ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

A Study on Cloud Computing Disaster Recovery

Mr.A.Srinivas, Y.Seetha Ramayya, B.Venkatesh

HOD and Associate Professor, Dept. Of CSE, Coastal Institute of Technology & Management, Vizianagaram, India

Students of Computer Science Engineering Coastal Institute of Technology & Management, Vizianagaram, India

Students of Computer Science Engineering Coastal Institute of Technology & Management, Vizianagaram, India

Abstract: As many business continuities, organizations use cloud for their work may experience disasters by nature or manmade results in loss of data. By using disaster recovery techniques like backup of data when disaster occurs. There are some difficulties like time complexity; cost effectiveness which makes user very difficult handle disasters. By using disaster recovery as a service one can handle these disasters and can recover data fast with low cost. As in other techniques DR as a Service doesn't need any initial payment to use it provides pay on use method.

Keywords: **Cloud Computing, Disaster recovery techniques, Traditional disaster recovery, Disaster recovery planning, Disaster recovery as a service.**

I. Introduction

To handle devices or licensed softwares in an organization having more employees and to provide those softwares to all employees for their work without any delay is slight difficult by using physical hardware. to overcome this problems cloud computing is developed. cloud computing is internet based computing process in which systems are interconnected with sharing resources by each other. internet is the medium acts between cloud and user. cloud has many servers of application, platform and infrastructure. client is connected to cloud server and can store data through internet and can access the data from anywhere. it is a real time communication network. we can run our programs from anywhere by accessing cloud. using cloud we can access any software or data without paying any money to cloud.

When a system crashes or power failure occurs there s a chance of loss of data and some times it may result it in financial loss. This system crashing and other problems occur due to natural **Disasters** or by human from causing expensive service disruptions. When a disaster occurs in business continuity the company may get huge loss of data and also financial loss. It is a phenomenon that can cause damage to life and property and destroy the economic, social and cultural life of people. When disaster occurs company need to protect the data from loss. Cloud providing companies like Google, Amazon, Microsoft etc., experienced cloud disaster with a huge loss of data and servers. When disaster occurs at client side backup will be stored in cloud but if disaster occurs in cloud data will be lost. Natural disasters may occur due to bad weather results in disaster

To overcome these disasters there are some disaster recovery techniques which are used to recover data. Backing up the data is the old technique which is used for disaster recovery. There are many companies which developed **Disaster recovery techniques** as required to their business continuity. Dedicated and shared models are the two approaches for disaster recovery based on cost and speed. Storing the data from cloud infrastructure inorder to recover when disaster occur. Every organization should have a documented disaster recovery process and should test that process at least twice each year.

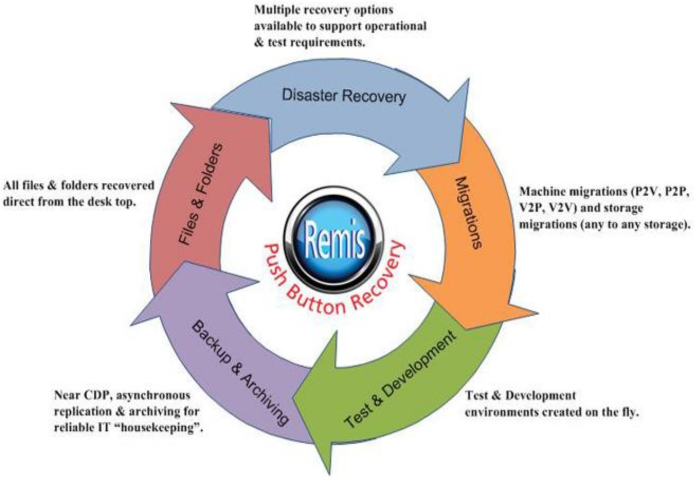
Multiple recovery options available to support operational & test requirements.
Disaster Recovery
Machine migrations (P2V, P2P, V2P, V2V) and storage migrations (any to any storage).
Migrations
Test & Development
Test & Development environments created on the fly.
Backup & Archiving
Near CDP, asynchronous replication & archiving for reliable IT "housekeeping".
Files & Folders
All files & folders recovered direct from the desk top.
Remis
Push Button Recovery

Fig-1 Disaster recovery process

II. **Causes of Data Loss**

There are 6 causes of data loss due to disaster occurrence

Natural Disasters: when natural disasters occur then 2% of the data will be lost. The main reasons of occurrence natural disasters are mundane and nefarious. Due to mundane and nefarious effects one cannot recognize the data loss when disaster occurs.
Mission critical application failure: when an application is left unusable for few days then it causes a catastrophic failure and in some organizations it may be mission critical. By using all applications that are stored in cloud may reduce the catastrophic failures.
Network failure: cloud and clients are connected by internet and when network fails the systems which are connected to cloud are crashed and data will be lost and applications which are working based on cloud will also suffer. As network failures IP based phones and telecommunications will also suffer.
Network intrusion: when a virus is invaded onto the applications then there is a chance of occurrence of disaster. By placing unusable applications in that place on a watch list we can prevent occurrence of disaster.
Hacking or malicious code: disaster occurs in inside or outside of the organization although they prevent hacking or malicious code from modifying data there is a loss of data. In US annually they spend $10 billion to recover this type of data loss.
System failure: if infrastructure in a organization fails then whole systems which are connected in that organization will crash. This will affect the operating systems.
The main reason for occurrence of disaster is human, 60% of the data centers are failed. According to US survey cloud in small businesses fails to reopen their business after catastrophic affect.

Problematic event	Affected business process	Impact Classification & Effect on finances, legal liability, human life, reputation
Fire	Class rooms, business departments	Crisis, at times Major,Human life
Hacking attack	Registration advising	Major, legal liability
Network unavailable	Registration advising class, education	crisis
Social engineering	Registration	Major, legal liability
Server failure	Registration advising class, education	Major at times crisis

III. **Traditional Disaster Recovery**

Traditional disaster recovery was developed by share group which are divided into 6 tiers.

Tier 0: no offsite data that means there is no disaster recovery plan and no saved data. To recover data it may take weeks and it is unsuccessful.

Tier 1: data backup without hotsite that means data is taken backup by offsite not by hotsite. To retrieve the data that is taken backup is time taken process. By not having their own redundant servers it is time taking process to locate and configure appropriate systems.

Tier 2: data backup with hotsite that means organizations maintain data backup as well as hotsite it is the fastest process. By having a hot backup site when disaster occurs we can run applications at stand by servers.

Tier 3: instead of taking backup by physical media it provides an **electronic vault** so that backup data is network accessible to hot site. As hotsite backup is cost effective it is better to access it by network.

Tier 4: point in time copies means that organization maintains more timely point in time backup of crucial data is network accessible to host site.

Tier 5: transaction integrity means that transactions are consistent between production systems and recovery sites. So, there should be no loss of data.

Traditional disaster recovery offers better RPO's and RTO's. Traditional geographic redundancy is an alternative technique that has data centers having sufficient equipment to store data when backup is made. To assure rapid recovery time objective it is necessary to deploy same type or hardware or software to geo-redundant sites. Virtualization simplifies traditional disaster recovery by relaxing compatibilities requirements by deploying hardware on recovery site. Hardware configuration on recovery site should be equal to primary site to carry the entire traffic load served by impacted site acceptable service quality, reliability and latency.

If applications are booted from scratch for disaster recovery then RTO onto virtual machines should be comparable with the RTO on traditional cold standby configurations

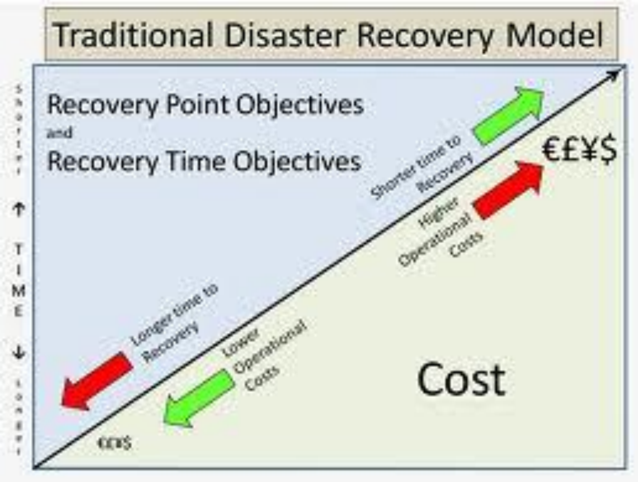

Fig-2 Traditional disaster recovery

IV. Disaster recovery requirements

This explains key features for effective cloud service when disaster occurs.

Recovery point objective: maximum time period taken for data loss when an disaster occurs is calculated RPO. The necessary RPO is generally a business decision—for some applications absolutely no data can be lost (RPO=0), requiring continuous synchronous replication to be used, while for other applications, the acceptable data loss could range from a few seconds to hours or even days. The recovery point objective identifies how much data you are willing to lose in the event of a disaster.
Your RPO is typically governed by the way in which you save and back up data:

- Weekly off-site backups will survive the loss of your data center with a week of data loss. Daily off-site backups are even better.
- Daily on-site backups will survive the loss of your production environment with a day of data loss plus replicating transactions during the recovery period after the loss of the system. Hourly on-site backups are even better.
- A NAS/SAN will survive the loss of any individual server, except for instances of data corruption with no data loss.
- A clustered database will survive the loss of any individual data storage device or database node with no data loss.
- A clustered database across multiple data centers will survive the loss of any individual data center with no data loss.

Recovery time objective: it is a measurement of time upto which it can withstand and bring back to the system when a disaster occurs. It may be minutes, hours, and days. It may also include detection of failure and preparing required servers at backup site to initialize an application which is interrupted in middle of execution. The recovery time objective identifies how much downtime is acceptable in the event of a disaster.

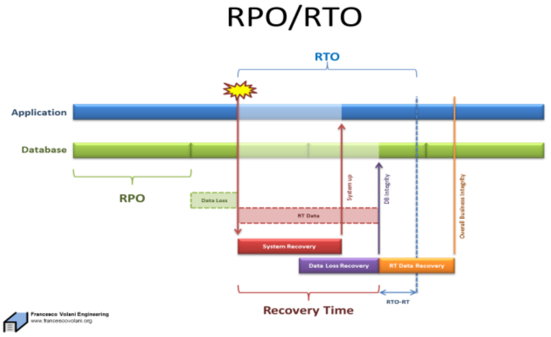

Fig-3 Disaster recovery requirements

Performance: to make DR service useful performance is to be protected under failure free operation by using synchronous replication of application to the backup site and complete the performance of application to make it ready to use.

Consistency: the application which is taken backup when disaster occurred should be replicated on same site after clearance of disaster at the consistent state. DR mechanism is useful to take backup when disaster occurs.

V. DISASTER RECOVERY PLANNING

Disaster recovery planning are of as:

Kind of data	**Description**
Fixed data	Fixed data, such as your operating system and common utilities, belong in your AMI. In the cloud, you don't back up your AMI, because it has no value beyond the cloud
Transient data	File caches and other data that can be lost completely without impacting the integrity of the system. Because your application state is not dependent on this data, don't back it up.
Configuration data	Run time configuration data necessary to make the system operate properly in a specific context. This data should be backed up semi-regularly
Persistent data	Your application state, including critical customer data such as purchase orders. It changes constantly and a database engine is the best tool for managing it.

Table-2 types of data backup

Geographic redundancy:

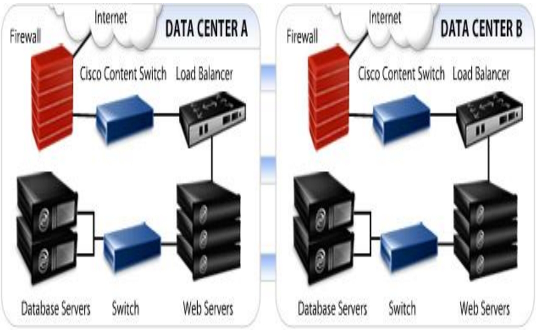

Fig-3 Geographic redundancy

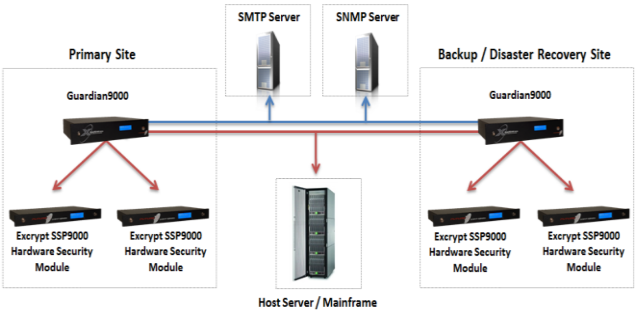
SMTP Server
SNMP Server
Primary Site
Backup / Disaster Recovery Site
Guardian9000
Guardian9000
Excrypt SSP9000 Hardware Security Module
Excrypt SSP9000 Hardware Security Module
Excrypt SSP9000 Hardware Security Module
Excrypt SSP9000 Hardware Security Module
Host Server / Mainframe

FIG-4 ORGANIZATIONAL REDUNDANCY

There are some mechanisms that are implemented for data backup when disaster recovery technique is used. So that when we want to take backup of a data we can follow some mechanisms.

Backup sites can come from three different sources:

- Companies specializing in providing disaster recovery services.
- Other locations owned and operated by your organization.
- A mutual agreement with another organization to share data center facilities in the event of a disaster.

Hot Backup Site: It is very expensive to operate. This site works with organizations that operate real time processes. It is the duplicate of the original site. Loss in data is very minimal as we can relocate the data and continue our work what we are performing. It will save as a virtual image of our current data. In a few hours hot backup site can bring up to full production. It is priory used in the situations where disaster happening.

Cool backup site: It is the least expensive to operate. It doesn’t take any backup of data copies or it doesn’t include hardware. Lack of hardware can startup with a minimal cost but require more time. Everything required to restore service to users must be procured and delivered to the site before recovery operation is performed.

Warm backup site: It is already stocked with a hardware configuration on the backup site that found in primary site. To apply warm backup site the last data backup should be delivered to their primary sites.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

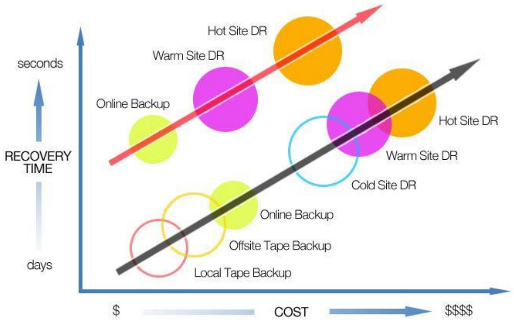

Fig-5 TYPES of backup sites

VI. Disaster Recovery as a service

Disaster recovery as a service is an upcoming service as a nomenclature of cloud computing. It is a low cost service when compared to traditional disaster recovery. It is flexible in replicating physically or virtually. It provides application consistent recovery for some working applications like SQL server. It has pre-built options for virtual recovery environments including security, network connectivity and server failover when continuously replication among servers. When disaster occurs we can take backup and we can run our applications on service provided by disaster recovery until we get backup to primary site. Disaster recovery as a service to replicate critical servers and data centre infrastructure in cloud.

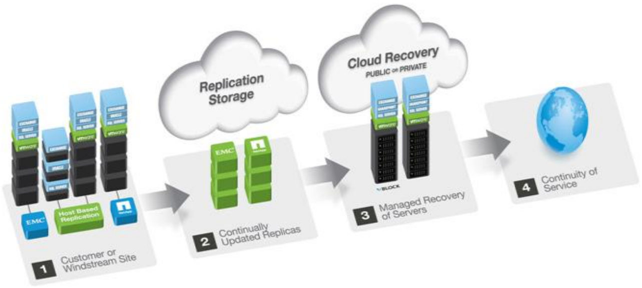

Fig-6 Disaster recovery as a service

Disaster recoveries as a service is free or pay on use offer. When incompatibilities are occurred due to software changes then breaking of DRaaS in cloud may occur.

The architecture of DRaaS is defined by three models.

From Cloud: when the primary application or data is in cloud and backup or recovery site is in private data centre.
In cloud: when both primary site and recovery site are in cloud.
To cloud: when the application is in primary data centre and backup or recovery site is in cloud.

To test the recovery processes sandboxes are used and they test without disrupting running application. It is only accessible to only system administrator.

Solutions are pre-packaged services that provide a standard DR Failover to a cloud environment that you can buy on a pay-per-use basis with varying rates based upon your recovery point objective (RPO) and recovery time objective (RTO).

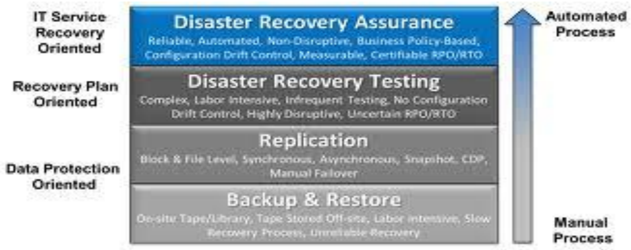
IT Service Recovery Oriented
Recovery Plan Oriented
Data Protection Oriented
Disaster Recovery Assurance
Reliable, Automated, Non-Disruptive, Business Policy-Based, Configuration Drift Control, Measurable, Certifiable RPO/RTO
Disaster Recovery Testing
Complex, Labor Intensive, Infrequent Testing, No Configuration Drift Control, Highly Disruptive, Uncertain RPO/RTO
Replication
Block & File Level, Synchronous, Asynchronous, Snapshot, CDP, Manual Failover
Backup & Restore
On-site Tape/Library, Tape Stored Off-site, Labor Intensive, Slow Recovery Process, Unreliable Recovery
Automated Process
Manual Process

Fig-7 Solutions for disaster

Differences between DRaaS and Traditional DR:

Traditional Disaster Recovery	Disaster recovery as a service
A secondary physical DR site means investment in additional data centre space, connectivity and servers. It also leads to additional operational costs-power and cooling, site maintenance and manpower requirements	A cloud based disaster recovery service provides virtual machine snapshots of physical or virtual servers at the primary data centre. The organization pays for storing the snapshots, application data in a suspended state, and replication of data from primary to secondary site for data synchronization. It pays for the infrastructure as a service feature only in case of a disaster, wherein virtual machines need to be brought online as a substitute for the primary site.
A physical dr site operates only during the actual disaster. the time taken to make a dr site live be more than a cloud dr resulting in huge data loss	With cloud disaster recovery services the DR site can be brought online within minutes. A cloud DR site that boosts up within a few seconds translates to data loss of just that timeframe
In case connectivity is unavailable then manual connection is needed to start the sites operations	A cloud based disaster recovery is triggered from anywhere using internet

Table-3 Differences between traditional DR and DRaas

VII. CONCLUSION

As cloud computing is becoming very important in day to day life and every company is based on cloud computing. They are not aware of disasters in cloud; they don't know any recovery mechanisms at first. When disaster occurred then all companies faced big loss of data and also financial then after many recovery mechanisms are introduced. As cloud nomenclature has a PaaS, IaaS, and SaaS as services which provide their service to cloud users in terms of infrastructure, software and platform as their requirement; so user can use cloud without any difficulty. By implementing DRaaS in cloud one can get recovered from data loss when he experiences a system failure or by natural disasters. So by implementing DRaaS in business continuity they can overcome their data loss.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cloud_computing
[2] http://www.webopedia.com/TERM/C/cloud_computing.html
[3] http://www.cs.uwp.edu/staff/lincke/infosec/notes/BC-DR.ppt
[4] http://blog.ussignalcom.com/blog-1/bid/257525/6-Causes-of-Data-Loss-Prepare-your-Disaster-Recovery#_ftn2
[5] http://books.google.co.in/books?id=q0FaSaNEYK0C&pg=PA179&dq=cloud+disaster+recovery&hl=en&sa=X&ei=wPXUYCPJIWIrAfSzICABA&ved=0CEIQ6AEwAg#v=onepage&q=cloud%20disaster%20recovery&f=false
[6] http://www.pushbuttonrecovery.com/App_Themes/pbr/images/diagram_home_V1.jpg
[7] http://t1.gstatic.com/images?q=tbn:ANd9GcQnWtey5vjlaDofAVj1aeSiivZ1WlH1bWcZnI_nYMEqhnE6q7p2
[8] http://www.francescovolani.org/techlog/wp-content/uploads/2012 /04/RPORTO_Schema.png
[9] http://en.wikipedia.org/wiki/Backup_site

[10] https://access.redhat.com/site/documentation/enUS/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_
Administration/s2-disaster-recovery-sites.html
[11] http://www.liquidweb.com/img/disaster-recovery.jpg
[12] http://www.futurex.com/images/blog/disasterrecovery-plan.png
[13] Cloud Application Architectures building applications and infrastructure in the cloud by O'RELLY and George Reese.
[14] http://www.windstreambusiness.com/data-center-solutions/disaster-recovery/disaster-recovery-as-a-service
[15] http://www.windstreambusiness.com/media/299685/draas-large.jpg
[16] http://t1.gstatic.com/images?q=tbn:ANd9GcS_LS3KtFVsC00YwagC2OmBV9GiX0EoZTjJJZXy38rzMLZk88HqqA
[17] http://en.wikipedia.org/wiki/Recovery_as_a_Service
[18] http://www.datacenterknowledge.com/wp- content/uploads/2011/10/netmagic-graphic1.jpg
[19] http://www.datacenterknowledge.com/wp- content/uploads/2011/10/netmagic-graphic3.jpg
[20] https://www.usenix.org/legacy/event/hotcloud10/tech/full_papers/Wood.pdf

BIOGRAPHY

Srinivas Adapa S/O A Siva Rao was born in Visakhapatnam (Dist) Andhra Pradesh, India. He did his graduation, Post Graduation in Engineering with consistently good academic record. He did his post graduation degree from Charles Sturt University, Australia and having 12 years experience which includes more than 8 years of IT industry experience in India & Abroad. He is pursuing PhD in New World Mission Dunamis International University, South Africa.

Seetha Ramayya Y S/O Y V L N Sastry was born in Nidadavole (dist) Andhra Pradesh India. He is pursuing b-tech final year in coastal institute of technology and management, Vizianagaram India.

Venkatesh B S/O B Lakshman Rao born in Rajamundry (dist) Andhra Pradesh India. He is pursuing b-tech final year in coastal institute of technology and management, Vizianagaram India.