JOURNAL OF PURE AND APPLIED MICROBIOLOGY, May 2015. Vol. **9**(Spl. Edn. 1), p. 653-664

Efficient Novel Framework for Disaster Recovery in Healthcare Cloud Computing using EDRSA Algorithm and Virtualization Mechanism

S. Suguna[1] and A. Suhasini[2]

[1]Department of Computer Science and Engineering,
Annamalai University, Chidambaram- 608002, India.
[2]Department of Computer Science and Engineering,
Annamalai University, Chidambaram- 608002, India.

(Received: 10 February 2015; accepted: 11 April 2015)

Disaster occurrence may cause extensive misfortunes in the medical data base and a little amount of information loss leads to the mismatches in the health details within the medical database. So, it is necessary to pursue the disaster recovery and data protection technique to prevent data loss from the event of disaster. The disaster recovery procedure is identified with the continuation of technology infrastructure which is imperative to an medical data base in the cloud environment. The research of this paper proposed an EDRSA algorithm (Efficient Disaster Recovery Swist algorithm) for the process of automatic setting of Recovery Process Objective (RPO), Recovery Time Objective (RTO) and novel approach by utilizing the virtualization machine of Hybrid VMware VSphere. The virtual machines are booted from the virtual disk images that are stored in the cloud storage. The cloud framework has the capacity to run as one of the large file, even in the occurrence of any disaster. The RTO focused on the data retrieval time after a disaster has occurred and RPO set an objective point between the last backup and before the occurrence of disaster. This paper assessed the efficient improvement in Disaster Recovery by using an Swist algorithm for RTO and RPO under diverse conditions regarding metrics improvement and essential identification of disaster data in the healthcare cloud computing. Nonetheless, disaster losses of data can be reduced effectively to a maximum extent by establishing our proposed system model.

Key words: Disaster Recovery, virtual machine, Recovery Process Objective (RPO), Recovery Time Objective (RTO), healthcare cloud computing.

Cloud computing is a rising model of leading healthcare cloud computing. The computing tasks are circulated to a substantial number of computers, so that all applications can get the calculation capability, storage space and software services.A lot of people substantially depends on the web vicinity. The reason for disasters can either be unintended occasions, for example, power disappointment or purposeful, a denial of service attack. The data disaster recovery[6] is a sort of administration with most noteworthy data reliability requirements. The most effective method to perform data disaster recovery administration utilizing cloud computing ideal model to boost the data reliability by decreasing the expense is still a test. There is no distinction with other machine frameworks, whereas cloud computing framework can additionally experience certain dangers, for example, software bug, hardware fault, network intrusion, human-caused damage, natural disasters, and so on. These dangers might lead to cloud administration intrusion, even loss of data in a few cases.To assess the risk, the sorts of disaster (regular or artificial) need to be distinguished.

* To whom all correspondence should be addressed.
E-mail: sugunaresearch14@gmail.com

The different inventive virtualization technologies are leveraged to reallocate or restore server, network and storage resources to a basic application in view of medical necessities. Virtualization can help and address many of the challenges and barriers of traditionaldisaster recovery and help the medical field to meet the key goals of a viabledisaster recovery plan. For example, the challenges faced by the medical concern are the consequence of the physicalboundaries of equipment's. The encapsulation of virtual machines (VMs) means, rather thanmaintainingthe correspondingserver at a recovery site instead of maintaining each serverat the primary site, Medical concerns can replicatephysical servers or VMs from the primarysite to virtualized servers at therecovery site, helping to reduce the costof protection or to increase the numberof servers that can be protected by existing the recovery infrastructure.

The probability of a disaster event needs to be evaluated together with the cost of corresponding disappointments. A proper cost function needs to be characterized to permit a quantitative evaluation of presently dynamic disaster recovery plans (DRP) as far as time required to restore administration (connected with RTO) and conceivable loss of information (connected with RPO). This work presents rules for cost investigation of reinforcement alternatives utilizing cost functions which can be utilized for the improvement of the arrangement and upkeep of the DRP. To guarantee high data reliability, cloud administration suppliers have sent numerous data assurance methodologies. Therefore, an association must have a disaster recovery plan (DRP) which is executable, testable, versatile and viable. Such a plan must fulfil the cost stipulations while accomplishing the target recovery objectives, that is the recovery time objective (RTO) and recovery point objective (RPO). Recovery Point Objective (RPO) is the point in time to which the data should be recovered as defined by organization, generally called an "acceptable loss" ina disaster situation. It allows the medical database to define a window of time before the occurrence of disaster, when the data may belost and is tightly dependent on the type of datareplication used. The higher granularity of data replication, the shorter is the RPO.Medical field requires to set the goals plainly, and assess the disaster recovery plans to pick the DRP that would be ideal, while RTO is purely a technical metric, the decision to trigger the failover can be detected.

These technologies offer another ideal model in which different options come up with small operations are coordinated into the routine operational life cycle of these applications. Leveraging virtualization technologies empowers us to quickly enhance the execution or restore the application and subsequently minimize the interference of the administrations they give. The "Constant" application is intended to be non-problematic application of the investmentthat could be analyzedin minutes to hours of relying medical hazard tolerance and moderateness. The research of this paper makes an application to shaft resource utilization profile through cloud frameworks and VMware VSphere. In this medical field it consists of complete, scalable and powerful virtualization platform, delivering the infrastructure and application services that are required by the medical concern in order to transform their information technology efficiently. VSphere is the suite wherein virtual desktops are made and run using a blend server, network- and storage-virtualization, in which application is particular to the RTO, RPO and data integrity checks adapted and where the disaster losses can be reduced effectively to a maximum extent.

Related work

In the paper[1] utilized the Automation of end-to-end failover of mission critical virtualized application, a SAN network and EMCClarion based storage to a remote site and measurement of RPO and RTO. Recovery PointObjective (RPO) is the point in time to which it recovers the data as dictated by the queries of medical concerns.Recovery Time Objective (RTO) is the period of timeafter an outage in which the application and its datamust be restored to a predetermined state defined by RPO[2]. It results in increasing the performance optimization by allocating the right resources (by tuning CPU, cache, throughput, bandwidth andserver, network & storage I/O) to the chosen application basedon workload demands and business priorities, High Availability (HA) by providing instant failover and recovery application to its normal operation yet results in Instant disaster Recovery, from a remote secondarysite when the primary site fails.

In[3] investigated the work of organization which requires a disaster recovery plan (DRP) falls withincost constraints while achieving the target recoveryrequirements in terms of recovery time objective (RTO) andrecovery point objective (RPO). The organizations mustidentify the likely events that can cause disasters and evaluatetheir impact. The paper examines tradeoffs involved andpresents guidelines for choosing among the disaster recoveryoptions. The optimal disaster recovery planningshould takeinto consideration the key parameters including the initial cost,the cost of data transfers, and the cost of data storage. Theorganization data needs and its disaster recovery objectivesneed to be considered. To evaluate the risk, the types ofdisaster (natural or human-caused) need to be identified. An appropriateapproach for the cost evaluation needs to be determined toallow a quantitative assessment of currently active disaster recovery plans (DRP) in terms of the time need to restore theservice (associated with RTO) and possible loss of data (associated with RPO) , yet needs guidance in future development ofthe plan and maintenance of the DRP .

In[4] which is intended in managing multiple patient' s such VMware. Treating VM data protection separately from overall data protection plan is a replication of effort and an inefficient use of resources. Traditional agent-based approaches to protect the data increases the load on system resources, so it can nullify the primary benefits of virtualization. In addition, since most of the service providers do not offer a solution that covers multiple virtual machine environment and the medical concernsend up engaging multiple providers. The research of this paper [5] offers an integrated solution for end- to- end data protection needs for the organization, including the ability to protect both physical and virtual machines across operating systems or virtualization platforms but produces slighter inefficient results when network congestion occurs in virtual machines. The led of HS-DRT Systemto seek agentless solutions for the backup [7] and recovery of virtual machines. But since there are few solutions in the cloud that offer combined physical and virtual machine protection, HS-DRT system enterprises have been forced to use separate solutions for backing up physical and virtual machines.

Data security and privacy protection are the important issues of Cloud computing[8]. Key management of encryption techniques in the cloud environment provides a separation of sensitive data form non-sensitive data and the isolates the of privacy data protection. In[9] the cloud computing technology is implemented in the medical science. This is identical way of analyzing and curing the disease, cloud computing plays a major role in providing the impact on medical field and contributes an overall improvement in its quality. Cloud security protocols are utilized for authenticated treatment, so that the encrypted information are uploaded in the cloud to enhance the security to the information.Different data[10] scheduling strategies based on DR-Cloud are suitablefor different kinds of data disaster recovery scenarios in the HR-DRT for high security. Experimental results show that the DR-Cloud model cancooperate with cloud service providers with various parameters for effective and high secureduring data scheduling strategies. It canachieve optimization objectives efficiently and widely applicable but results in multiple data center failures in a same period due to some common causes across data centers.

In[11] proposed the Datacenter consolidation by way of x86 virtualization is a trend which has gained tremendous momentum and offers many benefits. One workload type that is generally considered a virtualization candidate is Microsoft SQL Server. Although the physical nature of Microsoft SQL Server is transformed once it is virtualized, the necessity for data protection, retention, and recovery remains. The author in[12] dissected the work of VMware VCenter SiteRecovery Manager (SRM) designed to minimize the scheduled and unscheduled downtime caused by avariety of events, including the system failures, sitedisasters, user errors, data corruption, and maintenance tasks. VMware VCenter SRM is a workflow tooldesigned to accelerate and support successful recoveriesby automating the recovery process, helping to eliminate the complex manual recovery steps, andenabling non-disruptive testing. By taking advantageof the inherent disaster recovery capabilities of theVMware Infrastructure virtualization platform andarray-based replication using Dell hardware, thisarchitecture can help significantly simplify the

planningand execution of disaster recovery strategies but Design services can provide a comprehensive compensation.This document identifies a variety of options available for providing an automated disaster recovery solution for virtualized SQL Server workloads using Dell Compellent Storage Center, Replay Manager with varying levels of consistency yet inconsistent with unmatched capabilities to meet RTO and RPO requirements when compared to legacy[13] disaster recovery plans and physical servers.

The author in[14] investigated the work of multi-cloud based disaster recovery service with DR-Cloud, resources of multiple cloud service providers can be utilized cooperatively by the disasterrecovery service providerDR-Cloud proposes multiple optimization scheduling strategiesto balance the disaster recovery objectives, such as high data reliability, low backup cost, and short recovery time,which are also transparent to the customers. In order to achieve high flexibility the data are outsourced to the public cloud[15], which is also used to reduce the cost. Based on the simple keyword search on cloud computing is used to reduce the data utilization by encrypting the secure data. This searching service mandatory provides the ranking results while retrieving the stored files. Dell offers entry-level, mid-range, andhigh-end server and storage clusters built fromstandards-based components and designed toincrease availability by removing single points of failure within the cluster[16]. At each cluster level, Dell alsoprovides the ability to recover from additional failures,helping to protect against multiple component failures. . A simple and unified interface is exposed to the customers of DR-Cloud to adapt theheterogeneity of cloud service providers involved in the disaster recovery service[19], and the internal processes within clouds are invisible to the customers. Encryption standards in[20] cloud computing provides the key assumption and the data sharing in between the systems possess the access policies by escrow-free key issuing technique, in order to achieve efficient and secure data storage and distribution.

MATERIALS AND METHODS

Proposed disaster recovery system architecture

The cloud computing environment is a network-based, distributed data processing system that provides cloud computing services. The need for enhanced quality, efficiency, and predictability for disaster recovery [18] has increased significantly, highlighting the necessity of a well-defined set of recovery plans and regular testing. The cloud operating system comprises a module of automated computing machinery with multiple clouds, comprising a self-service portal and a deployment engine through a user interface exposed by the self-service portal, user specifications of the VM.

The virtual machine center ('VMC') in the cloud environment is deployed for the disaster recovery, where the VM is the module of automated computing machinery installed upon a cloud computer disposed within a medical database. The medical data base with respect to the VMsubject in which the VM is deployed for disaster recovery. The Fig. 1 includes a recovery data center that is separated physically from the medical database, so that it can be used to recover the loss information from the medical database. The recovery data center is to recover the copy from computer memory and deploy the copy as a VM in the recovery data center when the heartbeat signal ceases from cloud environment.

In each data center, the administration server provides the data center-level functions for communicating with hypervisors oncloud computers to install VMs, terminate VMs, and move VMs from one cloudcomputer to another within the data center. In addition, the data center administration servers called as a VM Manager, that implements a direct communications with the VM ware VSphereis installed through network in the VMs themselves.The research of this paper is intended to identify the disaster recovery in medical data, where the data points are affected by the disaster in order to recover the data through the automatic setting of Recovery Process Objective (RPO) and Recovery Time Objective (RTO)in the Efficient Disaster Recovery Swist algorithm (EDRSA). After the identification of recovery point in the medical database, it is fed in to the VMware vCenter Site Recovery Manager (SRM) to recover the disaster data. VMware vCenter Site Recovery Manager (SRM)-is the responsible to minimize the scheduled and

unscheduled downtime caused by a variety of events, including system failures, site disasters, user errors, data corruption, and maintenance tasks.VMware vCenter SRM is a work process apparatus intended for quick back up of fruitful medical data recoveries. By taking the preference of the intrinsic disaster recovering capacities of the VMware Infrastructure virtualization platform and array-based replication in VMware building designssignificantlyto simplify the planning and execution of disaster recovery strategies. The research of this work provides an efficient Diasaster Recovery of medical data to a maximum extent.

Recovery Process of Disastermedical Data and Virtualization from Primary Site

Disaster recovery plans have the biggest part in keeping up the indistinguishable recovery mechanism, in which hardware OS configurations at a primary and recovery site can empower the

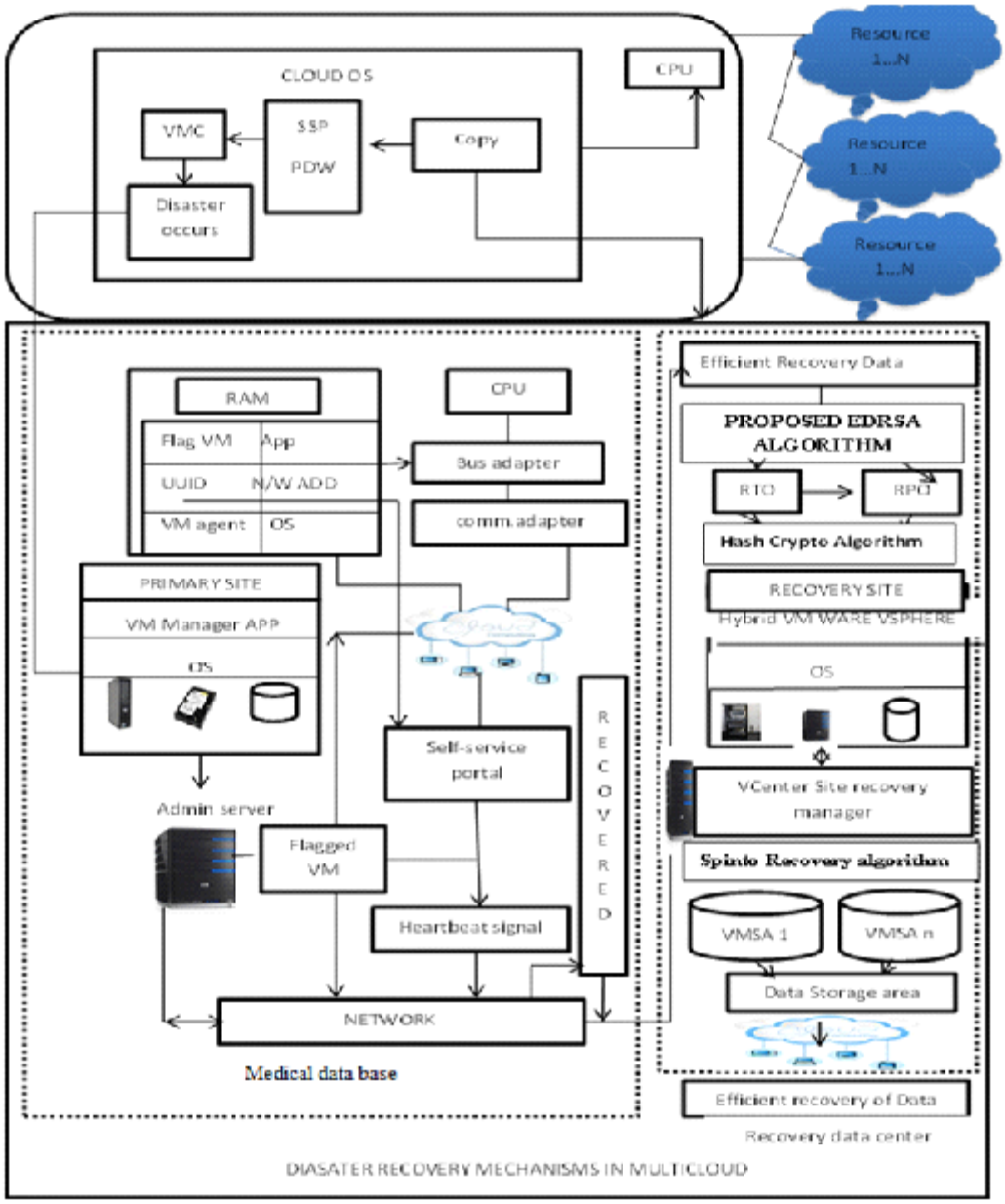

Fig. 1. Proposed Disaster Recovery System Architecture

operations rapidlyto continue when the essential site is occupied. This methodology requires ventures in servers and other hardware at the recovery site for a great part of the time in getting back of the disaster or loosed medical data. Specifically, a compelling disaster recovery plan possesses three key objectives:

Minimize downtime

The consequencesof extended downtime can be severe, not only in terms of losing the medical database but also, in order to maintain the secure health record information.

Minimize risk in recovering the disaster data

Not only having a disasterrecovery plan but also, suddenly constitutes anunacceptable level of risk.

Control costs

Traditional disasterrecovery plans are often limited inscope because of the costs associated with building and maintaining arecovery site, training staff membersin disaster recovery and testingthose processes, and so on.

The VM runs an application program and the VM is a module of automated computing machinery, configured by the hypervisor, to allow the application to get shared in the underlying physical machine resources of cloud computer, the CPU, the RAM, the communications adapter and so on. Each VM runs on its own separate operating system and each of the operating system presents that the system resources to applications as though each application were running on a completely separate computer. That is, each VM is 'virtual' in the sense of being actually a complete computer in almost every aspects. The abundant resources of data from multiple cloud operating systems get fed in to the virtual machine center. If there occurs disaster in data the copy of the data from the virtual machine center has been sent to the medical database to undergone into the virtualization process.

Virtualization can help in addressing challenges and barriers of traditionaldisaster recovery and help medical concerns tomeet the key goals of a viabledisaster recovery plan. The encapsulationof virtual machines (VMs) means, rather thanmaintainingthe correspondingserver at a recovery site instead of maintaining each serverat the primary site, or medical concerns can replicate thephysical servers or VMs from the primarysite

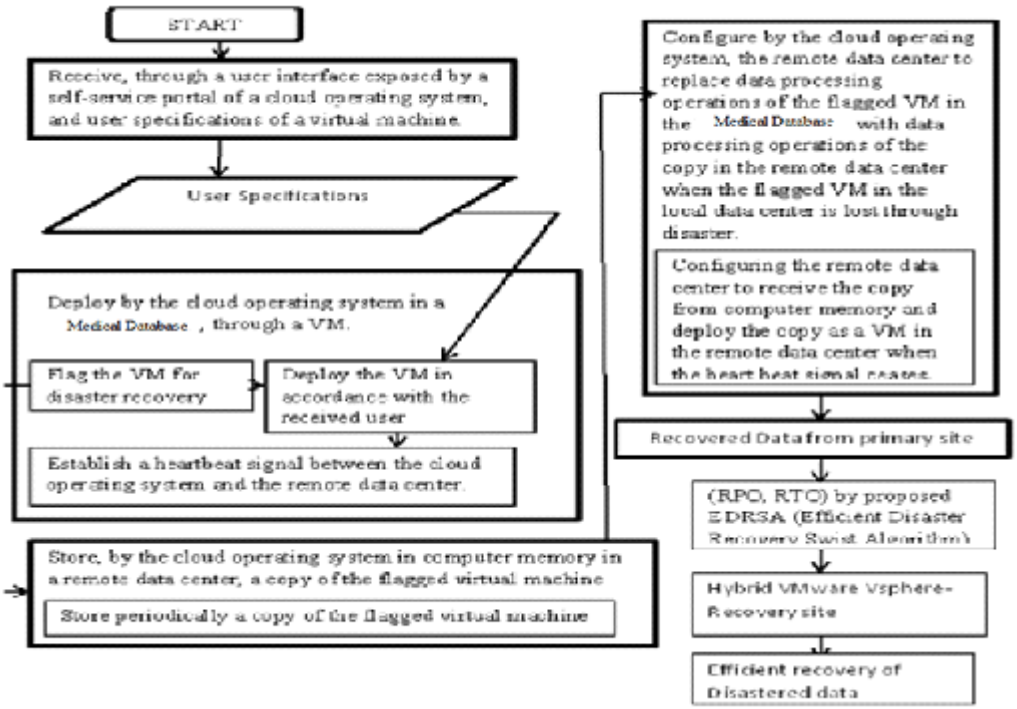

Fig. 2. Work Flow of Recovered Disaster medical data from Primary Site

to virtualized servers at therecovery site, helping to reduce the costof protection or to increase the numberof servers that can be protected by the proposed recovery infrastructure.The self-service portal of the cloud operating system stores in computer memory in a remote data center [17], a copy of the flagged VM. The self-service portal possesses data communications addresses, port numbers, and security permissions to enable it to store the copy in memory in the remote data center. In Fig. 2,The user specifications including the specifications of computer processors, random access memory, hard disk storage, input/output resources, application programs, and a requirement for disaster recovery. The copy of a VM can be fully characterized, at any point in time during the operation of the VM, by a complete template of the VM including user specifications and the contents of computer memory, including the contents of a CPU's architectural registers that are in use by the VM, the contents of RAM in use by the VM, and the contents of any hard disk space in use by the VM. When the heartbeat signal received from the self-service portal of the flagged virtual machine from the primary site of VM operating system, in which the data loss can be recovered. To achieve efficient data recovery, the research of this paper proposed an Efficient Disaster Recovery Swist Algorithm for the Recovery Process Objective (RPO), Recovery Time Objective (RTO) and processed by novel approach of VM ware vSphere recovery site.

Efficient Disaster Recovery Swist Algorithm for Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

Recovery Point Objective (RPO) is the point in time to which medical data must be recovered as characterized by the association and the large one's arecalled as an "acceptable loss" in a disaster situation. This method comprises ofcollecting the time-stamped samples of a usage metric for thedisaster medical data. The samples taken at determined time intervals stores the time-stamped samples in real time. The stored time-stamped samples can be accessed to determine an average usage metric at defined intervals for the first expected RPO failure tolerance.The RTO is a function of the extent, to which the interruption disrupts normal operations and the amount of revenue lost per unit time as a result of the disaster. These factors in turn depend on the affected equipment and applications.

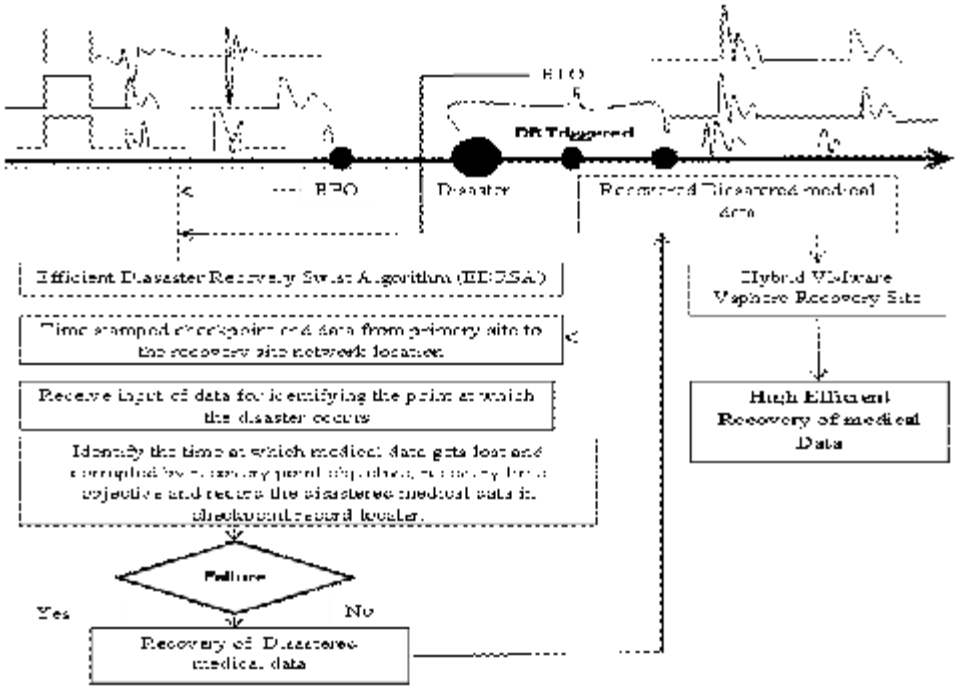

Fig. 3. Recovery mechanism ofRPO and RTO

An RTO is measured in seconds, minutes, hours, or days and it is an important consideration in disaster recovery planning.The duration of time required to bring critical systems back in which systems are assessed, repaired, replaced, and reconfigured. The amount of the disaster medical data available to achieve the target RPO and RTO was determined by using the proposed Efficient Disaster Recovery Swist Algorithm (EDRSA).The workflow of Recovery process objective and Recovery time objective by using theEfficient Disaster Recovery Swist Algorithm is shown in Fig. 3. The algorithm keeps the recovery checkpoint records in which the disaster data gets recorded at RC_p . It contains both the start and end process, which holds the k amount of data. When the recovery point objective process start by using Swiss algorithm it keeps the back up of medical data with the read and write access in acquiring the disaster medical data while performing the scanning and recording of the recovery point. Then the RTO calculates the time taken to recover the disaster medical data using Swist algorithm and locates the Time stamped values to recover the Data.

Efficient Disaster Recovery Swist Algorithm

functions locate recovery checkpoint ()
{ {
Start=0, end=C_t
while (T_s < RTO) and (RPO does not reach)
C_p= scan records recover point type (start, end)
for k in start to end
$R_p(k)$= log record(k- start) + (end-k)
if C_p is clean
start= recovery checkpoint of C_p
else
end= recovery checkpoint of C_p
end locate recovery checkpoint
}then
function locate Time stamped recovery checkpoint()
{
if $R_t(k)$= log record(k- start) + (end-k) < scan time stamped recovered data
then currentmin= $R_t(k)$
endlocate Time stamped recovery checkpoint }

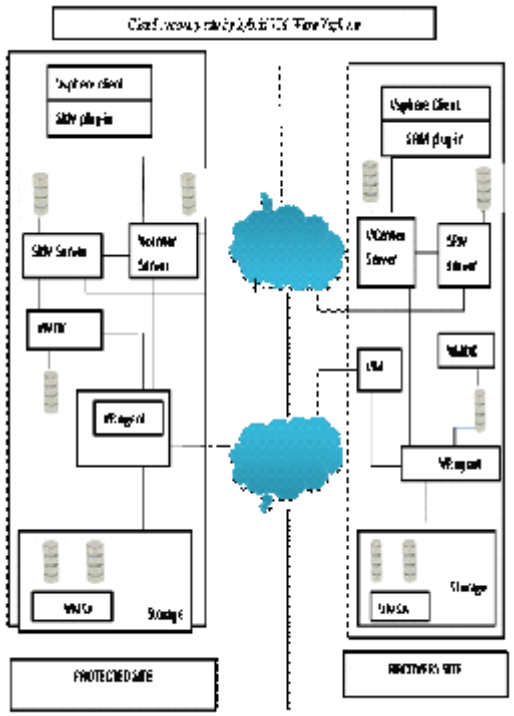

Fig. 4. Cloud recovery site by hybrid VM Ware Vsphere

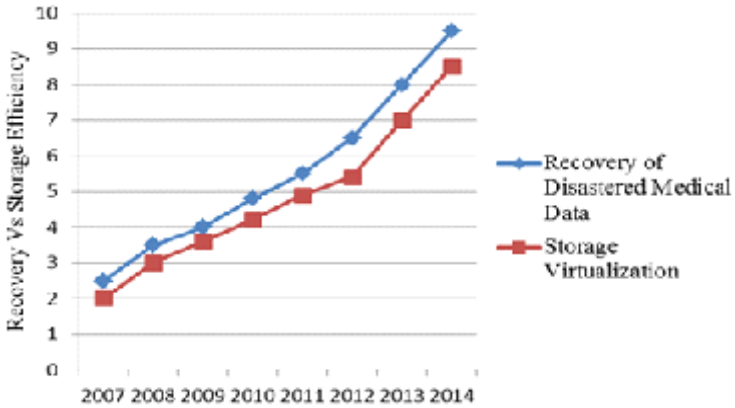

Fig. 5. Graph for Recovery of Disaster Medical data and storage virtualization

Where T_s is time spent for recovering those medical data in the medical database, C_t is the current time, C_p is current copy of data, k (which holds the entire medical database), $R_p(k)$ is the recovery point objective and $R_t(k)$ is recovery time objective and the equation is given by

$$RC_p = \frac{b_f \left({}^{C_r}/_{A_{fs}} \right) D_{ws}}{(r_b + w_b)} \quad ..(1)$$

$$Rp\,(k) = RC_p + n_p \quad ...(2)$$

$$R_t\,(k) = RC_p * t(n_p - 1) + t(1) + .. + t(i) + .. + t(n_p - i) \quad ...(3)$$

Where RC_p is the recovered current copy, b_f is the backup of medical data, C_r is the recovery parameter, A_{fs} is the average data file size, D_{ws} is the data write size, r_b and w_b is the read and write bandwidth for servers, n_p is the recovery checkpoint record, $R_p(k)$ is the recovered point objective and $R_t(k)$ is the recovered time objective.

Remote network storing of information in to the Hybrid VMware Vsphere

After the recovery mechanism by using the RTO and RPO objectivesof Efficient Disaster Recovery Swist Algorithm, the medical data is fed in to the virtual machine disk (VMDK) (Remote network of VMware Vsphere) using Hash crypto algorithm.Built on VMware vSphere Replication, supported by the vCloud Hybrid Service, Disaster Recovery provides a failover environment for dependable recovery of operational disruption. Replication allows for virtual machines (VMs) in vSphere to be easily configured for disaster recovery. VSphere Replication is the only hypervisor-based replication solution that operates in the individual virtual machine disk (VMDK) level, allowing replication between data stores hosted on any storage. Block changes in the virtual machine disk(s) is used for a running virtual machine at a primary site and it is sended to therecovery site. The hashcrypto algorithm is utilized to secure the medical data sets in the healthcare cloud computing.

Hash crypto Algorithm

// is the current (signature (Recovered information)) to be updated in to the Remote network of hybrid VMware vSphere?

```
if (no local signature or signature.hash!= backend.signature.hash)
get fresh signature from backend;// recovered information from RTO and RPO
for(block : blocksFromProvider // block refer to virtual machine disk in hybrid VMware Vsphere)
{
handle(block);
}
handle(block);
}
handle(block)
{
h = (block.data);
if (signature.getHashAt(block.offset) == h)
{
// nothing to do - block is the same as previous one
(update stats and progress only)
}
else
{
// check if we have seen this block earlier
prev = blocksIndex.get(h);
if (prev != null)
{
assert (prev.offset != block.offset); // if false then blockIndex is out of sync
// we have seen this block in a different offset
write block meta to BU_token.blkinfo;
signature.update (block.offset, h);
}
else // this is a new unseen block
{
write block meta to BU_token.blkinfo;
signature.update (block.offset, h);
blocksIndex.update (h, block.offset);
write raw block bytes to upload stream file (BU_token.blkraw);
}}}
```

Cloud recovery site of stored information from hybrid VM Ware Vsphere in to VMSA (Virtual machine Storage Area)

The stored information in the Remote area of VM Ware Vsphere can be recovered and fed into the Virtual machine storage area by using the Spinto recovery algorithm. Cloud Site Recovery management (SRM) is geographically diverse in the Disaster Recovery (DR) service, providing the recovery of Cloud Virtual Machine (VM). It operates in Public and Private Clouds, allowing public-to-public, private-to-public and private-to-private

recovery. It works by duplicating the Virtual Machine Disk (VMDK) to the recovery site and restores them in a site recovery environment. The storage system regularly replicates VMSA (VM Storage Area) to the recovery site where VMs are restarted using last replicated VMDK data and the Cloud site recovery is shown in Fig. 4.VSphere includes an agent inside the core vSphere installation package on each host, plus a set of the virtual appliances that are deployed from the management interface. The agent sends the changed medical data from a running virtual machine to the appliance at a remote site, the appliance then adds the replication to the offline disk files of the virtual machine. The appliance also manages the replication process, giving administrators visibility into virtual machine protection status as well as the ability to recover virtual machines with a few clicks. After baseline synchronization is complete, vSphere Replication will transfer only those blocks of data, which has been changed. The vSphere kernel tracks unique writes to protected virtual machines, identifying and replicating only those blocks that have unique writesduring the pre-set of RPO. This keeps network traffic to a minimum and allows for aggressive RPOs. Unique data alone requires of sending once. Only changes will be replicated and sent to the target location's vSphere Replication appliance.

Spinto Recovery Algorithm

Usage: java -jar BlocksTool.jar <action><options>
backup -cbt <cbt_xml_file> -srcvmdk
<vmdk_file>
[-sig signature_file] [-path files_path]
apply -srcraw <source_blkraw_file> -srcinfo
<source_blkinfo_file> -target
backup input file:
cbt_xml_file: CBT info file in the format created by 3RD PARTYagent
vmdk_file: flat ESX vmdk file used as source for point in time backup at VMSA

```
BlocksProvider p = new 3rdPartyVmdkBlocksProvider (
 "e:\backups\IMG00002\disk1.VMSA",
 "cbt_file.xml",
 new VddkBlocksReader(".\vddkBlocksTool.exe", cmdExecutor),
 );
 Iterator<BlockInfo> it = p.iterator( );
 while (it.hasNext( ))
 {
BlockInfo b = it.next( );
blocksHandler.handle (b);
//Recovered output files:
blkraw: raw blocks to upload
blkinfo: blocks information (refers to the blkraw file
blksig: blocks signature file of backed up disk in to VMSA.
<target_vmdk>
```

At the protected site, SRM shuts down the virtual machines, starting with the virtual machines designated with the lowest priority. At the recovery site, SRM prepares the data store groups for failover of the protected virtual machines. To provide more resources of the virtual machines and to be powered at the recovery site, SRM suspends any virtual machines running at the recovery site that are designated as noncritical. SRM restarts virtual machines at the recovery site, starting with the virtual machines that are designated as the highest priority. This mechanism of retrieving disaster data yields global efficient recovery process and results in providing greater potential retrievsl of the disaster medical data.

Performance evaluation

The Fig. 5 illustrates the performance evaluation for recovery of Disaster Medical data and storage virtualization. The Disaster data is recovered to a greater extent and the storage virtualization is increased through the proposed novel approach and by utilizing the virtual machine of Hybrid VMware VSphere along with process of automatic setting of Recovery Process Objective (RPO), Recovery Time Objective (RTO)and data integrity checks of Efficient Disaster Recovery Swist Algorithm (EDRSA)yields to the efficient performance in retrieving the Disastermedical data.

Experimental Setup

The experimental setup is done on HP Store Virtual VSA will turn a set of heterogeneous and disconnected physical disk drives in servers and storage devicesinto a single pool of logical storage capacity.The HP Store Virtual VSA manages the virtual storage systems and hard disk capacity. The HP Store Virtual VSA displays thepooled disk capacity of each DL500 server as an individual HP Store Virtual VSA storage system. A storage cluster is created fromthe individual

virtual storage systems at the Recovery Site. The volumes used for virtual machine storage are created usingNetwork RAID 10. Network RAID stripes and mirrors of multiple copies of data across a cluster of storage nodes, eliminating anysingle point of failure in the HP Store Virtual 4000 or VSA SRM. Applications have continuous data availability in the event of apower, network, disk, or controller failure.The HP Store Virtual 4000 SRA for VMware SRM enables the full featured use of VMware Site Recovery Manager. Combining HP Store Virtual VSA Remote Copy replication with VMware SRM provides an automated solution for implementing andtesting disaster recovery between geographically separated sites. The results generated produces 90% efficiency in recovering the Disastered data and increasing storage efficiency to a maximum extent.

CONCLUSION

The research of this paper isextended to the integration of vCloud Service into the novel hybrid VMware Vsphere along with the Recovery Process Objective (RPO), Recovery Time Objective (RTO) by using Efficient Disaster Recovery Swist Algorithm (EDRSA). Data disaster in the medical database can be recovered very efficiently through the proposed system of virtualization mechanism in Healthcare cloud computing system. Thus, the storage efficiency reaches to a maximum extent and the disaster recovery of medical database results in higher output.

REFERENCES

1. Rao Mikkilineni,"Using Virtualization to Prepare Your Data Center for "Real-time Assurance of Business Continuity", Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE, 2010.
2. Wood T, Cecchet E, Ramakrishnan K, Shenoy P, van der Merwe J, and Venkataramani A, " Disaster recovery as a cloud service: economic benefits & deployment challenges", Proc. 2nd USENIX Conference on Hot topics in cloud computing (HotCloud'10), Berkeley, CA, USA, 2010; 8-8.
3. Manish Pokharel, Seulki Lee, Jong Sou Park, "Disaster Recovery for Systems Architecture Using Cloud Computing,", IEEE/IPSJ Int. Symp. Applications and the Internet, , 2010; 304-307.
4. Zhang J and Zhang N, "cloud computing-based data storage and disaster recovery", IEEE International Conference on Future Computer Science and Education (ICFCSE), pp. 629-632, 2011.
5. Bermbach D, Klems M, Tai S, and Menzel M, "Meta storage of a federated cloud storage system to manage consistency-latency tradeoffs", in IEEE International Conference on Cloud Computing (CLOUD), 2011; 452-459.
6. Muppalla Prudhvi," Disaster recovery on double duty using cloud", International Journal of Computer Science & Communication Networks, 2011; **3**(2).
7. Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki & Kazuo Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network Applications in Cloud Computing Envionments", *International Journal on Advances in Networks and Services*, 2011; 4(1-2).
8. Deyan Chen & Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", *International Conference on Computer Science and Electronics Engineering*, 2012.
9. Avula Tejaswi, Nela Manoj Kumar, Gudapati Radhika, Sreenivas Velagapudi," Efficient Use of Cloud Computing in Medical Science", *American Journal of Computational Mathematics*, 2012.
10. Kruti Sharma, Kavita R Singh, "Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review", *International Journal of Engineering and Innovative Technology* (IJEIT), 2012; **2**(5).
11. Bajpai A, Rana P, and Maitrey S, "Remote mirroring: A disaster recovery technique in cloud computing", *International Journal of Advance Research in Science and Engineering*, 2013; **2**(8).
12. Omar H. Alhazmi, Yashwant K. Malaiya, "Evaluating Disaster Recovery Plans Using the Cloud", IEEE, 2013.
13. https://www-935.ibm.com/services/uk/en/it-services/VSR_Whitepaper_V2.pdf
14. Yu Gu, Dongsheng Wang, and Chuanyi Liu,"DR-Cloud: Multi-Cloud Based Disaster Recovery Service",Tsinghua Science and Technology, ISSN l1007-0214l l02/10l lpp13-23, 2014; **19**(1).
15. Ruturaj Desai, Nitin R. Thalhar," Privacy Preserving Data Search in Cloud Computing", *International Journal of Advanced Research in Computer Science and Software Engineering"*, 2014; **4**(11).
16. Mohammad Ali Khoshkholghi, Azizol Abdullah, Rohaya Latip, Shamala Subramaniam, Mohamed Othman, "Cluster as a Service for Disaster

Recovery in Intercloud Systems: Design and Modeling", *International Journal of Cloud Computing and Services Science* (IJ-CLOSER), 2014; **3**(3).

17. Kalyani Bangale, Nivedita Gupta, Swati Singh Parihar , Karishma Nadhe& Gunjan Mankar, "Remote Data Collection Server: E-Health Care", *International Journal of Innovative Research in Compute and Communication Engineering*, 2014; **2**(2).
18. R. V. Gandhi, M Seshaiah, A. Srinivas, C. ReddiNeelima," Data Back-Up and Recovery Techniques for Cloud Server Using Seed Block Algorithm", *Journal of Engineering Research and Applications*, 2015; **5**(3).
19. S. Deepa & G. Ramachandran, "Disaster Recovery System Using Seed Block Algorithm in Cloud Computing Environment", *International Journal of Advanced Research in Computer Science and Software Engineering*", 2015; **5**(2).
20. M.Saranya & R.Vasuki," improving data security in kp-abe with third party auditing", *International Journal of Inventions in Computer Science and Engineering*, 2015; **2**(2).