Efficient Cloud Security Back-Up System

Ms. Namita Jakulwar[1], Mr. Hirendra Hazare[2]
[1]Dept of CSE
[2]Asst. Professor, Dept of CSE
[1, 2] Ballarpur Institute of Technology (BIT), Ballarpur.

Abstract- *In cloud computing, data generated in electronic form are in large amount. To maintain this data efficiently, there is a necessity of data recovery services. To cater this, in this topic we propose a smart remote data backup plan using Seed Block Algorithm (SBA) with Advance Encryption Standard (AES) algorithm. In this topic we are proposing a procedure which allows users to store their data onto the cloud, as soon as the file is stored at the first cloud server it gets encrypted using AES. In case if the certain file gets deleted due to any reason, AES helps to recover that file from a backup file which is stored at a remote location. The time related issues are also being solved by proposed method such that it will take minimum time for the recovery process. Proposed method also focuses on the security concept for the back-up files stored at remote server using AES encryption algorithm.*

Keywords- Seed Block Algorithm, AES, Cloud back-up, Remote cloud, Main Cloud

I. INTRODUCTION

Cloud Computing is itself a gigantic technology because of its advantages over previous systems like grid or cluster computing. Cloud storage provides online storage where data stored in form of virtualized pool that is usually hosted by third parties. Number of users share the same cloudstorage provided by a certain service provider.

Faulty equipment's, a human error, network connectivity, a bug or any criminal intent may put our cloud storage's security at stake. Cloud service provider may also make some changes in the configuration; this may lead to loss of alteration of the information stored by user. There is possibility of data loss. To solve these difficulties, we need to provide data integrity for our cloud. In literature many techniques have been proposed PCS[1], HSDRT[2], Linux Box [3], ERGOT[4], Cold/Hotbackup strategy [5] etc. that, discussed the data recovery process. However, still various successful techniques are lagging behind in some critical issues like implementation complexity, low cost, security and time related issues.

To overcome the disadvantages of previously proposed systems we have proposed and are implementing a new method based on Seed Block Algorithm (SBA) and Advance Encryption Standards (AES) Algorithm. The mentioned procedure works in following manner: in first step it allows users to collect and store their files onto the main cloud. As soon as the files get stored at the cloud, those get encrypted using AES algorithm. In step two, in case of file deletion it helps user to recover the files.

This project is mainly indented to take Backup of data in LAN and WAN. As future expansion it can be implemented in World Wide Web. Another feature that can be implemented is incremental backup, which will enable to save storage space by smart backup. New technologies like Cloud Computing can be used to make the backup system more effective and efficient.

The smart data backup server has the facility to take secured backups of the systems in the network. This application will enable the clients to schedule them back up and take urgent backup of only the required files when needed. The encryption property of the Smart- Data Backup server ensures security of the data.

Also, the clients can have a detailed report of the backups as with all computer system, there is always the potential for hardware malfunctions such as hard disk failures. Often, such maintenance is required due to the accidental and sometimes even deliberate modification or deletion of files on a system by its users. In some cases, such alterations can be undone easily, while in others, the only remedy is to reinstall a system from scratch. Small businesses rely on the availability of their data to keep running, so data loss is arguably more catastrophic for them than for consumers. In fact, a recent study of small businesses had suffered data loss: "The top causes of small business' data loss included hardware/software failure (54 percent), accidental deletion (14 percent), computer viruses (22 percent) and theft (10 percent)," In such cases, it is of great benefit to administrators to have a backup of each available system that has been installed.

II. LITERATURE REVIEW

In literature survey, we have studied the most recent back-up and recovery techniques that have been developed in cloud computing domain such as PCS [1], HSDRT [2], Linux

Box [3], ERGOT [4], Cold/Hot backup strategy [5] etc. When we studied the existing methods in detail we found that, performance of the system is not satisfactory with respect to cost, security, low implementation complexity, redundancy and recovery in short span of time.

We inferred after study of various present techniques that PCS is comparatively reliable, simple, easy to use and more convenient for data recovery totally based on parity recovery service. It has higher probability and efficiency of recovering among present techniques. It generates a virtual disk in user system for data backup, make parity groups across virtual disk, and store parity data of parity group in cloud to recover the data. It makes use of the Exclusive OR functionality for creating Parity information. However, there are some problems associated with this method. This method is unable to control the implementation complexities.

On the other side, HSDRT method ensures as a powerful technique for the movable clients such as laptop, smart devices, palmtops etc. However, it is not economical for the implementation of the recovery and also unable to control the data replication. It an innovative _le back-up concept, which makes use of an effective ultra- widely distributed data transfer mechanism and a high-speed encryption technology.
The HS-DRT [2] is an innovative file back-up concept, which makes use of an effective ultra-widely distributed data transfer mechanism and a high-speed encryption technology. This system follows two sequences one is Backup sequence and second is Recovery sequence. In Backup sequence, it accepts the data to be backed-up and in Recovery Sequence, when some calamities occur or periodically, the Supervisory Server starts the recovery sequence. However, there are some limitations in this model and therefore, this model somehow fails to declare as perfect solution for back-up and recovery.
We also observed that Linux Box model is having very simple concept of data back-up and recovery with very low cost. But in this model protection level is very low. Process of migration from one cloud service provider to other seems to be very easy. It is economical for all consumers and Small and Medium Business.

This solution removes consumers dependency on the internet service provider and its associated backup cost. It incorporates an application on Linux box that will perform backup of the cloud onto local drives. The data transmission will be secured and encrypted. The limitation we found that a consumer can backup not only the Data but Sync the entire Virtual Machine [3] which somehow waste the bandwidth because every time when backup takes place it will do back-up of entire virtual machine.

Moreover, Efficient Routing Grounded on Taxonomy (ERGOT) [4] features the semantic analysis and fails to focus on time constraints and implementation complexity. It is a Semantic-based System which helps for Service Discovery in cloud computing. Similarly, we found a unique technique for data retrieval. We observed this technique as it is not a back-up technique but it provides an efficient retrieval of data that is completely based on the semantic similarity between service descriptions and service requests. ERGOT is built upon 3 components viz. 1) A DHT (Distributed Hash Table) protocol 2) A SON (Semantic Overlay Network), 3) A measure of semantic similarity among service description [4]. Hence, ERGOT combines both these network Concepts. By implementing a Semantic Overlay Network over a Distributed Hash Table, ERGOT proposed semantic-driven query answering in DHT-based systems. However, it does not go well with semantic similarity search models.

III. PROPOSED SYSTEM

In this paper specify, the project is a software system where Back-ups are done automatically over the network to a back-up server at regular intervals and system administration done periodically so that data security is maintained. It is a software package that provides centrally managed, reliable backup facilities for a variety of workstations. The programs permit you (or the system administrator) to man-age backup, recovery, and verification of computer data across a network of computers of different kinds. In technical terms, it is a network Client/Server based backup program. The Backup System is relatively easy to use and efficient, while offering many advanced storage management features that make it easy to find and recover lost or damaged files. Due to its modular design, Backup System is scalable from small single computer systems to systems consisting of hundreds of computers located over a large network.

IV. METHODOLOGY

When we think about Backup server of main cloud, we only talk about the replicate of main cloud server. When thisBackup server is at remote location and having the complete state of the main cloud, then this remote location server is identified as Remote Data Backup Server. And in case if the central repository loses its data under any scenarios both of any natural calamity or by human attack or deletion that has been done by mistake and then it uses the information from the remote server. The main purpose of the remote backup facility is to help user to collect information from any remote location even if data not available on main cloud. As shown in Fig-1 clients can access the files from remote repository even if the data is not available on central repository.

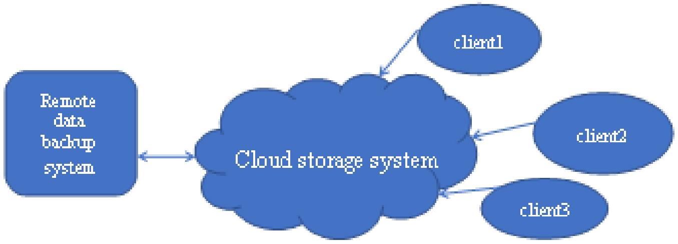

Fig 1: Arch. Of Remote Data Backup System

An analysis of the method is mentioned below,

Advance Encryption Standard

Encryption Phase: The Advanced Encryption Standard (AES) is a symmetric key encryption standard. The standard consists of three block ciphers AES-128 AES-192 and AES-256 adopted from Rijndael. Each of these ciphers has a 128-bit block size withkey sizes of 128, 192 and 256 bits respectively. The key sizeused for an AES cipher denotes the number of repetitions oftransformation rounds that converts the input called theplaintext into the final output called as cipher text. Aftergenerating the cipher text from the plain text, the encryptedfile is stored on the main cloud and that file is only gettingbacked-up on the remote server.

B. Seed Block Algorithm (SBA)

This algorithm basically uses the concept of Exclusive–OR (XOR) operation of the computing world. Seed Block hastwo sequences first is back-up sequence and second is restoresequence. In the main cloud we set a random number and seedfor each client that wants to store data onto the cloud. In thenext step, previously generated random number and seed areEXORed to form the seed. The seed which is generated by thisprocess is unique for each client. Whenever client creates thefile in cloud first time, it is stored at the main cloud and getsencrypted using AES. After that the main file of client is beingEXORed with the Seed Block of the particular client. In thismanner a back-up file for the main file is created by the serverand the back-up file is stored at the back-up cloud which is atremote location. Unfortunately if the file in the main cloudserver gets deleted due to any reason, user can retrieve the lostfile from remote back-up server with the help of Seed Blockwhich is unique for each user.

V. RESULT & FUTURE SCOPE

This project is mainly indented to take Backup of data in LAN and WAN. As future expansion it can be implemented in World Wide Web. Another feature that can be implemented is incremental backup, which will enable to save storage space by smart backup. New technologies like Cloud Computing can be used to make the backup system more effective and efficient.

VI. CONCLUSIONS

Disasters both natural and human-caused can threaten your precious files at any time: a fire, power surge, or leaking pipe could fry your system. Even without suffering a calamity, there are plenty of other threats to locally stored data hard drive failure, accidental erasures, or a lost or stolen laptop could make you a victim of data loss. By data, here, we mean things like your irreplaceable family photos, videos, and music as well as documents. Secure Network Backup System, securely store your files away from your premises at onsite - site server locations, your data will stay intact and available even if your local disks are stolen or your premises suffer some disaster. With more and more emphasis on "cloud computing," it only makes sense that backup should take advantage of this hot trend in technology.

REFERENCES

[1] Java2 complete reference: Herbert Schildt (Tata McGrawHill)

[2] Using java2 platform: Joseph Weber (PHI) ++

[3] Java2, AWT, Swing, XML and JavaBeans Programming Black Book: Steven Holzner, Wiley Dreamtech.

[4] Details about NetBeans: http://roseindia.com

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

[6] Giuseppe Pirro, Paolo Truno , 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.

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

[8] http://www.eecs.berkeley.edu/Pubs/ TechRpts /2009// EEC S-2009-28.pdf.