ISSN:0975-9646

Designing Secured Incremental Backup System for Cloud

Shyamsunder Ingle , Rajesh Kulkarni

Dept of Computer Engg
TSSM's Bhivarabai Sawant College Of Engineering & Research
Narhe, Pune – 41

Abstract— Due to extensive usage of Cloud Computing for different application which has complete data storage on Cloud.. It has become necessary to have proper backup system which can reduce the overall maintenance window plus provide some sort of security for the backup over the cloud. Hence this is an effort to provide the backup to the application which can be taken and different time interval. After the first backup, subsequent backups will be incremental in nature as they will just backup the difference of two backups. By doing this it will improve the performance and system up time.
As the huge data is transferred over the cloud it is vital to provide the security to data passing over to Cloud. We can provide it by putting encryption Mechanism to data chunks which are getting transferred to Cloud.
It will also have user level authorization which can help in restoring the backup files any where irrespective of the instruments which has been used while backups.

Index Terms— Incremental Backup, security, Performance

I. INTRODUCTION

Availability of network and mobile devices has made information and files readily available to users globally. Along with the convenience comes the challenge of keeping all the data consistent and minimize the data loss as huge number of users will be working on the application in cloud environment. As there are multiple users will access application it become pivotal to maintain data privacy even for the backed up data kept on data server.

The incremental backup does not take full copy of files available in file system instead it backups the files which have modified since last backup and hence it is faster than full backup and will save time. By saving time we will be able to achieve one of the objectives with respect to increase up time of the system. Incremental backup will have multiple backup windows with smaller gaps between two backups compare to full backup and hence data discrepancies or loss will be less.

To solve the related security issue, encryption is necessary when the backup data is stored in storage server. Separate encryption key will be set for each of the user instead of at each file. This will help each user separating his data and encrypting the same, by doing this user will not be able to access data stored by other user as it will have same key to decrypt and thus the privacy will be maintain. Also even if entire storage server access got compromised data will not be accessible as it is encrypted and there need separate key for each user in order to decrypt it.

Entire operation will be controlled from server side, it will have separate modules to keep track of encryption keys, backup configuration, storage location and check on different modified files since last backup. By keeping it at server will have central point of control on the overall operation.

A. Approaches in Existing System

In the existing system incremental backup has been done without server side programming. Where files been pushed from client to different storage servers. Here all the logical evaluation of files been determined on client side and just the data getting passed to storage servers.

Existing research efforts [1], [2], [3], [4], [5], [6] use different approaches towards backup process

[6] Determining the optimum time interval between two incremental backups so that the data loss can be kept minimal.

[5]File System Filter Driver method Monitor detects the file operation at kernel level as any changes happened in file. Backup does the backup of the modified files to storage server. Recovery module. reads the data from storage whenever recovery of data is needed.

[4] Ultimate challenge in Cloud Computing is data level security. Security need to be move to data level so that enterprises can be sure of their data protection wherever it goes. The main contribution of this paper is to introduce the first provable secure and practical backup cloud data regularly that provide reconstructs the original cloud data by downloading cloud data.

[2] It has analysed the differences between existing cloud storage interfaces, and pointed out most cloud backup software's deficiencies in directory backup and large file backup. Detailed how to realize backup of clients, found it feasible to mask differences between cloud storage interfaces by increasing layer of cloud storage interface, found it effective to make directory backup by making mapping between directory hierarchy and cloud data model and adopting hierarchical transmission. Found large file backup could be realized through the mechanism of file segment and breakpoint transmission, and increasing file appends interfaces.

B. Observations

The existing solutions is appropriate with small scale systems, however of data is getting transferred over the net and cloud cannot be sufficient with respect to security and in current scenario where huge amount of data lies on

cloud. With progress of information technology there lies the threat to the data as all types of data is on server and in term appropriate security measure need to be in place. Also it becomes vital to have backup mechanism at appropriate interval with optimal time to complete the entire operation.

C. Proposed Work

This paper proposes backup system for devices connected over cloud. It will have control shared with client as well as cloud server. Different steps involved

1. Authorization :-
   Every user who posses to keep this facility will have the valid user id and password. These users will have access to the cloud and storage server. User A will not be able to see the files of user B and vice a versa
2. Identification of files :-
   For taking the backup this step will identify the files which have been modified since last backup. It will have the list of all the files which has been modified since last backup.
3. Encryption of files :-
   Encryption will be done using AES algorithm , for each file one key will get generated and file get encrypted before it moves to cloud server.
4. File backup :-
   Encrypted files will get moved to server. Each file will get one file id which will get associated with the user which the file is associated with.
5. File Restore :-
   Restore file will provide the option file restoring the previously backup files to any device which has client installed

D. Contributions

This paper proposed a mechanism that uses incremental backup along with encryption. Process encrypts the file before sending it to the Cloud storage.

- Proposes a novel approach for user level authentication which provides the privacy to the data even though they use same application.
- Uses a method which will only send the delta of data from the previous backup and sends the data which has change hence reduces the traffic over net
- Proposed solution has encryption method which will protect data while in transit as well as at the storage.

The rest of this paper is organized as follows: Section II describes the design work. Section III presents the implementation of solution. Section IV is evaluation results, and Section V concludes the paper.

II. Design Section

The proposed work's key research objective is to design a system over the cloud which will provide the option of taking incremental backup to reduce the backup time plus do the encryption to store it securely on storage server
Architecture of this approach needs client and cloud server as shown in the figure 1.

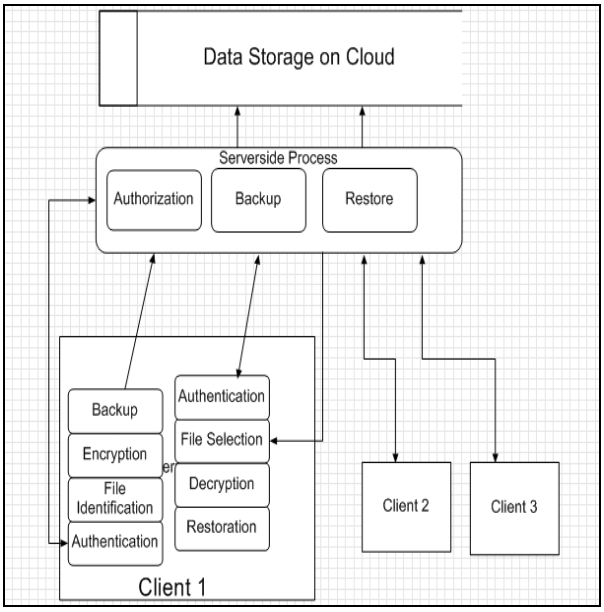


Fig 1- Architecture

Clients can be any machines which can connect to cloud environment using authorized user id and password. Client machine will need the application on it so that it will have functionality as shown in fig.
Using this application one can backup from any machine and can restore the data anywhere once he has authorized credentials for the system.
Server side process will have database where the user can be maintain and the time wise backups will be stored in database, this method only keeps the files which has been modified at least once.
For restoration, user gets a choice of restoring entire folder or a specific file. Restoration will have in different folder than from where it has been backup. Restoration will have file first getting to client and then decrypting it to normal file.

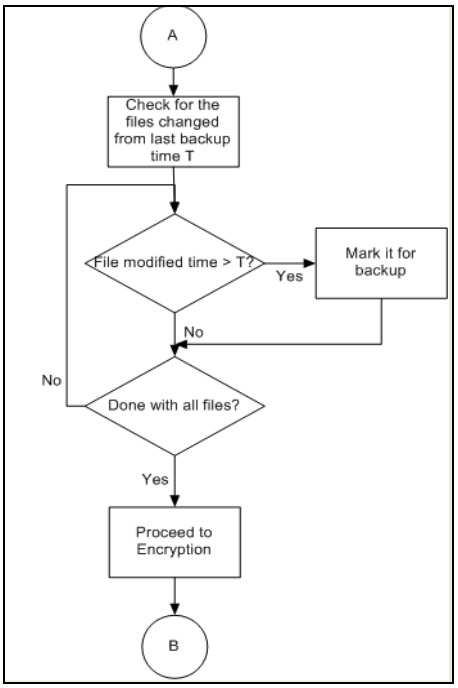


Fig 2 – File Identification

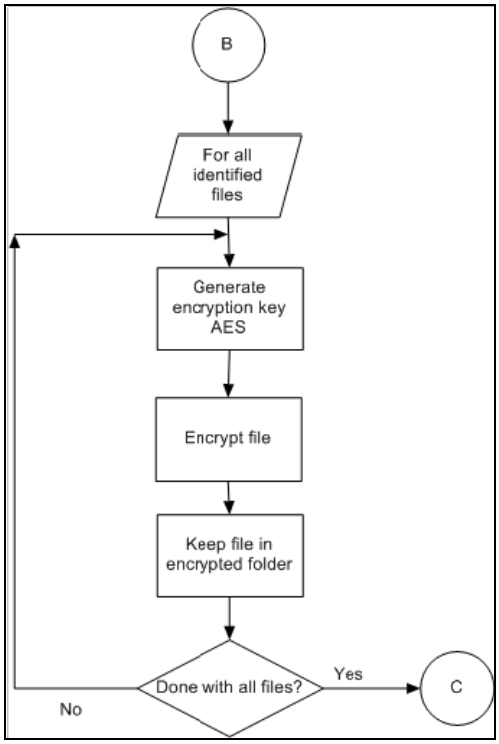
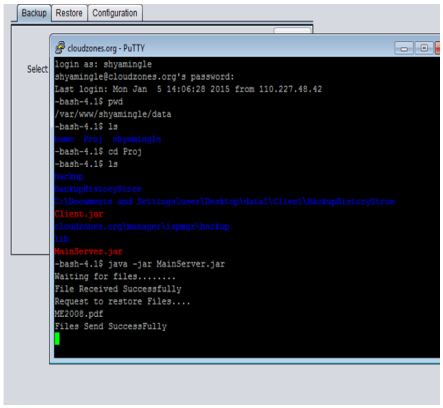


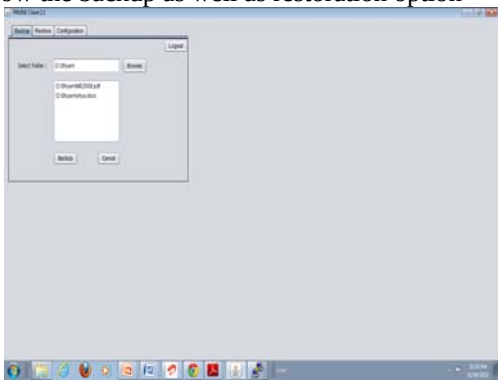
Fig 3 - Encryption

III. Implementation Details

Cloud Server: - We have our server processes running on the cloud server which waits for the files from the client. It does have database created on server which will keep the track of files being backed up.



Clientside program will have graphical user interface which will show the backup as well as restoration option



IV. Results And Discussion

Backup system divided in following systems

i. File Identification
ii. Encryption
iii. Incremental Backup
iv. Restoration

Following table shows the output of the system when we used normal backup and incremental backup

Table 1: Normal Backup

Sr. No	Backup Interval	Backup Volume	Time for Backup
1	10	100	40
2	20	125	65
3	30	140	90
4	40	150	105
5	50	160	120

If you see table above the time is increasing for backup continuously as the volume of backup is going up.

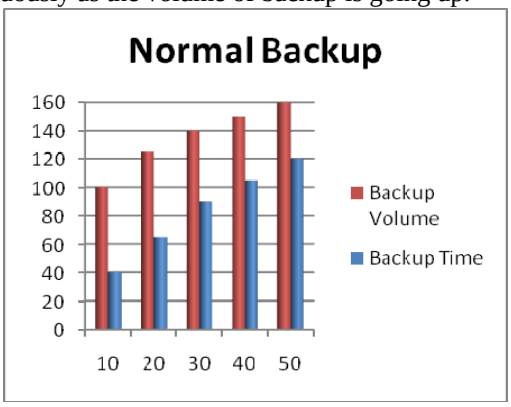


Figure 4: Graph for normal backup

As compare to normal backup we could see improvement with backup time as we are only considering the backup changed files from last backup interval.

Table 2: Incremental Backup

Sr. No	Backup Interval	Backup Volume	Time for Backup
1	10	100	40
2	20	30	20
3	30	26	15
4	40	40	25
5	50	35	18

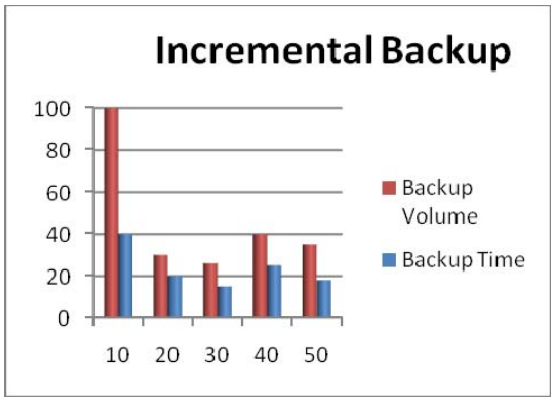


Figure 5: Graph of Incremental Backup

V. CONCLUSION

By experiment it has been demonstrated that incremental backup is improving the performance of the system by reducing the backup time. By putting user level encryption this has security enhanced around the backup. On storage we have stored encrypted data hence security is around the storage.

REFERENCES

[1] Shih-Yu Lu, "Encrypted Incremental Backup without Server-Side Software", 2013 27th International conference on Advance Information Networking and applications Workshop.

[2] Jing Nie, "Design the Desktop Backup System Based on Cloud Computing", 2012 Eighth International Conference on Computational Intelligence and Security.

[3] Yashpalsinh Jadeja,Kirit Modi, "Cloud Computing - Concepts, Architecture and Challenges ", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[4] Amir Mohamed Talib,Rodziah Atan, Rusli Abdullah & Masrah Azrifah Azmi Murad CloudZone: Towards an Integrity Layer of Cloud Data Storage Based on Multi Agent System Architecture ", 2011 IEEE Conference on Open Systems (ICOS2011), September 25 - 28, 2011, Langkawi, Malaysia.

[5] Zhao Zhongmeng,Yao Hangtian, "A Data Backup Method Based on File System Filter Driver ", 2010 Second WRI World Congress on Software Engineering.

[6] S. Nakamura, K.Nakayama, T.Nakagawa, "Optimal backup interval of database by incremental backup method.

[7] Palivela Hemant, Nitin.P.Chawande, Avinash Sonule, Hemant Wani, "DEVELOPMENT OF SERVERS IN CLOUD COMPUTING TO SOLVE ISSUES RELATED TO SECURITY AND BACKUP." IEEE CCIS 2011

[8] Kuan-Ying Huang,Guo-Heng Luo,Shyan-Ming Yuan, "SSTreasury+: A Secure and Elastic Cloud Data Encryption System" 2012 Sixth International Conference on Genetic and Evolutionary Computing.

[9] Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System" 2012 Sixth International Conference on Genetic and Evolutionary Computing.