ISSN 2395-1621

A Remote Smart Data Back-up Technique Using Cloud Computing

Jamadar Ruksana[#1] , Shinde Sarika[#2],Mande Deepika[#3]

[1]ruksanajamadar217@gmail.com
[2]shindesarika22@gmail.com
[3]mandedipika98@gmail.com
[#123]Dept. of Computer Engineering
H.S.B.P.V.T's COE,
Savitribai Phule, Pune University,
Kashti, Ahmednagar, Maharashtra.

ABSTRACT

Cloud computing, generated data in electronic form which are very large in amount. There is a requirement to maintain this data efficiently of data recovery services. To fulfil these requirements, we discussed Remote Smart Data Back-up Technique Using Cloud Computing (SBA) we propose. There are two objectives of our proposed system, Firstly, it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed or crashed due to any reason. Proposed SBA will take small time of recovery process. So that the time related issues are being solved by Proposed Seed Block Algorithm. It dose use used any of the existing encryption techniques ,proposed SBA and also focuses on the security or privacy concept for the back-up files stored at remote server.

Keywords: **Central Repository, Remote Repository, Parity Cloud Service, Seed Block, Backup, Privacy.**

ARTICLE INFO

Article History

Received : 13th April, 2015

Received in revised form :

16th April, 2015

Accepted : 21st April, 2015

Published online :

24th April, 2015

I. INTRODUCTION

Cloud computing provide us to online data storage where data stored in form of virtualized pool that is usually hosted by third parties. There are number of client share the resources and memory .So that it is possible that other customers can access your data. . The cloud computing also gigantic technology which is surpassing all the previous technology of computing like cluster, grid, etc. Remote data integrity is required because, to archiving and taking backup of data, the services are not limited. Because, the complete state of the server that takes care of the heavily generated data which remains unchanged during storing at main cloud remote server and transmission.

Network access to a share pool of configurable computing service, National Institute of Standard and Technology defines as a model for enabling convenient that can released with minimal management effort or services provider and provisioned rapidly. . Our cloud storage may be destroy and danger due to either human errors faulty equipment's, a bug, any criminal attack or network connectivity. And the changes in the cloud may also be made frequently, which is also called as data dynamics. The data dynamics is supported by various operations such as insertion, deletion and block modification. To overcome the disadvantages of previous computing techniques, the need of cloud computing increasing now a days due to its advantages. On large data center the hosting company operates large data and according to the requirements of the customer these data center virtualized the resources and expose them as the storage pools that help user to store files or data objects.

For back-up and recovery services integrity is very important.

II. LITERATURE SURVEY

In literature many techniques have been proposed, which are HSDRT[1], PCS[2], ERGOT[4], Linux Box [5], Cold/Hot backup strategy [6] etc. These all techniques discussed the data recovery process. However, behind the various successful techniques, there are same critical issue like, implementation complexity, low cost, security and time related issues. To fulfil these issues, in this paper we propose a smart remote data backup algorithm, Seed Block Algorithm (SBA). There are two objectives of our proposed system, first it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason.

2.1 Performance Evaluation of a Disaster Recovery System and Practical Network System Applications:

In this paper author presents evaluation results for a high security disaster recovery system using distribution and rake technology. In an experimental evaluation, the encryption and spatial scrambling performance and the average response time have been estimated in terms of the data file size. Discussion is also provided on an effective shuffling algorithm to determine the dispersed location sites. Finally, this paper describes a proto type system configuration for several practical network applications, including the hybrid utilization of cloud computing facilities and environments which are already commercialized.

2.2 Parity Cloud Service (PCS): A Privacy-Protected Personal Data Recovery Service

As most data are generated in an electronic format, the necessity of data recovery service became larger and the development of more efficient data recovery technology and backup has been an important issue during the past decade. While lots of effective recovery and backup technologies, including data DE duplication and incremental backup have been developed for enterprise level data backup service, few works have been done for personal efficient data recovery service. Since the privacy protection and security is a crucial issue for providing a personal data recovery service, a plain data back-up based recovery service is not adequate for public service. Users are unexpected to upload their critical data to the internet backup server until they can fully trust the service provider in terms of the privacy protection. In this paper, we propose a data recovery service framework on cloud infrastructure, a Parity Cloud Service (PCS) that provides a privacy-protected personal/private data recovery service [7] [9].

The proposed framework does not require any user data to be uploaded to the server for data recovery. Also the necessary server-side resources for providing the service are within a reasonable bound. In the backup system proposed file backup mechanism, the combination of the following technologies such as a subsequent random fragmentation of the file, a spatial random scrambling of file data, the corresponding encryption and duplication for each fragmented one by using a stream cipher in each encryption stage, and the corresponding notification of the history data of the used encryption key code sequence which we call metadata in addition can effectively realize the prompt file backup and highly secure system economically only when they are combined at the same time. In case of disaster occurrences in data backup centre, the prompt data recovery can be easily and securely achieved by making use of a widely distributed great amount of PCs or cellular phones via several supervisory servers which are secretly diversified and functionally combined mutually. This paper proposes the above mentioned state-of-the art hybrid disaster recovery mechanism and its basic characteristics.

2.4 ERGOT: Distributed Infrastructures of a Semantic-based System for Service Discovery

Semantics to enable their precise and efficient retrieval. Two common approaches toward this goal are Distributed Hash Tables (DHTs and Semantic Overlay Networks (SONs with semantic extensions. This paper presents ERGOT, a system that combines SONs [8] and DHTs [9] to enable semantic-based service discovery in distributed infrastructures such as Clouds and Grids . ERGOT takes advantage of semantic annotations that enrich service specifications in two ways: first services are advertised in the DHT on the basis of their annotations, thus allowing to establish a SON among service providers, second annotations enable semantic-based service matchmaking, using a novel similarity measure between service descriptions and requests. Experimental evaluations confirmed the efficiency of ERGOT in terms of accuracy of search and network traffic.

III. PROPOSED SYSTEM

We think, Backup server is duplicate of main cloud. When this Backup server is at far away from the main server and having the complete state of the main cloud, then this remote location server is called as Remote Data Back-up server. The main cloud is called as the central repository and remote backup cloud is called as remote repository.

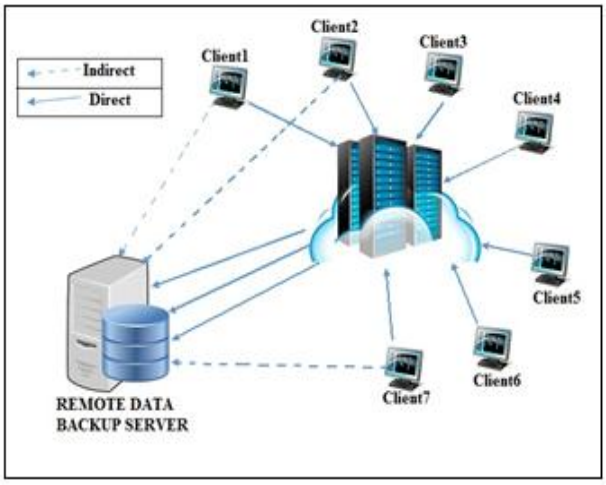

Fig 1: Architecture of Remote data Backup Server

When the central repository loss/lost its data under any circumstances either of any natural calamity or by human attack or deletion which has been done mistakenly and then it uses the information from the remote repository. The main purpose of the remote backup facility is to help user to collect information from any remote location if network connectivity is not available or if data not found on main cloud. As shown in Fig-1 If the data is not found on central repository clients are allowed to access the files from remote repository (i.e. not directly).The Remote backup services should cover the following issues:

1) Information Integrity

Information Integrity is certain with complete state and the whole structure of the server. It is the measure of the validity and fidelity of the data present in the server. It verifies that data such that it does not changed during translate process and reception.

2) Information security

Giving full protection to the client's data is also the utmost priority for the remote server. And either unintentionally or intentionally, it should be unable to access by third party or any other users/client's.

3) Information Confidentiality

Sometimes client's data files should be kept confidential such that if no. of users one by one accessing the cloud, then data files that are personal to only particular client must be able to hide from other clients on the cloud during accessing of file.

4) Trustworthiness

The remote cloud must possess the Trustworthiness characteristic. Because the client /user stores their private data; therefore the cloud and remote backup cloud must play a trustworthy role.

5) Cost efficiency

The cost of process of data recovery should be efficient so that most of company/clients can take advantage of back-up and recovery service.

IV. DESIGN OF THE PROPOSED SEED BLOCK ALGORITHM

Many techniques have been proposed for recovery and backup which are HSDRT[1], ERGOT[4], PCS[2], Linux Box[5], Cold/Hot backup strategy[6] etc. security, Less implementation complexity, low cost, and time related issues are still challenging in the field of cloud computing. To overcome these issues we propose SBA algorithm, we will discuss the design of proposed SBA in detail.

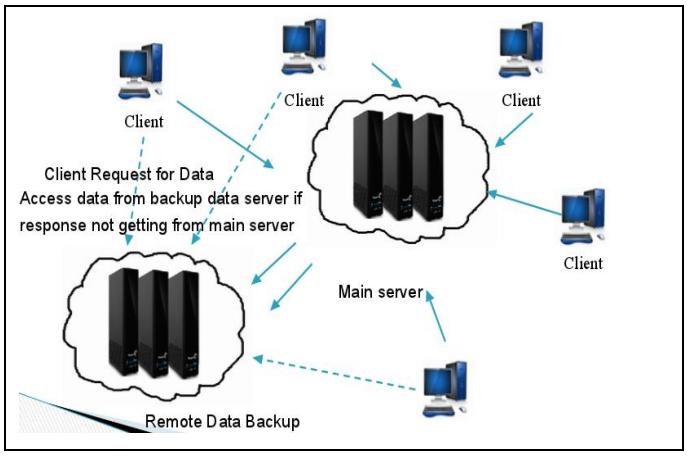

Fig. 2. System Architecture

Seed Block Algorithm (SBA) architecture:

The main purpose of this algorithm is focuses on simplicity of the recovery and back-up process. In this algorithm uses the concept of Exclusive– OR (XOR) operation of the computing world. For ex: - Suppose there are two data files: A & B. When we XOR A & B it produced X. If we want our A data file back which was destroyed then we are able to get A data file back, then it is very easy to get back it with the help of B & X data file. The Seed Block Algorithm works to provide the simple recovery and Back-up process. The architecture of this algorithm is shown in Fig.2. Fig.2 consist of the Main Cloud and it's the Remote Server and clients. 1st we set a random number in the cloud and unique client id for every client. 2nd, whenever the client id is being register in the main cloud; then client id and random number is getting EXORed ( ) with each other to generate seed block for the particular client. The generated seed block corresponds to all each client is stored at remote server.

When client upload the file in cloud first time, it is stored at the main cloud. When it is stored in main server, the main file of client is being encrypted using EXORed with the Seed Block of the particular client. And that EXORed file is stored at the remote server in the form of file'(dash file). If either unfortunately file in main cloud damaged /crashed or file is been deleted mistakenly, then the user will get the original file by EXORing file' with the seed block of the corresponding client to produce the original file and return the resulted file i.e. original file back to the requested client.

SBA Algorithm

Initialization: Main Cloud:M_C Remote Server: R_S;

Clients of Main Cloud: C_i; Files:a_1 and a_1';

Seed block:S_i; Random Number:r ;

Client's id:$Client\_Id_i$

Input:$a_1$make by C_i; $r$is generated at M_c;

Output: Recover file$a_1$after deletion atM_c

Given: Authenticated clients could allow downloading uploading and do modification on its own the files only.

Step 1: Generate a random number [rand()].

Int $r = rand\ ()$

Step 2: Create a seed Block S_i for each $C_i$and Store

S_i at R_ε

$S_i = r \oplus Client\_Id_i$(Repeat step 2 for all clients)

Step 3: If$C_i/Admin$creates/modifies aa_1 and stores

atM_c,

then a_1'create as

$a_1' = a_1 \oplus S_i$

Step 4: Storea_1' at S_i

Step 5: If server crashesa_1 deleted from M_c,

then, we do EXOR operation to retrieve the original asa_1: $a_1 = a_1' \oplus S_i$

Step 6: Returna_1 toC_1.

Step 7: END.

V. Result Analysis

In this section, Depending on the how much security is present. The data recovery is becoming easy. For the main cloud's server and remote server respectively, as we are in the initial stage we will definitely handles all the .

we studied the experimentation and result of the SBA algorithm. For experimentation we focused on different minimal system requirement for main cloud's server.

V. Conclusion

In this paper ,we can concluded that Proposed SBA is helping the users to collect information from any remote location in the absence of network connectivity and also to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason.

The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process**.**

VI. REFRENCES

[1]. Yoichiro Ueno, Noriharu Miyaho, Kazuo Ichihara Shuichi Suzuki, Muzai Gakuendai, Inzai-shi, Chiba, , 2010, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications,pp 256-259.

[2]. Chi-won Song, Dong-wook Kim, Sungmin Park, Sooyong Kang, 2011, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.

[3]. Y.Ueno, S.Suzuki, N.Miyaho, 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.

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

[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, 2011.

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

[7]. Xi Zhou, Junshuai Shi, Weiwei Sun, Yingxiao Xu and Yinsheng Li and 2008, "A backup restoration algorithm of service composition in MANETs," Communication Technology ICCT 11th IEEE International Conference, pp. 588-591.

[9]. M. Armbrust et al, "Above the clouds: A berkeley view,cloud computing,"http://www.eecs.berkeley.edu/Pubs/Tec Rpts/2009//EECS-2009-28.pdf.

[10]. F.BKashani, C.Shahabi.WSPDS , C.Chen, , 2004, "Web Services Peerto- Peer Discovery Service ," ICOMP.

[11] Eleni Palkopoulouy, Thomas Bauscherty, Dominic A. Schupke, 2011, "Recovery Time Analysis for the Shared Backup Router Resources (SBRR) Architecture", IEEE ICC.

[12] Lili Sun, Jianwei An, Ming Zeng, Yang Yang, 2011, "Recovery Strategies for Service Composition in Dynamic Network," International Conference on Cloud and Service Computing, pp. 221–226.

[13] P.Demeester et al., 1999, "Resilience in Multilayer Networks," IEEE Communications Magazine, No. 8 , p.70-76, Vol. 37.

[14] S. Zhang, X. Chen, and X. Huo, 2010, "Cloud Computing Research and Development Trend," IEEE Second International Conference on Future Networks, pp. 93-97.

[15] S. L. Linfoot and T. M. Coughlin, 2010, "A Novel Taxonomy for Consumer Metadata," IEEE ICCE Conference.

[16] K. Keahey, , A. Matsunaga, M. Tsugawa, J. Fortes, 2009, "Sky Computing", IEEE Journal of Internet Computing, vol. 13, pp. 43-51.

