International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

Cloud Computing in Data Backup and Data Recovery

Monisha. S[1], Dr. S. Venkateshkumar[2]
[1]IIIMCA, [2]Head
Department of Computer Applications, Dr. Sns Rajalakshmi College of Arts & Science,
Coimbatore, Tamilnadu, India

ABSTRACT

Data backup and Disaster Recovery/Business Continuity issues are appropriate essential in networks since the importance and shared value of digital data is continuously rising. Every organization requires business continuity plan or disaster recovery plan and data backup which reduce within the cost constraints while achieving the target recovery requirements in terms of recovery time objective and recovery point objective. The aim of this paper is to overview of various techniques in data backup and disaster recovery in the cloud environment.

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

INTRODUCTION

Cloud computing becomes more popular in large-scale computing day by day suitable to its capability to share worldwide distributed resources. Users can access to cloud-based services throughout Internet around the world. Backup and recovery refers to the method of backing up data in case of a loss and setting up systems that allocate to data recovery due to data loss. Backing up data requires replication and archiving computer data, so that it is easy to get to in case of data deletion or corruption. Data from a previously time may only be recovered if it has been backed up. Data backup is a form of disaster recovery and should be part of any disaster recovery arrangement.

DISASTER RECOVERY:

A disaster is an unpredicted event in a system lifetime. It can be made by environment (like the tsunami and earthquake), hardware/software failures. Cloud-based DR solution is an increasing tendency because of its ability to accept disasters and to achieve the consistency and availability.

DISASTER RECOVERY CHALLENGES:

1. **Dependency :**
   Data backup is on position of service providers as well. This problem makes dependency on CSPs for customers (such as organizations) and also loss of data because of disaster.
2. **Cost:**
   Initializing cost amortized once a year cost. Ongoing cost: storage cost, data transfer cost and giving out cost .Cost of potential disaster: Cost of improved disasters and also cost of unrecoverable disaster
3. **Failure Detection :**
   Failure detection time powerfully affects on the organization downtime, so it is critical to detect and information a failure as soon as potential for a fast and correct DR.
4. **Security:**
   DR can be produced by nature or can be human-made. Cyber-terrorism attack is one of human-made disasters which can be expert for many reasons. In this case, security and recovery of important data will be a main purpose in DR plans beside of system restoration.

DISASTER RECOVERY SOLUTION:

Local Backup:

Local storage can be updated through a protected channel. By this technique, migration between cloud service providers and also relocation between public to private, and private to public is possible. In the experience of a disaster, local backup can supply the services that were served by the service provider.

Inter-Private Cloud Storage (IPCS):

Users data should be stored in three different environmental locations: Servers, Local backup server (LBS) and remote backup server (RBS).

CLOUD SERVER CENTRAL REPOSITORY:

In some respects cloud servers work in the same way as physical servers but the functions they give can be very different. There are two main options for hosting.

- Shared hosting
- Dedicated hosting

- **Shared hosting :**
  Shared hosting is the cheaper selection whereby servers are shared between the hosting provider's clients. One client's website will be hosted on the same server as websites belong to other clients.
- **Dedicated hosting :**
  Dedicated hosting is a much more difficult form of hosting, whereby clients obtain whole physical servers.

BACKUP REPOSITORY:

The main cloud is termed as the central depository and remote backup cloud is termed as Backup repository. And if the central repository misplaced its data under any situation either of any natural disaster (for ex -earthquake, flood, fire etc.) or by human attack or deletion that has been done incorrectly and then it uses the in sequence from the remote repository.

The Remote backup services should cover the subsequent issues:

- Privacy and ownership.
- Relocation of servers to the cloud.
- Data security.
- Reliability.
- Cost effectiveness.

Privacy and ownership:

Different clients access the cloud with their similar login or after any verification process. They are liberally allowed to upload their private and necessary data on the cloud.

Relocation of server:

For data recovery there must be transfer of server to the cloud. The Relocation of server means to remove main server's data to another server however the new of location is unidentified to the client.

Data security:

The client's data is stored at central repository with complete security.

Reliability:

The remote cloud must have the reliability characteristics. Because in cloud computing the main cloud stores the complete data and each client is independent on the main cloud for each and every small amount of data; therefore the cloud and remote backup cloud must participate a reliable role.

Cost effectiveness:

The cost for execution of remote server and its recovery & back-up technique also play an important role while creating the structure for main cloud and its reporter remote cloud.

CLOUD SERVICE MODELS:

Software as a Service (SaaS):

SaaS is a group of application and software; it allows the clients to give to the software instead of purchase it. Software application is available as service to the customer based on their demand. Twitter, Face book, whatsapp provide Software as a service.

Platform as a Service (PaaS):

This model provide platform as a service. This provides clients to develop his own application using the tools and program languages. This service is hosted in cloud and right of entry by clients using internet. Google App engine, Amazon provides the platform as service.

Infrastructure as a Service (IaaS):

This model provides the common resource services. It provides the computing communications like storage, virtual machine, network connection, bandwidth, IP address. IaaS is complete package for computing.

CLOUD DEPLOYMENT MODELS:

- **Public Cloud:** A public cloud is available to any client with an internet ability, is less secure than the private cloud because it can be access by general public.
- **Private Cloud:** Private cloud is available to a specific organization so that the user who belong to that organization can have access the data. It is more secure than the public
- **Hybrid Cloud:** The hybrid cloud is basically combination of no less than two clouds such as combination of private, community or public cloud.

- **Community Cloud:** Community cloud allows the property and system to be accessible by quantity of associated organization.

CLOUD STORAGE:

Cloud Storage is a PaaS, and requirements careful planning and a thorough implementation. This requires using an included adoption of multiple vendors' solutions. Cloud Storage is an area to experience fast growth in user requirements and disk space use. Therefore, it must be easy to use, and able to manage with an increasing demand.

There are three data services are

- Backup Automation
- Data recovery
- Data migration

- **BACKUP AUTOMATION :**
  Cloud Storage uses a number of enterprise solutions such as Iomega/EMC, Lacie, Western Digital and HP to distribute a fast and consistent automation services. The experiment performs backup automation between 1,000 and 10,000 files, which are available in the accessible system for user support.
- **DATA RECOVERY** :
  Data recovery is an significant service to recover lost data due to accidents or emergency services. In the previous experience, it took two weeks to recover 5 TB of data for disaster recovery as it requires different skill and systems to retrieve data and restore good quality data back to Cloud services. Data archived as Virtual Machines or Virtual Storage speed up recovery process.
- **DATA MIGRATION :**
  Data migration is common amongst Clouds and is also applicable to data exhaustive research. When there are more organizations going for private cloud deployment, data migration between Clouds is common and may authority the way service delivery. But there is no analysis the impact of moving single large documents between private clouds.

CONCLUSION:

In Cloud Computing has been the need for condition of security features of data, especially now that data is getting stored and shared on the cloud. Therefore backup and recovery services have become a complete requirement when it comes to management of data. It is most capable way to approach data organization, certainly preferable to spending valuable time and resources to try and recover data manually. Positive backup and recovery services are provide at a small yearly cost.

REFERENCES:

1. Vic (J. R) Winkler. Securing the cloud - cloud Computer Security Techniques and Tactics. Elsevier Inc, 2011.
2. Abdul Nasir Khan, M. L. Mat Kiah, Sammie U. Khan, Sajjad A. Madani. Towards secure mobile cloud computing: A survey. Future Generation Computer Systems (2012), doi:10.1016/j.future.2012.08.003.
3. J. Sinduja, S. Prathiba. Modified Security Frame Work for PIR cloud Computing Environment. International Journal of Computer Science and Mobile Computing-2013.
4. Clara Leonard. PRISM: la NSA argumente, le Guardian fait de nouvelles revelations. Fromhttp://www.zdnet.fr/actualites/prism-lansaargumente-le-guardian-fait-de-nouvellesrevelations-39791924.htm. ZDNet, Jun 28, .2013. consulted Nov 20, 2013.
5. Glenn Greenwald, Ewen MacAskill, Laura Poitras. Edward Snowden: the whistleblower behind the NSA surveillance revelations.

   http://www.theguardian.com/world/2013/jun/09/edwardsnowdennsa-whistleblowersurveillance. The Guardian, jun 10, 2013.
6. Almokhtar Ait El Mrabti, Anas Abou El Kalam, Abdellah Ait Ouahman. Data Security In The Multi-Cloud. The International Conference On Networked Systems May 2-4, 2013, Marrakech, Morocco. The First International Workshop on Security Policies in cloud Environment (PoliCE2013)
7. Keiko Hashizume, David G Rosado, Eduardo Fernndez-Medina, Eduardo B Fernandez. An analysis of security issues for cloud computing. Hashizume et al. Journal of Internet Services and Applications. SpringerOpen Journal. 2013, 4:5
8. A. B. Chougule, G. A. Patil. Implementation and Analysis of EFRS Technique for Intrusion Tolerance in Distributed Systems. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.