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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Seed Block Algorithm: Remote Smart Data-Backup Technique for Cloud Computing

Kailas Pophale[1], Priyanka Patil[2], Rahul Shelake[3], Swapnil Sapkal[4]

Department of Computer Engineering Sinhgad Institute of Technology, Lonavala, Maharashtra, India[1,2,3,4]

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 onlinethrough the internet, from wherever at any time withoutworrying about technical/physical management and maintenance problems of the original resources. The National Institute of Standard and Technology state that cloud computing as: A modelfor permitting convenient, on-demand network access to a sharedpool of configurable computing resources (i.e. networks,servers, storage, applications, and services) that can be hastilyprovisioned and released with minimal management effort orservice provider interaction.

In earlier days electronic data is increased in huge amount. Thisrequires large space over the data storage devices to store data. So the size of HDD increased up to Terabyte. Because of storage size problem users prefer to cloud where they can store large amount of data. But the problem is arise of data security in case of cloud damaged or that can be corrupt, in this situation important data might be loss to avoid this situation there should be some mechanism to cater backup of stored data and retrieve that data if above situation might be occur in whichi.e cloud failure or data can be loss.There are different technique which will be known as plain data back-up technique. But these techniques are having many reliability and security issues. As well as they are not convenient and reliable. To overcome these drawback from plain data backup and recovery issues, it requires more secure and effective system i.e. HSDRT [1], PCS [2], ERGOT [3], Linux Box [4], Cold and Hot back-up technique [5], SBBR [6] these are recent backup technique gives high security and reliability but the cost is also increase and implementation may be complicated to handle this problem we propose seed block algorithm.

SBA is useful for collecting the information from any remote location and it also help for recover the data in case of deleting the data or cloud may be destroyed.

This paper is divide as follows:-

II. Literature survey include in this section
III. Whereas remote data backup server is discuss in section.
IV. Stretegy of seed block algorithm
V. Implementation and Result
VI. Conclusion

II. LITERATURE SURVEY

In our literature survey, We study the recently used backup & recovery technique used in cloud computing domain. i.e. HSDRT [1], PCS [2], ERGOT [3], Linux Box [4], Cold and Hot back-up technique [5]. After the detail study of this technique,we can say that above techniques are unable to give better performances under all circumstances. Such as implementation, cost, security, complexity, recovery &redundancy in short period of time. Among all above technique PCS is comparatively easy, simple & reliable and more convenient for data recovery which is totally on the basis of parity recovery service. PCS recover data with higher probability. It uses the Exclusive-OR($\oplus$)for getting parity information. However, Implementation is little bit complex.

On the opposed site, HSDRT [1] is an efficient technique for movable devices such as smart phones, laptop etc. The cost require for implementation is high. HSDRT is an innovative file backup technique, which makes use of an effective widely used distributed data transfer mechanism with high speed encryption technique. This proposed system divide into two sections first is backup and second is recovery sequence. But there are some limitation in this model which unable to give perfect solution for backup & recovery.

Relatively Efficient Rounding Grounded on Taxonomy(ERGOT) [3] isentirely depend on semantic analysis and it failed to focus on time complexity.It is semantic based method which support for service Discovery in cloud computing.We can say this is not a backup technique but it provide an efficient way of data retrieval. ERGOT is built upon 3 components 1) A DHT (DistributedHash Table) protocol 2) A SON (Semantic Overlay Network), 3) A measure of semantic similarity among service description Hence, ERGOT combines both these network Concept. By constructing a SON over a DHT, ERGOT proposed semantic-driven query answering in DHT-based systems.

In adding Linux Box [4] is one of the simple method for data back-up and recovery with minimum cost. However security level is very low. Migration can be possible using Linux Box from one cloud service provider to another one easily.In Linux Box method data transmission will be

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

encrypted and secure.The limitation of Linux Box is that whole virtual machine is sync that waste some bandwidth because when we take backup will do backup of whole virtual machine.

Cold and Hot Backup Service [5] 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) [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 with maintaining the cost of implementation as low as possible.

Sr. No	Method	Merits	Demerits
1	ParityCloud Service[2]	- Reliable - Privacy - Low cost	- Implementation - Complexity is high
2	HSDRT[1]	-Used for movable Client such as laptop,smart phone	- Costly - Increase redundancy
3	Linux Box[4]	-Simple -Low cost for implementation	-Require higher bandwidth - Privacy -Complete server backupAt atime
4	ERGOT[3]	-Perform exact match retrieval Privacy	-Time complexity -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 -Unable to includes optimization conceptwith cost reduction

Table-1 Comparison between various backup and recovery technique

III. REMOTE DATA-BACKUP SERVER

The backup server of main cloud is nothing but the copy of main cloud. When this server is remotely located and they having complete copy of main cloud, then this remotely located server called as Remote Data Backup Server where as main cloud known as central repository and remote cloud known as remote repository.In case of central repository lost its data in some situations i.e.earthquake,flood, fire etc.). or that can be happen through human attack like file deletion at that time it uses the data store in remote repository.

The main purpose of remote backup is to collect the information from only remote location and or data not found in main cloud as shown in diagram user can access data from remote server if that not found over the central repository.

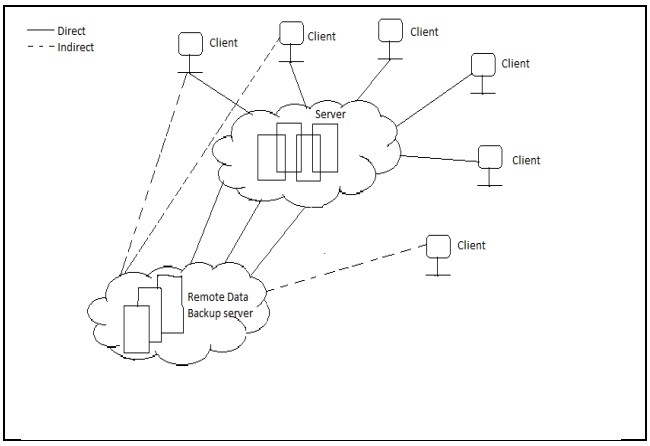

Fig1.Remote Data Backup server and Its Architecture

Remote Data-backup provide following services :

1) Data Security
2) Data Integrity
3) Data Confidentiality
4) Trustworthiness
5) Cost Efficiency

IV. STRATEGY OF SEED BLOCK ALGORITHM

There are many techniques which will be discussed in literature servey i.e. HSDRT[], PCS[], ERGOT[], Linux Box[], Cold /Hot Backup Technique[], SBBR[] etc. but these technique having some issues with different circumstances. To handle these issues we propose seed block algorithm.

The algorithm concerns about the simplicity of backup and recovery process. SBA uses exclusive OR(XOR) operation for computation. e.g. We having two data files A and B A+B produces X .When A file may be destroy or delete and we want that file so can be retrieve by using X-OR of file X and B i.e A=X B

Fig 2 shows the architecture of main cloud with its clients and remote server, users get unique id as well as set random numbers in cloud. when the client id register in main cloud then client id and random number is getting X-OR to generate seed block for that particular client.To generate seed block correspond to each client is stored in remote server. Whenever client generate the file initially in cloud that stored in main cloud.When it stored in main server that file being X-ORed with seed block of particular client. The X-ORed file is stored in remote server. In case file damaged or deletion in main cloud at that time user can get original file with X-ORing that file with seed block of particular client to getting the original file.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

ALGORITHMS USED

A. Seed Block Algorithm(SBA)

Initialization: Main Cloud: $\mathbf{M_c}$; Remote Server: $\mathbf{R_s}$;
Clients of Main Cloud: $\mathbf{C_i}$;Files:$\mathbf{a_1}$ and $\mathbf{a_1}$;
Seed block: $\mathbf{S_i}$; Random Number**: r ;**
Client's ID: ***Client_ID***
Input: $\mathbf{a_1}$created by $\mathbf{C_i}$**; r** is generated at $\mathbf{M_c}$;
Output: Recovered file $\mathbf{a_1}$after deletion $\mathbf{M_c}$ at
Given: Authenticated clients could allow uploading, downloading and do modification on its own the files only.

Step 1: Generate a random number.

$$intr = rand(\ );$$

Step 2: create a seed Block $\mathbf{S_i}$ for each $\mathbf{C_i}$ and Store $\mathbf{S_i}$ at $\mathbf{R_s}$

$\mathbf{S_i}$ = **rClient_ID**

(Repeat step 2 for all clients)

Step 3: If $\mathbf{C_i}$ **/Admin** creates/modifies a and stores $\mathbf{a_1}$ at $\mathbf{M_c}$,
then$\mathbf{a'_1}$create as
a'1=a1 Si
Step 4: Store **a'** at $\mathbf{R_s}$.
Step 5: If server crashes $\mathbf{a_1}$ deleted from $\mathbf{M_c}$,
then, we do EXOR to retrieve the original a_1 as:
$\mathbf{a_1 = a'_1\ S_i}$
Step 6: Return $\mathbf{a_1}$ to $\mathbf{C_i}$.
Step 7: STOP.

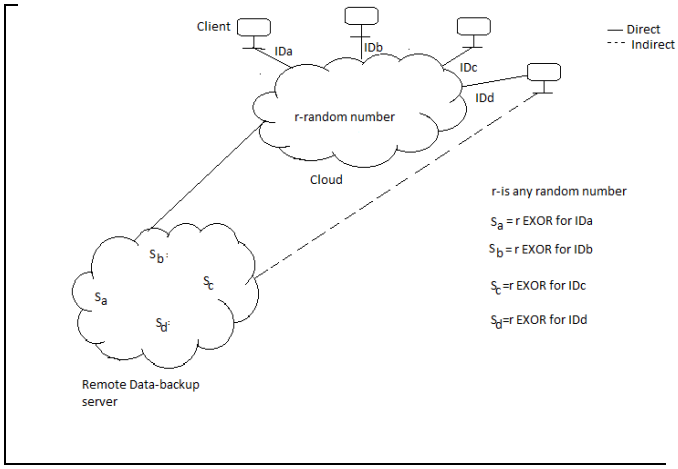

Fig 2.SBA Architecture

AdvancedEncryption StandardAlgorithm

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 respectively.Symmentric or secret-keyciphers use the same key for encrypting and decrypting,so boththe sender and receiver must know and use of 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 ciphertext.

Initialization:String encrypt (String Data)
Key key=generate key();
Cipher c=Cipher,getInstance (ALGO);
c.init(cipher,encrypt.MODE,Key);
byte[] enval=c.dofinal(Data.getbytes());
StringencryptedValue= new BASE64Encode().
encode(encVal);
Return encrypted Value
Key generatekey
Key key=new Secret keyspec(keyValue.ALGO)
returnkey;

V. IMPLEMENTATION AND RESULT OFPROPOSED SYSTEM

This section is about the system requirement and that should be minimal for main cloud and remote server. During the implementation, we observed that the size of original file uploaded by the client over thecloud is exactly same as sizof backup file which is stored at the remote server and is same about the different types of file.So we can say that SBA is capable to maintain the size of recovered file compare to the original file.Finally we say that SBA recover the file without data loss.

Type	size of original file	Size of backup file	Size of recovered file
Text(txt/doc/pdf xl/)	540KB	540KB	540KB
	3MB	3MB	3MB
Image(jpeg/png Gif/)	826KB	826KB	826KB
	5MB	5 MB	5MB

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 or cloud can be destroyed.According to the result we can say that SBA focuses on security for backup the file stored at the remote server.SBA also reduce the time required to recover the file.

ACKNOWLEDGEMENT

Special thanks to our guide for giving such a helpful guidance.

REFERENCES

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

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

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

[4] Xi Zhou, Junshuai Shi, YingxiaoXu, 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.

[5] Ms..KrutiSharma,ProfK.R.Singh, 2012, "Online data Backup And Disaster Recovery techniques in cloud computing:A review", JEIT, Vol.2, Issue 5.

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