connection between disaster recovery and business continuity plans. [9]

The primary reason for the widespread use of cloud computing is its significant ability to reduce the overall cost of ownership for technological infrastructure and its many benefits in the field of Information Technology (IT) [9, 10]. High data availability is ensured by keeping data in the cloud, which is one of its unique features. When storing sensitive data, it's critical to make sure the information is accessible. Consumers in cloud environments depend on cloud services to store sensitive data, therefore maintaining data availability is critical to meeting client needs [10]. Due to the present problems with data recovery and backup in a single cloud, massive amounts of data storage are being used by duplicating data to many data centres within the same cloud. Furthermore, a single cloud may run into issues including hardware malfunction, software bugs, network intrusions, natural catastrophes, and human-caused harm that affect the data that is stored [10, 11]. These issues often cause service interruptions, and in the worst scenario, they might corrupt data and cause the system to collapse.

It is not ideal to develop cloud-based systems with a single data centre in order to serve people without considering the possible hazards and their repercussions. Certain providers of cloud services came up with workable strategies to prevent this issue, such as using regional data dispersion to safeguard the most important data. Additionally, [11, 12] one cloud service provider has data centres in many locations, and these centres often employ comparable infrastructures—bulk purchases, operation mechanisms, and management teams—and software stacks.

The procedure used by an organisation to restore business operations after a disruptive incident is known as disaster recovery, or DR. The Disaster Recovery (DR) services provider might collaborate with other cloud service providers to use their resources. The multi-cloud approach makes an effort to use two or more clouds, which reduces the possibility of data loss, privacy violations, and service outages. Utilising many clouds at once may help to further lower the risk to data and apps in public clouds [12]. The customary obstacles to cloud adoption—security, dependability, expense, and loss of control—remain in place. Organisations may thus increase their flexibility by implementing multi-cloud environments, giving them greater control over the services they utilise as well as the opportunity to choose where and what workloads to execute.

1.1 Recovering from disasters

The main requirements of DR as a process for its appropriate planning and, therefore, its successful execution, will be briefly reviewed in this section.

i. **Recovery Point Objective (RPO):** This condition often refers to the quantity of data that may be lost between the moment of a critical incident and the most recent backup, within a time frame that is most relevant to a company, before severe damage arises. RPO is dependent on business decisions, as mentioned in [11], yet it should be remembered that certain software applications and technologies still need RPO=0 in spite of this determination.

ii. **Recovery Time Objective (RTO):** The maximum amount allowable time interval between a service interruption and its restoration is represented by this condition. This goal establishes, within the parameters set by the organisation, the acceptable time range during which service is unavailable [12, 13]. According to, the RTO parameter encompasses more than just the system activating time; it also takes into account the time it takes to detect an outage, set up the server infrastructure, reconfigure the active network equipment to reroute all network traffic in accordance with the new working conditions, and more [12].

iii. **Performance:** Performance is one of the criteria; it is the capacity of the disaster recovery system to support the preservation system and application functionality throughout both the process of recovery and asynchronous replication for protection [12, 13]. This need is crucial for the process of delivering either asynchronous or synchronous replication with the DC's DR as well as for situations when an outage occurs and the DR is implemented, mostly because of the relationship with the RTO [14].

iv. **Consistency:** When discussing consistency in the post-outage recovery process, we first consider the condition in which the IT structure's services as well as application solutions are operational again [14, 15]. As per and, synchronous replication of a programme, support, system, or full site may guarantee consistency [15]. Emphasises the consistency that is offered by states that are kept on the local storage system; these states seem to be consistent with incremental backups.

1.2 Objectives of the Study

- Examine the foundational ideas and procedures of cloud-based disaster recovery.
- Examine the financial effects of putting disaster recovery plans into place in cloud settings.

II. LITERATURE REVIEW

(Jasgur, C. 2019) [16] The "cloud" has gotten more and more popular throughout time as a means of helping companies become more resilient. Building on achievements like Office 365 application migrations, enterprises are increasingly considering cloud-based disaster recovery as a practical means of safeguarding vital applications in the event of an emergency. This essay examines a single organization's path through the disaster recovering cloud deployment labyrinth. It will examine the organization's past experience with cloud-based applications, the difficulties it encountered, and the solutions it used to overcome those difficulties, the outcomes of the deployment, the dangers, and ultimately the solution's future advantages using a case study methodology. The article will conclude by guiding the reader through the 10 actions that a company should take to migrate its own disaster recovery setup to the cloud.

(Al-Sharidah, A. H., 2017) [17] To guarantee availability and continuation of their operations amid unfavourable events and outages, a lot of organisations depend on Disaster Recovery services. The idea of company effect Analysis facilitates sufficient planning for the continuation of company operations by providing vital information on the effect of offerings on business operations and their criticality levels. Technology and communication advancements have changed how disaster recovery solutions are developed, making cloud-based solutions an appealing option and essential component of continuing corporate operations. The model that best combines cost, software configuration, repairs, and control level should be chosen by organisations. We examine disaster recovery architecture in terms of networking, hardware, software, data replication, and access points in this article. The article also lists the main obstacles, advantages, security issues, and safeguards for cloud-based disaster recovery solutions.

(Gupta, V., 2016) [18] The rules and practices that guarantee an enterprise's ability to continue operating in the event of an unanticipated interruption are known as business continuity planning. Disaster Recovery is an Information Technology (IT) component that falls under Business Continuity Planning. The process of disaster recovery planning includes a thorough examination of company procedures, risk assessment, setting goals for disaster recovery, developing and evaluating a plan, and testing the plan. The catastrophe recovery plan is influenced by a multitude of factors. For corporate organisations, disaster recovery is a very essential topic. There isn't a research in the literature that offers a comprehensive list of criteria that affect the Disaster Recovery Strategy at different stages of the Disaster Recovery preparation procedure.

III. METHODOLOGY

The suggested work's technique is shown in this section. Additionally, it suggests a research paradigm with two primary parts: database recovery and ensuring the uninterrupted operation of database services across several clouds [19]. Creating a strategy for database service recovery in a multi-cloud environment that transfers data from the main site to the recovery site in before, during, and after a catastrophe is the first component's concentration.

3.1 Methodology of the Research

The methodology of this research work can be outlined as follows:

1. Review the Literature

At this stage, we go over the background information and relevant literature for this study project. The review addresses the following:

i. Determining a definition for database recovery in cloud infrastructure and assessing disaster recovery methods relevant to the study [19, 20]. The evaluation examined the recovery of database services in a multi-cloud context and assessed how the recovery affected backup storage costs, turnaround times, and performance.

ii. A collection of research on current initiatives to preserve database services' BC in multicolour environments.

2. Create a Multi-coloured Database Recovery Method

The steps of the suggested method for determining database recovery in multi-cloud environments have been identified and meticulously planned at this point. The three primary stages that follow are noted:

i. Outlining the DR components that have an impact on the functioning of important database services and establishing acceptable downtime thresholds like RTO and RPO

ii. Create and put into practice a database recovery strategy in a multi-cloud context using the appropriate tools to apply the suggested fix.

iii. Testing and assessing the suggested fix and the procedures required to get the database.

3. Create a Plan to Ensure Database Services Continue to Run in a Multi-Cloud Environment

The steps to maintain the BC of databases services in multi-cloud environments are identified at this point. These stages are:

i. Examining how data in several clouds affects performance, time, and storage costs.

ii. Examining the effects of many data centres on backup storage costs, turnaround times, and performance [20].

iii. Using the following three indicators of performance to assess the two stages and ascertain the DR and BC performance:

a) Recovery Time Objective (RTO)

b) Recovery Point Objective (RPO)

c) Backup storage cost

4. Put the Research Framework into Practice

The two strategies that have been developed throughout the phases of designing an approach for database recovery in multi-cloud environments and designing an approach to preserve the BC of database services in multi-cloud environments make up the suggested framework [20, 21]. Regarding implementation, the performance measures RTO and RPO were used to assess how well the suggested methodologies performed in this study project.

5. Assess the Suggested Method

At this point, RTO, RPO, and the cost of backup storage are used to assess how well the suggested methods perform in terms of database disaster recovery and maintaining business continuity in cloud environments [21]. The stages of this research project's technique are shown in Figure 1.

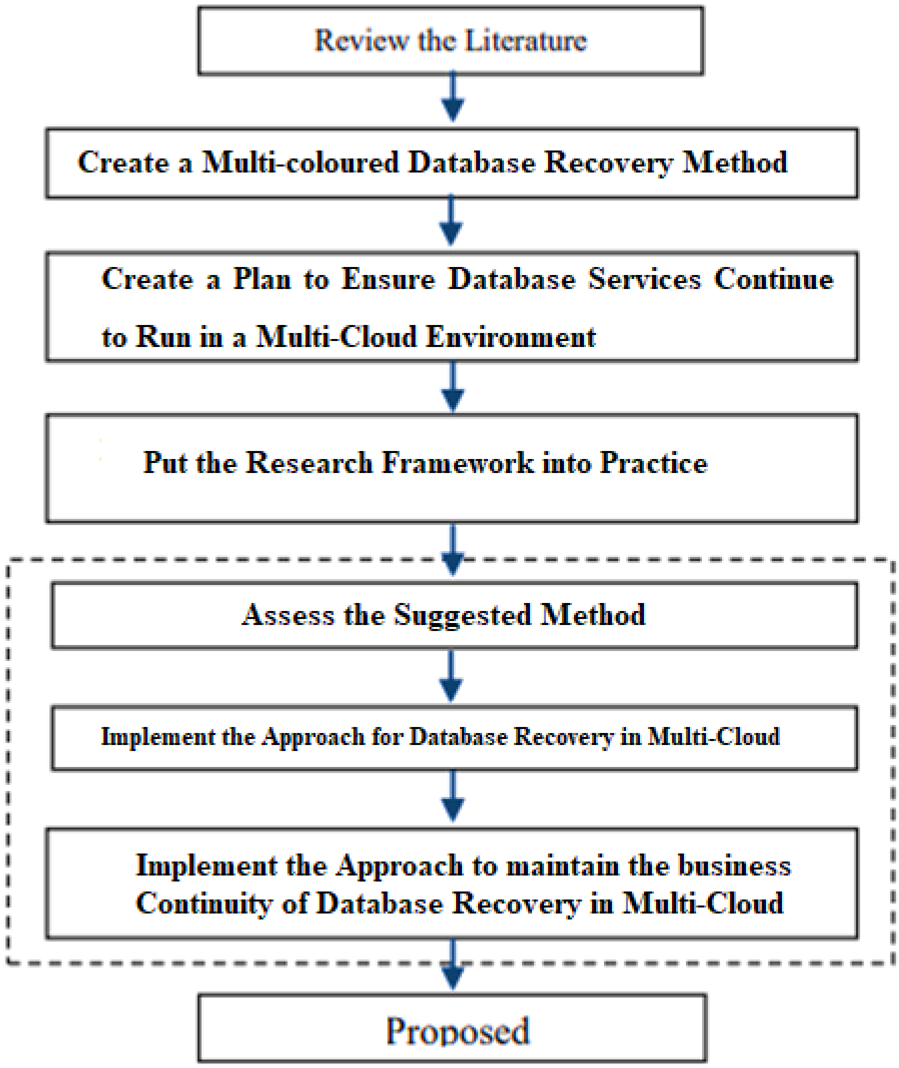
Review the Literature
Create a Multi-coloured Database Recovery Method
Create a Plan to Ensure Database Services Continue to Run in a Multi-Cloud Environment
Put the Research Framework into Practice
Assess the Suggested Method
Implement the Approach for Database Recovery in Multi-Cloud
Implement the Approach to maintain the business Continuity of Database Recovery in Multi-Cloud
Proposed

Fig. 1 Research Framework. [21]

3.2 The Suggested Disaster Recovery Framework for Databases

3.2.1 Multi-cloud environment-based services

Database recovery in a multicolour ecosystem and maintaining the business continuation of database applications in a multicolour context make up the two primary parts of the suggested DR architecture for database services based on multicolour environments. The two primary functions of such components are data recovery and data backup. Ensuring the recovery of database services following a catastrophe is one of the research framework's primary responsibilities [21, 22]. Figures 2 and 3 describe the suggested database services disaster recovery structure for a multi-cloud context.

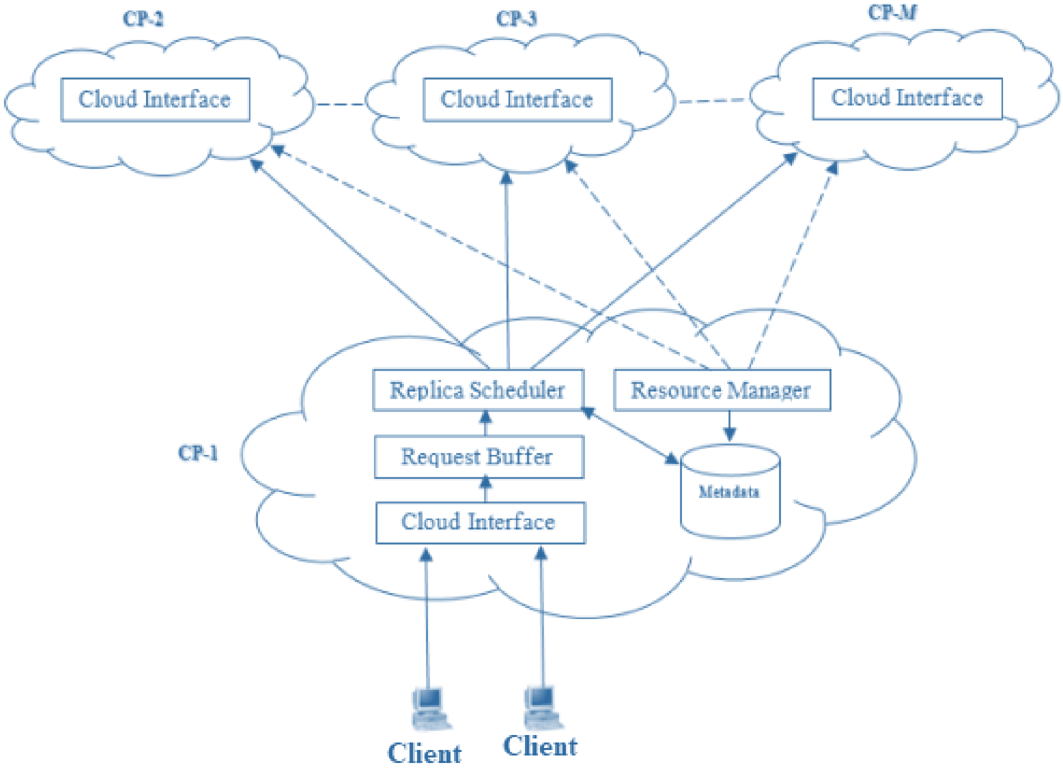

Fig. 2 Data Backup Processing. [22]

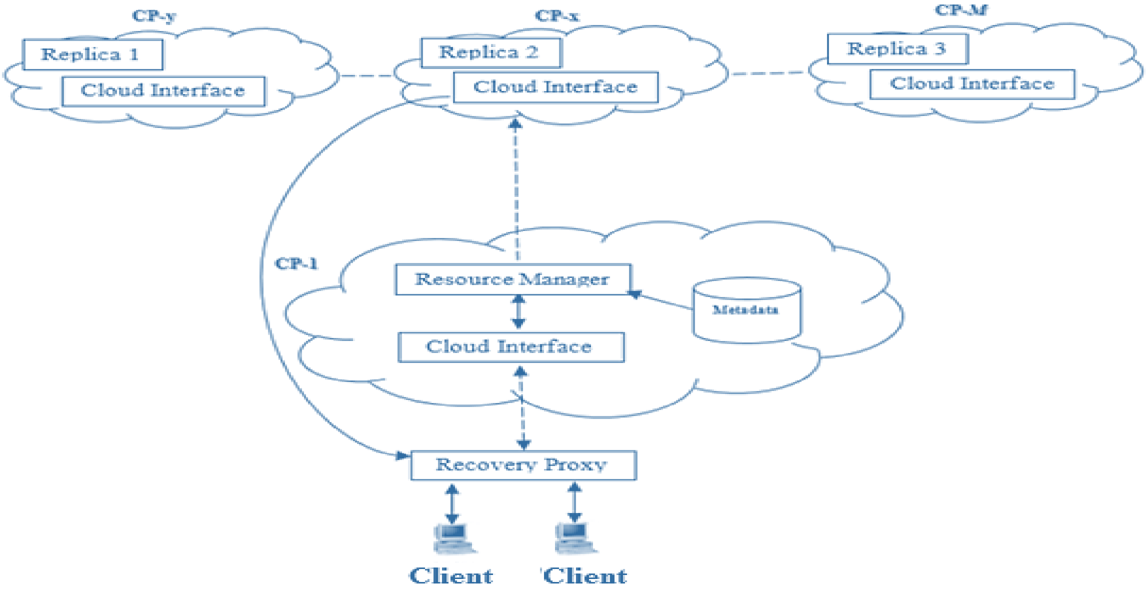

Fig 3. Procedure for Data Recovery. [22, 23]

i. A module for producing experiment parameters that creates parameters for data disaster recovery scenario involving several clouds [24].

ii. The information gathering module, which is in charge of obtaining backup job specifications and keeping track of Cloud Providers' (CPs') resource modifications [25, 26].

iii. A replica scheduling module that creates backup plans using various approaches by imitating Cloud Provider 1's replica scheduler.

iv. A result recording module that logs each backup plan and determines the overall cost of backup storage and RTO for the duration of the simulation.

IV. CONCLUSION

In modern business continuity planning, cloud disaster recovery plays a critical role by providing enterprises with scalable, robust, and reliable solutions to protect their critical data and processes. Organisations hoping to succeed in an evolving and interconnected business landscape must embrace cloud-based disaster recovery due to the increasing reliance on digital assets and services.

This study presents a conceptual multi-cloud system that ensures high data availability before to, during, and after a catastrophe. Additionally, it guarantees that database services will continue both during and after the crisis. This study presents a conceptual framework that aims to minimise costs for database recovery in multi-cloud environments. It also presents a method for maintaining the BC of database services across many clouds in terms of backup storage cost savings, RPO, and RTO. We want to use Clouds in the simulator to implement the suggested framework in a later project. Additionally, we want to assess the suggested methodologies' efficacy using a few datasets in terms of RTO and RPO.

V. REFERENCES

1. Sengupta, S., & Annervaz, K. M. (2014). Multi-site data distribution for disaster recovery—A planning framework. Future Generation Computer Systems, 41, 53-64.
2. Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European journal of operational research, 242(1), 261-273.
3. F. Gibb and S. Buchanan, “A Framework for Business Continuity Management,” International Journal of Information Management, vol. 26, no. 2, pp. 128–141, 2006.
4. J. Rittinghouse and J. Ransome, Business Continuity and Disaster Recovery for Infosec Managers, 1st ed. Amsterdam: Elsevier Digital Press, 2005.
5. H. Brotherton and J. E. Dietz, “Data Center Business Continuity Best Practice,” Information Technology: New Generations (ITNG), 2014 11th Int’l Conference on, Las Vegas, NV, 2014, pp. 496–501.
6. M. Swanson, et al., “Contingency Planning Guide for Federal Information Systems,” NIST Special Publication 800-34 Revision 1, May 2010.
7. E. Brewster, R. Griffiths, A. Lawes, and J. Sansbury, IT Service Management: A Guide for ITIL Foundation Exam Candidates, 2nd ed. BCS, the Chartered Institute for IT, 2012.
8. J. Van Bon, Service Transition Based on ITIL V3, 1st ed. [Zaltbommel (Netherlands)]: Van Haren, 2008.
9. W. Van Grembergen, S. De Haes, and J. Moons, 2005, “Linking Business Goals to IT Goals and COBIT Processes,” Information Systems Control Journal, vol. 4, 2005.
10. M.M. Alshammari, A.A. Alwan, A. Nordin, I.F. Al-Shaikhli, "Disaster Recovery in Single-Cloud and Multi-Cloud Environments: Issues and Challenges", (ICETAS), 2017, Salmabad, Bahrain.
11. T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van Der Merwe, A. Venkataramani, "Disaster recovery as a cloud service: Economic benefits & deployment challenges", 2010, Boston.

12. A.A. Tamimi, R. Dawood, L. Sadaqa, "Disaster Recovery Techniques in Cloud Computing", IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019, Amman, Jordan
13. Kahan, S. (2014). Global benchmark study reveals 73% of companies are unprepared for disaster recovery.
14. Kamath, J.-P. (2007). Disaster planning and business continuity after 9/11. ComputerWeekly.com.
15. Kirvan, P. (2015). Today’s most popular business continuity/disaster recovery standards. Tech Target.
16. Jasgur, C. (2019). Leveraging disaster recovery in the cloud as a cloud migration path: A case study. Journal of Business Continuity & Emergency Planning, 13(2), 150-159.
17. Al-Sharidah, A. H., & Al-Essa, H. A. (2017, September). Toward cost effective and optimal selection of IT disaster recovery cloud solution. In 2017 9th Computer Science and Electronic Engineering (CEEC) (pp. 43-48). IEEE.
18. Gupta, V., Kapur, P. K., & Kumar, D. (2016, February). Exploring disaster recovery parameters in an enterprise application. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 294-299). IEEE.
19. T. Tsubaki, R. Ishibashi, T. Kuwahara, Y. Okazaki, "Effective disaster recovery for edge computing against large-scale natural disasters", IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, Las Vegas, NV, USA.
20. S. Togawa and K. Kanenishi, “Private cloud cooperation framework of e-learning environment for disaster recovery,” Proc. - 2013 IEEE Int. Conf. Syst. Man, Cybern. SMC 2013, pp. 4104–4109, 2013.
21. Z. Saquib, V. Tyagi, S. Bokare, S. Dongawe, M. Dwivedi, and J. Dwivedi, “A new approach to disaster recovery as a service over cloud for database system,” 2013 15th Int. Conf. Adv. Comput. Technol., pp. 1–6, 2013.
22. S. Suguna and A. Suhasini, “Overview of data backup and disaster recovery in cloud,” 2014 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2014, no. 978, 2015.
23. W. Al Shehri, “Cloud Database - Database as a Service,” Int. J. Database Manag. Syst., vol. 5, no. 2, pp. 1–12, 2013.
24. R. J. Thara, S. Shine, and C. Sanu, “Optimizing the performance of Database as a Service (DaaS) model - A distributed approach,” 2013 4th Int. Conf. Comput. Common. Netw. Technol. ICCCNT 2013, 2013.
25. S. Pippal, V. Sharma, S. Mishra, and D. S. Kushwaha, “Secure and efficient multitenant database for an ad hoc cloud,” Proc. - 2011 1st Int. Work. Secure. Serv. Cloud, IWSSC 2011, pp. 46–50, 2011.
26. T. H. Lin, H. T. Chang, M. J. Chen, and P. Y. Yang, “Using a database as a service for providing electronic health records,” 2014 IEEE-EMBS Int. Conf. Biomed. Heal. Informatics, BHI 2014, no. 133, pp. 9–12, 2014.
27. Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization. Tuijin Jishu/Journal of Propulsion Technology, 40(4), 50-56.

28. Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service . (2019). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
29. Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service. International Journal
30. ofTranscontinental Discoveries, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
31. Choppadandi, A., Kaur, J., Chenchala, P. K., Kanungo, S., & Pandian, P. K. K. G. (2019). AI-Driven Customer Relationship Management in PK Salon Management System. International Journal of Open Publication and Exploration, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128
32. AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128
33. Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
34. Shah, J., Prasad, N., Narukulla, N., Hajari, V. R., & Paripati, L. (2019). Big Data Analytics using Machine Learning Techniques on Cloud Platforms. International Journal of Business Management and Visuals, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
35. Mahesula, Swetha, Itay Raphael, Rekha Raghunathan, Karan Kalsaria, Venkat Kotagiri, Anjali B. Purkar, Manjushree Anjanappa, Darshit Shah, Vidya Pericherla, Yeshwant Lal Avinash Jadhav, Jonathan A.L. Gelfond, Thomas G. Forsthuber, and William E. Haskins. "Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis." Electrophoresis 33, no. 24 (2012): 3820-3829. https://doi.org/10.1002/elps.201200515.
36. Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
37. Shah, D., Salzler, R., Chen, L., Olsen, O., & Olson, W. (2019). High-Throughput Discovery of Tumor-Specific HLA-Presented Peptides with Post-Translational Modifications. MSACL 2019 US.
38. Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
39. Purohit, M. S. (2012). Resource management in the desert ecosystem of Nagaur district_ An ecological study of land agriculture water and human resources (Doctoral dissertation, Maharaja Ganga Singh University).
40. Kumar, A. V., Joseph, A. K., Gokul, G. U. M. M. A. D. A. P. U., Alex, M. P., & Naveena, G. (2016). Clinical outcome of calcium, Vitamin D3 and physiotherapy in osteoporotic population in the Nilgiris district. Int J Pharm Pharm Sci, 8, 157-60