IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Survey: Cloud Security with a Remote Smart Data Backup Technique

Akshay Gondke[1], Kaustubh Gage[2], Sneha Annappanavar[3]

Student, Computer Engineering, Vidyalankar Institute of Technology, Mumbai, India [1,2]

Assistant Professor, Computer Engineering, Vidyalankar Institute of Technology, Mumbai, India [3]

Abstract: In cloud computing a large amount of data is generated, to maintain the efficiency of the outsourced data there is a need for data backup services. A major security challenge is to protect this data. Hence we have introduced a Smart Data Backup algorithm called as "Seed Block Algorithm" (SBA) which we are using as a smart remote data backup storage. The two main objectives of this algorithm are as follows. The first is to gather information from a remote storage location and the second is recovery of the files if the file gets deleted or if the cloud gets destroyed due to any circumstances. This algorithm takes care of the time associated problems and performs recovery of data in minimum time.

Keywords: Cloud Computing, Seed Block, Advanced Encryption Standard (AES), Cloud Security, Backup Algorithm, Central Repository, Remote Repository, Cloud Environment (ULTEO).

I. INTRODUCTION

Nowadays, everything is computerized and data is stored everywhere in large quantity. This requires large volume of data storage devices to store this large amount of data generated in Terabytes. Therefore, usually consumer prefers to store large amount of private data in cloud. Unfortunately, if cloud gets corrupted or damaged it leads to the loss of all important and private data then there should be some mechanisms to take back-up of the data, and provide the data at the time of cloud failure or loss of data. As we know that plain data back-up techniques are having many reliability and security problems. However the plain back-up techniques are not convenient and reliable as well. To overcome from old plain data backup technique and recovery problem, more safer and effective systems such as HSDRT, PCS, ERGOT, Linux Box, Cold and Hot back-up technique etc. were developed for cloud. These systems provide high privacy protection or reliability however some increases the cost where as some are unable to maintain the low implementation complexity.

However, still these techniques are lagging behind some critical issues like implementation complexity, less cost, security and time related issues. To overcome these issues, in this paper we propose a smart remote data backup algorithm called as Seed Block Algorithm (SBA).

The Seed Block Algorithm works in two ways:-

1. SBA helps the users to collect information from any remote location
2. To recover the files in case of the file deletion or if the cloud gets destroyed due to any reason.

II. LITERATURE REVIEW

In literature, we have surveyed most of the recent back-up techniques like PCS, HSRDT, ERGOT, Linux Box etc. which are developed for cloud computing environment.

The detailed review was not up to the mark as none of these techniques was able to provide excellent performance under multiple circumstances like cost, security, complexity, redundancy and recovery of data in minimal time.

HSDRT (High Speed Data Rate Transfer) is a technique used for movable clients like cellular phone, tablets and laptops. It fails to manage the low cost implementation of the recovery and it also fails to control the duplication of data. The HSRDT uses an ultra-wide data transfer mechanism and high speed encryption. However the limitation of this model is it cannot recover exact data for backup and recovery process.

PCS (Parity Cloud Service) is comparatively reliable because it is simple and easy to use and the data recovery is based on its parity recovery service. It recovers data with a very high probability. It creates a virtual disk as a backup, makes parity groups across the disk. It uses Exclusive-OR ($\oplus$) for creating parity information. But the drawback is it cannot control the high implementation complexity.

ERGOT (Efficient Rounding Grounded on Taxonomy) is completely depended on semantic analysis and it fails to focus on time complexity as well as implementation complexity. It is technique which supports for service Discovery in cloud computing .Data retrieval is provided in an efficient way.

Linux Box is one of the simplest method for data back-up and recovery with low cost. However this model is not so secured. Migration can be possible using Linux Box from one cloud service provider to another one easily It can be used by all the customers having small and medium business .The drawback of Linux Box is that whole virtual machine is synced instead of backing up just the data

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

which waste huge bandwidth because whenever we take a backup of data, it backs up the whole virtual machine.

Cold/Hot Back-up Strategy performs backup and recovery on trigger failure basis. But the major limitation of this strategy is the increase in cost with the increase in data.

TABLE I:EXISTING CLOUD BACKUP TECHNIQUES

Sr. No	Method	Advantages	Disadvantages
1	**HSDRT (High Speed Data Rate Transfer)**	-Used for mobile clients like laptop, tablet and cell phones.	-Expensive -Data Redundancy
2	**PCS (Parity Cloud Service)**	-Reliable -Security -Less Expensive	-Difficult to implement due to high implementation complexity
3	**ERGOT (Efficient Rounding Grounded on Taxonomy)**	-Perform perfect retrieval of data -Low cost for implementing	-Time complexity -Implementation Complexity
4	**Linux Box**	-Simple -Low cost for implementation	-Requires a higher bandwidth -Not secure -Backs up the whole virtual machine every time.
5	**Cold/Hot Back-up Strategy**	-Triggers only when failure is detected	-Cost increases as data increases gradually.

The above table states that none of the existing backup techniques are able to solve all the issues of remote data backup. Hence we proposed a SBA algorithm which overcomes all the issues which are faced by existing backup techniques.

III. ARCHITECTURE

A) REMOTE DATA BACKUP SERVER

The backup server of main cloud stores the binary form of the data file. This backup storage is placed at a remote location (far away from main cloud server) and has the complete state of main cloud. The main cloud is basically the Central Repository and remote backup cloud is termed as Remote Repository.

In case of loss of data or destruction of the main cloud by natural causes or by deletion of data by human intervention, the lost data can be retrieved from the remote backup server. The proposed SBA algorithm keeps the data secure in the main server as well as the cloud server.

The remote server should have features like:-

1. **Integrity of data**:
   Integrity refers to maintaining and assuring the accuracy and consistency of data stored on the cloud server.
2. **Security of data:**
   The data stored on server should not be accessed by third party owners or any other clients/user on remote server.
3. **Confidentiality of data:**
   Only their personal details should be displayed and the details of other clients should be kept hidden.
4. **Low Cost:**
   The cost for establishing the remote setup and for implementing its technique must be minimum such that small business can afford such system and large business can spend less money as possible.

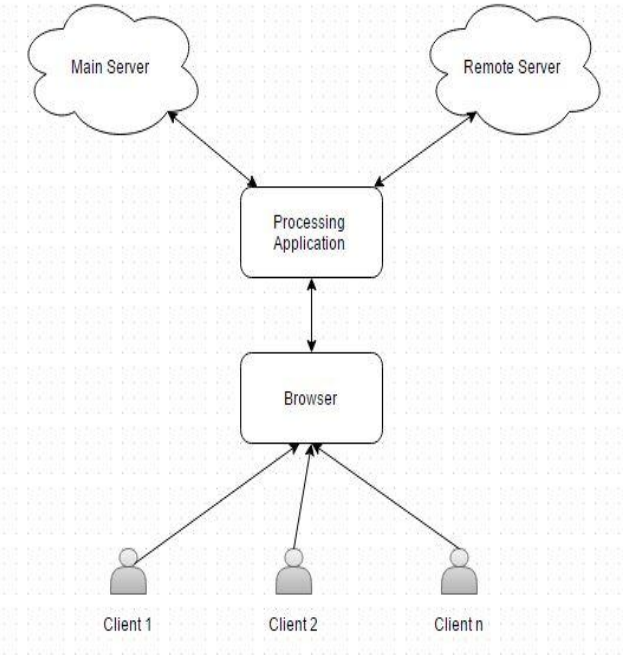

Fig. 1. Architecture of Cloud Servers and Application

B) ULTEO ARCHITECTURE

Ulteo Open Virtual Desktop (OVD) is a base that assists on-demand access to virtual desktops and apps from public/ private cloud hosted environments. Ulteo OVD supports Windows Remote Desktop Services and Linux desktops & application sessions as well as SaaS apps, enabling organizations to integrate and seamlessly deliver them as a secure service to clients based on Windows, Linux, Mac OS, Android and iOS platforms.

Advantages of ULTEO cloud environment

1. Provides virtual cloud environment.
2. Universal access.
3. Open source cloud environment to provide control processing and storage.
4. Storage and processing are clubbed with each other.

Two machines are needed where one will act as a main cloud server and the other will act as remote data server. With the help of ULTEO cloud we created a virtual environment on which we deployed our application.

1. First machine has the application and the main storage integrated as a frequent communication is needed between them.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

2. The second machine stores a backup storage from which the retrieval of lost data can be done. This storage is connected to the application on Tier-2.
3. The clients would be the browsers on Tier-1 from which they will login to the cloud and store the data.

As ULTEO is platform dependent it creates a virtual cloud environment on any operating system such as Windows, Linux, MAC OS and others. But we are using Windows OS as majority of people are familiar with Windows OS as it has a user friendly interface.

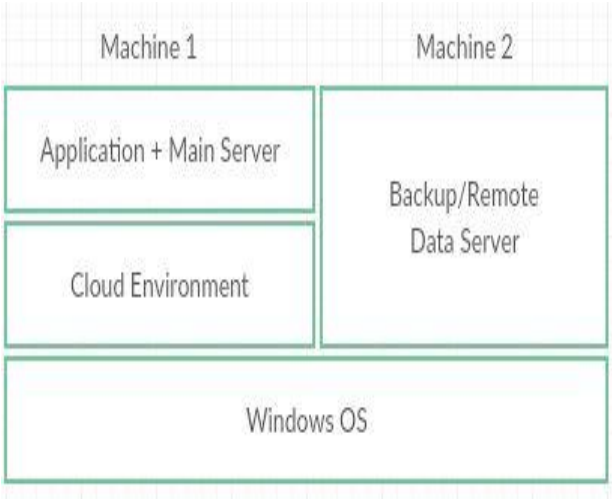

Fig. 2. Overview of the application

IV. ALGORITHMS

A. Seed Block Algorithm (SBA)

The algorithm concerns about the simplicity of backup and recovery process. SBA uses Exclusive OR (XOR) operation for computation. e.g. If we have two data files A and B , when we XOR A⊕ B = X is generated .Incase if file A is destroyed or deleted and we want that file back so using XOR of file X and B i.e. A=X ⊕ B file A can be obtained.

Working:-

1. First we set a random number in the main storage and unique client-id for every user is generated.
2. Whenever the client id is being register in the main storage, then client id and random number is getting XORed with each other to generate SB value for the particular client which is encrypted and stored in the remote server .The client need to verify his account via email after that he will receive a Seed value.
3. Whenever client uploads the file in the cloud first time, it is stored in the main storage.
4. This file is encrypted using AES algorithm for security purpose.
5. When it is stored in main storage, the main file of client is being XORed with the Seed Block of the particular client simultaneously.
6. Output file generated by SB is stored on the backup storage in the form of file' (called as File dash).
7. During Retrieval/View/Download, check if data present in main storage
8. If present then decrypt the data using AES and get the original data
9. If absent, retrieve data from backup storage
10. During Retrieval from backup storage, the seed value and backup data will be XORed to get the original data. The data will be transferred to main storage as well for future use.
11. The user will get the original file by XORing on decrypted file' with the seed block of the corresponding client to produce the original file and return the resulted file in case of crash.

B. Advanced Encryption System (AES)

AES Comprises three block ciphers, AES-128, AES-192 and AES-256.Each cipher encrypts and decrypt data in block of 128 bits using cryptographic keys of 128,192,256 bits. Symmetric use the same key for encryption and decryption, so both the sender and receiver must know and use the same secret key. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, exchange and mixing of the input plaintext and transform it into the final output of cipher text. We are using AES-128 for encryption of the text/image data.

V. PROPOSED SYSTEM

The size of file on the remote server and that of the file on the main cloud will be exactly same. The algorithm will help the system to obtain the recovered files based on the original files. This will make the proposed SBA algorithm robust in nature. From this it can be concluded that the proposed SBA will recover the data file without any data loss.

Type of File	Size on Main Server	Size on Remote Server	Recovered File Size
Text(.txt/.docx/.doc)	1MB	1MB	1MB
Image(.jpeg/.png/.gif)	3MB	3MB	3MB

VI. CONCLUSION

In this paper, we present design of proposed SBA algorithm. SBA is used for collecting the information from remote location and for recover that file in case of file deletion from the remote cloud if the main cloud is destroyed. According to the result we can say that SBA focuses on security for backup files stored at the remote server. SBA also reduce the time required to recover the file and the complexity of the algorithm is also less compared to others.

REFERENCES

[1] Ms.Kruti Sharma,Prof Kavita R Singh,A remote data backup technique for cloud computing ,2013 International Conference on Communication Systems and Network Technologies.
[2] Sonal Patil, Harshad.S.Patil Association Rules in Horizontally Distributed Databases with Enhanced Secure

Mining.COMPUSOFT, An international journal of advanced computer technology, 3 (8), August-2014 (Volume-III, Issue-VIII)

[3] 97 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT) Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud Systemby Prakash.G.L,Dr.Manish Prateek,Dr.Inder Singh.

[4] Fatemi Moghaddam F,Karimi O,Alrashdan M T, A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments, in IEEE 2nd International Conference on Cloud Networking, pages 185-189, 2013.

[5] Ms..Kruti Sharma,Prof K.R.Singh, 2012, "Online data Backup And Disaster Recovery techniques in cloud computing:A review", IJEIT, Vol.2, Issue 5.

[6] ULTEO cloud environment for deploying our project https://www.ulteo.com/home/

BIOGRAPHIES

Akshay Gondke, Computer Engineering Vidyalankar Institute of Technology, Wadala.

Kaustubh Gage, Computer Engineering Vidyalankar Institute of Technology, Wadala.

Sneha Annappanavar, Vidyalankar Institute of Technology, Wadala. DESIGNATION: Assistant Professor BRANCH: Computers.

DOI 10.17148/IJARCCE.2016.51105