International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 10 Issue 08, August-2020,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

DISASTER RECOVERY METHODS IN CLOUD COMPUTING: A STUDY

Dr. Rajesh Kumar
Assistant Professor in Computer Science
Govt College for Girls Sec14 Gurugram
Mail Id Rajeshbeniwal78@Gmail.Com

Abstract

Cloud computing is one of the largest technology industries that has been adopted globally and has provided a wide range of useful services for its users. However, with the increasing popularity of cloud computing, the need for disaster recovery methods in cloud computing has become extremely significant. In this study, we will investigate some of the commonly used disaster recovery methods in cloud computing.

When it comes to IT disaster recovery, it's nearly impossible to avoid it. Because Cloud Service Providers (CSPs) have to and should provide services to their clients even if the knowledge Center is down, owing to a disaster, this problem becomes more critical and complex in cloud computing Research on disaster recovery using cloud computing has increased dramatically in the recent few years, and a substantial body of work has been published and discussed on the subject. In spite of this, cloud-based disaster recovery analysis has always lacked significant subjects and points. Disaster recovery principles and research in cloud computing systems are examined in this study to answer these questions. The most pressing issues and potential remedies.

Keywords: *Cloud Computing, Disaster Recovery, Replication, Backup, Survey.*

1. INTRODUCTION

As a result of its global resource sharing capabilities, cloud computing is mostly utilised on powerful workstations on a daily basis. Cloud computing advancements are influencing several industries, such as the 61% of UK enterprises that rely on particular cloud service types. In order to ensure company continuity and higher user satisfaction, various security concerns must be addressed, including risk management, trusted procedures, and restructuring. Disasters, both man-made and natural, can cause significant damage to valuable resources. It is possible to prevent CSPs and network failures by utilising two different methods of disaster recovery (DR): Personalized and cloud-based service options are available. As a sanctified structure or a shared system, the classical paradigm can be used. Customers can select the model that best suits their needs based on speed and cost. The costs and speeds associated with providing infrastructure exclusively to one customer are both substantial. In contrast, infrastructure is made available to a

large number of users in a circulated model. Recovery time and costs are both reduced with this approach. **Figure 1** illustrates the advantages of a dedicated and shared approach through cloud computing. With DR, you may get high-quality results at a low price.

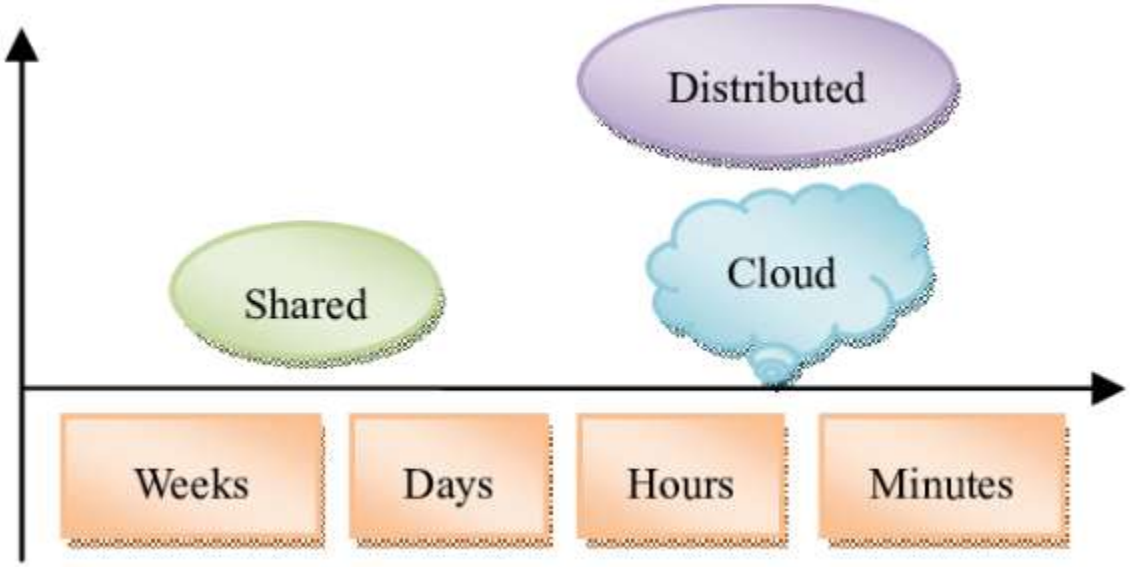

Figure 1: Link between customary and cloud DR models

Cloud service companies offer Disaster Recovery (DR) services to a wide range of businesses and organisations. Data security and uptime are both ensured for consumers that make use of these services. In this work, we explore the difficulties and potential solutions associated with deploying disaster recovery (DR) machines in the cloud. The primary goal of disaster recovery (DR) for businesses is to restore services that have been disrupted. As a return method, every return method strives to increase the RTO and RPO, the two key components of recovery. Business continuity can be accomplished by lowering the RTO and RPO. The RTO is the amount of time it takes for the service to be restored after a disaster, while the RPO is the quantity of data that is lost. Depending on the extent of backup, there are five steps to the failover process **(Alhazmi & Malaiya, 2013)**

"**S1:** Hardware setup

S2: OS boot time

S3: Time to process the application

S4: Data recovery time/process

S5: Time to change IP Therefore, RPO and RTO can be defined as:

$$RPO\ \mu\ \frac{1}{Fb}$$

When Fb is in the Backup folder"

$$To = fraction\ of\ RPO + \overset{ss}{\underset{j\min}{\mathring{a}}} Tj$$

2. DISASTER RECOVERY

In the course of the system's existence, a disaster occurs. Natural disasters software/hardware problems, and even human mistake can all lead to downtime for a system (human error or burglary). You may lose a lot of money or even put your life at risk. As a result, DR consumes between 2% and 4% of large corporations' IT budgets each year. Solid-based disaster recovery (DR) solutions are becoming increasingly popular because of their high level of disaster resistance, dependability, and availability. Small and medium-sized businesses (SMEs), which lack the financial and human resources of larger corporations, can greatly benefit from this technology. **Table 1** shows the three DR levels indicated by programme requirements: data level, system level, and application level.

DR Level	**Description**
Data Level	Security of Application Data
System Level	Reducing Recovering lime as short as possible
Application Level	Application Continuity

Table 1: DR levels

DR approaches to be effective, they must meet the following criteria:

- RPO and RTO should be reduced
- In general, it has little effect on the standard system's performance.
- It is recommended that the locations be separated by distance.
- There must be a restoration of this request
- Privacy and confidentiality must be protected.

3. DISASTER RECOVERY PLAN

For a cloud system, there are a variety of DR methods that can be used to create an effective recovery plan. They are a reflection of the system's character. Redundancy and backup solutions are the foundation of all of these approaches, according to the research. Instead of using replication, the backup approach relies on redundant sites that can be brought back online quickly in the event of an emergency **(Lwin & Thein, 2009)** Based on the degree of DR feature provided in **Table 2,** these options have varying levels of speed and security **(Guster & Lee, 2011)** In addition, there are three alternative reproduction technologies to choose from: VM and host replication, database replication, and storage replication are all included in this package...

Model	**Synchronize Time**	**Recovery Time**	**Backup Characteristics**	**Tolerance Support**
Hot	Seconds	Minutes	Physical Minoring	Very High
Modified Hot	Minutes	1 Hour	Virtual Minoring	High
Warm	Hours	1-24 Hours	Limited Physical Minoring	Moderate
Cold	Days	More then 24 Hours	Off site backup	Limited

Table 2: Cloud-based DR models

In order to reduce RTO, RPO, cost, and delay, Disaster Recovery (DR) can construct a recovery plan that considers system limits such as CPU, network requirements, and storage. As a result, the DR's reorganization can be viewed as an efficiency issue. Two phases are necessary for DR Strategies.:

Phase alignment: There should be no room for error when it comes to disaster recovery plans at this point.

Planning phase: Selecting a DR solution that reduces costs for each data bar's necessary QoS.

An outline of the DR planning process is provided by ENDEAVOR (Nayak et al., 2010) Figure 2 shows the three modules that make up the system:

Installation modules: Incorporates DR needs (such protection type, RTO, RPO, and usage delay) as well as discovery engine and database.

Planning modules: Requirements and Comparing Models, Downloading (DR strategy classification by attributes such as cost, risk, and latency, and Global optimization (choosing the optimal DR Plan) are all included in the product design process. **(Wang et al., 2016)**

Outputs: Application-specific data, such as target resources and devices, protocol setup, are included in the ENDEAVOR release.

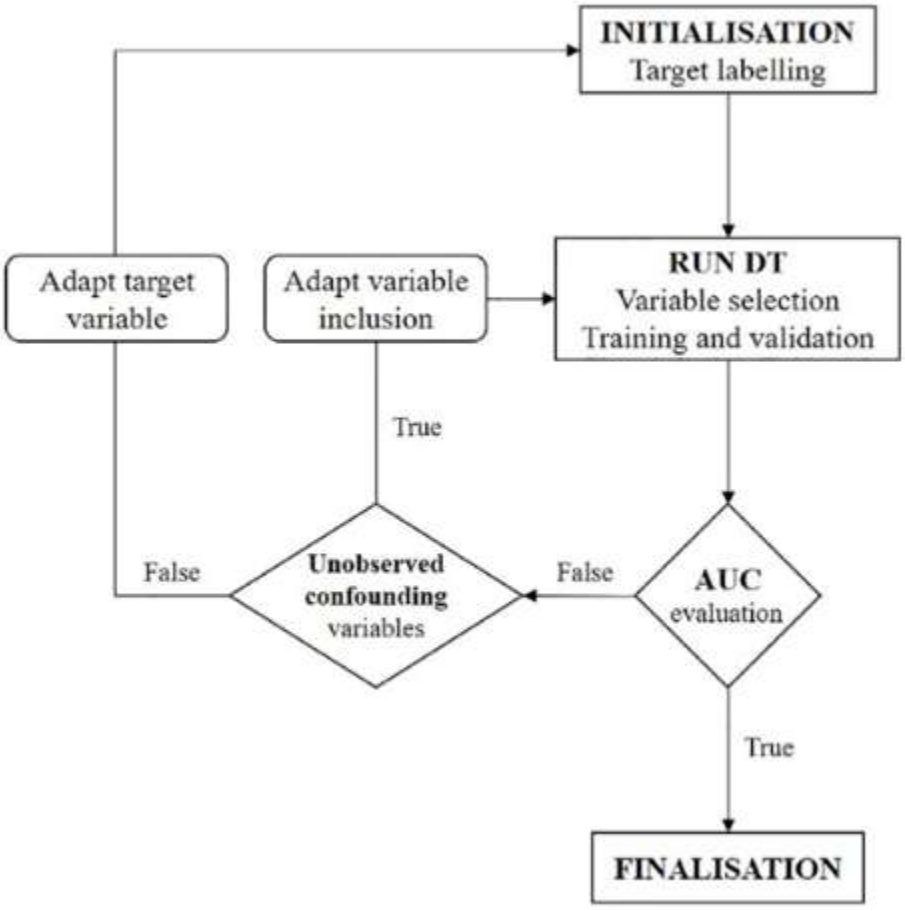

Figure 2: Endeavor flowchart (Vedashree et al., 2015)

4. CLOUD COMPUTING

Cloud computing is becoming more commonplace in everyday computing because of its ability to share resources from around the globe. In the event of a disaster, you may restore and back up important company files using cloud-based storage and recovery options. It is possible for the business to quickly resume or complete important duties following a disaster thanks to the adaptability of Disaster Recovery (DR). Restoring operations to pre-disaster levels is the goal of Disaster Recovery (DR). In order to ensure high availability, the data is stored in a safe and secure cloud environment. Using this service, businesses of any size can customise their disaster recovery plans to meet their unique needs.

5. CAUSES OF DATA LOSS

5.1Natural Disasters

The greatest uncontrollable factor is undoubtedly natural calamities. We can't control things like fires, floods, earthquakes, or even power outages. Fortunately, only one book of users reported data loss as a result of natural calamities, according to the poll.

5.2Mission-critical

When the application is left idle for a long period of time, it may be damaged, resulting in the loss of crucial information in some businesses.

5.3Network Failure

When the network goes down, as cloud-based systems and customers are both connected via the internet.IP-based telephony and telecommunications will be adversely affected if the network goes down.

5.4Network Intrusion

It's a disaster when virus-infested programmes penetrate a network. Using anti-virus software and putting programmes on a disaster watch list can help you avert a catastrophe.

5.5Hacking or Malicious Code

If you're familiar with the world of computer viruses, you know that they have the ability to limit your access and steal your MasterCard data. Your essential data might be damaged by computer viruses and other malware that spread like wildfire. As a result, it's imperative that you install and maintain a high-quality antivirus programme.

5.6System Failure

An organization's infrastructure failure can lead to the failure of all of the organization's systems, including operating systems.

5.7Human Errors

Most disasters are caused by human error, with 60% of information centres failing. Two types of human errors can lead to data loss: accidentally deleting or formatting something we don't intend to, and mistakenly dropping or breaking our equipment.

6. DISASTER RECOVERY TECHNIQUES

6.1Parity Cloud Service

Public usage of the basic data recovery service is not permitted due to a lack of privacy protection for the data of actual customers. It is illogical to expect customers to upload their sensitive data to an online backup server before they have confidence in the service provider's privacy protections. In order to protect user data, the Parity Cloud Service architecture has been designed (PCS). The following four aspects should be considered while creating apersonal data recovery service.**(Shahzadi et al., 2018)**

1. Consistency.
2. Economic efficiency.
3. Easiness
4. Privacy protection

It is easy to use, has low server costs, and is capable of restoring user data to a high enough degree to allay users' privacy worries. Conceptual PCS architecture is depicted in Figure 3.

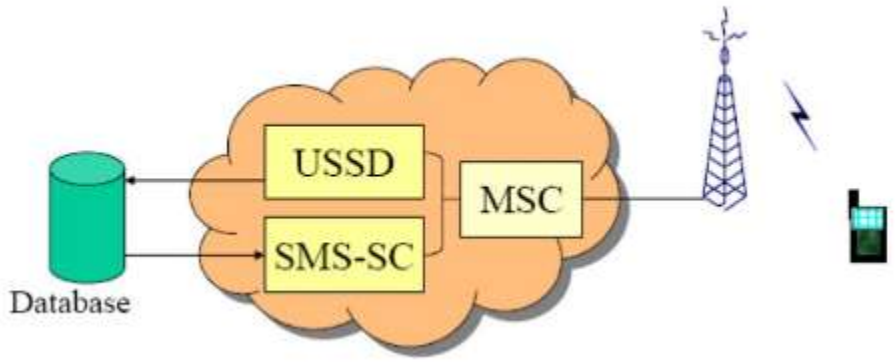

Figure 3: PCS architecture

6.2Seed Block Algorithm (SBA)

To provide safe data backup to the cloud and the distant server, does the suggested system's algorithm use the concept of a computer-based exclusive OR (XOR) process? In total, it consists of three primary sections.

1. Cloud Server Master
2. Cloud clients and
3. Remote Server

In the event of a cloud disaster, a unique XOR number provided to each new customer can be utilised to retrieve lost data by XORing data from the Seed database associated with that customer. This method offers the benefit of retrieving data files that are highly accurate and reliable. Figure 4 shows how clients can still access these files from a distant repository when data is not available in a central location due to the cloud and remote server both having to share a limited amount of storage space **(Al–shammari & Alwan, 2018)**.

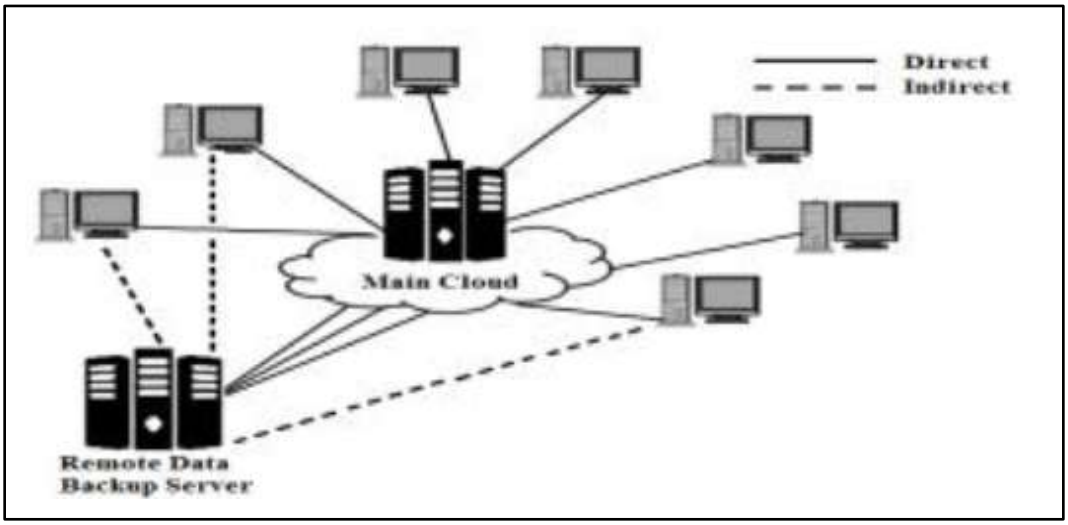

Figure 4: Seed Block Algorithm (SBA)

7. CONCLUSION

In this research, we have examined the current state of the art for disaster recovery (DR) in the cloud. When it comes to disaster recovery, cloud-based services are a better option than traditional methods. DR mechanisms too face major hurdles, and we've come up with strategies to help them overcome them. DR platforms, as well as outstanding challenges and future

directions in cloud-based DR procedures, are also covered. Finally, a DR technique that may be applied to any DR mechanism is proposed.

Reference

1. Al–shammari,M. M., & Alwan, A. A. (2018). Disaster recovery and business continuity for database services in multi-cloud. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 1–8.

2. Alhazmi, O. H., & Malaiya, Y. K. (2013). Evaluating disaster recovery plans using the cloud.*2013Proceedings Annual Reliability and Maintainability Symposium (Rams)*, 1–6.

3. Guster, D., & Lee, O. F. (2011). Enhancing the disaster recovery plan through virtualization. *Journal of Information Technology Research (JITR)*, *4*(4), 18–40.

4. Lwin, T. T., & Thein, T. (2009). High availability cluster system for local disaster recovery with Markov modeling approach. *ArXiv Preprint ArXiv:0912.1835*.

5. Nayak, T., Routray, R., Singh, A., Uttamchandani, S., & Verma, A. (2010). End-to-end disaster recovery planning: From art to science. *2010 IEEE Network Operations and Management Symposium-NOMS 2010*, 357–364.

6. Reid, J. G., Carroll, A., Veeraraghavan, N., Dahdouli, M., Sundquist, A., English, A., Bainbridge, M., White, S., Salerno, W., & Buhay, C. (2014). Launching genomics into the cloud: deployment of Mercury, a next generation sequence analysis pipeline. *BMC Bioinformatics*, *15*(1), 1–11.

7. Shahzadi, S., Ubakanma, G., Iqbal, M., & Dagiuklas, T. (2018). Autonomous, Seamless and Resilience Carrier Cloud Brokerage Solution for Business Contingencies during Disaster Recovery. *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science*

8. Vedashree, N., Kumar, P., & Anilkumar, G. (2015). Data Recovery in Cloud Environment Using Seed Block Algorithm. *(IJCSIT) International Journal of Computer Science and Information Technologies*.

9. Wang, L., Harper, R. E., Mahindru, R., & Ramasamy, H. V. (2016). Disaster Recovery for Cloud-Hosted Enterprise Applications. *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)*, 432–439.