Remote Data Collection Server: E-Health Care

Kalyani Bangale[1], Nivedita Gupta[2], Swati Singh Parihar[3] , Karishma Nadhe[4], Gunjan Mankar[5]

Student, Dept. of CSE, DBACER, Nagpur, India[1,2,3,4]

Lecturer, CSE, DBACER, Nagpur, India[5]

ABSTRACT: Remote data collection server means the data which is collected can be stored and access from remote distance. So the objective of Remote Data Collection Server is to provide Auto Response Server, Better Solutions for Data Backup and Restore using Cloud, Availability of data remotely using safer protected data transmission and Confidentiality of data remain intake. It can collect data and send to a centralized repository in a platform independent format without any network consideration. The central repository is also a source for other vendors/depts. to use the information for their specific requirement. This paper presents a method to secure data collection server by protecting and developing backups using Cloud Server.

KEYWORDS: Seed block algorithm; Cloud Server; Remote repository; Data Backup and Restore;

I. INTRODUCTION

The data files or information regarding clients which is stored in computer or laptop is lost due to hardware problem like if the system gets physically crashed or data gets corrupted then there is no other source to recover it. It is very tedious job to manage various client records since work is done manually and there are lots of chances of that errors can occur in maintaining the users and there is large data storage problem in centralized system. So the data is lost from main server and there is no other backup facility to restore this data. So this application provides a feasible solution that collects data and sends it to a centralized storage location smartly and we can access the data remotely.

Remote Data Collection server includes E-Health Care Service which delivers services to doctors and users. This application is powerful, flexible, and easy to use and is designed and developed to deliver benefits to doctors and users. More importantly it is backed by reliable and dependable Health Care Server support. The data backup and restore is done through cloud server.

Cloud storage provides online storage where data stored in form of virtualized pool that is usually hosted by third parties. The hosting company operates large data on large data centre and according to the requirements of the customer these data centre virtualized the resources and expose them as the storage pools that help user to store files or data objects. The need of cloud computing is increasing day by day as its advantages overcome the disadvantage of various early computing techniques.

II. RELATED WORK

In literature, different algorithms are already define for recent back-up and recovery techniques that have been developed in cloud computing domain such as HSDRT[2], PCS[3], ERGOT[4],Linux Box [5], Cold/Hot backup strategy [6] .The following review shows that none of these techniques are able to provide best performances under all circumstances such as cost, security, low implementation complexity, redundancy and recovery in short span of time A survey and comparison of these techniques are given as follows.

PCS is comparatively reliable, simple, easy to use and more convenient for data recovery totally based on parity recovery service but it is unable to control the implementation complexities [3]. On the contrary, HSDRT has come out an efficient technique for the movable clients such as laptop but it fails to manage the low cost for the implementation of the recovery and also unable to control the data duplication [2].

Rather, ERGOT provides efficient way of retrieval of that is based on the semantic analysis but is unable to focus on time and implementation complexity [4]. Similarly, we also found that one technique in addition, Linux Box model is having very simple concept of data back-up and recovery with very low cost. However, in this model protection level is very low [5]. Similarly, we also found that one technique basically focuses on the significant cost reduction and router failure scenario i.e. (SBBR) [8]. The lowest cost point of view we found a model "Rent Out the Rented Resources". Its goal is to reduce the cloud service's monetary cost. It proposed a three phase model for cross cloud federation that are discovery, matchmaking and authentication. This model is based on concept of cloud vendor that rent the resources

from venture(s) and after virtualization, rents it to the clients in form of cloud services[9].

All these techniques tried to cover different issues maintaining the cost of implementation data increases i.e. cold and hot back-up strategy [6] that performs backup and recovery on trigger basis of failure detection. And due to the high applicability of backup process in the companies, the role of a remote data back–up server is very crucial and hot research topic.

III. PROPOSED PLAN

In cloud computing, data generated in electronic form are large in amount so to maintain this data efficiently, there is a necessity of data recovery services. To solve this, in this paper we propose a smart remote data backup algorithm, Seed Block Algorithm. The objective of proposed algorithm is to help the users to collect information from any remote location in the absence of network connectivity and 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. Proposed SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques.

In proposed system, the data which will be lost due to certain conditions like if the system gets physically crash can be recovered using cloud server. Most of the organization including government as well as private can use this software to prevent from data loss permanently.

A. *Remote Data Backup Server:*

A backup server sometimes marketed as cloud backup, is a service that provides users with a system for the backup, storage, and recovery of computer files. When this Backup server is at remote location (i.e. far away from the main server) then this remote location server is termed as Remote Data Backup Server. The main cloud is termed as the central repository and remote backup cloud is termed as remote repository.

1) *Architecture:*

The architecture of remote data backup server is shown in Fig.1.It contains various clients, repository (web service), main database, users and architecture is explained as follows.

The client application can be ported to any other machine like laptop or handheld devices. The stored data is platform independent that are sent to a central repository. When connected to network, the client application is authenticate into a central repository using a web service and submit all collected information. And if the central repository lost its data under any circumstances either of any natural calamity (for ex - earthquake, flood, fire etc.) or by human attack or deletion that has been done mistakenly and then it uses the information from the remote repository. The main objective of the remote backup facility is to help user to collect information from any remote location even if network connectivity is not available or if data not found on main cloud. As shown in Fig.1 clients are allowed to access the files from remote repository if the data is not found on central repository (i.e. indirectly).
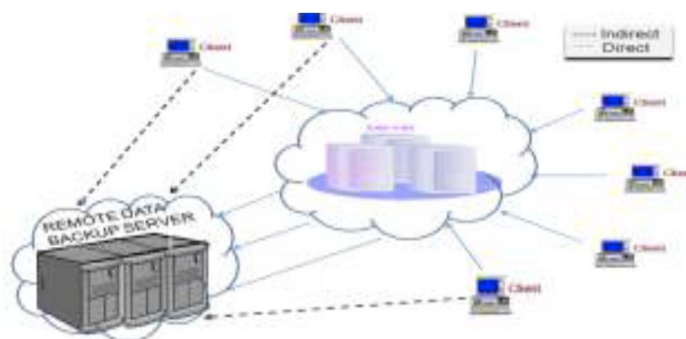

Fig.1.Remote Data Backup Server

2) *Characteristics of Remote Data Backup Server:*
1) Flexibility: Any new facility or the new work can be added easily. It is extremely adaptable, with the ability to be used in a variety of environments.
2) Portability: It can work in any environment thus it is able to collect application data from various application similarly as in a platform independent way.
3) Proper Backup Facility: Database is centralized, recover same size data.
4) Reliability: It possesses the reliability characteristic. Because the user/client stores their private data; therefore the cloud and remote backup cloud must play a reliable role.
5) Maintenance: It is easy to maintain because of cloud computing application, they do not need to be installed on each user's computer and can be accessed from different places.

B. *Role of Users:*

Fig.2 shows two main users of the system that is internal user and external user. Internal user consists of administrator and doctors. The second main user is external user that consist of patients or general user. Data related to both internal user and external user is stored in the database. Then backup from this database is taken into the cloud server and if required data can be restored from the cloud server.
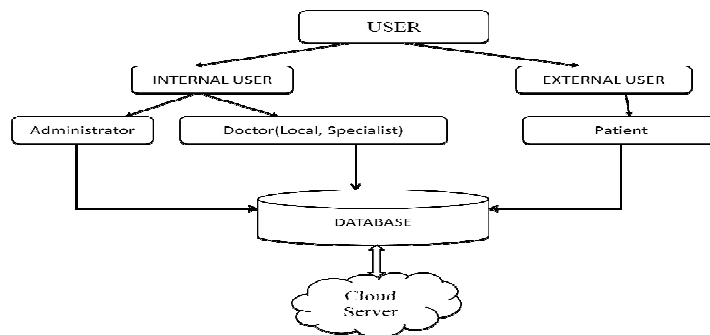

Fig. 2 .Users and Roles

C. *Algorithm Technique:*

The algorithm technique in Remote Data Collection Server is Seed Block Algorithm (SBA) which focuses on simplicity of the back-up and recovery process. It basically uses the concept of Exclusive-OR (XOR) operation of the computing world.Suppose there are two data files: A and B. When we XOR A and B it produced X i.e. $X = A \text{ XOR } B$. If suppose A data file get destroyed and we want A data file back then it is very easy to get back it with the help of B and X data file .i.e. $A = X \text{ XOR } B$.

a) Original file   b) EXORed file   c) Recovered file

Fig. 3. Sample output image of SBA Algorithm

As fig-3(a) shows the original file which is uploaded by the client on main cloud. Fig-3 (b) shows the EXORed file which is stored on the remote server. This file contains the secured EXORed content of original file and seed block

content of the corresponding client. Fig-3 (c) shows the recovered file; which indirectly sent to client in the absence of network connectivity and in case of the file deletion or if the cloud gets destroyed due to any reason.

IV. PSEUDO CODE

Initialization: Main Cloud: M_c; Remote Server: R_s; Clients of Main Cloud:C_i;Files:a_1 and a_1';
             Seed Block: Si; Random Number: R_i; Client's Id: $Client\_Id_i$.

Input: a_1 created by c_i ;r is generated at M_c.

Output: Recovered File a_1 after deletion at M_c.

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

Step 1: Generate a random number.
         int r=rand( );

Step 2: Create a Seed Block for each C_i and Store S_i at R_s.
         S_i=r XOR $Client\_Id_i$ (Repeat Step2 for all clients).

Step 3: If C_i/Admin creates/modifies a_1 and stores at M_c,
         then a_1' creates as
         a_1' =a_1 XOR S_i;

Step 4: Store a' at R_s;

Step 5: If server crashes a_1 deleted from M_c, then we do
         XOR to retrieve the original a_1 as
          a_1=a_1' XOR S_i;

Step 6: Return a_1 to C_i.
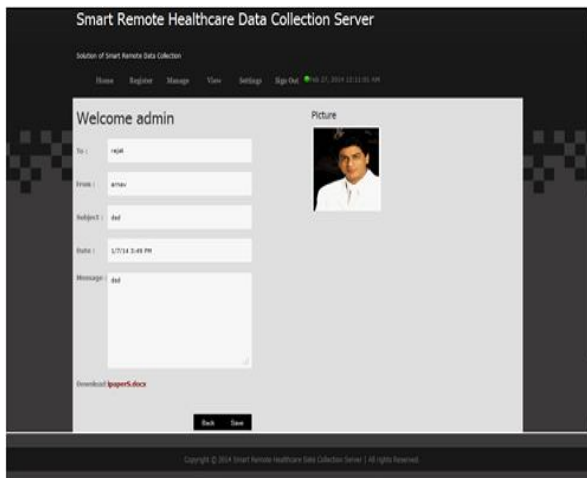
Step 7: End.
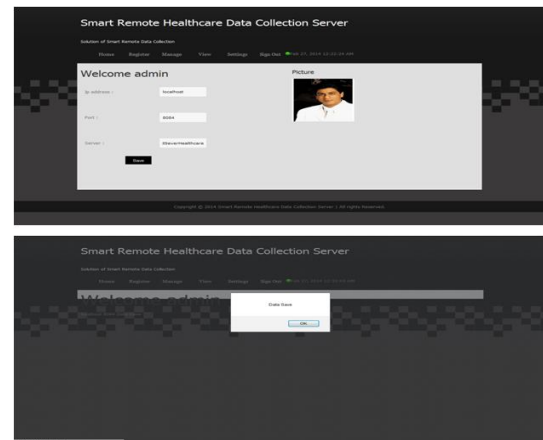
V. SNAPSHOTS

Fig.4. Select data for backup

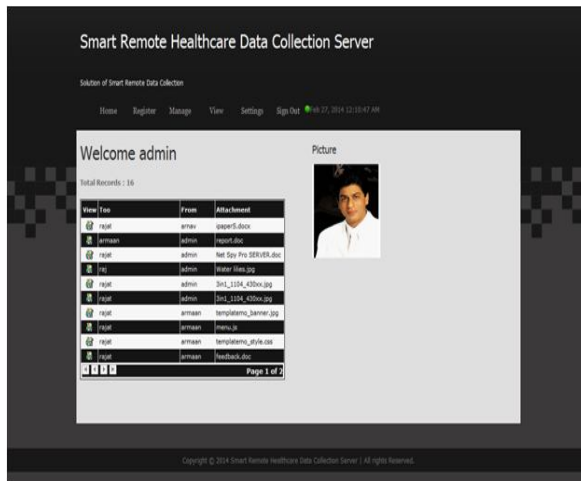Fig. 5. View details of selected data
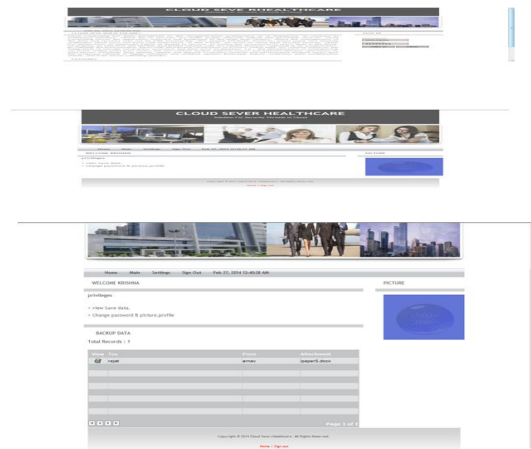
Fig.6. Enter details and saving data

Fig.7. Cloud Server, Cloud Home and View saved data

The above figure shows data saving process in cloud. Fig4 shows admin selects data for backup. On selecting the view option the details of data are shown as in Fig5. If admin selects the save option then connection details must be filled and data is saved in cloud as shown in Fig.6. Fig.7 shows cloud server, cloud home and saved data on cloud.

VI. CONCLUSION

Due to computerization and availability of data from remote location , vast amount of data is going to be collected on the web servers. It helps in reducing allocation of geographical area required for storing records and also promotes paperless work. Time consumed for searching required documents is less. Thus we propose a novel resource allocation algorithm for cloud system that supports VM-multiplexing technology, aiming to minimize user's payment on his/her task. Every organization prefers computerization as well as remotely accessible web services. Hence data security and protection comes in highest priority so recent developments will be on securing and protecting data collection on web server. Thus, Remote Data Collection Server aims the same.

REFERENCES

1. Harsha Girish Chandra, 'Remote Data Collection and Analysis using Mobile Agents and Service- Oriented Architectures',2008.
2. Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai,Inzai-shi, Chiba,Kazuo Ichihara,'Performance Evaluation of a Disaster Recovery System and Practical Network SystemApplications ', Fifth International Conference on Systems Networks Communications.
3. Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, 'Parity Cloud Service: A Privacy Protected Personal Data Recovery Service', International Joint Conference of IEEETrustCom-11/IEEE ICESS-11/FCST-11,2011.
4. Giuseppe Pirr´o, Paolo Trunfio , Domenico Talia, Paolo Missier andCarole Goble,,'ERGOT: A Semantic-based System for ServiceDiscovery in Distributed Infrastructures,'10th IEEE/ACMInternational Conference on Cluster, Cloud and Grid Computing,2008.
5. Vijaykumar Javaraiah , ' Backup for Cloud and Disaster Recovery for Consumers and SMBs', IEEE 5th InternationalConference, 2011.
6. Lili Sun, Jianwei An, Yang Yang, Ming Zeng,,'RecoveryStrategies for Service Composition in Dynamic Network,' International Conference on Cloud and Service Computing,2011.
7. Ms..Kruti Sharma,Prof K.R.Singh, 'Online data Backup And Disaster Recovery techniques in cloud computing:A review', IJEIT, Vol.2, Issue 5,2012.
8. Eleni Palkopoulouy, Dominic A. Schupke, Thomas Bauscherty,'Recovery Time Analysis for the Shared Backup Router Resources (SBRR) Architecture', IEEE ICC,2011.
9. Sheheryar Malik, Fabrice Huet, 'Virtual Cloud:Rent Out the Rented Resources', 6th International Conference on Internet Technology and Secure Transactions, 2011.