International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4| ISSN : 2456-3307

# Data Backup and Recovery Techniques in Cloud Computing

**K.Laxmi[1], K.Deepika[2], N.Pranay[2], V.Supriya[2]**
[1]Assistant Professor, Department of Information Technology in TeegalaKrisha Reddy Engineering College, Telangana, India
[2]UG Scholar, Department of Information Technology in TeegalaKrisha Reddy Engineering college, Telangana, India

## ABSTRACT

In earlier days, large amount of data is generated in electronic format, to maintain this data there is need of data recovery services. To provide these services in this paper we introduce seed block algorithm which we used for remote smart data backup. There are two objective of this algorithm. The first one is gather information from any remote location and the second is recover the files which might be delete or that can be loss because of cloud destroy. This algorithm also reduce the time require for recovery process.

**Keywords :** Backup Privacy, Central Repository, Seed Block, Parity Cloud, Parity cloud service, AES encryption.

## I. INTRODUCTION

Cloud computing enables consumers to access resources In our literature survey, We study the recently used backup onlinethrough the internet, from wherever at any time & recovery technique used in cloud computing domain. withoutworrying about technical/physical management i.e. HSDRT , PCS , ERGOT , Linux Box , and maintenance problems of the original resources. The Cold and Hot back-up technique . After the detail study National Institute of Standard and Technology state that of this technique,we can say that above techniques are cloud computing as: A modelfor permitting convenient, unable to give better performances under all on-demand network access to a sharedpool of configurable circumstances. Such as implementation, cost, security, computing resources (i.e. networks,servers, storage, complexity, recovery &redundancy in short period of time. applications, and services) that can be hastilyprovisioned Among all above technique PCS is comparatively easy, and released with minimal management effort orservice simple & reliable and more convenient for data recovery provider interaction. which is totally on the basis of parity recovery service. In earlier days electronic data is increased in huge amount. PCS recover data with higher probability. It uses the Thisrequires large space over the data storage devices to Exclusive-OR( )for getting parity information. However, store data. So the size of HDD increased up to Terabyte. Implementation is little bit complex.Because of storage size problem users prefer to cloud On the opposed site, HSDRT is an efficient technique where they can store large amount of data. But the for movable devices such as smart phones, laptop etc. The problem is arise of data security in case of cloud damaged cost require for implementation is high. HSDRT is an or that can be corrupt, in this situation important data innovative file backup technique, which makes use of an might be loss to avoid this situation there should be some effective widely used distributed data transfer mechanism mechanism to cater backup of stored data and retrieve that with high speed

encryption technique. This proposed data if above situation might be occur in whichi.e cloud system divide into two sections first is backup and second failure or data can be loss.There are different technique is recovery sequence. But there are some limitation in this which will be known as plain data back-up technique. But model which unable to give perfect solution for backup & these techniques are having many reliability and security recovery.

SBA is useful for collecting the information from anyremote location and it also help for recover the data in caseof deleting the data or cloud may be destroyed.

## II. OBJECTIVE

Cold and Hot Backup Service technique is trigger based.It is triggered when service failures detect and will not be triggered when service is available.In Hot Backup Service replacement strategy (HBSRS) during the implementation of service backup services in dynamic state. And then first gives result of services will be adopted to provide successful implementation of service composition. Among the CSBRS and HSBRS , the HSBRS reduce the service recovery time. Shared Backup Router resources(SBBR) focuses on the significant cost reduction and router failure. It concerns IP logical connectivity that unchanged even after router failure and it also provide network management system with multi- layer signalling. However it concern with cost reduction as well as there are some inconsistencies among the logical and physical configuration which gives problem to performance.

Shared Backup Router resources(SBBR) [6] focuses on the significant cost reduction and router failure. It concerns IP logical connectivity that unchanged even after router failure and it also provide network management system with multi- layer signalling. However it concern with cost reduction as well as there are some inconsistencies among the logical and physical configuration which gives problem to performance.All these method tried to handle different problem withmaintaining the cost of implementation as low as possible.

| Sr. No | Method | Merits | Demerits |
|---|---|---|---|
| 1 | ParityCloud Service[2] | - Reliable<br>- Privacy<br>- Low cost | - Implementation<br>- Complexity is high |
| 2 | HSDRT[1] | -Used for movable Client such as laptop,smart phone | - Costly<br>- Increase redundancy |
| 3 | Linux Box[4] | -Simple<br>-Low cost for implementation | -Require higher bandwidth<br>- Privacy<br>-Complete server backupAt atime |
| 4 | ERGOT[3] | -Perform exact match retrieval Privacy | -Time complexity<br>-Implementation complexity |
| 5 | Cold /Hot Backup Strategy[5] | -Triggered only when failure detected | -Cost increase as data increase |
| 6 | Shared Backup Router Resources[6] | -It concerns with cost reduction works even if router fails | -Inconsistencies laeds to problem which reduce performance<br>-Unable to includes optimization conceptwith cost reduction |

**Figure 1:**Comparisons of Backup Method

## III. PROPOSAL

A method for managing a remote backup database to provide protection from disasters that destroy the primary database is presented. The method is general enough to accommodate the ARIES-type recovery and concurrency control methods as well as the methods used by other systems such as DB2, DL/I and IMS Fast Path. It provides high performance by exploiting parallelism and by reducing inputs and outputs using different means, like log analysis and choosing a different buffer management policy from the primary one. Techniques are proposed for checkpointing the state of the backup system so that recovery can be performed quickly in case the backup system fails, and for allowing new transaction activity to begin even as the backup is taking over a

primary failure. Some performance measurements taken from a prototype are also presented.

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion or corruption. Data loss can be a common experience of computer users; a 2008 survey found that 66% of respondents had lost files on their home PC.[2] The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required. Though backups represent a simple form of disaster recovery, and should be part of any disaster recovery plan, backups by themselves should not be considered a complete disaster recovery plan. One reason for this is that not all backup systems are able to reconstitute a computer system or other complex configuration such as a computer cluster, active directory server, or database server by simply restoring data from a backup.

Since a backup system contains at least one copy of all data considered worth saving, the data storage requirements can be significant. Organizing this storage space and managing the backup process can be a complicated undertaking. A data repository model may be used to provide structure to the storage. Nowadays, there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability. Before data are sent to their storage locations, they are selected, extracted, and manipulated. Many different techniques have been developed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and de-duplication, among others. Every backup scheme should include dry runs that validate the reliability of the data being backed up. It is important to recognize the limitations and human factors involved in any backup scheme.

Parity Cloud Service technique (PCS) is a very simple, easy to use and more convenient for data recovery which is based on parity recovery service. A PCS has low cost for recovery and can recover data with very high probability. For data recovery, PCS uses a new technique of generating virtual disk in user system for data backup, make parity groups across virtual disk, and store parity data of parity group in cloud.

The basic procedure in the proposed network system is as follows in two sequences one is Backup sequence and second is Recovery sequence. In Backup sequence, when the Data Center receives the data to be backed-up, it encrypts scrambles, divides into some fragmentations, and thereafter duplicates that data to some extents to satisfy with the required recovery rate according to the pre-determined service level. The Data Center encrypts the fragmentations again at the second stage and distributes them to the client nodes in a random order. At the same time, the Data Center sends the metadata used for deciphering the series of fragments. The metadata are composed of encryption keys (both at the first and second stages), several related information of fragmentation, duplication, and distribution . In Recovery Sequence, it is the recovery process when some disasters occur or periodically, the Supervisory Server starts the recovery sequence. It collects the encrypted fragmentations from various appropriate clients like rake reception procedure and they are decrypted, merged, and descrambled in the reverse order at the second stage and the decryption will be completed. Though these processes, the Supervisory Server can recover the original data that should be backed-up. How

## IV. CONCLUSIONS

In this paper, we presented detail review of most recent back-up and recovery techniques that have been developed in cloud computing domain. Detail review of this paper shows that these techniques have its own advantages and disadvantages which are summarized in the Table-1. All these approaches are able to provide best performances under all uncontrolled circumstances such as cost, security, low implementation complexity, redundancy and recovery in short span of time.

## V. REFERENCES


[1]. Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications,2010, pp 256-259.

[2]. Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 2011.

[3]. Y.Ueno, N.Miyaho, and S.Suzuki, "Disaster Recovery Mechanism using Widely Distributed Networking and Secure Metadata Handling Technology", Proceedings of the 4th edition of the UPGRADE-CN workshop, 2009, pp. 45-48.

[4]. Giuseppe Pirr´o, Paolo Trunfio , Domenico Talia, Paolo Missier and Carole Goble, "ERGOT: A Semantic-based System for Service Discovery in Distributed Infrastructures," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing,2010.

[5]. Vijaykumar Javaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS), "Backup for Cloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.

[6]. Lili Sun, Jianwei An, Yang Yang, Ming Zeng, "Recovery Strategies for Service Composition in Dynamic Network," International Conference on Cloud and Service Computing, 2011.

[7]. Xi Zhou, Junshuai Shi, Yingxiao Xu, Yinsheng Li and Weiwei Sun, 2008, "A backup restoration algorithm of service composition in MANETs," Communication Technology ICCT 11th IEEE International Conference, pp. 588-591.

[8]. Online Data Backup and Disaster Recovery... (PDF Download Available). Available from: https://www.researchgate.net/publication/268079118_Online_Data_Backup_and_Disaster_Recovery_Techniques_in_cloud_computing_A_Review accessed Apr 07 2018].