*International Journal For Technological Research In Engineering*
*Volume 9, Issue 10, June-2022* *ISSN (Online): 2347 - 4718*

# DATA BACKUP AND RECOVERY

1Ketan Singh, 2Mrs. Gurpreet Kaur
[1]Student, [2]Assistant Professor
Department of Computer Science Engineering
Bhagwan Mahaveer College of Engineering and Management, Sonipat, India

***Abstract: In an increasingly digital business environment, backing up data is essential for an organization for working. You can be hacked or ransomed, and lose your data to people who can sell your trade secrets or misuse them. An unsafe computer program can ruin your hard-working information. Employee with bad intention or other internal threats can take away your valuable digital assets. Can you recover from data loss?***
***Backup is a practice that combines strategies and solutions to make a backup effective and inexpensive. Your data is copied to one or more locations, with pre-determined frequencies, and with varying intensity. You can set up a flexible backup job, use your architecture, or use available backup solutions as a (BaaS) backup, and mix them with local storage. In this article we explain different aspects of Data Backup in organizations***


## 1. INTRODUCTION

What is Data Backup?
A backup copy of the data is the practice of copying data from first to second location, for protection in the event of a disaster, accident or malicious action. Data is the backbone of modern organizations, and data loss can cause great damage and disrupt business operations. That's why backing up your data is important for all businesses, large and small.
What does backup data mean?
Normally data backup means all the necessary data for the activities that run on your server. This may include documents, media files, configuration files, machine images, operating systems, and registry files. In fact, any data you want to keep can be saved as backup data.

The data backup includes a few key concepts:
Backup solutions and tools— while it is possible to make a backup copy of data manually, to ensure that systems are always supported and consistently, many organizations use a technical solution to make a backup copy of their data.
Backup administrator— every organization should appoint an employee who is responsible for keeping backups. The employee should ensure that the backup systems are properly configured, periodically inspected and ensure that important data is truly supported.
Backup scope and schedule— the organization should decide on the backup policy, specify which files and systems are important enough to make a backup copy, and how often the data should be stored.
Recovery Point Objective (RPO) — RPO is the amount of data an organization intends to lose in the event of a disaster, and is determined by the frequency of the repository. If the systems are backed up once a day, the RPO is 24 hours. When the RPO is low, more data storage, computer and network resources are needed to achieve common backups.
Recovery Time Objective (RTO) — RTO is the time it takes for an organization to restore data or systems to backup and restart normal operations. With large amounts of data and / or backups stored outside buildings, copying data and restoring programs can take time, and robust solutions are needed to ensure a low RTO [1].

## 2. The Importance of a Disaster Recovery Plan: Alarming Statistics

To understand the potential impact of disasters on businesses, and the importance of having a data backup strategy as part of a comprehensive disaster recovery plan, consider the following statistics: (i) Cost of Downtime — according to Gartner, average median business expenses are $ 5,600 per minute. [2]

(ii) Survival rate - another Gartner study found that only 6% of companies affected by a disaster that did not have a disaster recovery in the area survived and continued to operate for more than two years after the disaster.

(iii) Causes of data loss — the most common causes of data loss are hardware / system failures (31%), human error (29%) and viruses, and malware of ransomware (29%).

## 3. Types of Data Backup.

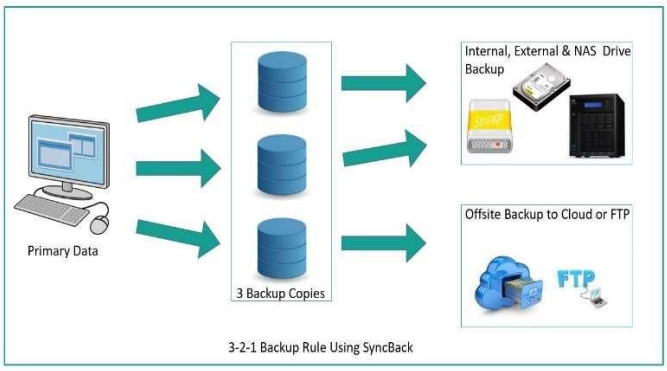
There are Various ways to backup or store data. Selection of right method in creating data backup plan plays important role. Mentioned below are some common techniques or technologies used:
• Removable Media: This is the basic and cheapest backup option where data is stored on media such as DVDs,

CDs, USB Flash Drives. This is practical for only small volumes of data, maintaining log of data in these small media can be difficult.

- Backup Servers: In this backup type, Data is stored in large capacity servers with high grade hard drives. These are deployed in your network and archive software are used to save files on servers. Different formats of storage are selected depending upon the nature of files and importance of files. This ensure that data is safe even when few drives get failed.
- Redundancy: You can set up an additional hard drive that is an image of a critical system drive at a specific point of time, or the whole system is no longer working. For example, another email server in standby, supports your main email server. Redundancy is a powerful but complex process to manage. It requires duplication between integrated systems, and is only useful against certain system failures unless the systems are no longer working remotely. [3]
- Cloud Backup Services: Many Cloud Storage Services provide user's a platform to store their data on company's server. This removes all the hassle of building and maintain their own servers to backup data. Cloud Backup Services get extremely costly as the size of data to be backed up increases.

4. "3-2-1" Backup Strategy




The 3-2-1 archive backup strategy is a way to ensure that your data is duplicated and reliably recoverable. In this strategy, three copies of your data are created from at least two different media sources and at least one copy is stored remotely:

- Three copies of data — three copies of your original data and two duplicates. This ensures that the lost backup or corrupt media does not affect recovery.
- Two different types of storage — reduce the risk of location-related failure by using two different technologies. Common options include internal and external hard drives, removable media, or cloud storage.

- One copy off-site — removes risk associated with single point failure. Out-of-place duplicates are required for solid disaster and data recovery techniques and may allow for failover during site shutdown.

5. CONCLUSION

In today's digital world, data seems like new gold. The Internet is full of articles that explain the value of data, how much can be achieved by analyzing data, and how data driven by data can be a great aid to business growth. However, when data turns out to be an important asset, sought after by many, it also draws the attention of terrifying characters. Data, after all, is a threat that people can steal from the digital ecosystem. To ensure data protection across all distributed and complex systems, storage and retrieval strategies must be developed. Meanwhile, IoT deployments continue to grow, but not many businesses and end users are taking the necessary steps to protect data in these environments. This could create problems in the future, as smart homes, offices, and city connections increase, and the data becomes more and more transparent in more efficient ecosystems.

ACKNOWLEDGMENT

I wish to express my gratitude to all those who provided help and cooperation in various ways at the different stages for this research. Also, I would like to express my sincere appreciation to the director sir of Bhagwan Mahaveer College of Engineering and Management, Head of Computer Science Engineering Department.

REFERENCES

[1] https://cloudian.com/guides/data-backup
[2] https://www.evolveip.net/blog/4-benefits-disaster-recovery-planning
[3] https://www.lightedge.com/blog/backups-and-redundancy-why-your-business-needs-both
https://www.computer.org/tech-news/trends/the-future-of- data-backup
https://cloudian.com/guides/data-backup
https://en.wikipedia.org/wiki/Backup