International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

Secure Backup Software System

Rajeswari D

Asst.Professor Mrs.J.Kalaivani

Krishnasamy College Of Engineering &Technology,

Cuddalore.

ABSTRACT

Cloud computing is important in IT industry. Cloud service has a widespread acceptance but the fear pertaining to security and privacy of these services still continue to be an open challenge. While talking about cloud security there are many aspects which one needs to consider such as trusted authentication, authorization, data security. There are different algorithms for data encryption like RSA, AES, DES, RC4, 3DES etc. These algorithms are broadly classified as being symmetric or asymmetric in nature. While creating a secure cloud there are faced too many challenges like data protection, loss of data etc. Many security services which are certain by the secure cloud system. In that system hybrid cryptographic approach used which gives benefits of both symmetric and asymmetric encryption. That system is for single cloud and it was implemented on cloud sim framework. In cloud computing, data generated in electronic form are large in amount. To maintain this data efficiently, there is a necessity of data recovery services. This paper is about the reviews on data security and data backup/recovery in multicloud.

1.INTRODUCTION

As data is the heart of the enterprise, it becomes crucial as well as important for us to protect it. And to protect our organization's data, we need to implement a data backup and recovery plan. Backing up files can protect against accidental loss of user data, database corruption, hardware failures, and even natural disasters. It's our job as an administrator to make sure that backups are performed and are stored in a secure location. In information technology, a backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. Backups have two distinct purposes.

The primary purpose is to recover data after its loss, be it by data deletion or corruption. 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 popularly represent a simple form of disaster recovery, and should be part of a disaster recovery plan, by themselves, backup should not alone be considered disaster recovery. One reason for this is that not all backup systems or backup applications are able to reconstitute a computer system or other complex configurations such as a computer cluster, active directory servers, or a database server, by restoring only data from a backup. Since a backup system contains at least one copy of all data worth saving, the data storage requirements can be significant. Organizing this storage space and managing the backup process can be complicated undertaking. A data repository model can be used to provide structure to the storage. Nowadays, there are many different types of data storage devices that are useful for making.

2. EXISTING SYSTEM

The storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. One of storing files remotely is the transfer speed. Remote data backup may lack a while depending on the speed of your communication devices. A high-speed LAN could transmit fast, but others could be doubtful, because of upload problems and firewalls. One of the disadvantages of backup cloud security is that it usually means your sensitive data will have to traverse the internet. Granted, this data should be encrypted and will usually be confined to a VPN. Even so, there is no way to guarantee the security of data passing through a public medium with absolute certainty. It is worth noting that some public cloud providers do offer the option of leasing a dedicated connection between your data center and the cloud, which can mitigate the risks associated with transmitting sensitive data over the internet.

2.1 DISADVANTAGE

There might be delay in receiving the OTP if the network is disconnected. Once the file is deleted, it can't be recovered. Data Redundancy and Replication. Risk to backing up data to the cloud is that of account hijacking. This occurs when a hacker manages to crack or guess a tenant's cloud password, and then logs in as the tenant, and changes the account's password, effectively locking the tenant out of their own data. While it is true that account

hijacking can occur on-premises, on-premises systems containing highly sensitive data might not be as readily exposed to the internet as those systems residing in a public cloud.

3. PROPSED SYSTEM

A effective and flexible distributed scheme with explicit dynamic data support to ensure data. The correctness of user data in the cloud. We rely on erasure correcting code. The file distribution preparation to provide redundancies and guarantee the data dependability. Using Software backup system, users can store files, documents, images, videos through windows application in a secured manner. In this user can store documents and files in any format which is kept in a separate folder made for each user. The stored folder is only accessible to the authorized users who can access their own folder. It's a windows application, where all the file details store in SQL Database. If the user found to be unauthorized by the admin, then admin can block a user and also can unblock it whenever required.

3.1 ADVANTAGE

Access to automatic updates for your IT requirements may be included in your service fee. Depending on your cloud computing service provider, your system will regularly be updated with the latest technology. This could include up-to-date versions of software, as well as upgrades to servers and computer processing power. Scale down your operation and storage needs quickly to suit your situation, allowing flexibility as your needs change. Ability to access your file via the internet.

4. IMPLEMENTATION

The object design consists of 5 modules.

4.1 Admin Model

Login: Admin need to login first to access the below given modules.

Add User: System allows admin to add / register new user into the system.

View / Delete User: Admin can view all registered user's and also can delete a user from the system.

Block User: Admin has the right to block a user from the system.

4.2 User Module:

Login: User needs to login using their valid username and password to login into the system.

Upload a File: After successful login, user can now upload a file, which will be stored in their own folder.

Copy / Delete a File: Once a file is uploaded, user can copy or delete the uploaded file.

Download a File: Whenever user request to download a file, the file from the user's folder gets downloaded into local system.

4.3 Backup module:

In the backup utility service the back module is responsible for taking backup of data to destination. This is totally automatic service. We just have to schedule the service when it should run in the profile. When user initializes machine the backup utility service starts with date and time specified in profile. User can create number of profiles with different source locations. The user have to specify time at which back up should be taken with source file of which backup should be taken & destination file at which back should be stored.

4.4 Query processing module

In the Query processing module to retrieve data from backup server there is application window. In this application window we have to specify the date or date range from which we want data. This request is sent to file processor. File processor checks for files which it has to retrieve in the database. To retrieve files stored at backup server the software checks for list of files stored at database at particular date. Then copy processor take names of files from database which it has to retrieve & copies that files to specified location. After the copying of file is completed the log is generated for it. If retrieval is successful then it creates log which contains name of files retrieved If file is not copied back then it creates log & error log for it .The error log consist of reason of failure. After the log generation the database is also updated which gives information about whether retrievel is successful or not.

4.5 Report module

The report module generates reports whenever there is request for report then data is retrieved from database. The report generator process takes data from database & generates report. The report generator process generates report as specified by user. In report module the user sends request for report which include type.

5. System Requirements

5.2 Software Requirement

Operatingsystem :Windows7

CodingLanguage :php

Server :xampp

BackEnd : PHPMYADMIN

5.2 Hardware Requirement

System :PentiumIV 2.4GHz

HardDisk :40GB

Ram :512Mb

6. Conclusion

Application backup data at given location successfully if required conditions are available. Profile wise working is successful according to given creating. Editing, deleting, restoring. Consequently, many organizations have significant amounts of backup data stored on tape, and are interested in improving performance of tape based data protection solution.

In this paper, we pursue a goal for automated design of a backup that minimizes the overall completion time for a given set of backup jobs.

In this paper, we proposed an automatic data backup which helps the user to recover the disaster files from the remote location.

Experimentation and results shows that there is no modification can be done in the original file so the integrity of the file should be maintained and the time related issues also being solved by the proposed automatic backup so, it took minimum time to recover the files from remote server.

7. Future scope

Future backup and recovery systems have been envisioned with such user interface which can simplify the tasks. But at the same time, it should be capable enough to achieve the complexity of the task. Future backup and recovery mediums should provide the user with auto-discovery of required actions and their interdependence.

The scope of backup and recovery is so vast that there has been continuous research and development regarding future backup and recovery plans. Research is being carried out on the ways to make B&R plans more effective as well as to know the scope to which B&R plans can go on. The scope of backup and recovery for the business continuity is highly dependent on the trends in the IT sector, especially those concerning with the data.

Data protection has become the main concern of any IT infrastructure. There has been exponential growth in the need for the provision of security to data. Especially when a lot of data is being parked in cloud storage. There are a lot of companies and individuals who store sensitive information and confidential data on their computer systems. In this situation, the need for

protecting such vital data is increasing as this sensitive and confidential shouldn't be accessed by the thieves or hackers.

8. References

[1] Ludmila Cherkasova, "Design of Efficient Backup", IEEE, 2010.

[2] S. Deepa and Dr. G. Rsmschandran, "Disaster Recovery System Using Seed Block Algorithm in Cloud Computing Environment", IEEE, 2015.

[3]Lucy.cherkasova,alex.zhang,xiaozhou.li@hp.com [4] R. V. Gandhi and M Seshaiah "Data Back-Up and Recovery Techniques for Cloud Server Using Seed Block Algorithm", 2015.

[4] Akyildiz IF, Su W, S Y, Cayirci E. *"A survey on sensor networks," IEEE Communications Magazine 2002.*

[5] Kunal V. Raipurkar, Anil V. Deorankar, "Improve Data Security in Cloud Environment by Using LDAP and Two Way Encryption Algorithm", 2016. Symposium on Colossal Data Analysis and Networking (CDAN)

[6] Arun Singh, Darshan Jain, Paresh Chavan, Sweta Jain, "Multi Cloud Data Security" 2016 International Research Journal of Engineering and Technology (IRJET) .

[7]. 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.

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