International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 96-100
Published Online April 2025 in IJEAST (http://www.ijeast.com)

CLOUD BASED DISASTER RECOVERY SYSTEM

Sarthak Dugar, Alice Patel, Rabindra Nath Maurya
Department of CSE-CTIS
Jain University, Bengaluru, Karnataka, India

Abstract— **Disaster recovery of information technology is a hot area of security for protecting data against unsatisfactory events, which involves a set of procedures for system continuation. Business continuity is a superset of disaster recovery, whereas the disaster recovery planning is a superset of business continuity planning. There are numerous policies for disaster recovery. This essay starts with an illustrative study of some models for disaster recovery. Subsequently, it presents a discussion of some cloud-based disaster recovery strategies and compares them with the conventional disaster recovery. The findings indicate that the cloudbased disaster recovery performed better than conventional disaster recovery. Additionally, the paper emphasizes value of disaster recovery planning.**

Index Terms— **Disaster Recovery (DR), Disaster recovery planning, Cloud-based disaster recovery**

I. INTRODUCTION

The rapid development of information technology is continually exposing the security of information systems to more issues. One being more disasters; natural or man-made. The very necessity to look ahead and engage in in the issue of Disaster Recovery (DR), which is part of the security planning process that aims to protect an organization from the bad effects of unacceptable events [1]. There are cloud-based disaster recovery which is a facility applied to DR models so that machines located remotely on a cloud-based platform can be backed up and restored and exemplifies multiple benefits including faster disaster recovery, more scalability for the IT (Information Technology) infrastructure and again less costs and higher availability of data [2]. Recently various models for cloud based DR have been presented in a number of studies, e.g. [3,4] that provide considerable recommendations on how to substitute traditional strategies of DR for cloud based. Disaster recovery planning is a documented process describing how to identify risks that might negatively affect an organization. The goal is to develop, document, implement, test, and prescribe a process for recovering and protecting the IT infrastructure while resuming normal operations [5,6]. Good planning depends on two important factors, or measures, which are the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). RTO is the maximum amount of time the appli- cation could be offline after a Major Incident (MI). RPO is the maximum tolerable period the data could be lost according to MI [7,8]. The key aim of DR planning is to reduce down time, avoid data loss, and shorten the RPO and RTO. Each section of the DR plan requires both the RTO and RPO. This paper will offer its contribution to the area of disaster recovery by representing the importance of cloud computing in DR, instead of traditional DR.

Consequently, this paper explores several cloud-based disaster recovery models and presents a comparison to the traditional method. It also shows the necessity of creating the right plans that could eliminate, and mitigate, various forms of disaster. In addition, it shows the cloud-based DR strategies. The outline of the paper is structured as follows: Section 2, in this section the literature search is presented; Section 3 addresses the importance of the disaster recovery planning; Section 4 demonstrates the cloud-based DR strategies; and finally, Section 5 provides the conclusion of the paper.

This paper is structured as follows: Section II provides details on the literature survey. Section III explains the parallelization of the N-Body problem. In Section IV the details about experimental results have been provided; followed by conclusions and references. Appendix provides the performance statistics of the Barnes-Hut algorithm in OpenMP on galactic datasets chosen from Princeton University [4]; with number of bodies ranging from 5 to 30,002.

II. LITERATURE SURVEY

A. Background

The concepts of disaster recovery planning concepts, and the processes associated with the disaster recovery planning process are described in [5] where the use of Fuzzy Cognitive Maps (FCM) is introduced and is rep- resented in a structured graph that incorporates many of the complex relationships between the considered disaster recovery plan with respect to IT systems. On the other hand, the FCM entails capabilities to enhance the under- standing of systems and their risks. The FCM model has the potential to be used for a risk analysis, and aspects that may arise for a given organization. In [9], a multi- location recovery model

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 9, Issue 12, ISSN No. 2455-2143, Pages 96-100
Published Online April 2025 in IJEAST (http://www.ijeast.com)

derived from specific economic theory is presented. This recovery model contains two broad sectors, an internal and an external sector. These sectors require information in order to sort through the transactions and the time to located them. The transaction level may be simple, compound or complex in nature. In
[9] friction and uncertainty are also presented as being obstacles to completing the transactions. The friction has five distinctive categories including communication, engineering, information, procedures, and political action. These distinct categories encompass a set of areas requir- ing recovery. Multilocation recovery studies can help to reduce the friction costs, and foster a better conception of a general recovery model across different geographical spaces.
In [3], the diversity disaster recovery problems of struc- ture and infrastructure storage subsystem security backup problems are all addressed. This paper introduces the technology of disaster recovery backup that originated from a virtual network storage study that theoretically solved these problems, and protected the backup data using a transparent encryption mechanism. The paper also created a double live cloud computing data center with a Net App 3250 double live disaster Metro storage technology Cluster in [3]. Therefore, when any fault oc- curs the other main memory will take place rapidly and automatically to ensure the continuity of the business. In [4], the authors propose the enriched multi objective optimization models using the enriched genetic algorithm for an efficient disaster recovery in a cloud computing environment. This paper is an analysis of a massive data storage process, and develops a data storage cost based on communication cost, data storage cost, and data migra- tion cost, through a cloud computing environment. The models can ensure high data storage reliability, minimize small recovery time, and moderate backup costs.
Some elements affecting IT risk management are as-sessed in [10] to ensure that the organization business continuity. The focus of the authors is on the risk of the disaster recovery center. The authors build upon some aspects of information theory to derive a mathematical function for IT risk management. Decision support could then be implemented within an organization based on certain mathematical formulas to understand the levels for the disaster recovery center. In [11], four different approaches of backup and disaster recovery solutions are considered. Amazon Cloud (AWS) used a combination of these approaches to maintain business continuity. These approaches consist of backup and recovery, pilot light approach, warm standby approach, and multi-site ap- proach. AWS also provided business continuity at the least cost. Table 1 summarizes the earlier discussed research of disaster recovery models.

B. Literature Survey

Importance of the Disaster Recovery Planning. With the rising number and severity of disasters, organization should take care designing the disaster recovery planning. The disaster recovery plan is made to protect the business processes in the event of a disaster happened. It is part of an important process for the whole business planning avoiding the risks may be occur in organizations [1,6]. In the previous studies several studies mentioned above which had touches in disaster recovery (DR) planning; for that reason this study will focused on highlighting the importance in DR planning. While disasters cannot always be avoided by organizations, having strong and detailed planning may possibly minimize the impact of disaster in the level of operations. The disaster recovery panning would need to define the recovery strategies, be in the format of system DR implemented in cloud or traditional disaster recovery. In the event of natural disasters, and man-made, the future operations of an organization relies on having the IT systems and data able to be replicated. Disaster recovery planning offers insights into how an organization will prepare for a disaster, how it will respond, and what steps it will take to be able to recover its operations. As such, preparing for the continuing and the recovery is important. The benefits of the disaster recovery plan include: • Minimizes any expected risk.
• Prevent a disaster event from occurring. • Provides security for data and information. • Provides a standard to test the disaster recovery plan. • Provides the ensuring of business continuity. • Lowers the cost of damage. • Helps organizations to watch the amount of loss and downtime and at the same time provides the best and fastest opportunity to recover from a disaster. • Lessens decision-making during a disaster.

III. N-BODY PROBLEM

A. Sequential All-Pairs Algorithm

Cloud-Based Disaster Recovery Strategies. The tradi- tional disaster recovery (DR) usually involves cut-over or switch-over systems. The organization has a separate recovery location and backup to maintain the informa- tion and technology. That means the organization has a primary data center, and a separate location that will be used in the event of a failure of the main site. You have traditional DR, and it can either be dedicated or shared. Dedicated means that the DR site is dedicated to one customer, and shared means that the DR site is shared amongst multiple customers [12]. The traditional model tends to be costly, complicated, and lengthy because it is dependent on the continuous updates of the technology, and it requires many forms of resources such as hard- ware, storage devices, bandwidth and labor. Therefore, the cloud-based DR could serve to reduce many of the costs associated with both RTO and RPO. Cloud-based systems are more efficient and provide many benefits.

In this section some of the strategies for back-up and disaster recovery strategies using cloud-based DR are presented.

B. Parallelization of All-Pairs Algorithm

The private cloud can be used for DR. The cloud is only available for individual organization and has privacy, control and security. The private cloud computing for disaster recovery is the restoration of data back to the IT infrastructure, data must be reloaded to return the sys- tems back to its previous circumstances. Furthermore, the private cloud can provide a backup of off-site system. A very commonly seen type of the private cloud computing is the virtual private cloud, the private cloud is another way of managing a backup. The private cloud can provide security for data storage in cloud [2,13]. The private cloud for DR is shown in Figure 1 below.

Public cloud for DR. Public cloud is based on the standard cloud computing model in which resources can be shared in an efficient way. Applications,storage and data run on the same public pool of resources and are available to the general public via the Internet. The public cloud is only good for specific public offerings, like e- commerce applications. The public wants to ensure their data is at least recoverable within a specific period. The public cloud is a great place to store your backup and disaster recovery information [2,13]. Figure 2 shows the public cloud for disaster recovery. 4.3. Hybrid cloud for DR. A hybrid cloud is just another option for disas- ter recovery. Hybrid clouds include at least one public and one private cloud environment [14]. Public cloud resources are combined with a private or virtually private cloud component to perform distinct functions within the same organization. Hybrid cloud configurations can come from different cloud providers for the private and public services, or entirely from one cloud provider as a hybrid offering. Hybrid clouds are flexible and offer many capabilities, including backup and disaster recovery [13,15]. Figure 3 shows the hybrid cloud for DR.

It seems imperative that continuity of business is guaranteed, whatever you do, irrespective of owning the primary systems or renting them from the cloud. The reliability, availability and scalability of cloud-based DR outshines the traditional model. The traditional model could be private, public, hybrid, or virtual cloud, but the benefits of cloud-based DR are undeniable [13,16].

•Cost savings: all resources are shared, and with the "pay-as-you-go" billing structure, the costs will effectively be a fraction of the touch or all off-line system, there is essentially no cost to maintain many backup tapes.

•Faster recovery: cloud-based DR can reduce RTO and RPO from days or weeks to hours or minutes. • Security: cloud service providers can offer greater security features over the conventional model. You can even choose from different security algorithms for more protection during disaster recovery. • Scalability: your ability to increase or decrease your storage capacity is met with less friction than the conventional model.

IV. CONCLUSIONS

The investigation focuses on strengthening the vital strategies that could prevent and respond to many di- verse disasters. It also has provided an example of some templates for disaster recovery and how model recovery informs planning and cloud-based DR. Some cloud-based DR plans are reported since they seem to potentially attain the reliability, scalability and availability in ways that are more efficient than the traditional model. In addition, a comparative analysis is made with traditional models and cloud-based models. Subsequently, it can be concluded to be shown that the cloud-based DR is a better and easier way than the traditional model. Finally, this work could provide a great value to future researchers who might like to study the cloud-based DR and planning.

APPENDIX

This appendix gives an overview of the various cloud- based disaster recovery strategies explored in this paper. Table 2 contains a summary of the options and their associated strengths and weaknesses.

ACKNOWLEDGMENT

We thank Dr. Geetha G for her constructive comments and suggestions to enhance the overall quality of the paper. We also thank Dr. Sonal Sharma for guiding us to review our draft regularly. Finally, we also appreciate the Department of Computer Science and Engineering, Jain (Deemed-To-Be) University for lending us Cloud GPU to test our code..

REFERENCES

[1]. E. Maiwald and W. Sieglein, Security Planning & Disaster Recovery, McGraw-Hill/Osborne, USA, 2002.

[2]. V. Spoorthy, M. Mamatha and B. S. Kumar, A survey on data storage and security in cloud comput- ing, The International Journal of Computer Science and Mobile Computing, vol.3, no.6, pp.306-313, 2014.

[3]. J. Yu and L. Yang, The cloud technology double live data center information system research and design based on disaster recovery platform, Procedia Engineering, vol.174, pp.1356-1370, 2017.

[4]. S. Suguna and A. Suhasini, Enriched multi objective optimization model based cloud disaster recov- ery, The Karbala International Journal of Modern Science, vol.1, no.2, pp.122-128, 2015.

[5]. M. Mohammadian, Artificial intelligence applications for risk anal- ysis, risk prediction and decision making in disaster recovery planning, in Artificial Intelligence Applications and Innovations, L. Iliadis et al. (eds.), Springer, 2012.

[6]. B. C. Martin, Disaster recovery plan strategies and processes, SANS Institute as Part of the Infor- mation Security Reading Room, pp.1- 12, 2002.

[7]. Z. Yonga, C. Jiea, L. Leia and L. Jina, The design of data disaster recovery of national fundamental geographic information system, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Suzhou, China, pp.353-356, 2014.

[8]. Creative Commons Attribution 3.0 License, How to Design a Disaster Recovery Plan,2017, https://cloud.google.com/solutions/designing-a-disaster-recovery- plan, accessed on Jan. 25, 2018.

[9]. W. J. Siembieda, Transactions and friction as concepts to guide disaster recovery policy, The International Journal of Disaster Risk Science, vol.3, no.1, pp.38-44, 2012.

[10]. J. Sembiring and M. Siregar, A decision model for IT risk man- agement on disaster recovery center in an enterprise architecture model, Proc. of the 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013), pp.1142-1146, 2013.

[11]. N. Roy, Four Approaches Backup Disaster Recovery Explained Us- ing Amazon Cloud, 2017, https://blog.blazeclan.com/4-approaches- backup-disaster-recovery-explained-amazon-cloud/, accessed on Jan. 25, 2018.

[12]. M. Khoshkholghi, A. Abdullah, R. Latip, S. Subramaniam and M. Othman, Disaster recovery in cloud computing: A survey, Computer and Information Science, vol.7, no.4, pp.39-54, 2014.

[13]. R. Rajan and S. Shanmugapriyaa, Evolution of cloud storage as cloud computing infrastructure service, The IOSR Journal of Com- puter Engineering, vol.1, no.1, pp.38-45, 2012.

[14]. A. Dubey, G. Shrivastava and S. Sahu, Security in hybrid cloud, The Global Journal of Computer Science and Technology Cloud and Distributed, vol.13, no.2, pp.1-7, 2013.

[15]. P. Gapat, S. Khillare, A. Khiste and R. Pise, A survey paper on removal of data duplication in a hybrid cloud, The International Re- search Journal of Engineering and Technology, vol.3, no.1, pp.1327- 1332, 2016.

[16]. S. Challagidad, S. Dalawai and N. Birje, Efficient and reliable data recovery technique in cloud computing, Internet of Things and Cloud Computing, vol.5, no.1, pp.13-18, 2017.

TABLE I
A SUMMARY OF SOME RESEARCHES ON DISASTER RECOVERY

Author	Year	Model	Usage	Results
Mohammadian [5]	2012	Fuzzy cognitive maps for risk prediction	Disaster recovery planning	• Provide facilities to represent com- plex relationship in implementing a disaster recovery plan. • DR plan can be regularly reviewed, improved and controlled.
Siembieda [9] recovery	2012	Multilocational using analogs from eco- nomic theory	Disaster recovery interactions over large geographical areas and over time	• Help CIO's and managers to analyze the risks. • Multilocational recovery can lower friction cost. • Also it can perform a better un- derstanding of recovery in different geographical spaces.
Yu and Yang [3] com-	2017	Double live cloud puting data center	Cloud-based disaster recovery based on virtual storage	• Solve the traditional data replication existing in two centers that cannot read and write at the same time. • Data availability is more and higher. • Protect data using transparent en- cryption mechanism. • Lower costs.

Suguna and Suhasini [4]	2015	Enriched multi objective optimization using en- riched genetic algorithm	Cloud-based disaster recoverv	• Efficient DR in a cloud environment. • This model can guarantee short re- covery time, low backup cost and high reliability.
Sembiring and Siregar [10]	2013	IT risk management on disaster recovery center	Decision support in case of risk	• The model will help an organization to decide which Tier of disaster re- covery center should be developed based on risk factors.